Traductions de deux extraits du livre *Generators and relations for discrete groups* de H. S. M. Coxeter et W. O. J. Moser

pages 63 à 66.

6.2 Le groupe symétrique. Les premières présentations du groupe symétrique $\mathfrak{S}_n$ ont été données par Burnside (1897) et Moore (1897). La présentation de Burnside

$$R^n = R_1^2 = (RR_1)^{n-1} = [R^{-r+1}(RR_1)^{r-1}]^r = (R^{-j}R_1R^jR_1)^2 = E \qquad \left(2 \leq r \leq n, 2 \leq j \leq \frac{n}{2}\right),$$

en fonction des générateurs

$$R = (1\ 2\ 3 \ldots\ n), \qquad R_1 = (1\ 2),$$

a de nombreuses relations redondantes. En fonction des mêmes générateurs, Moore a donné la présentation plus simple

$$R^n = R_1^2 = (RR_1)^{n-1} = (R_1R^{-1}R_1R)^3 = (R_1R^{-j}R_1R^j)^2 = E \qquad (2 \leq j \leq n-2). \tag{6.21}$$

Moore a aussi donné la présentation

$$\begin{cases} R_1^2 = R_2^2 = \ldots = R_{n-1}^2 = E & \\ (R_iR_{i+1})^3 = E & (1 \leq i \leq n-2), \\ (R_iR_k)^2 = E & (i \leq k-2), \end{cases} \tag{6.22}$$

en fonction des générateurs

$$R_1 = (1\ 2), R_2 = (2\ 3), \ldots, R_{n-1} = (n-1\ n)$$

(Burnside 1911, p. 464 ; Carmichael 1923, p. 238). Les deux ensembles de générateurs sont reliés par les équations

$$R_{i+1} = R^{-i}R_1R^i \qquad (1 \leq i \leq n-2)$$

et

$$R = R_{n-1}R_{n-2}\ldots R_2R_1.$$

Trivialement, 6.22 est équivalente aux trois ensembles de relations

$$R_1^2 = E, \tag{6.23}$$

éditions : Springer-Verlag Berlin Heidelberg GmbH, 3ème édition, 1972.

(6.24) $$R_iR_{i+1}R_i = R_{i+1}R_iR_{i+1} \qquad (1 \leq i \leq n-2)$$

(6.25) $$R_iR_k = R_kR_i \qquad (i \leq k-2)$$

Puisque 6.24 et 6.25 définissent le groupe de tresses d'Artin[1] (cf. 6.11 et 6.12), qui est également défini par les relations

(6.26) $$R^n = (R_1R)^{n-1}, R_1R^{-j}R_1R^j = R^{-j}R_1R^jR_1 \qquad \left(2 \leq j \leq \frac{n}{2}\right)$$

(cf. 6.16), il en découle que $\mathfrak{S}_n$ est défini par 6.23 et 6.26 (Artin 1926, p. 54 ; Nielsen 1940) ou par

(6.27) $$R^n = (R_1R)^{n-1}, R_1^2 = (R_1R^{-j}R_1R^j)^2 = E \qquad \left(2 \leq j \leq \frac{n}{2}\right)$$

(cf. 6.21). Coxeter (1937, p. 317) a observé que, quand n est pair, on a la présentation alternative

(6.271) $$R^n = (R_1R)^{n-1}, R_1^2 = (R_1R^{-1}R_1R)^3 = (R_1R^{-j}R_1R^j)^2 = E \qquad \left(2 \leq j \leq \frac{n}{2} - 1\right),$$

dans laquelle la relation $(R_1R^{-1}R_1R)^3 = E$ remplace $(R_1R^{-n/2}R_1R^{n/2}) = E$.

Carmichael (1937, p. 169) préfère la présentation

(6.28) $$S_i^2 = (S_iS_{i+1})^3 = (S_iS_{i+1}S_iS_j)^2 = E \qquad (i, j = 1, 2, \ldots, n-1\ ;\ j \neq i, i+1)$$

en fonction des transpositions

$$S_i = (i\ n) \qquad (i = 1, 2, ..., n-1)$$

(avec $S_n = S_1$). En fonction de

$$V_1 = S_1 = (1\ n), V_j = S_1S_j = (1\ j\ n) \qquad (j = 2, 3, ..., n-1),$$

une présentation encore plus simple est

(6.281) $$V_1^2 = V_j^3 = (V_iV_j)^2 = E \qquad (1 \leq i < j \leq n-1)$$

(Coxeter 1934c, p. 218).

On obtient une interprétation géométrique de 6.22 en considérant $\mathfrak{S}_n$ comme le groupe des permutations des n sommets d'un simplexe régulier $P_1P_2...P_n$ dans le (n-1)-espace euclidien. Ces permutations sont juste les opérations symétriques du simplexe. En particulier, R_i est la réflexion dans l'hyperplan qui joint le point au milieu de P_iP_{i+1} aux $n-2$ sommets restant. Les $\binom{n}{2}$ arêtes

[1] Le groupe de tresses amène au groupe symétrique quand on remplace les chaînes μ_i par leur projections ν_i, en renonçant à faire la distinction entre σ_i et σ_i^{-1}. Par conséquent les R satisfont trivialement les mêmes relations que les σ et également 6.23 (qui implique $R_i^2 = E$ puisque, par 6.24, tous les R sont conjugués).

P_iP_j amènent $\binom{n}{2}$ tels hyperplans, en décomposant la sphère circonscrite (ou n'importe quelle sphère concentrique) en $n!$ simplexes sphériques. Les R apparaissent comme des réflexions dans les hyperplans frontières d'un de ces simplexes : la région fondamentale (cf. Figs. 4.3a, 4.5h, m, r, t).

En fonction des n coordonnées cartésiennes, on peut prendre P_i à distance a de l'origine le long du $i^{\text{ième}}$ axe, de telle façon que $P_1P_2...P_n$ soit dans le (n-1)-espace $\sum x_i = a$. Alors R_i en interchangeant x_i et x_{i+1}, est la réflexion dans $x_i = x_{i+1}$, et la région fondamentale est donnée par

$$x_1 \leq x_2 \leq \ldots \leq x_n,\ \sum x_i = a_i,\ \sum x_i^2 = b \qquad (b > a^2/n). \tag{6.29}$$

Les autres simplexes sphériques, étant des images de celui-ci, sont dérivés en permutant les x dans 6.29. Les trois parties de 6.22 expriment que les réflexions sont involutives, et que l'angle entre $x_i = x_{i+1}$ et $x_k = x_{k+1}$ est $\pi/3$ ou $\pi/2$ selon que $i = k-1$ ou que $i \leq k-2$ (Coxeter 1963a, pp. 80, 188).

Le diagramme de Cayley est dérivé de cela en prenant un point convenable à l'intérieur de chaque simplexe sphérique (Robinson 1931). La façon la plus simple de faire cela est de prendre les points dont les coordonnées sont les permutations de $(0, 1, n-1)$. Dans la région fondamentale 6.29 on a $(0, 1, ..., n-1)$ lui-même. Les arêtes du diagramme joignent ces $n!$ points par paires : chacun à ses $n-1$ voisins, distants de $\sqrt{2}$. En fait, le diagramme est constitué des sommets et des arêtes d'un polytope uniforme Π_{n-1}, dont les faces places sont des hexagones et des carrés représentant les seconde et troisième parties de 6.22.

De façon triviale, Π_0 est un point, Π_1 est un segment de droite, et Π_2 est un hexagone régulier, comme dans la figure Fig. 3.3d (avec les S-arêtes omises) ou la Fig. 6.2 (où la région fondamentale est un sixième du cercle). Π_3 est l'octaèdre tronqué, délimité par huit hexagones et six carrés (Kepler 1619, p. 125, Fig. 23[9] ; Kelvin 1894, p. 15 ; Steinhaus 1950, . 154-157). Π_4 est un polytope à quatre dimensions dont les cellules sont constituées de dix octaèdres tronqués et vingt prismes hexagonaux (Hinton 1906 ; pp. 135, 225 ; Coxeter 1962c, p. 154).

Par conséquent, toute région fondamentale convexe pour un groupe de translation 3-dimensionnel est un parallélohédron. En utilisant les mêmes termes dans les espaces de dimensions supérieures, Voronoi a donné une démonstration remarquablement simple du fait qu'un parallélohédron n-dimensionnel a au plus $2(2^n - 1)$ hyperplans frontières (Voronoi 1907, p. 107 ; 1908, p. 204 ; Bambah et Davenport 1952, p. 225). Cette limite supérieure est atteinte par le polytope Π_n (Schoute 1912), dont les cellules ($n-1$)-dimensionnelles consistent en $\binom{n+1}{i}$ prismes généralisés $\Pi_{n-i} \times \Pi_{i-1}$ (Coxeter 1963a, p. 124) pour chaque valeur de i de 1 à n.

Selon Fedorov (1885, pp. 286-298), un *parallélohédron* est un polyèdre qui peut être reproduit et translaté pour remplir la totalité de l'espace euclidien (ou affine)

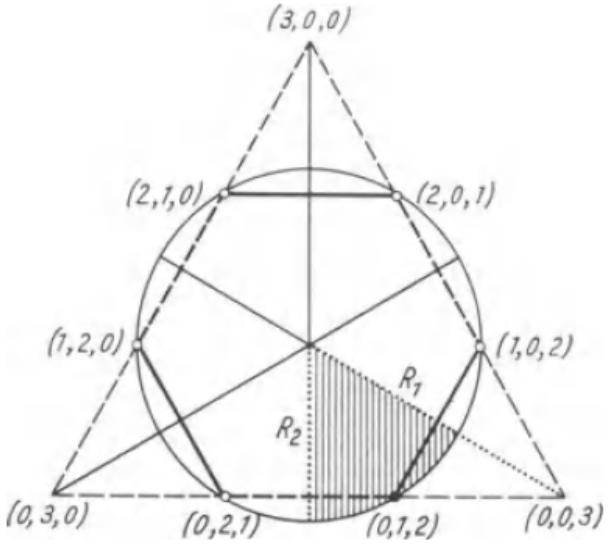


Fig. 6.2

En étendant la notation de § 4.3, on peut exprimer 6.22 sous la forme

$$\mathfrak{S}_n \simeq [3^{n-2}],$$

signifiant $[3, 3, \ldots, 3]$ (Todd 1931, p. 225 ; Coxeter 1963a, p. 199). On discutera des autres groupes engendrés par les réflexions au chapitre 9.

---

page 35 à 38

4.3 Groupes engendrés par des réflexions. Les groupes engendrés par des réflexions méritent une considération particulière pour deux raisons : il y a une théorie générale qui les englobe tous, et ils contiennent les groupes de points restants comme sous-groupes.

Le groupe engendré par des réflexions dans un nombre quelconque de plans est également engendré par des réflexions dans toutes leurs transformations : une configuration de plans qui est symétrique par réflexion selon chacun. Si le groupe est fini, les plans contiennent tous le point (ou les points) invariant et déterminent une configuration correspondante de grands cercles sur une sphère. Ces grands cercles décomposent la sphère en un nombre fini de régions (notamment des hémisphères, des lunes, ou des triangles sphériques) dont les angles sont des sous-multiples de π (Coxeter 1963a, pp. 76-77). Toutes ces régions sont congruentes (avec une possible inversion du sens), puisque chacune se réfléchit dans ses voisines.

L'instance la plus simple est le groupe [1], d'ordre 2, engendré par la réflexion par rapport à un unique plan qui coupe la sphère en deux hémisphères. Quand un groupe est engendré par deux réflexions, on peut prendre pour angle entre les plans réfléchis π/q ($q \geq 2$). Les plans et leurs transformés rencontrent la sphère en un pinceau de q méridiens qui la décomposent en $2q$ lunes.

Le diagramme de Cayley est un $2q$-gone avec un sommet dans chaque lune. Par conséquent, on a le groupe

$$[q] \simeq \mathfrak{D}_q,$$

d'ordre $2q$, ayant pour définition abstraite

$$R_1^2 = R_2^2 = (R_1 R_2)^q = E. \tag{4.31}$$

D'autres tels groupes sont engendrés par des réflexions R_1, R_2, R_3 par rapport aux trois côtés d'un triangle sphérique d'angles $\pi/p_{23}, \pi/p_{31}, \pi/p_{12}$, disons. Les réflexions satisfont clairement

$$R_1^2 = R_2^2 = R_3^2 = E$$

et les trois relations de la forme $(R_i R_j)^{p_{ij}} = E$. Les remarques suivantes montrent que toute relation satisfaite par les R est une conséquence algébrique de celles-ci.

En appelant le triangle initial "région E", on observe que tout élément S du groupe le transforme en une "région S" congruente. En particulier les générateurs transforment la région E en ses régions voisines R_i ; l'élément S transforme E et ses voisins R_i en S et ses voisins $R_i S$. Par conséquent, on passe par le $i^{\text{ième}}$ côté de la région S à la région $R_i S$. Toute expression de S comme mot

$$\ldots R_k R_j R_i$$

correspond à un chemin d'une position à l'intérieur de la région E à une position à l'intérieur de la région S, en passant à travers le $i^{\text{ième}}$ côté de E, puis à travers le $j^{\text{ième}}$ côté de R_i, puis à travers le $k^{\text{ième}}$ côté de $R_j R_i$, et etc. (en lisant de droite à gauche[2]). Deux chemins différents de E à S peuvent être combinés pour former un chemin fermé de E vers $S^{-1}S = E$, correspondant à un mot qui est égal à E. Puisque la sphère est simplement-connexe, un tel chemin fermé peut être décomposé en circuits élémentaires de deux sortes : l'un allant de S à une région voisine $R_i S$ et revenant à $R_i^2 S = S$, et l'autre passant autour d'un sommet en lequel se rencontrent $2p_{ij}$ régions, de S à $(R_i R_j)^{p_{ij}} S = S$. Un rétrécissement graduel du chemin correspond à la réduction du mot jusqu'à E en utilisant les relations $R_i^2 = E$ et $(R_i R_j)^{p_{ij}} = E$. Il découle de cela que les relations suffisent pour une définition abstraite, et que le triangle est une *région fondamentale* : il existe un seul tel triangle pour tout élément du groupe ; et tout point de la sphère, étant à l'intérieur ou bien sur la frontière d'une telle région S, est dérivable d'un point correspondant de la région E par la transformation S.

Les triangles couvrant la sphère peuvent être regardés comme les faces d'une carte (§ 3.2). En nommant les points à l'intérieur de ces faces, plutôt que les faces elles-mêmes, on obtient la carte duale, dont les arêtes traversent les côtés des triangles. Les remarques ci-dessus servent à identifier cette carte duale avec le diagramme de Cayley (§ 3.3), qui, en accord avec cela, a, en chaque sommet, un $2p_{23}$-gone,un $2p_{31}$-gone, et un $2p_{12}$-gone, représentant les relations

$$(R_2 R_3)^{p_{23}} = (R_3 R_1)^{p_{31}} = (R_1 R_2)^{p_{12}} = E.$$

[2]Selon les mots d'une lettre de A. Speiser (Décembre 1954) : "Wenn man ein Produkt von Substitutionen geometrisch deutet, muß man sie "raumfest" deuten, falls man von links nach rechts liest. Liest man aber von rechts nach links, so muß man sie, "körperfest" deuten". Trad. DeepL "Si l'on interprète géométriquement un produit de substitutions, on les interprète "fixes dans l'espace" si l'on lit de gauche à droite. Mais si l'on lit de droite à gauche, on les interprète de manière "köriste"." ?...

Puisque la région fondamentale est un triangle sphérique, la somme de ses angles doit excéder π ; donc

$$\frac{1}{p_{23}} + \frac{1}{p_{31}} + \frac{1}{p_{12}} > 1$$

Puisque $\frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1$, le plus petit des p doit être 2, et les autres, disons p et q, satisfont

$$\frac{1}{p} + \frac{1}{q} > \frac{1}{2}, \qquad \text{ou} \qquad (p-2)(q-2) < 4.$$

On obtient par conséquent les cas $[2,q], [3,3], [3,4], [3,5]$ du groupe

$$[p,q] \qquad \text{ou} \qquad [q,p],$$

définis par

$$R_1^2 = R_2^2 = R_3^2 = (R_1R_2)^p = (R_2R_3)^q = (R_3R_1)^2 = E, \tag{4.32}$$

dont la région fondamentale est un triangle d'angles $\pi/p, \pi/q, \pi/2$. Ce groupe est le groupe complet de symétrie de n'importe lequel des deux polyèdres réguliers réciproques $\{p,q\}, \{q,p\}$ (Coxeter 1963a, p. 83). Le diagramme de Cayley contient les sommets et les arêtes (non dirigées) du polyèdre semi-régulier

$$t\left\{ \begin{array}{c} p \\ q \end{array} \right\}$$

(Coxeter 1940a, p. 394) qui a, en chaque sommet, un $2p$-gone, un $2q$-gone, et un carré. (Le cas [3, 5] est illustré sur la figure Fig. 4.3, qui ressemble à un dessin de R. Fricke, voir Pascal 1927, p. 945. Les symboles classiques de tous ces groupes sont donnés dans la Table 2.)

Puisque l'aire de la région fondamentale est mesurée par son excès angulaire, l'ordre de $[p,q]$ est égal au nombre de tels triangles qui sera nécessaire pour couvrir la totalité de la sphère, notamment

$$\frac{4}{\frac{1}{p} + \frac{1}{q} - \frac{1}{2}} = \frac{8pq}{4 - (p-2)(q-2)}$$

Fig. 4.3. The group $[3,5] \cong \mathfrak{C}_2 \times \mathfrak{A}_5$

(Coxeter 1963a, p. 82).

4.4. Sous-groupes du groupe de réflexion.

Les trois rotations

$$R = R_1R_2, S = R_2R_3, T = R_3R_1,$$

ou n'importe quelles deux d'entre elles, engendrent un sous-groupe "polyédral" $[p, q]^+$ ou $[q, p]^+$ d'ordre $4pq\{4 - (p - 2)(q - 2)\}^{-1}$, défini par

$$R^p = S^q = T^2 = RST = E \tag{4.41}$$

ou

$$R^p = S^q = (RS)^2 = E \tag{4.42}$$

ou

$$S^q = T^2 = (ST)^p = E \tag{4.43}$$

(voir Coxeter 1940a, où $[p, q]^+$ était appelé $[p, q]'$).

Le concept de région fondamentale reste valide ; mais puisque les générateurs ne laissent pas ses côtés invariants, la forme de la région n'est plus déterminée de manière unique. Puisque $[p, q]^+$ est d'indice 2 dans $[p, q]$, l'aire de sa région fondamentale est le double de celle du triangle considéré ci-dessus. Il est naturel de choisir une forme telle que le réseau des régions congruentes et le diagramme de Cayley forment des cartes duales (Burnside 1911, pp. 406, 423). Dans le cas de 4.43, on combine deux triangles adjacents de façon à former un triangle plus grand avec deux angles π/p et un angle $2\pi/q$, et le diagramme de Cayley est $t\{p, q\}$ (qui a, en chaque sommet, deux $2p$-gones et un q-gone). Dans le cas de 4.42 avec $q > 2$, on combine à nouveau deux des triangles rectangle, mais maintenant, on choisit une paire de triangles qui partagent leur hypothénuse, de façon à obtenir un quadrilatère en forme de cerf-volant, et le diagramme de Cayley est $r\left\{ \begin{array}{c} p \\ q \end{array} \right\}$ (qui a, en chaque sommet, deux carrés non adjacents séparés par un p-gone et un q-gone). Dans le cas de 4.41, on combine un triangle avec des portions de ses trois voisins (disons un triangle blanc avec des portions de ses trois triangles adjacents noirs) pour former un pentagone (ou, si $p = 2$, un quadrilatère), et le diagramme de Cayley est $s\left\{ \begin{array}{c} p \\ q \end{array} \right\}$ (Voir Burnside 1911, frontispiece, pour le cas $[3, 4]^+$. Malheureusement, la direction de ses flèches n'est pas en accord avec le texte des pages 424, 427. L'opération $S_1S_2S_3$ devrait nous amener à parcourir une S_3-arête, puis une S_2-arête, puis une S_1-arête.)

Presque tous ces diagrammes de Cayley ont été fournis par Maschke (1896, pp. 156-194, Figs. 2-10, 16-18 ; cf. R. P. Baker 1931, pp. 645-646 ; Coxeter, Longuet-Higgins et Miller 1954, pp. 403, 439, Figs. 15 -25, 27, 29-32).

Quand $p = 3$ et $q = 4$ ou 5, l'élément $(R_1R_2R_3)^{2q-5}$ de $[p, q]$ est l'inversion centrale Z (COXETER 1963a, p. 91). Il en découle que $[p, q]$ est alors le produit direct du groupe $\{Z\}$ d'ordre 2 et du sous-groupe de rotation $[p, q]^+$.

Quand q est pair, $[p, q]$ a un autre sous-groupe d'indice 2, disons

$$[p^+, q] \quad \text{ou} \quad [q, p^+],$$

engendré par la rotation $R = R_1R_2$, et la réflexion R_3. On déduit aisément de 4.32 la définition abstraite

$$R^p = R_3^2 = (R^{-1}R_3RR_3)^{q/2} = E \tag{4.44}$$

(COXETER 1940a, p. 387). Il est plus naturel de prendre comme région fondamentale un triangle avec deux angles π/q et un angle $2\pi/p$ (ou, si $p = 2$, une lune), et le diagramme de Cayley est $t\{q, p\}$ (ou, si $p = 2, \{2q\}$). Cela ressemble au diagramme pour $[p, q]^+$ sous la forme

$$R^p = T^2 = (RT)^q = E,$$

qui diffère seulement par la manière dont sont dirigées les différentes R-arêtes. Quand $q = 2$, on a $[p^+, 2]$ ou $[2, p^+]$, le produit direct des $\mathfrak{G}_p$ engendrés par R et de $\mathfrak{G}_2$ engendré par R_3.

Les groupes de cette sorte les plus intéressants sont $[3^+, 4]$, le produit direct de $\mathfrak{G}_2$ engendré par l'inversion centrale $(RR_3)^3$ et $[3, 3]^+$ engendré par R et R_3RR_3. C'est le groupe de symétrie du dodécaèdre avec un cube inscrit, ou d'un octaèdre avec un icosaèdre inscrit (COXETER 1940a, p. 396), ou *pyritoèdre* cristallographique.

Quand $p = 2$, les relations 4.44 se réduisent à

$$R^2 = R_3^2 = (RR_3)^q = E \qquad (q \text{ pair}).$$

Dans ce groupe diédral $[2^+, q]$, les inversions rotationnelles RR_3 engendrent un sous-groupe cyclique d'ordre q. En utilisant la convention selon laquelle chaque exposant $^+$ diminue l'ordre de moitié, on dénote ce sous-groupe par

$$[2^+, q^+] \qquad (q \text{ pair})$$

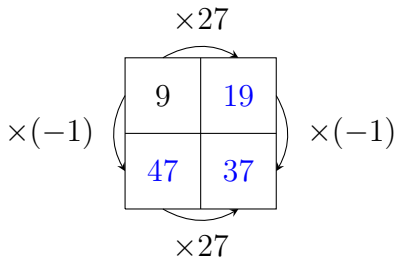
(voir la Table 2 de la page 135). C'est, bien sûr, un sous-groupe d'ordre 4 dans $[2, q]$, et il est engendré par $R_1R_2R_3$. On note pour comparaison que, quand q est impair, cet élément de $[2, q]$ engendre $[2, q^+]$ (d'indice 2).

Bidominos bicolores (Denise Vella-Chemla, novembre 2023).

Cette note fait suite à celles-ci : 1, 2, 3 4 et compile le peu dont on dispose.

On va représenter certaines connaissances par des bidominos bicolores. On aura deux sortes de bidominos, les bidominos (qu'on appellera bidominos bleus) qui représentent la relation "est un décomposant de Goldbach de n" et qui vérifient certaines contraintes multiplicatives, et les bidominos (qu'on appellera bidominos verts) qui représentent la relation "est un résidu quadratique de n".

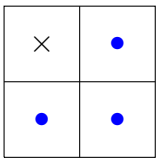
Pour n un nombre pair, une permutation de $[1, \ldots, n]$ par multiplication par k premier à n peut être représentée par la composition d'un certain nombre de transpositions, qui mettent en correspondance deux nombres et leurs opposés (leur complémentaire à n). On représentera, par exemple, une paire de telles transpositions par un bidomino bleu ainsi ($n = 56$) :



Le bidomino bleu ci-dessus représente les 4 congruences suivantes :

$$\begin{cases} 9 \times 27 & = 4 \times 56 + 19 & \equiv 19 \pmod{56} \\ 19 \times 27 & = 9 \times 56 + 9 & \equiv 9 \pmod{56} \\ 9 \times (-1) & = (-1) \times 56 + 47 & \equiv 47 \pmod{56} \\ 19 \times (-1) & = (-1) \times 56 + 37 & \equiv 37 \pmod{56} \end{cases}$$

On "résumera" un tel bidomino bleu en oubliant les nombres ainsi :



Qu'a-t-on constaté[1] également sur les permutations étudiées ? En termes de signature des permutations, on a vu (voir [6] pages 2 et 5) que pour n double d'un nombre impair, toutes les permutations engendrées par multiplication par un nombre premier à n sont de signature paire, tandis que pour n double d'un nombre pair, la parité des signatures des permutations alterne : la permutation est de signature paire pour une multiplication par m de la forme $4k+1$ et impaire pour une multiplication par m de la forme $4k + 3$.

D'autre part, on a la relation "est un résidu quadratique de". Sa table, pour les nombres premiers, est fournie par Gauss dans les Recherches arithmétiques (voir en annexe). On représentera

1. qui serait à démontrer.

cette propriété “est un résidu quadratique de n”, qui “appose” sur les nombres $[1, \ldots, n]$ un motif périodique, par des bidominos dits verts, chacun d'eux ayant comme caractéristique que les deux nombres entiers en hauts du bidomino sont des nombres entiers successifs croissants et les deux nombres entiers en bas du bidomino vert sont des nombres entiers successifs décroissants.

On dispose aussi de données sur le nombre de résidus quadratiques d'un nombre entier : Lehmer en 1913 [1] ou Stang en 1996 [2] fournissent des formules de calcul de ce nombre ; la fonction “nombre de résidus quadratiques de” est multiplicative et elle est définie par les formules suivantes sur les nombres premiers et leurs puissances :

$$\begin{cases} \text{nbRQ}(2) = 2; \\ \text{nbRQ}(p) = \dfrac{p-1}{2} & \text{pour } p \text{ premier, } p \geq 3; \\ \text{nbRQ}(2^k) = \begin{cases} \dfrac{2^{k-1}+4}{3}, & \text{pour } k \text{ pair ;} \\ \dfrac{2^{k-1}+5}{3} & \text{pour } k \text{ impair } \mathrm{k} \geq 3 \end{cases} & ; \\ \text{nbRQ}(p^k) = \begin{cases} \dfrac{p^{k+1}+p+2}{2(p+1)} & \text{pour } k \text{ pair et } p \neq 2, p \text{ premier} \\ \dfrac{p^{k+1}+2p+1}{2(p+1)} & \text{pour } k \text{ impair } \geq 3 \text{ et } p \neq 2, p \text{ premier} \end{cases} \end{cases}$$

Voyons un exemple : pour $98 = 2.7^2$, on trouve nbRQ(98) = 44. Les résidus quadratiques obéissent au motif périodique (hormis au milieu) R-R-N-R-N-N-N de longueur 7 ainsi (dans la suite des nombres, les résidus quadratiques sont verts) :

0	1	2	3	4	5	6	7
	8	9	10	11	12	13	14
	15	16	17	18	19	20	21
	22	23	24	25	26	27	28
	29	30	31	32	33	34	35
	36	37	38	39	40	41	42
	43	44	45	46	47	48	49
	50	51	52	53	54	55	56
	57	58	59	60	61	62	63
	64	65	66	67	68	69	70
	71	72	73	74	75	76	77
	78	79	80	81	82	83	84
	85	86	87	88	89	90	91
	92	93	94	95	96	97	

Remarque : pour n un nombre pair, la moitié de n est un résidu quadratique de n.

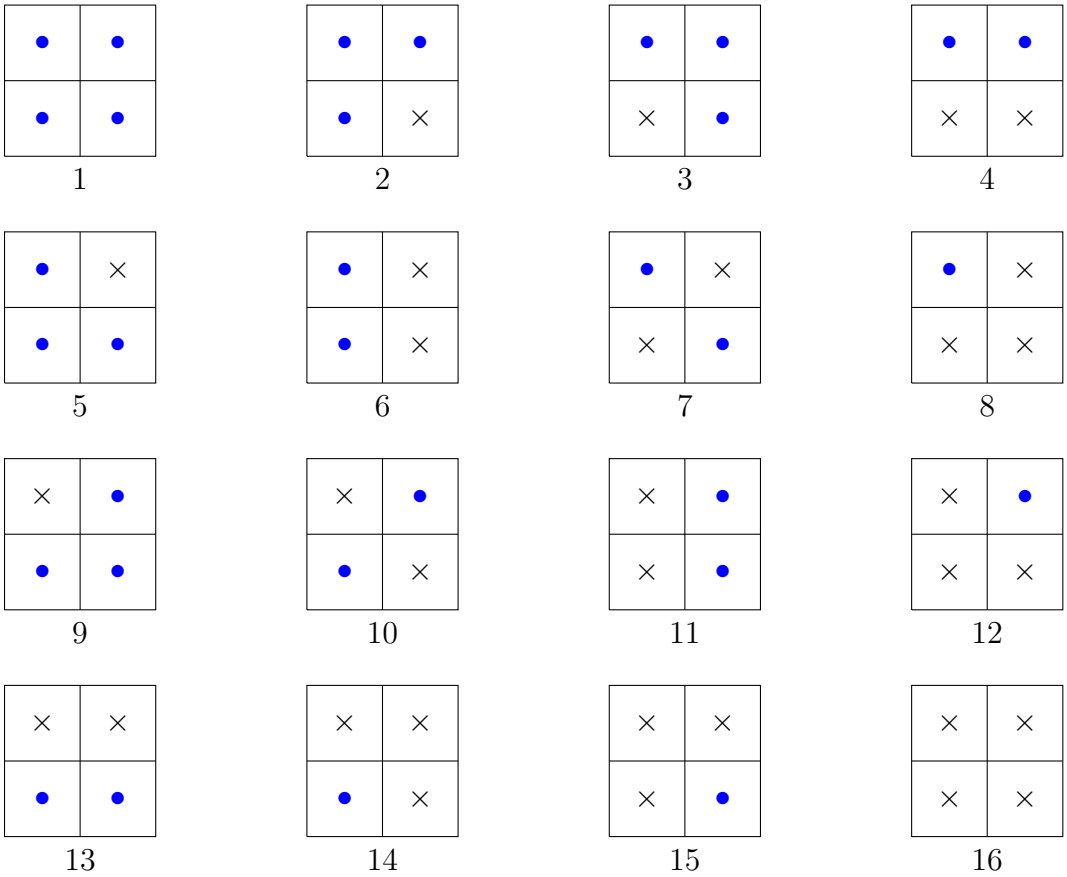
On représentera un tel bidomino vert, de connaissance de certaines relations “est un résidu quadratique de n” ainsi :

29	30
69	68

et on le résumera par :

•	•
×	×

On rappelle qu'un bidomino bicolore bleu (selon la multiplication vue plus haut) a 16 configurations possibles :



Les possibilités 1, 2, 3, 5, 6, 9 et 11 contiennent une décomposition de Goldbach au moins (un nombre premier (•) au-dessus d'un autre nombre premier (•)).

Notre but est de montrer qu'on a toujours pour n un bidomino bleu qui contient deux nombres premiers complémentaires à n, mais on ne sait pas comment établir un lien entre les bidominos

bleus des transpositions, obtenus par les multiplications dans $(\mathbb{Z}/n\mathbb{Z})^\times$, et les bidominos verts pour la relation "est un résidu quadratique de".

Il faudrait :

— soit démontrer qu'il est impossible, compte-tenu des contraintes qui doivent être vérifiées par les transpositions (i.e. on multiplie horizontalement par un nombre et cette opération de multiplication s'avère être une involution modulo n tandis que verticalement, on multiplie par -1 modulo n puisqu'un nombre se transpose verticalement en son opposé) et compte-tenu des contraintes de résiduosité quadratique qui lient les nombres selon leur factorisation et leur forme $4k+1$ ou $4k+3$, que les seules paires de transpositions (bidominos bleus) possibles soient toutes des seules formes 4, 7, 8, 10, 12, 13, 14, 15 et 16 énumérées ci-dessus ;

— soit démontrer par récurrence que si les bidominos sont "agréables" jusqu'à n, on a un bidomino contenant une paire de nombres premiers complémentaires pour $n+2$ (qui est le nombre pair suivant n pair).

Annexe : table de la relation "est un résidu quadratique de" fournie par Gauss dans ses Recherches arithmétiques

On colore en cyan les entête de lignes et de colonnes correspondant aux nombres premiers de la forme $4k+1$ (qui sont sommes de 2 carrés de manière unique) pour souligner la symétrie de la relation "est résidu quadratique de" qu'ils amènent (pour eux, ligne=colonne). On a omis la colonne correspondant au nombre premier 2 car un nombre impair est toujours congru à un carré modulo 2 puisqu'il est congru à 1 modulo 2, et que 1 est son propre carré.

	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
2			×			×		×		×		×		×					×	×	×		×	×
3	×			×	×			×			×			×		×	×		×	×		×		×
5		×		×			×		×	×		×				×	×		×		×		×	
7	×		×				×		×	×	×			×	×	×						×		
11		×	×	×			×				×		×		×						×	×	×	×
13	×				×	×		×	×				×		×		×				×			
17					×	×	×						×	×	×	×		×				×	×	
19	×	×				×	×			×						×	×	×	×	×	×			
23			×	×	×		×	×	×			×	×					×		×	×	×		
29		×	×		×			×	×						×	×		×	×			×		
31	×	×		×				×		×		×	×								×	×		×
37	×		×	×							×	×		×	×			×	×	×		×		
41		×						×		×	×	×	×			×	×			×		×		
43	×		×		×	×	×					×	×		×				×					×
47				×		×	×	×		×	×		×	×	×		×	×					×	×
53			×	×	×	×			×		×		×	×	×	×							×	×
59		×		×		×		×	×	×		×	×	×	×	×		×				×		
61	×	×			×		×					×		×			×			×		×		×
67	×		×	×		×			×	×	×		×					×		×	×		×	
71		×	×	×				×	×	×	×			×		×		×	×	×			×	
73	×						×	×			×	×					×	×	×	×	×		×	×
79	×	×	×		×								×	×		×			×	×	×		×	×
83						×	×		×		×	×	×	×			×	×	×		×	×		
89		×		×		×								×	×			×	×	×	×		×	×
97	×			×						×			×	×	×		×			×	×		×	×

On vérifie que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

La relation "est résidu quadratique de" est réflexive, symétrique si l'un au moins de p ou q est de la forme $4k+1$ et anti-symétrique sinon (si p et q sont tous les deux de la forme $4k+3$).

Références

[1] Lehmer D. N., *Certain Theorems in the Theory of Quadratic Residues*, The American Mathematical Monthly, Vol. 20, No. 5 (May, 1913), pp. 151-157, https://www.jstor.org/stable/2972413. Traduction http://denise.vella.chemla.free.fr/trad-Lehmer-nb-RQ.pdf.

[2] Stangl W. D., *Counting squares in* $\mathbb{Z}_n$, Mathematics magazine, vol. 69, n° 4, octobre 1996, p. 285. Traduction http://denise.vella.chemla.free.fr/trad-Stangl.pdf.

[3] Denise Vella-Chemla, *Des nombres qui en permutent d'autres*, http://denise.vella.chemla.free.fr/permutations.pdf, octobre 2023.

[4] Denise Vella-Chemla, *Annexe 2 : permutations associées aux nombres premiers à n (sauf 1 et n − 1) pour n compris entre 64 et 100 et non double d'un nombre premier*, http://denise.vella.chemla.free.fr/permutations-annexe-2.pdf, octobre 2023.

[5] Denise Vella-Chemla, *Annexe 3 : permutations associées aux nombres premiers à n (sauf 1 et n − 1) pour n compris entre 14 et 100 et n double d'un nombre premier de la note Des nombres qui en permutent d'autres*, http://denise.vella.chemla.free.fr/permutations-doubles-de-premiers.pdf, octobre 2023.

[6] Denise Vella-Chemla, *Utilisation de permutations à la recherche de décompositions de Goldbach*, http://denise.vella.chemla.free.fr/indu.pdf, novembre 2023.

Utilisation de permutations à la recherche de décompositions de Goldbach (Denise Vella-Chemla, octobre 2023).

Dans les notes ici, là ainsi que là , on a cherché par programme les permutations des nombres $[1, n]$ pour n un nombre pair compris entre 6 et 100 en les multipliant, modulo n, par un nombre k premier à n.

Un théorème énonce qu'une permutation est toujours décomposable en un produit de transpositions. On recopie l'extrait du cours [1] énonçant ce théorème et soulignant la non-commutativité du produit de transpositions.

> *Théorème 4.6. Toute permutation $\sigma \in \mathcal{S}(E)$ se décompose en produit de transpositions (le groupe $\mathcal{S}(E)$ est engendré par les transpositions).*
>
> *Démonstration. On a $Id = \tau^2$ pour toute transposition τ.*
>
> *D'après le théorème 4.2 et la proposition 4.5, toute permutation $\sigma \in \mathcal{S}(E)\backslash\{Id\}$ est produit de cycles et un cycle est produit de transpositions.*
>
> *Remarque 4.7. Dans la décomposition d'une permutation en produit de transpositions, il n'y a pas d'unicité et les transpositions ne commutent pas nécessairement. Par exemple, on a*
>
> $$(2, 3) = (1, 2)(1, 3)(1, 2)$$
>
> *et*
>
> $$(1, 2)(2, 3) = (1, 2, 3) \neq (2, 3)(1, 2) = (3, 2, 1) :$$

On va s'intéresser aux transpositions pour classer les nombres pairs. Il semblerait, au vu des seuls exemples étudiés, que les nombres pairs soient à classer en 4 ensembles, selon leur reste modulo 8 : les $8k$, les $8k + 4$, les $8k + 2$ et les $8k + 6$.

1) Pour les $8k$ (voir annexe 2), la fonction de multiplication par $4k - 1$ est constituée de $4k - 1$ transpositions et admet 2 points fixes : $4k$ et $8k$. Elle est impaire.
exemple : $\boldsymbol{n = 32}$
15 impaire ordre 2
(1 15)(2 30)(3 13)(4 28)(5 11)(6 26)(7 9)(8 24)(10 22)(12 20)(14 18)(17 31)(19 29)
(21 27)(23 25)

2) Pour les $8k + 4$ (voir annexe 3), la fonction de multiplication par $4k + 1$ est constituée de $4k$ transpositions et de 4 points fixes $2k + 1, 4k + 2$ et $6k + 3$. Elle est paire.
exemple : $\boldsymbol{n = 36}$
17 paire ordre 2
(1 17)(2 34)(3 15)(4 32)(5 13)(6 30)(7 11)(8 28)(10 26)(12 24)(14 22)(16 20)(19 35)
(21 33)(23 31)(25 29)

3) Pour les $8k+2$ (voir annexe 4), la fonction de multiplication par $4k-1$ est constituée d'un nombre pair de transpositions.
exemple : $\boldsymbol{n}$ **=42**
19 paire ordre 6
(1 19 25 13 37 31)(2 38 8 26 32 20)(3 15 33 39 27 9)(4 34 16 10 22 40)(5 11 41 23 17 29)
(6 30 24 36 12 18)

4) Pour les $8k+6$ (voir annexe 5), la fonction de multiplication par $4k+1$ est constituée d'un nombre pair de transpositions.
exemple : $\boldsymbol{n}$ **=30**
13 paire ordre 4
(1 13 19 7)(2 26 8 14)(3 9 27 21)(4 22 16 28)(6 18 24 12)(11 23 29 17)

5) Pour les nombres pairs n doubles de nombres premiers (de la forme $2p$), p est toujours point fixe et toutes les permutations sont paires (voir là).

On reporte les résultats trouvés dans un tableau, en cherchant à généraliser.

	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50
3	i2	p4		p6	i4		i4	p5		p3	i6		i8	p16		p18	i4		i10	p11		p20
5			p2	p6	p4	p6		p5	p2	p4	p6		p8	p16	p6	p9		p6	p5	p22	p4	
7					i2	p3	i4	p10	i2	p12		p4	i4	p16	i6	p3	i4		i10	p22	i2	p4
9							p2	p5		p3	p6		p4	p8		p9	p2		p5	p11		p10
11									i2	p12	i6	p2	i8	p16	i6	p3	i2	p6		p22	i4	p5
13											p2	p4	p8	p4	p3	p18	p4	p2	p10	p11	p4	p20
15													i2	p8		p18			i10	p22		
17															p2	p9	p4	p6		p22		p20
19																	i2	p6	p10	p22	p2	p10
21																			i10	p22	i4	p5
23																			p2		i2	p20
φ	4	4	4	6	8	6	8	10	8	12	12	8	16	16	12	18	16	12	20	22	16	20

Dans les colonnes correspondant aux nombres n avec n un nombre pair double d'un nombre impair, toutes les permutations de la colonne sont paires.

Dans les colonnes correspondant aux nombres n avec n un nombre pair double d'un nombre pair, les signatures des permutations de la colonne alternent : impaire, paire, impaire, paire, etc (elles sont impaires pour les lignes des $4k+3$ et paires pour les lignes des $4k+1$).

Si l'on ne s'intéresse qu'aux signatures des mises sous la forme produit de transpositions :
- on trouve le mot i2 pour produit de transpositions de signature impaire en bas de toute colonne de n de la forme $8k$;
- on trouve le mot p2 pour produit de transpositions de signature paire en bas de toute colonne de n de la forme $8k+4$;
- même si on ne le trouve pas toujours directement dans les colonnes correspondantes, les produits de transpositions pour les nombres n des formes $8k+2$ et $8k+6$ sont systématiquement de signature paire.

On rappelle que pour les nombres pairs doubles de nombre premier, i.e. de la forme $n = 2p$, p est un point fixe pour la multiplication : $p^2 \equiv p \pmod{2p}$, par exemple, $31^2 = 961 \equiv 31 \pmod{62}$.

Comme attendu, l'ordre (i.e. la longueur de son orbite multiplicative) d'un nombre impair (entête de ligne) dans la colonne d'un nombre pair n divise toujours $\varphi(n)$, l'indicatrice d'Euler de n, qu'on a noté en bas du tableau[1].

Là, on a deux idées : la première consiste à se dire, selon la phrase résumant la théorie de Galois "'*les groupes se réduisent et les corps s'étendent*", comme on sait que la conjecture de Goldbach est vérifiée pour tous les nombres jusqu'à $n = 4.10^{18}$ et qu'à ces nombres n correspondent les groupes qu'on a un peu étudiés ici, il suffirait peut-être pour un "nouveau" nombre pair n de trouver une bijection entre une transposition lui correspondant et une transposition correspondant à un nombre n' qui a une décomposition de Goldbach.

La seconde idée est qu'après tout, on peut voir tous les nombres premiers comme correspondant à une seule classe de nombres, et tous les nombres composés comme correspondant à l'autre classe. Il y a là le statut de 2 qui interroge, étant le seul nombre premier pair, faut-il qu'il ait un statut spécial ou pas ? Selon cette seconde idée, il serait peut-être judicieux de "regrouper" les transpositions par 2 : en effet, pour une transposition contenant les nombres $(x_1 \quad x_2)$, il existe une transposition contenant les nombres $(n - x_1 \quad n - x_2)$ quand ceux-ci ne sont pas fixes pour l'opération étudiée (cette assertion que les "opposés", i.e. les complémentaires à n de deux nombres, ces nombres étant images l'un de l'autre par une involution étudiée, sont eux-aussi (les complémentaires) images l'un de l'autre par l'involution en question doit être démontrée).

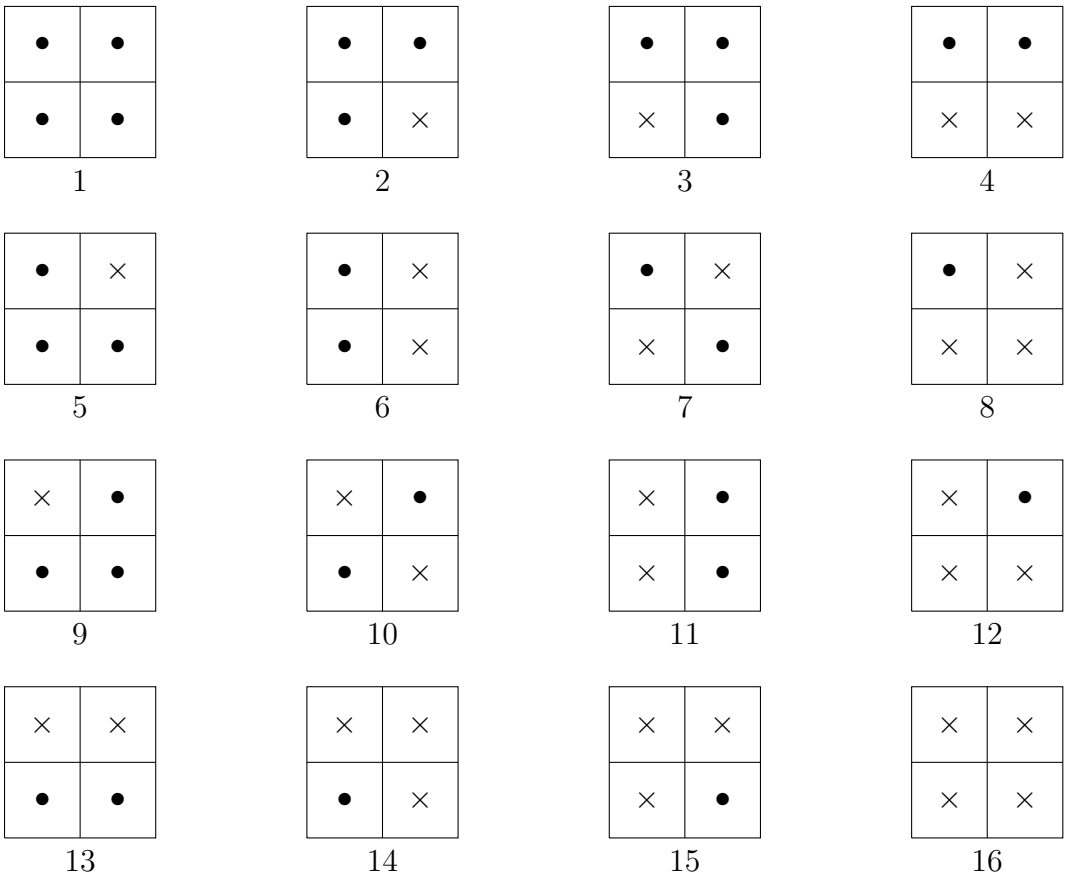
On va représenter ces regroupements de deux transpositions "regroupées" ou "associées" définies au paragraphe ci-dessus par des petits tableaux à 4 cases ainsi ($\bullet$ est le symbole pour nombre impair premier tandis que $\times$ est le symbole pour nombre impair composé). Puisqu'une transposition $(x \quad y)$ peut s'écrire $(x \quad y)$ ou $(y \quad x)$, par convention, on mettra l'un au-dessus de l'autre le caractère de primalité d'un nombre x et de son complémentaire à n, égal à $n - x$. Selon les conventions fixées, le dessin

$\bullet$	$\bullet$
$\bullet$	$\bullet$

représente la paire de transpositions $(x_1 \quad x_2)$ et $(n - x_1 \quad n - x_2)$, dont tous les nombres sont des nombres premiers (par exemple, la paire des transpositions (7 17) et (41 31) qu'on obtient par multiplication par 23 quand on travaille modulon 48.

1. La suite du tableau est fournie en annexe.

Ces tableaux de 4 bits donnent lieu à 16 possibilités :



Les possibilités 1, 2, 3, 5, 6, 9 et 11 contiennent une décomposition de Goldbach au moins (un nombre premier (•) au-dessus d'un autre nombre premier (•)).

Il faudrait démontrer qu'il est impossible, compte-tenu des contraintes qui doivent être vérifiées par les transpositions (i.e. on multiplie horizontalement par un nombre et cette opération de multiplication s'avère être une involution modulo n tandis que verticalement, on multiplie par -1 modulo n puisqu'un nombre se transpose verticalement en son opposé), que les seules paires de transpositions possibles soient toutes des formes 4, 7, 8, 10, 12, 13, 14, 15 et 16.

Annexe 1 : tableau des signatures et ordres des permutations pour n compris entre 52 et 80 puis entre 82 et 100

	52	54	56	58	60	62	64	66	68	70	72	74	76	78	80
3	i6		i6	p28		p30	i16		i16	p12		p18	i18		i4
5	p4	p18	p6	p14		p3	p16	p10	p16		p6	p36	p9	p4	
7	i12	p9		p7	i4	p15	i8	p10	i16		i6	p9	i6	p12	i4
9	p3		p3	p14		p15	p16		p8	p6		p9	p9		p2
11	i12	p18	i6	p28	i2	p30	i16		i16	p3	i6	p6	i6	p12	i4
13		p9	p2	p14	p4	p30	p4	p10	p4	p4	p6	p36	p18		p4
15	i12		i2	p28		p30	i4		i8			p36	i18		
17	p6	p6	p6	p4	p4	p30	p4	p10		p12	p2	p36		p12	i4
19	i12	p3	i6	p28	i2	p15	i16	p10	i8	p6	i2	p36		p12	i4
21	p4			p28		p30	p16		p4			p18	p18		p4
23	i6	p18	i6	p7	i4	p10	i8	p2	i16	p12	i6	p12	i18	p6	i4
25	p2	p9	p3	p7		p3	p8	p5	p8		p3	p18	p9	p2	
27			i2	p28		p10	i16		i16	p4		p6	i6		i4
29					p2	p10	p16	p10	p16	p2	p6	p12	p18	p6	p4
31							i2	p5	i16	p6	i6	p4	i6	p4	i2
33									p2	p12		p9	p18		p4
35											i2	p36	i18	p6	
37													p2	p12	p4
39															i2
φ	24	18	24	28	16	30	32	20	32	24	24	36	36	24	32

	82	84	86	88	90	92	94	96	98	100
3	p8		p42	i10		i22	p23		p42	i20
5	p20	p6	p42	p10		p22	p46	p8	p42	
7	p40		p6	i10	p12	i22	p23	i4		i4
9	p4		p21	p5	p6	p11	p23		p21	p10
11	p40	i6	p7			i22	p46	i8	p21	i10
13	p40	p2	p21	p10	p12	p11	p46	p8	p14	p20
15	p40		p21	i10		i22	p46		p7	
17	p40	p6	p21	p10	p4	p22	p23	p2	p42	p20
19	p40	i6	p42	i10	p2	i22	p46	i8	p6	i10
21	p20		p7	p2		p22	p23			p5
23	p10	i6	p21	i2	p12		p46	i4	p21	i20
25	p10	p3	p21	p5		p11	p23	p4	p21	
27	p8		p14	i10		i22	p23		p14	i20
29	p40	p2	p42	p10	p6	p11	p46	p8	p7	p10
31	p10	i6	p21	i10		i22	p46	i2	p6	i10
33	p20		p42		p3	p22	p46		p42	p20
35	p40		p7	i10		i22	p46	i8		
37	p5	p3	p6	p10	p4	p22	p23	p8	p21	p20
39	p20		p14	i10		i22	p46		p21	i10
41		p2	p7	p10	p6	p11	p46	p4	p14	p5
43				i2	p12	i22	p46	i8	p7	i4
45						p2	p46		p42	
47								i2	p42	i20
49										p2
φ	40	24	42	40	24	44	46	32	42	40

Annexe 2 : les $8k$

Nombres étudiés : 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96.

$n = 8$

3 impaire ordre 2

(1 3)(2 6)(5 7)

$n = 16$

7 impaire ordre 2

(1 7)(2 14)(3 5)(4 12)(6 10)(9 15)(11 13)

$n = 24$

11 impaire ordre 2

(1 11)(2 22)(3 9)(4 20)(5 7)(6 18)(8 16)(10 14)(13 23)(15 21)(17 19)

$n = 32$

15 impaire ordre 2

(1 15)(2 30)(3 13)(4 28)(5 11)(6 26)(7 9)(8 24)(10 22)(12 20)(14 18)(17 31)(19 29)
(21 27)(23 25)

$n = 40$

19 impaire ordre 2

(1 19)(2 38)(3 17)(4 36)(5 15)(6 34)(7 13)(8 32)(9 11)(10 30)(12 28)(14 26)(16 24)(18 22)
(21 39)(23 37)(25 35)(27 33)(29 31)

$n = 48$

23 impaire ordre 2

(1 23)(2 46)(3 21)(4 44)(5 19)(6 42)(7 17)(8 40)(9 15)(10 38)(11 13)(12 36)(14 34)(16 32)
(18 30)(20 28)(22 26)(25 47)(27 45)(29 43)(31 41)(33 39)(35 37)

$n = 56$

27 impaire ordre 2

(1 27)(2 54)(3 25)(4 52)(5 23)(6 50)(7 21)(8 48)(9 19)(10 46)(11 17)(12 44)
(13 15)(14 42)(16 40)(18 38)(20 36)(22 34)(24 32)(26 30)(29 55)(31 53)(33 51)
(35 49)(37 47)(39 45)(41 43)

$n = 64$

31 impaire ordre 2

(1 31) (2 62) (3 29) (4 60) (5 27) (6 58) (7 25) (8 56) (9 23) (10 54) (11 21) (12 52) (13
19) (14 50) (15 17) (16 48) (18 46) (20 44) (22 42) (24 40) (26 38) (28 36) (30 34) (33 63)
(35 61) (37 59) (39 57) (41 55) (43 53) (45 51) (47 49)

$n = 72$

35 impaire ordre 2

(1 35) (2 70) (3 33) (4 68) (5 31) (6 66) (7 29) (8 64) (9 27) (10 62) (11 25) (12 60) (13
23) (14 58) (15 21) (16 56) (17 19) (18 54) (20 52) (22 50) (24 48) (26 46) (28 44) (30 42)
(32 40) (34 38) (37 71) (39 69) (41 67) (43 65) (45 63) (47 61) (49 59) (51 57) (53 55)

$n = 80$

39 impaire ordre 2

(1 39) (2 78) (3 37) (4 76) (5 35) (6 74) (7 33) (8 72) (9 31) (10 70) (11 29) (12 68) (13 27) (14 66) (15 25) (16 64) (17 23) (18 62) (19 21) (20 60) (22 58) (24 56) (26 54) (28 52) (30 50) (32 48) (34 46) (36 44) (38 42) (41 79) (43 77) (45 75) (47 73) (49 71) (51 69) (53 67) (55 65) (57 63) (59 61)

n=88

43 impaire ordre 2

(1 43) (2 86) (3 41) (4 84) (5 39) (6 82) (7 37) (8 80) (9 35) (10 78) (11 33) (12 76) (13 31) (14 74) (15 29) (16 72) (17 27) (18 70) (19 25) (20 68) (21 23) (22 66) (24 64) (26 62) (28 60) (30 58) (32 56) (34 54) (36 52) (38 50) (40 48) (42 46) (45 87) (47 85) (49 83) (51 81) (53 79) (55 77) (57 75) (59 73) (61 71) (63 69) (65 67)

n=96

47 impaire ordre 2

(1 47) (2 94) (3 45) (4 92) (5 43) (6 90) (7 41) (8 88) (9 39) (10 86) (11 37) (12 84) (13 35) (14 82) (15 33) (16 80) (17 31) (18 78) (19 29) (20 76) (21 27) (22 74) (23 25) (24 72) (26 70) (28 68) (30 66) (32 64) (34 62) (36 60) (38 58) (40 56) (42 54) (44 52) (46 50) (49 95) (51 93) (53 91) (55 89) (57 87) (59 85) (61 83) (63 81) (65 79) (67 77) (69 75) (71 73)

Annexe 3 : les $8k + 4$

Nombres étudiés : 12, 20, 28, 36, 44, 52, 60, 68, 76, 84, 92, 100.

n = 12

5 paire ordre 2

(1 5)(2 10)(4 8)(7 11)

n =20

9 paire ordre 2

(1 9)(2 18)(3 7)(4 16)(6 14)(8 12)(11 19)(13 17)

n =28

13 paire ordre 2

(1 13)(2 26)(3 11)(4 24)(5 9)(6 22)(8 20)(10 18)(12 16)(15 27)(17 25)(19 23)

n =36

17 paire ordre 2

(1 17)(2 34)(3 15)(4 32)(5 13)(6 30)(7 11)(8 28)(10 26)(12 24)(14 22)(16 20)(19 35)(21 33)(23 31)(25 29)

n =44

21 paire ordre 2

(1 21)(2 42)(3 19)(4 40)(5 17)(6 38)(7 15)(8 36)(9 13)(10 34)(12 32)(14 30)(16 28)(18 26)(20 24)(23 43)(25 41)(27 39)(29 37)(31 35)

n =52

25 paire ordre 2

(1 25)(2 50)(3 23)(4 48)(5 21)(6 46)(7 19)(8 44)(9 17)(10 42)(11 15)(12 40)
(14 38)(16 36)(18 34)(20 32)(22 30)(24 28)(27 51)(29 49)(31 47)(33 45)(35 43)(37 41)

n =60

29 paire ordre 2

(1 29)(2 58)(3 27)(4 56)(5 25)(6 54)(7 23)(8 52)(9 21)(10 50)(11 19)(12 48)(13 17)
(14 46)(16 44)(18 42)(20 40)(22 38)(24 36)(26 34)(28 32)(31 59)(33 57)(35 55)(37 53)
(39 51)(41 49)(43 47)

n=68

33 paire ordre 2

(1 33) (2 66) (3 31) (4 64) (5 29) (6 62) (7 27) (8 60) (9 25) (10 58) (11 23) (12 56) (13 21) (14 54) (15 19) (16 52) (18 50) (20 48) (22 46) (24 44) (26 42) (28 40) (30 38) (32 36) (35 67) (37 65) (39 63) (41 61) (43 59) (45 57) (47 55) (49 53)

n=76

37 paire ordre 2

(1 37) (2 74) (3 35) (4 72) (5 33) (6 70) (7 31) (8 68) (9 29) (10 66) (11 27) (12 64) (13 25) (14 62) (15 23) (16 60) (17 21) (18 58) (20 56) (22 54) (24 52) (26 50) (28 48) (30 46) (32 44) (34 42) (36 40) (39 75) (41 73) (43 71) (45 69) (47 67) (49 65) (51 63) (53 61) (55 59)

n=84

41 paire ordre 2

(1 41) (2 82) (3 39) (4 80) (5 37) (6 78) (7 35) (8 76) (9 33) (10 74) (11 31) (12 72) (13 29) (14 70) (15 27) (16 68) (17 25) (18 66) (19 23) (20 64) (22 62) (24 60) (26 58) (28 56) (30 54) (32 52) (34 50) (36 48) (38 46) (40 44) (43 83) (45 81) (47 79) (49 77) (51 75) (53 73) (55 71) (57 69) (59 67) (61 65)

n=92

45 paire ordre 2

(1 45) (2 90) (3 43) (4 88) (5 41) (6 86) (7 39) (8 84) (9 37) (10 82) (11 35) (12 80) (13 33) (14 78) (15 31) (16 76) (17 29) (18 74) (19 27) (20 72) (21 25) (22 70) (24 68) (26 66) (28 64) (30 62) (32 60) (34 58) (36 56) (38 54) (40 52) (42 50) (44 48) (47 91) (49 89) (51 87) (53 85) (55 83) (57 81) (59 79) (61 77) (63 75) (65 73) (67 71)

n=100

49 paire ordre 2

(1 49) (2 98) (3 47) (4 96) (5 45) (6 94) (7 43) (8 92) (9 41) (10 90) (11 39) (12 88) (13 37) (14 86) (15 35) (16 84) (17 33) (18 82) (19 31) (20 80) (21 29) (22 78) (23 27) (24 76) (26 74) (28 72) (30 70) (32 68) (34 66) (36 64) (38 62) (40 60) (42 58) (44 56) (46 54) (48 52) (51 99) (53 97) (55 95) (57 93) (59 91) (61 89) (63 87) (65 85) (67 83) (69 81) (71 79) (73 77)

Annexe 4 : les $8k+2$

Nombres étudiés (quand ce ne sont pas des doubles de nombres premiers, on a indiqué ceux-ci par $2p$ entre parenthèses) : 10 ($2p$), 18, 26 ($2p$), 34 ($2p$), 42, 50, 58 ($2p$), 66, 74 ($2p$), 82 ($2p$), 90, 98.

n =18
7 paire ordre 3
(1 7 13)(2 14 8)(4 10 16)(5 17 11)

n =42
19 paire ordre 6
(1 19 25 13 37 31)(2 38 8 26 32 20)(3 15 33 39 27 9)(4 34 16 10 22 40)(5 11 41 23 17 29)
(6 30 24 36 12 18)

n =50
23 paire ordre 20
(1 23 29 17 41 43 39 47 31 13 49 27 21 33 9 7 11 3 19 37)
(2 46 8 34 32 36 28 44 12 26 48 4 42 16 18 14 22 6 38 24)(5 15 45 35)(10 30 40 20)

n=66
31 paire ordre 5
(1 31 37 25 49) (2 62 8 50 32) (3 27 45 9 15) (4 58 16 34 64) (5 23 53 59 47) (6 54 24 18 30) (7 19 61 43 13) (10 46 40 52 28) (12 42 48 36 60) (14 38 56 20 26) (17 65 35 29 41) (21 57 51 63 39)

n=90
43 paire ordre 12
(1 43 49 37 61 13 19 7 31 73 79 67) (2 86 8 74 32 26 38 14 62 56 68 44) (3 39 57 21) (4 82 16 58 64 52 76 28 34 22 46 88) (5 35 65) (6 78 24 42) (9 27 81 63) (10 70 40) (11 23 89 47 41 53 29 77 71 83 59 17) (12 66 48 84) (18 54 72 36) (20 50 80) (25 85 55) (33 69 87 51)

n=98
47 paire ordre 42
(1 47 53 41 65 17 15 19 11 27 93 59 29 89 67 13 23 3 43 61 25 97 51 45 57 33 81 83 79 87 71 5 39 69 9 31 85 75 95 55 37 73) (2 94 8 82 32 34 30 38 22 54 88 20 58 80 36 26 46 6 86 24 50 96 4 90 16 66 64 68 60 76 44 10 78 40 18 62 72 52 92 12 74 48) (7 35 77 91 63 21) (14 70 56 84 28 42)

Annexe 5 : les $8k+6$

Nombres étudiés (quand ce ne sont pas des doubles de nombres premiers, on a indiqué ceux-ci par $2p$ entre parenthèses) : 6 ($2p$), 14 ($2p$), 22 ($2p$), 30, 38 ($2p$), 46 ($2p$), 54, 62 ($2p$), 70, 78, 86 ($2p$), 94 ($2p$).

n =30
13 paire ordre 4

(1 13 19 7)(2 26 8 14)(3 9 27 21)(4 22 16 28)(6 18 24 12)(11 23 29 17)

n =54

25 paire ordre 9

(1 25 31 19 43 49 37 7 13)(2 50 8 38 32 44 20 14 26)(3 21 39)
(4 46 16 22 10 34 40 28 52)(5 17 47 41 53 29 23 35 11)(6 42 24)(12 30 48)(15 51 33)

n=70

33 paire ordre 12

(1 33 39 27 51 3 29 47 11 13 9 17) (2 66 8 54 32 6 58 24 22 26 18 34) (4 62 16 38 64 12 46 48 44 52 36 68) (5 25 55 65 45 15) (7 21 63 49) (10 50 40 60 20 30) (14 42 56 28) (19 67 41 23 59 57 61 53 69 37 31 43)

n=78

37 paire ordre 12

(1 37 43 31 55 7 25 67 61 73 49 19) (2 74 8 62 32 14 50 56 44 68 20 38) (3 33 51 15 9 21 75 45 27 63 69 57) (4 70 16 46 64 28 22 34 10 58 40 76) (5 29 59 77 41 35 47 23 71 53 11 17) (6 66 24 30 18 42 72 12 54 48 60 36)

Références

[1] Khalid Koufany, *Cours d'Algèbre, chapitre 4, Groupe de permutations, groupe symétrique*, voir là https://khalid-koufany.perso.math.cnrs.fr/Algebre2/ch4-groupes-symetriques.pdf.

[2] Larochette Jérémy, *Cours de MPSI, 2018*, voir là https://mp1.prepa-carnot.fr/wp-content/uploads/2020/11/15$_G roupe_s ymetrique.pdf$.

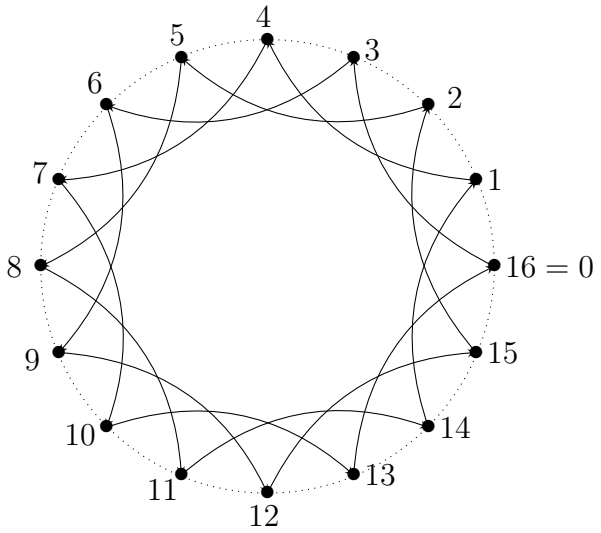
[3] Barôme Frédéric, *Chapitre 3 : Groupes symétriques*, voir là https://iremi.univ-reunion.fr/IMG/pdf/Barome$_g roupes_s ymetriques.pdf$.

Des nombres qui en permutent d'autres (Denise Vella-Chemla, octobre 2023).

Dans cette note, on utilise les définitions d'un cours d'algèbre sur le groupe symétrique et les permutations ([1], [2], [3]).

On s'intéresse à la conjecture de Goldbach qui stipule que tout nombre pair n (supérieur ou égal à 4) est somme de deux nombres premiers (impairs si $n > 4$). On rappelle que deux nombres différents sont premiers entre eux si leur plus grand diviseur commun est égal à 1. Dans la suite, on ne va s'intéresser, à la recherche des décomposants de Goldbach de n, qu'aux nombres premiers à n[1], car les décomposants de Goldbach de n, étant premiers, sont notamment premiers à n.

On sait qu'à chacun des nombres premiers à n peut être associée une permutation des entiers $[1, \ldots, n]$ en illustrant cela sur un exemple : plaçons sur un cercle les entiers de 1 à 16. Considérons des sauts de 3 en 3 sur le cercle à partir d'un des entiers en question. Comme 3 ne divise pas 16, tous les entiers vont être parcourus avant que l'on ne revienne à notre point de départ. On a parcouru les nombres de 1 à 16 dans l'ordre suivant $[1, 4, 7, 10, 13, 0, 3, 6, 9, 12, 15, 2, 5, 8, 11, 14]$, etc., et on peut considérer cet ordre comme une permutation des entiers de 1 à 16[2].



Existe également, isomorphe à la permutation additive ci-dessus, une permutation qui envoie tout x de 1 à n sur son produit par k premier à n. Cette permutation, en prenant $k = 3, n = 16$ envoie 1 sur 3, 2 sur 6, 3 sur 9, 4 sur 12, 5 sur 15, 6 sur 2 ($= 18 \pmod{16}$), etc.

1. appelés aussi éléments du groupe des unités $(\mathbb{Z}/n\mathbb{Z})^\times$. Par définition, le groupe des unités $(\mathbb{Z}/n\mathbb{Z})^\times$ de l'anneau des classes de congruences sur les entiers $\mathbb{Z}/n\mathbb{Z}$ a pour éléments les générateurs du groupe additif de l'anneau. Son cardinal est donné par l'indicatrice d'Euler, notée $\varphi(n)$. Les valeurs de l'indicatrice d'Euler pour les nombres de 1 à 100 peuvent être retrouvées ici http://denise.vella.chemla.free.fr/indicEuler.jpg.

2. On peut rapprocher le fait de parcourir tous les entiers de 1 à 16 ici, du fait de l'indivisibilité de 16 par 3, comme analogue au fait de parcourir l'ensemble du tore là (voir vidéo https://www.youtube-nocookie.com/embed/Zh9mVUq0ZQM), du fait de l'irrationnalité du pas. Voir aussi cette vidéo https://www.youtube-nocookie.com/embed/QfZLKxKTS2c aux minute 28 et suivantes et notamment la phrase "Les feuilles ne reviennent pas au même endroit, elles s'enroulent indéfiniment.".

En annexe sont fournies les permutations multiplicatives associées aux nombres premiers à n pour n (non double d'un nombre premier, car les doubles de nombres premiers vérifient trivialement la conjecture de Goldbach) compris entre 8 et 60.

Rappelons qu'une permutation est décomposable en cycles disjoints et que l'ordre de la permutation est le *ppcm* des longueurs des cycles qui la constituent.

On note dans un tableau, en regard des nombres pairs, les unités à n dont la permutation associée est d'ordre minimum et celles dont la permutation associée est d'ordre maximum. On constate que les décomposants de Goldbach (en bleu) de n apparaissent de façon erratique dans l'une et/ou l'autre colonne et qu'aucune généralité ne semble donc émerger des exemples étudiés.

n	permut. d'ordre min.	permut. d'ordre max
8	3	3
12	5	5
16	7	3, 5
18	7	5
20	9	3, 7
24	5, 7, 11	5, 7, 11
28	13	3, 9, 11
30	11	7, 13
32	15	3, 5, 11, 13
36	17	5, 7, 11
40	9, 11, 19	3, 7, 13, 17
42	13	5, 11, 17, 19
44	21	3, 13, 15, 17, 19
48	7, 17, 23	5, 11, 13, 19
50	7	3, 13, 17, 23
52	25	7, 11, 15, 19
54	19	5, 11, 23
56	13, 15, 27	3, 5, 11, 17, 19, 23
60	11, 19, 29	7, 13, 17, 23

Annexe : permutations associées aux nombres premiers à n (sauf 1 et $n-1$) pour n compris entre 8 et 60 et non double d'un nombre premier (les décomposants de Goldbach de n sont notés en bleu)

$n = 8$
3 impaire ordre 2
(1 3)(2 6)(5 7)

$n = 12$
5 paire ordre 2

(1 5)(2 10)(4 8)(7 11)

n =16

3 impaire ordre 4

(1 3 9 11)(2 6)(4 12)(5 15 13 7)(10 14)

5 paire ordre 4

(1 5 9 13)(2 10)(3 15 11 7)(6 14)

7 impaire ordre 2

(1 7)(2 14)(3 5)(4 12)(6 10)(9 15)(11 13)

n =18

5 paire ordre 6

(1 5 7 17 13 11)(2 10 14 16 8 4)(3 15)(6 12)

7 paire ordre 3

(1 7 13)(2 14 8)(4 10 16)(5 17 11)

n =20

3 impaire ordre 4

(1 3 9 7)(2 6 18 14)(4 12 16 8)(5 15)(11 13 19 17)

7 impaire ordre 4

(1 7 9 3)(2 14 18 6)(4 8 16 12)(5 15)(11 17 19 13)

9 paire ordre 2

(1 9)(2 18)(3 7)(4 16)(6 14)(8 12)(11 19)(13 17)

n =24

5 paire ordre 2

(1 5)(2 10)(3 15)(4 20)(7 11)(8 16)(9 21)(13 17)(14 22)(19 23)

7 impaire ordre 2

(1 7)(2 14)(3 21)(5 11)(6 18)(9 15)(10 22)(13 19)(17 23)

11 impaire ordre 2

(1 11)(2 22)(3 9)(4 20)(5 7)(6 18)(8 16)(10 14)(13 23)(15 21)(17 19)

n =28

3 impaire ordre 6

(1 3 9 27 25 19)(2 6 18 26 22 10)(4 12 8 24 16 20)(5 15 17 23 13 11)(7 21)

5 paire ordre 6

(1 5 25 13 9 17)(2 10 22 26 18 6)(3 15 19 11 27 23)(4 20 16 24 8 12)

9 paire ordre 3

(1 9 25)(2 18 22)(3 27 19)(4 8 16)(5 17 13)(6 26 10)(11 15 23)(12 24 20)

11 impaire ordre 6

(1 11 9 15 25 23)(2 22 18)(3 5 27 17 19 13)(4 16 8)(6 10 26)(7 21)(12 20 24)

13 paire ordre 2

(1 13)(2 26)(3 11)(4 24)(5 9)(6 22)(8 20)(10 18)(12 16)(15 27)(17 25)(19 23)

n =30

7 paire ordre 4
(1 7 19 13)(2 14 8 26)(3 21 27 9)(4 28 16 22)(6 12 24 18)(11 17 29 23)

11 paire ordre 2
(1 11)(2 22)(4 14)(5 25)(7 17)(8 28)(10 20)(13 23)(16 26)(19 29)

13 paire ordre 4
(1 13 19 7)(2 26 8 14)(3 9 27 21)(4 22 16 28)(6 18 24 12)(11 23 29 17)

n =32

3 impaire ordre 8
(1 3 9 27 17 19 25 11)(2 6 18 22)(4 12)(5 15 13 7 21 31 29 23)(8 24)(10 30 26 14)(20 28)

5 paire ordre 8
(1 5 25 29 17 21 9 13)(2 10 18 26)(3 15 11 23 19 31 27 7)(4 20)(6 30 22 14)(12 28)

7 impaire ordre 4
(1 7 17 23)(2 14)(3 21 19 5)(4 28)(6 10)(8 24)(9 31 25 15)(11 13 27 29)(12 20)(18 30)
(22 26)

9 paire ordre 4
(1 9 17 25)(2 18)(3 27 19 11)(5 13 21 29)(6 22)(7 31 23 15)(10 26)(14 30)

11 impaire ordre 8
(1 11 25 19 17 27 9 3)(2 22 18 6)(4 12)(5 23 29 31 21 7 13 15)(8 24)(10 14 26 30)(20 28)

13 paire ordre 8
(1 13 9 21 17 29 25 5)(2 26 18 10)(3 7 27 31 19 23 11 15)(4 20)(6 14 22 30)(12 28)

15 impaire ordre 2
(1 15)(2 30)(3 13)(4 28)(5 11)(6 26)(7 9)(8 24)(10 22)(12 20)(14 18)(17 31)(19 29)
(21 27)(23 25)

n =36

5 paire ordre 6
(1 5 25 17 13 29)(2 10 14 34 26 22)(3 15)(4 20 28 32 16 8)(6 30)(7 35 31 11 19 23)
(12 24)(21 33)

7 impaire ordre 6
(1 7 13 19 25 31)(2 14 26)(3 21)(4 28 16)(5 35 29 23 17 11)(8 20 32)(9 27)(10 34 22)
(15 33)

11 impaire ordre 6
(1 11 13 35 25 23)(2 22 26 34 14 10)(3 33)(4 8 16 32 28 20)(5 19 29 31 17 7)(6 30)
(9 27)(12 24)(15 21)

13 paire ordre 3
(1 13 25)(2 26 14)(4 16 28)(5 29 17)(7 19 31)(8 32 20)(10 22 34)(11 35 23)

17 paire ordre 2
(1 17)(2 34)(3 15)(4 32)(5 13)(6 30)(7 11)(8 28)(10 26)(12 24)(14 22)(16 20)(19 35)
(21 33)(23 31)(25 29)

n =40

3 impaire ordre 4
(1 3 9 27)(2 6 18 14)(4 12 36 28)(5 15)(7 21 23 29)(8 24 32 16)(10 30)(11 33 19 17)

(13 39 37 31)(22 26 38 34)(25 35)

7 impaire ordre 4

(1 7 9 23)(2 14 18 6)(3 21 27 29)(4 28 36 12)(5 35)(8 16 32 24)(10 30)(11 37 19 13)
(15 25)(17 39 33 31)(22 34 38 26)

9 paire ordre 2

(1 9)(2 18)(3 27)(4 36)(6 14)(7 23)(8 32)(11 19)(12 28)(13 37)(16 24)(17 33)(21 29)
(22 38)(26 34)(31 39)

11 impaire ordre 2

(1 11)(2 22)(3 33)(5 15)(6 26)(7 37)(9 19)(10 30)(13 23)(14 34)(17 27)(18 38)(21 31)
(25 35)(29 39)

13 paire ordre 4

(1 13 9 37)(2 26 18 34)(3 39 27 31)(4 12 36 28)(5 25)(6 38 14 22)(7 11 23 19)(8 24 32 16)
(15 35)(17 21 33 29)

17 paire ordre 4

(1 17 9 33)(2 34 18 26)(3 11 27 19)(4 28 36 12)(6 22 14 38)(7 39 23 31)(8 16 32 24)
(13 21 37 29)

19 impaire ordre 2

(1 19)(2 38)(3 17)(4 36)(5 15)(6 34)(7 13)(8 32)(9 11)(10 30)(12 28)(14 26)(16 24)(18 22)
(21 39)(23 37)(25 35)(27 33)(29 31)

n =42

5 paire ordre 6

(1 5 25 41 37 17)(2 10 8 40 32 34)(3 15 33 39 27 9)(4 20 16 38 22 26)(6 30 24 36 12 18)
(7 35)(11 13 23 31 29 19)(14 28)

11 paire ordre 6

(1 11 37 29 25 23)(2 22 32 16 8 4)(3 33 27)(5 13 17 19 41 31)(6 24 12)(7 35)(9 15 39)
(10 26 34 38 40 20)(14 28)(18 30 36)

13 paire ordre 2

(1 13)(2 26)(3 39)(4 10)(5 23)(6 36)(8 20)(9 33)(11 17)(12 30)(15 27)(16 40)(18 24)
(19 37)(22 34)(25 31)(29 41)(32 38)

17 paire ordre 6

(1 17 37 41 25 5)(2 34 32 40 8 10)(3 9 27 39 33 15)(4 26 22 38 16 20)(6 18 12 36 24 30)
(7 35)(11 19 29 31 23 13)(14 28)

19 paire ordre 6

(1 19 25 13 37 31)(2 38 8 26 32 20)(3 15 33 39 27 9)(4 34 16 10 22 40)(5 11 41 23 17 29)
(6 30 24 36 12 18)

n =44

3 impaire ordre 10

(1 3 9 27 37 23 25 31 515)(2 6 18 10 30)(4 12 36 20 16)(7 21 19 13 39 29 43 41 35 17)
(8 24 28 40 32)(11 33)(14 42 38 26 34)

5 paire ordre 5

(1 525 37 9)(2 10 6 30 18)(3 15 31 23 27)(4 20 12 16 36)(7 35 43 39 19)(8 40 24 32 28)
(13 21 17 41 29)(14 26 42 34 38)

7 impaire ordre 10

(1 7 5 35 25 43 37 39 9 19) (2 14 10 26 6 42 30 34 18 38) (3 21 15 17 31 41 23 29 27 13) (4 28 20 8 12 40 16 24 36 32) (11 33)

9 paire ordre 5
(1 9 37 25 5)(2 18 30 6 10)(3 27 23 31 15)(4 36 16 12 20)(7 19 39 43 35)(8 28 32 24 40)(13 29 41 17 21)(14 38 34 42 26)

13 paire ordre 10
(1 13 37 41 521 9 29 25 17)(2 26 30 38 10 42 18 14 6 34)(3 39 23 35 15 19 27 43 31 7) (4 8 16 32 20 40 36 28 12 24)

15 impaire ordre 10
(1 15 5 31 25 23 37 27 9 3)(2 30 10 18 6)(4 16 20 36 12)(7 17 35 41 43 29 39 13 19 21) (8 32 40 28 24)(11 33)(14 34 26 38 42)

17 paire ordre 10
(1 17 25 29 9 21 5 41 37 13)(2 34 6 14 18 42 10 38 30 26)(3 7 31 43 27 19 15 35 23 39) (4 24 12 28 36 40 20 32 16 8)

19 impaire ordre 10
(1 19 9 39 37 43 25 35 5 7)(2 38 18 34 30 42 6 26 10 14)(3 13 27 29 23 41 31 17 15 21) (4 32 36 24 16 40 12 8 20 28)(11 33)

21 paire ordre 2
(1 21)(2 42)(3 19)(4 40)(5 17)(6 38)(7 15)(8 36)(9 13)(10 34)(12 32)(14 30)(16 28) (18 26)(20 24)(23 43)(25 41)(27 39)(29 37)(31 35)

n =48

5 paire ordre 4
(1 5 25 29)(2 10)(3 15 27 39)(4 20)(6 30)(7 35 31 11)(8 40)(9 45 33 21)(13 17 37 41) (14 22)(16 32)(18 42)(19 47 43 23)(26 34)(28 44)(38 46)

7 impaire ordre 2
(1 7)(2 14)(3 21)(4 28)(5 35)(6 42)(9 15)(10 22)(11 29)(12 36)(13 43)(17 23)(18 30) (19 37)(20 44)(25 31)(26 38)(27 45)(33 39)(34 46)(41 47)

11 impaire ordre 4
(1 11 25 35)(2 22)(3 33 27 9)(4 44)(5 7 29 31)(6 18)(8 40)(10 14)(12 36)(13 47 37 23) (15 21 39 45)(16 32)(17 43 41 19)(20 28)(26 46)(30 42)(34 38)

13 paire ordre 4
(1 13 25 37)(2 26)(3 39 27 15)(5 17 29 41)(6 30)(7 43 31 19)(9 21 33 45)(10 34) (11 47 35 23)(14 38)(18 42)(22 46)

17 paire ordre 2
(1 17)(2 34)(4 20)(5 37)(7 23)(8 40)(10 26)(11 43)(13 29)(14 46)(16 32)(19 35) (22 38)(25 41)(28 44)(31 47)

19 impaire ordre 4
(1 19 25 43)(2 38)(3 9 27 33)(4 28)(5 47 29 23)(6 18)(7 37 31 13)(10 46)(11 17 35 41) (12 36)(14 26)(15 45 39 21)(20 44)(22 34)(30 42)

23 impaire ordre 2
(1 23)(2 46)(3 21)(4 44)(5 19)(6 42)(7 17)(8 40)(9 15)(10 38)(11 13)(12 36)(14 34)(16 32) (18 30)(20 28)(22 26)(25 47)(27 45)(29 43)(31 41)(33 39)(35 37)

n =50

3 paire ordre 20

(1 3 9 27 31 43 29 37 11 33 49 47 41 23 19 7 21 13 39 17)
(2 6 18 4 12 36 8 24 22 16 48 44 32 46 38 14 42 26 28 34)(5 15 45 35)(10 30 40 20)

7 paire ordre 4
(1 7 49 43)(2 14 48 36)(3 21 47 29)(4 28 46 22)(5 35 45 15)(6 42 44 8)(9 13 41 37)
(10 20 40 30)(11 27 39 23)(12 34 38 16)(17 19 33 31)(18 26 32 24)

9 paire ordre 10
(1 9 31 29 11 49 41 19 21 39)(2 18 12 8 22 48 32 38 42 28)(3 27 43 37 33 47 23 7 13 17)
(4 36 24 16 44 46 14 26 34 6)(5 45)(10 40)(15 35)(20 30)

11 paire ordre 5
(1 11 21 31 41)(2 22 42 12 32)(3 33 13 43 23)(4 44 34 24 14)(6 16 26 36 46)
(7 27 47 17 37)(8 38 18 48 28)(9 49 39 29 19)

13 paire ordre 20
(1 13 19 47 11 43 9 17 21 23 49 37 31 3 39 7 41 33 29 27)
(2 26 38 44 22 36 18 34 42 46 48 24 12 6 28 14 32 16 8 4)(5 15 45 35)(10 30 40 20)

17 paire ordre 20
(1 17 39 13 21 7 19 23 41 47 49 33 11 37 29 43 31 27 9 3)
(2 34 28 26 42 14 38 46 32 44 48 16 22 24 8 36 12 4 18 6)(5 35 45 15)(10 20 40 30)

19 paire ordre 10
(1 19 11 9 21 49 31 39 41 29)(2 38 22 18 42 48 12 28 32 8)
(3 7 33 27 13 47 43 17 23 37)(4 26 44 36 34 46 24 6 14 16)(5 45)(10 40)(15 35)(20 30)

21 paire ordre 5
(1 21 41 11 31)(2 42 32 22 12)(3 13 23 33 43)(4 34 14 44 24)(6 26 46 16 36)
(7 47 37 27 17)(8 18 28 38 48)(9 39 19 49 29)

23 paire ordre 20
(1 23 29 17 41 43 39 47 31 13 49 27 21 33 9 7 11 3 19 37)
(2 46 8 34 32 36 28 44 12 26 48 4 42 16 18 14 22 6 38 24)(5 15 45 35)(10 30 40 20)

n =52

3 impaire ordre 6
(1 3 9 27 29 35)(2 6 18)(4 12 36)(5 15 45 31 41 19)(7 21 11 33 47 37)(8 24 20)
(10 30 38)(13 39)(14 42 22)(16 48 40)(17 51 49 43 25 23)(28 32 44)(34 50 46)

5 paire ordre 4
(1 5 25 21)(2 10 50 42)(3 15 23 11)(4 20 48 32)(6 30 46 22)(7 35 19 43)(8 40 44 12)
(9 45 17 33)(14 18 38 34)(16 28 36 24)(27 31 51 47)(29 41 49 37)

7 impaire ordre 12
(1 7 49 31 9 11 25 19 29 47 17 15)(2 14 46 10 18 22 50 38 6 42 34 30)
(3 21 43 41 27 33 23 5 35 37 51 45)(4 28 40 20 36 44 48 24 12 32 16 8)(13 39)

9 paire ordre 3
(1 9 29)(2 18 6)(3 27 35)(4 36 12)(5 45 41)(7 11 47)(8 20 24)(10 38 30)(14 22 42)
(15 31 19)(16 40 48)(17 49 25)(21 33 37)(23 51 43)(28 44 32)(34 46 50)

11 impaire ordre 12
(1 11 17 31 29 7 25 15 9 47 49 19)(2 22 34 10 6 14 50 30 18 42 46 38)
(3 33 51 41 35 21 23 45 27 37 43 5)(4 44 16 20 12 28 48 8 36 32 40 24)(13 39)

15 impaire ordre 12
(1 15 17 47 29 19 25 11 9 31 49 7)(2 30 34 42 6 38 50 22 18 10 46 14)

(3 45 51 37 35 5 23 33 27 41 43 21)(4 8 16 32 12 24 48 44 36 20 40 28)(13 39)

17 paire ordre 6

(1 17 29 25 9 49)(2 34 6 50 18 46)(3 51 35 23 27 43)(4 16 12 48 36 40)
(5 33 41 21 45 37)(7 15 47 19 11 31)(8 32 24 44 20 28)(10 14 30 42 38 22)

19 impaire ordre 12

(1 19 49 47 9 15 25 7 29 31 17 11)(2 38 46 42 18 30 50 14 6 10 34 22)
(3 5 43 37 27 45 23 21 35 41 51 33)(4 24 40 32 36 8 48 28 12 20 16 44)(13 39)

21 paire ordre 4

(1 21 25 5)(2 42 50 10)(3 11 23 15)(4 32 48 20)(6 22 46 30)(7 43 19 35)(8 12 44 40)
(9 33 17 45)(14 34 38 18)(16 24 36 28)(27 47 51 31)(29 37 49 41)

23 impaire ordre 6

(1 23 9 51 29 43)(2 46 18 50 6 34)(3 17 27 49 35 25)(4 40 36 48 12 16)
(5 11 45 47 41 7)(8 28 20 44 24 32)(10 22 38 42 30 14)(13 39)(15 33 31 37 19 21)

25 paire ordre 2

(1 25)(2 50)(3 23)(4 48)(5 21)(6 46)(7 19)(8 44)(9 17)(10 42)(11 15)(12 40)
(14 38)(16 36)(18 34)(20 32)(22 30)(24 28)(27 51)(29 49)(31 47)(33 45)(35 43)(37 41)

n =54

5 paire ordre 18

(1 5 25 17 31 47 19 41 43 53 49 29 37 23 7 35 13 11)
(2 10 50 34 8 40 38 28 32 52 44 4 20 46 14 16 26 22)(3 15 21 51 39 33)
(6 30 42 48 24 12)(9 45)(18 36)

7 paire ordre 9

(1 7 49 19 25 13 37 43 31)(2 14 44 38 50 26 20 32 8)(3 21 39)
(4 28 34 22 46 52 40 10 16)(5 35 29 41 17 11 23 53 47)(6 42 24)(12 30 48)(15 51 33)

11 paire ordre 18

(1 11 13 35 7 23 37 29 49 53 43 41 19 47 31 17 25 5)
(2 22 26 16 14 46 20 4 44 52 32 28 38 40 8 34 50 10)(3 33 39 51 21 15)
(6 12 24 48 42 30)(9 45)(18 36)

13 paire ordre 9

(1 13 7 37 49 43 19 31 25)(2 26 14 20 44 32 38 8 50)(3 39 21)
(4 52 28 40 34 10 22 16 46)(5 11 35 23 29 53 41 47 17)(6 24 42)(12 48 30)(15 33 51)

17 paire ordre 6

(1 17 19 53 37 35)(2 34 38 52 20 16)(3 51)(4 14 22 50 40 32)
(5 31 41 49 23 13)(6 48)(7 11 25 47 43 29)(8 28 44 46 26 10)(9 45)
(12 42)(15 39)(18 36)(21 33)(24 30)

19 paire ordre 3

(1 19 37)(2 38 20)(4 22 40)(5 41 23)(7 25 43)(8 44 26)(10 28 46)
(11 47 29)(13 31 49)(14 50 32)(16 34 52)(17 53 35)

23 paire ordre 18

(1 23 43 17 13 29 19 57 53 31 11 37 41 25 35 49 47)
(2 46 32 34 26 4 38 10 14 52 8 22 20 28 50 16 44 40)
(3 15 21 51 39 33)(6 30 42 48 24 12)(9 45)(18 36)(7 53)

25 paire ordre 9

(1 25 31 19 43 49 37 7 13)(2 50 8 38 32 44 20 14 26)(3 21 39)

(4 46 16 22 10 34 40 28 52)(5 17 47 41 53 29 23 35 11)(6 42 24)(12 30 48)(15 51 33)

n =56

3 impaire ordre 6
(1 3 9 27 25 19)(2 6 18 54 50 38)(4 12 36 52 44 20)(5 15 45 23 13 39)
(7 21)(8 24 16 48 32 40)(10 30 34 46 26 22)
(11 33 43 17 51 41)(14 42)(29 31 37 55 53 47)(35 49)

5 paire ordre 6
(1 525 13 9 45)(2 10 50 26 18 34)(3 15 19 39 27 23)(4 20 44 52 36 12)
(6 30 38 22 54 46)(7 35)(8 40 32 48 16 24)(11 55 51 31 43 47)(17 29 33 53 41 37)(21 49)

9 paire ordre 3
(1 9 25)(2 18 50)(3 27 19)(4 36 44)(5 45 13)(6 54 38)(8 16 32)(10 34 26)
(11 43 51)(12 52 20)(15 23 39)(17 41 33)(22 30 46)(24 48 40)(29 37 53)(31 55 47)

11 impaire ordre 6
(1 11 9 43 25 51)(2 22 18 30 50 46)(3 33 27 17 19 41)(4 44 36)(5 55 45 47 13 31)
(6 10 54 34 38 26)(7 21)(8 32 16)(12 20 52)(14 42)(15 53 23 29 39 37)(24 40 48)(35 49)

13 paire ordre 2
(1 13)(2 26)(3 39)(4 52)(5 9)(6 22)(7 35)(8 48)(10 18)(11 31)(12 44)(15 27)(16 40)
(17 53)(19 23)(20 36)(21 49)(24 32)(25 45)(29 41)(30 54)(33 37)(34 50)(38 46)
(43 55)(47 51)

15 impaire ordre 2
(1 15)(2 30)(3 45)(5 19)(6 34)(7 49)(9 23)(10 38)(11 53)(13 27)(14 42)(17 31)
(18 46)(21 35)(22 50)(25 39)(26 54)(29 43)(33 47)(37 51)(41 55)

17 paire ordre 6
(1 17 9 41 25 33)(2 34 18 26 50 10)(3 51 2711 19 43)(4 12 36 52 44 20)
(5 29 45 37 13 53)(6 46 54 22 38 30)(8 24 16 48 32 40)(15 31 23 55 39 47)

19 impaire ordre 6
(1 19 25 27 9 3)(2 38 50 54 18 6)(4 20 44 52 36 12)(5 39 13 23 45 15)(7 21)
(8 40 32 48 16 24)(10 22 26 46 34 30)(11 41 51 17 43 33)(14 42)
(29 47 53 55 37 31)(35 49)

23 impaire ordre 6
(1 23 25 15 9 39)(2 46 50 30 18 22)(3 13 19 45 27 5)(4 36 44)
(6 26 38 34 54 10)(7 49)(8 16 32)(11 29 51 53 43 37)(12 52 20)(14 42)
(17 55 33 31 41 47)(21 35)(24 48 40)

25 paire ordre 3
(1 25 9)(2 50 18)(3 19 27)(4 44 36)(5 13 45)(6 38 54)(8 32 16)
(10 26 34)(11 51 43)(12 20 52)(15 39 23)(17 33 41)(22 46 30)(24 40 48)
(29 53 37)(31 47 55)

27 impaire ordre 2
(1 27)(2 54)(3 25)(4 52)(5 23)(6 50)(7 21)(8 48)(9 19)(10 46)(11 17)(12 44)
(13 15)(14 42)(16 40)(18 38)(20 36)(22 34)(24 32)(26 30)(29 55)(31 53)(33 51)
(35 49)(37 47)(39 45)(41 43)

n =60

7 impaire ordre 4

(1 7 49 43)(2 14 38 26)(3 21 27 9)(4 28 16 52)(5 35)(6 42 54 18)(8 56 32 44)
(11 17 59 53)(12 24 48 36)(13 31 37 19)(15 45)(22 34 58 46)(23 41 47 29)(25 55)
(33 51 57 39)

11 impaire ordre 2
(1 11)(2 22)(3 33)(4 44)(5 55)(7 17)(8 28)(9 39)(10 50)(13 23)(14 34)(15 45)(16 56)
(19 29)(20 40)(21 51)(25 35)(26 46)(27 57)(31 41)(32 52)(37 47)(38 58)(43 53)(49 59)

13 paire ordre 4
(1 13 49 37)(2 26 38 14)(3 39 27 51)(4 52 16 28)(6 18 54 42)(7 31 43 19)(8 44 32 56)
(9 57 21 33)(11 23 59 47)(12 36 48 24)(17 41 53 29)(22 46 58 34)

17 paire ordre 4
(1 17 49 53)(2 34 38 46)(3 51 27 39)(4 8 16 32)(5 25)(6 42 54 18)(7 59 4311)
(9 33 21 57)(10 50)(12 24 48 36)(13 41 37 29)(14 58 26 22)(19 23 31 47)(20 40)
(28 56 52 44)(35 55)

19 impaire ordre 2
(1 19)(2 38)(3 57)(4 16)(5 35)(6 54)(7 13)(8 32)(9 51)(11 29)(12 48)(14 26)(15 45)
(17 23)(18 42)(21 39)(22 58)(24 36)(25 55)(27 33)(28 52)(31 49)(34 46)(37 43)(41 59)
(44 56)(47 53)

23 impaire ordre 4
(1 23 49 47)(2 46 38 34)(3 9 27 21)(4 32 16 8)(5 55)(6 18 54 42)(7 41 43 29)(10 50)
(11 13 59 37)(12 36 48 24)(14 22 26 58)(15 45)(17 31 53 19)(20 40)(25 35)(28 44 52 56)
(33 39 57 51)

29 paire ordre 2
(1 29)(2 58)(3 27)(4 56)(5 25)(6 54)(7 23)(8 52)(9 21)(10 50)(11 19)(12 48)(13 17)
(14 46)(16 44)(18 42)(20 40)(22 38)(24 36)(26 34)(28 32)(31 59)(33 57)(35 55)(37 53)
(39 51)(41 49)(43 47)

Les permutations pour les nombres pairs de 64 à 100 sont à trouver ici :

http://denise.vella.chemla.free.fr/permutations-annexe-2.pdf.

Les permutations pour les nombres pairs de 14 à 100 qui sont des doubles de nombres premiers sont à trouver ici :

http://denise.vella.chemla.free.fr/permutations-doubles-de-premiers.pdf.

Références

[1] Khalid Koufany, Cours d'Algèbre, chapitre 4, Groupe de permutations, groupe symétrique, https://khalid-koufany.perso.math.cnrs.fr/Algebre2/ch4-groupes-symetriques.pdf.

[2] Larochette Jérémy, *Cours de MPSI, 2018*, voir là https://mp1.prepa-carnot.fr/wp-content/uploads/2020/11/15$_{G}roupe_{s}ymetrique.pdf$.

[3] Clark Allan, *Elements of Abstract Algebra*, Dover, 1971, sections 30 et 76 à 86. Voir la traduction de la section 82 ici http://denise.vella.chemla.free.fr/trad-Allan-Clark-trois-cycles.pdf.

Groupe d'étude d'Analyse ultramétrique
(Y. Amice, G. Christol, P. Robba)
8e année, 1980/81, no 36, 14 p. 15 juin 1981

Histoire de la loi de réciprocité quadratique : Gauss et Tate

par Roger Cuculière
Lycée Carnot (Paris)

1. La première démonstration de Gauss revue par Dirichlet.

1.1. Histoire de cette démonstration.

C'est à Legendre que l'on peut reconnaître la paternité de la loi de réciprocité quadratique et du symbole grâce auquel elle s'exprime naturellement (voir [1]). Dès 1785, il avait énoncé ce théorème et en avait ébauché une preuve. Mais celle-ci s'appuyait sur la propriété suivante, que Legendre ne croyait pas difficile à démontrer : toute progression arithmétique, dont le premier terme est premier avec la raison, contient une infinité de nombres premiers. C'est ce que l'on nomme aujourd'hui le "théorème de la progression arithmétique".

Or, cette dernière propriété, d'apparence si simple, n'a été démontrée qu'en 1837 par Lejeune-Dirichlet. De sorte qu'en 1795, lorsque Gauss, agé de 18 ans, s'engage dans l'étude de la théorie des nombres, la loi de réciprocité n'est pas complétement démontrée.

Un an après, c'est chose faite on peut lire cette première démonstration de Gauss dans ses "Recherches arithmétiques", dont elle occupe les articles 131 à 145, pages 96 à 103 de l'édition française (voir [2]), après une vingtaine de pages consacrées à des lemmes et à l'étude de divers cas particuliers de la loi de réciprocité. Il s'agit d'une démonstration longue et difficile, qui avance à l'aide d'un grand nombre de cas et de sous-cas : un texte fort rébarbatif.

Pourtant, cette démonstration présente un grand intérêt et occupe une place à part. Gauss dira par la suite que c'est la seule qui soit "homogène". C'est parce que, concernant une propriété des nombres entiers, elle n'utilise que la méthode spécifique aux nombres entiers : la récurrence.

En effet, lorsque Gauss s'est engagé dans l'étude de la théorie des nombres, il l'a fait sans connaître l'état de cette science, dont il a repris l'étude à la base, par ses seules forces. Cette réflexion originale a produit les "Recherches arithmétiques". C'est pourquoi sa démonstration de la loi de réciprocité ne prolonge pas les efforts infructueux de Legendre, mais procède d'un principe différent, simple dans sa conception, difficile dans son exécution. Mais cet avantage ne va pas sans inconvénient: Gauss se prive également du symbole que Legendre a introduit et qui est particulièrement adapté à ce problème. Mis à même, par la suite, de connaître les apports de ses prédécesseurs, il ne daignera pas y faire emprunt, et sa première démonstration restera en l'état. Gauss en publiera plusieurs autres, très différentes dans leurs principes (voir [1]).

Texte reçu le 5 juin 1981.
Roger CUCULIÈRE, 10 cité Falaise, 75018 PARIS.

En 1857, Lejeune-Dirichlet est revenu sur cette question en montrant que la complexité de cette preuve est fortuite, attendu qu'on la simplifie grandement en utilisant le symbole de Legendre, et plus précisément la généralisation donnée par Jacobi en 1837. Rappelons le contenu de cet article de Dirichlet [3].

1.2. Les prémisses.

On suppose connu le symbole de Legendre, ainsi que les propriétés des résidus -1 et 2, exprimées par

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

pour p premier impair.

La première de ces relations équivaut à une propriété de la forme quadratique $x^2 + y^2$, énoncée par Fermat, démontrée par Euler. La seconde provient de même d'une propriété de la forme $x^2 - 2y^2$, énoncée par Fermat, démontrée partiellement par Euler et entièrement par Lagrange ; Gauss en donne aussi, d'ailleurs, une démonstration par récurrence.

On suppose connus également le symbole de Jacobi et ses propriétés :

$$\left(\frac{-1}{P}\right) = (-1)^{(P-1)/2}, \quad \left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8},$$

où P désigne cette fois un nombre entier impair > 1, premier ou non.

Si P et Q sont deux nombres impairs, notons $LRQ(P, Q)$ la relation :

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{(P-1)(Q-1)/4}.$$

La loi de réciprocité quadratique dit que l'on a $LRQ(p, q)$ pour tous les entiers naturels p, q premiers, impairs, distincts : c'est ce que nous voulons démontrer.

Si S est un ensemble de nombres premiers impairs, notons $\mathcal{N}(S)$ l'ensemble des entiers naturels dont tous les diviseurs premiers appartiennent à S.

Voici alors une assertion qui intervient dans la démonstration en question : si l'on a $LRQ(p, q)$ pour toute paire de nombres premiers impairs positifs appartenant à S, alors on a $LRQ(P, Q)$ pour toute paire d'entiers impairs premiers entre eux appartenant à $\mathcal{N}(S)$.

Ceci fait l'objet des sections 133 et 134 des "Recherches Arithmétiques", mais sous une forme peu explicite, faute d'un symbolisme adéquat.

Pour le démontrer, il suffit de constater que si on écrit un entier R forme sous la forme

$$R = \prod_i r_i \quad \text{(facteurs impairs)}$$

Alors :

$$R - 1 = \sum_i (r_i - 1) \pmod 4$$

et par suite $(R-1)/2$ et $\sum_i (r_i - 1)/2$ ont même parité.

1.3. La démonstration.

L'idée de la démonstration est de procéder par récurrence sur les nombres premiers. Considérons la propriété suivante pour un nombre q, premier impair : pour tous les nombres premiers impairs u et v tels que $u < q, v < q, u \neq v$, on a $LRQ(u, v)$.

Elle est vraie pour $q = 7$ parce que l'on a $LRQ(3, 5)$. Nous allons montrer que, si elle est vraie pour un nombre premier impair q, elle est vraie pour le suivant. Et pour cela, nous établirons qu'elle implique $LRQ(p, q)$ pour tout nombre premier impair $p < q$.

Soit donc q vérifiant la propriété ci-dessus, et $p < q$, tous deux premiers impairs. Nous voulons montrer que l'on a $LRQ(p, q)$.

Premier cas : $(p/q) = 1$. Il existe alors un entier rationnel e tel que $e^2 \equiv p \pmod q$. On peut choisir cet entier pair, et vérifiant $0 < e < q$. Il existe un autre entier f tel que $e^2 - p = qf$. On a f impair, et $0 < f < q$.

(a) Si p ne divise pas f, f et p sont premiers entre eux, impairs, et tous leurs diviseurs premiers sont $< q$. D'après l'hypothèse de récurrence et le lemme ci-dessus, on a donc $LRQ(p, f)$ c'est-à-dire

$$\left(\frac{p}{f}\right)\left(\frac{f}{p}\right) = (-1)^{(p-1)(p-1)/4}.$$

Mais on a aussi $(p/f) = 1$ car $p \equiv e^2 \pmod f$. Donc $(f/p) = (-1)^{(p-1)(f-1)/4}$. Or, l'égalité $e^2 - p = qf$ nous indique aussi que $(qf/p) = 1$. D'où il découle

$$\left(\frac{q}{p}\right) = \left(\frac{f}{p}\right)\left(\frac{qf}{p}\right) = (-1)^{(p-1)(f-1)/4}.$$

Il reste à prouver que

$$\frac{(p-1)(f-1)}{4} \equiv \frac{(p-1)(q-1)}{4} \pmod 2,$$

ce qui provient de considérations élémentaires sur les congruences, et il s'avère que l'on a $LRQ(p, q)$ dans ce cas.

(b) Si p divise f, alors il existe f' tel que $f = f'p$, et aussi e' tel que $e = e'p$, d'où $e'^2 p - 1 = qf'$. Par suite, f' est impair, e' est pair, $f' < f$, p et f' sont premiers entre eux. Comme au paragraphe (a),

la relation $LRQ(p, f')$ est vérifiée, et puisque $(p/f') = 1$, on en déduit $(f'/p) = (-1)^{(p-1)(f'-1)/4}$. Or, nous avons cette fois $qf' = -1 \pmod{p}$ d'où $(qf'/p)(-1/p)$, et enfin

$$\left(\frac{q}{p}\right) = \left(\frac{qf'}{p}\right)\left(\frac{f'}{p}\right)(-1)^{(p-1)/2}(-1)^{(p-1)(f'-1)/4} = (-1)^{(p-1)(f'+1)/4}.$$

On termine comme ci-dessus, en montrant que les entiers $((p-1)(f'+1))/4$ et $(p-1)(q-1))/4$ ont même parité.

Deuxième cas : $\left(\frac{p}{q}\right) = -1$ et $q \equiv 3 \pmod{4}$. Pour pouvoir user d'un raisonnement analogue au précédent, il faut disposer de nombres qui **soient** résidus quadratiques. On écrit donc

$$\left(\frac{-1}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)/2}\left(\frac{p}{q}\right) = 1.$$

D'où découle l'existence de e tel que $e^2 \equiv -p \pmod{q}$ et de f tel que $e^2 + p = qf$, et la suite se déroule à peu près comme au premier cas.

Troisième cas : $\left(\frac{p}{q}\right) = -1$ et $q \equiv 1 \pmod{4}$. Ici, l'on doit faire intervenir un lemme :
Pour tout nombre premier $q \equiv 1 \pmod{4}$ *il existe un nombre premier impair* $p' < q$ *tel que* $\left(\frac{q}{p'}\right) = -1$.

Si l'on avait $(p'/q) = 1$, on pourrait appliquer à p' les considérations du "premier cas" ci-dessus, et l'on aurait $LRQ(p', q)$, d'où $(q/p') = -1$, ce qui n'est pas. Par suite, p' et q vérifient $(p'/q) = -1$, et donc $(pp'/q) = 1$. C'est dire qu'il existe deux entiers e et f tels que $e^2 - pp' = qf$, etc.

Voici en résumé le schéma de la démonstration, comprenant la liste des cas à envisager :

$$\left(\frac{p}{q}\right) = 1, \quad e^2 - p = qf \begin{cases} \nearrow p \nmid f \\ \searrow p \mid f \end{cases}$$

$$\left(\frac{p}{q}\right) = -1, q \equiv 3 \pmod 4, \left(\frac{-p}{q}\right) = 1,$$

$$e^2 + p = qf \begin{cases} \nearrow p \nmid f \\ \searrow p \mid f \end{cases}$$

$$\left(\frac{p}{q}\right) = -1, q \equiv 1 \pmod 4, \left(\frac{q}{p'}\right) = -1, \left(\frac{pp'}{q}\right) = 1,$$

$$e^2 - pp' = qf \begin{cases} \nearrow p \nmid f, p' \nmid f \\ \nearrow p \mid f, p' \nmid f \\ \nearrow p \nmid f, p' \mid f \\ \searrow p \mid f, p' \mid f \end{cases}$$

1.4. Le lemme.

Ce lemme invoqué au troisième cas a été démontré par Gauss au cours des articles 125 à 129 des "Recherches arithmétiques" :

"si q est premier, si $q \equiv 1 \pmod 4$, alors il existe p' premier impair, tel que $p' < q$ et $(q/p') = -1$. (En d'autres termes : tout nombre premier q de la forme $4k+1$ est non-résidu de certains nombres premiers plus petits que lui.)"

Gauss distingue encore deux cas : $q = 8k + 5$, ou $q = 8k + 1$.

(a) Si $q = 8k + 5$, on a $q - 2 \equiv 3 \pmod 8$ donc l'un des facteurs premiers de $q - 2$ est de la forme $8k \pm 3$ Si l'on note p' ce facteur, on a $q \equiv 2 \pmod{p'}$ et par suite

$$\left(\frac{q}{p'}\right) = \left(\frac{2}{p'}\right) = (-1)^{(p'^2-1)/8}.$$

Or, si $p = 8k \pm 3$, alors $(p'^2 - 1)/8$ est impair.

C. Q. F. D.

Remarquons que l'on pouvait éviter d'utiliser le caractère quadratique de 2, en notant que $q + 1 = 2(4k + 3)$, et en appelant p' un diviseur premier de $4k + 3$, tel que $p' = 4h + 3$, car il en existe

nécessairement. Il est clair qu'alors $(q/p')(-1/p') = -1$.

(b) Si $q = 8k+1$, soit m la partie entière de $\sqrt{q}$. Raisonnons par l'absurde et supposons que tout p' premier impair tel que $p' \leq 2m+1$ vérifie $(q/p') = 1$.

Les propriétés des résidus, suivant des modules composés (voir par exemple [2], soit section 4, n° 100 à 103), permettent d'affirmer que q esr résidu de $(2m+1)! = M$: il existe k tel que $k^2 \equiv q \pmod{M}$ D'où la congruence :

$$(k^2-1^2)(k^2-2^2)\dots(k^2-m^2) \equiv (q-1^2)(q-2^2)\dots(q-m^2) \pmod{M}.$$

Or, le nombre

$$k(k^2-1^2)(k^2-2^2)\dots(k^2-m^2) = (k-m)(k-m+1)\dots(k-1)k(k+1)\dots(k+m-1)(k+m)$$

est le produit de $2m+1$ entiers consécutifs : il est donc multiple de $(2m+1)! = M$. Mais l'entier M est premier avec q, donc avec k. Il divise donc le premier membre de la congruence ci-dessus, et aussi, dès lors, son second membre $(q-1^2)(q-2^2)\dots(q-m^2)$.

Mais ceci est impossible car la définition de m implique que $(m+1)^2 > q$, et par suite

$$M = (m+1)((m+1)^2-1^2)((m+1)^2-2^2)\dots((m+1)^2-m^2) > (q-1^2)(q-2^2)\dots(q-m^2).$$

Notre hypothèse ci-dessus se révèle fausse : il est ainsi prouvé qu'il existe $p' < 2\sqrt{q}+1$ tel que $(q/p') = -1$. On termine en remarquant que l'inégalité $2\sqrt{q}+1 < q$ est vérifiée dès que $q \geq 11$.

1.5. Remarque.

La démonstration de ce lemme utilise la propriété suivante :

Le produit de n entiers consécutifs, par exemple $A = a(a+1)\dots(a+n-1)$, est toujours divisible par $n!$. Ceci est très clair, parce que le quotient de ces deux nombres est égal à C^n_{a+n-1} : Gauss indique justement (n° 127) que cette proposition est "connue par la théorie des nombres figurés", nous dirons par la Combinatoire. Mais, toujours à l'affût de démonstrations "homogènes", il éprouve le besoin de produire une preuve purement arithmétique, donnant l'expression de $v_p(n!)$, et montrant que $v_p(A) \geq v_p(n!)$ pour tout nombre premier p. C'est ce p que reprend Milnor dans [4], p. 105.

1.6. Conclusion.

Ayant ainsi mis en lumière la simplicité du principe de cette démonstration, nous pouvons, après Dirichlet, affirmer son intérêt méthodologique qui vient s'ajouter à son intérêt historique. C'est ainsi que, pendant plus d'un siècle, on a vu la "Première démonstration de Gauss".

Mais John Tate a montré de plus qu'on pouvait la reconsidérer dans le cadre de la K-théorie : c'est ce que nous allons voir.

2. Symboles et K-théorie.

2.1. Symboles de Steinberg

Soit F un corps commutatif, et $F^* = F - \{0\}$.

Définition. Un symbole de Steinberg est une application c de $K^* \times K^*$ dans un groupe abélien A, bimultiplicative, et qui vérifie

$$c(x, 1-x) = 1 \text{ si } x \neq 0 \text{ et } x \neq 1.$$

Un tel symbole vérifie nécessairement

$$c(1,x) = c(x,1) = 1\ ; \qquad c(x, 1-x^{-1}) = 1\ ; \qquad c(x,-x) = 1;$$

$$c(x,x) = c(-1,x) = c(x,-1), \quad \text{élément de carré 1;}$$

Enfin

$$c(y,x) = (c(x,y))^{-1} \qquad ([4], p.94).$$

2.2. Symbole de Hilbert, ou symbole des restes normiques quadratique.

On considère $F = \mathbb{Q}_p$, p premier fini, ou $F = R = \mathbb{Q}_\infty$ et A= {-1, 1}.

On note $\left(\frac{a,b}{p}\right) = 1$ s'il existe des éléments (x,y,z) de F non tous nuls tels que $ax^2 + by^2 - z^2 = 0$ (ou s'il existe u et v éléments de F tels que $ax^2 + by^2 = 1$), et l'on note $\left(\frac{a,b}{p}\right) = -1$ dans le cas contraire.

Ce symbole vérifie tout d'abord les propriétés :

$$\left(\frac{a,b}{p}\right) = \left(\frac{b,a}{p}\right)\ ;\ \left(\frac{a,1-a}{p}\right) = 1\ ;\ \left(\frac{a,-a}{p}\right) = 1$$

$$\text{et } \left(\frac{a,c^2}{p}\right) = 1 \text{ pour tout } a.$$

Lorsque b n'est pas un carré dans F, on a $\left(\frac{a,b}{p}\right) = 1$ si, et seulement si, a appartient au groupe des normes $N(F(\sqrt{b})^*)$.

La valeur de $\left(\frac{a,b}{p}\right)$ ne dépend que de la classe de a et de b modulo $(F^*)^2$: il suffit de le calculer lorsque a et b décrivent un ensemble de représentants de $F^*/(f^*)^2$. On peut alors distinguer trois cas :

(a) Si p est un nombre premier impair, alors l'extension $\mathbb{Q}_p(\sqrt{b})$ est modérement ramifiée, et le groupe $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ a quatre éléments. Les éléments a et b de $\mathbb{Q}_p^*$ se mettent de manière unique sous

la forme

$$a = p^\alpha a',\ b = p^\beta b' \quad \text{avec} \quad \alpha \in \mathbb{Z},\ \ \beta \in \mathbb{Z},\ \ a' \in \mathbb{Z}_p^*,\ \ b' \in \mathbb{Z}_p^*,$$

et l'on a

$$\alpha = v_p(a),\ \ \beta = v_p(b).$$

On en déduit :

$$\left(\frac{a,b}{p}\right) = (-1)^{\alpha\beta(p-1)/2} \left(\frac{\overline{a}'}{p}\right)^\beta \left(\frac{\overline{b}'}{p}\right)^\alpha,$$

où $\overline{a}'$ et $\overline{b}'$ désignent les images de a' et b' par le morphisme de réduction modulo $p : z \mapsto \overline{z}$, de $\mathbb{Z}_p^*$ dans $(\mathbb{Z}/p\mathbb{Z})^*$ (voir [5], p. 39).

(b) Si p = 2, le groupe $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ est d'ordre 8, avec pour générateurs $\{-1, 2, 5\}$. Tout élément a de $\mathbb{Q}_2^*$ se met de manière unique sous la forme :

$$a = (-1)^i 2^j 5^k a',$$

avec $i = 0$ ou 1, $j = v_2(a) \in \mathbb{Z}$, $k = 0$ ou 1, $a' \in 1 + 8\mathbb{Z}_2 \subset (\mathbb{Q}_2^*)^2$. Soit, de même, $b = (-1)^I 2^J 5^K 5b'$. Alors, on a

$$\left(\frac{a,b}{2}\right) = (-1)^{iI+jK+kJ}.$$

Remarquons que, si l'on pose $a = 2^j u$, alors i et k sont égaux respectivement aux classes modulo 2 de $\dfrac{u-1}{2}$ et $\dfrac{u^2-1}{8}$ ([5], p. 39).

(c) Si $p = \infty$, alors on a :

$$\left(\frac{a,b}{\infty}\right) = 1 \text{ si } a > 0 \text{ ou } b > 0, \ \text{ et } \ \left(\frac{a,b}{\infty}\right) = -1 \text{ si } a < 0 \text{ et } b < 0.$$

La bimultiplication de ce symbole en résulte, et c'est donc un symbole de Steinberg.

2.3. La formule du produit.

Tous les symboles $\left(\dfrac{x,y}{p}\right)$, ainsi que $\left(\dfrac{x,y}{\infty}\right)$, sont définis sur $\mathbb{Q}^*$. Si p et q sont des entiers naturels premiers impairs, on a $\left(\dfrac{p,q}{p}\right) = \left(\dfrac{q}{p}\right)$; $\left(\dfrac{p,q}{r}\right) = 1$ si r est premier impair, $r \neq p$, $r \neq q$; $(p, q/\infty) = 1$; et enfin $\left(\dfrac{p,q}{2}\right) = (-1)^{(p-1)(q-1)/4}$. Da sorte que, si l'on désigne par V l'ensemble des nombres premiers auxquels on adjoint ∞, on a :

$$\prod_{v \in V} \left(\frac{p,q}{v}\right) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}.$$

Ainsi, la relation $LRQ(p,q)$ équivaut à $\prod_{v\in V}\left(\frac{p,q}{v}\right)=1$. En fait, la loi de réciprocité, jointe aux propriétés des résidus -1 et 2 équivaut à la formule du produit, de Hilbert :

$$\prod_{v\in V}\left(\frac{a,b}{v}\right)=1$$

quels que soient a et b rationnels non nuls ([5], p. 44, et [7], p. 313).

2.4. Symbole de Steinberg associé à une valuation.

Soit F un corps valué commutatif, avec valuation discrète v. Soit $\bigwedge$ l'anneau de valuation $\{x/v(x)\geq 0\}$, et $\mathcal{P}$ son idéal premier $\{x/v(x)>0\}$ Le corps résiduel est $\bigwedge/\mathcal{P}$. Si x et y sont des éléments non nuls de F alors l'élément de F : $(-1)^{v(x)v(y)}(x^{v(y)}/y^{v(y)})$ a une valuation nulle. C'est donc un élément de $\bigwedge$ non nul modulo $\mathcal{P}$. On note $d_y(x,y)$ sa classe mod $\mathcal{P}$, et l'on définit ainsi une application d_v de $F^*\times F^*$ dans $(\bigwedge/\mathcal{P})^*$, qui est le groupe multiplicatif du corps résiduel. On montre par le calcul qu'il s'agit d'un symbole de Steinberg ([4], p. 98).

En particulier, si $F=\mathbb{Q}_p$ avec p premier impair et v la valuation p-adique $d_{v_p}(x,y)=(x,y)_p$, symbole de Steinberg avec, pour groupe d'arrivée, $(\mathbb{Z}_p/p\mathbb{Z}_p)^*$ isomorphe au groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$, que nous noterons A_p ([4], p. 99).

Il existe une relation simple entre le symbole $(a,b)_p$ associé à la valuation p-adique et le symbole de Hilbert $\left(\frac{a,b}{p}\right)$.

En comparant les formules des n° 2.2 (a) et 2.4, on voit que

$$\left(\frac{x,y}{p}\right)=((x,y)_p)^{(p-1)/2}.$$

Si $p=2$, la définition ci-dessus conduit à un symbole trivial, l'application $\mathbb{Q}_2^*\to\{1\}$. Dans ce cas, on pose simplement $(a,b)_2=\left(\frac{a,b}{2}\right)$, à valeurs dans le groupe multiplicatif $\{-1,1\}$, que nous noterons A_2.

2.5. Les symboles de Steinberg et le K_2 d'un corps.

Si F est un corps commutatif, on pose par définition

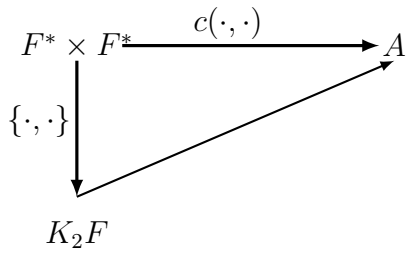
$$K_2F=H_2(SL_\infty(F),\mathbb{Z})\qquad([6],p.202).$$

Le lien entre K-théorie et symboles de Steinberg est assuré par le théorème suivant.

Théorème. (Matsumoto, 1969). *Le groupe abélien K_2F est défini par les générateurs $\{x,y\}$, où $x\in F^*$ et $y\in F^*$ vérifient les relations :*

$$\begin{array}{l}\{x,1-x\}=1\ \text{ si }\ x\neq 0\ \text{ et }\ x\neq 1\ ;\\ \{x_1x_2,y\}=\{x_1,y\}\{x_2,y\};\\ \{x,y_1y_2\}=\{x,y_1\}\{x,y_2\}\qquad([4],p.93).\end{array}$$

Il en résulte que tout symbole de Steinberg c sur F^* se factorise à travers K_2F.



Autrement dit, il existe un unique morphisme $\varphi : K_2F \to A$ tel que, pour tout $x \in F^*$ et tout $y \in F^*$,

$$c(x,y) = \varphi(\{x,y\}).$$

Le groupe K_2F apparaît ainsi comme la solution d'un problème universel.

2.6. Structure de K_2

Le théorème de Tate (1970) affirme que $K_2\mathbb{Q} \approx \bigcup_{p \text{ premier}} A_p$, l'isomorphisme étant donné par la correspondance :

$$\{x,y\} \mapsto \prod_p (x,y)_p,$$

car les $(x,y)_p$ sont presque tous égaux à 1. On peut trouver cet énoncé dans [6], p. 202, et sa démonstration dans [4], p. 100. Comme le fait remarquer son auteur, elle se fonde sur le même argument que la "Première démonstration de Gauss" décrite ci-dessus : toutes deux usent d'une récurrence sur les nombres premiers.

Mais il y a plus. Au-delà de cette simple analogie, Tate a pu déduire de ces considérations une nouvelle démonstration de la loi de réciprocité.

3. Démonstration de Tate de la loi de réciprocité.

3.1. Une formule de produit.

Les théorèmes de Matsumoto et de Tate conduisent au corollaire suivant :

Théorème. *Pour tout symbole de Steinberg $\mathbb{Q}^* \times \mathbb{Q}^* \to A$, il existe une seule famille d'homomorphismes $\varphi : A_p \to A$ telle que*

$$c(x,y) = \prod_p \varphi_p((x,y)_p).$$

En effet, d'après le théorème de Matsumoto, il existe un seul homomorphisme $\varphi : K_2\mathbb{Q} \to A$ tel que $c(x,y) = \varphi(\{x,y\})$; si l'on assimile $K_2\mathbb{Q}$ à $\bigcup_p A_p$ et que l'on note i_p l'injection canonique

$A_p \to K_2\mathbb{Q}$, on obtient

$$\varphi_p = \varphi \circ i_p.$$

Si nous appliquons ce théorème au symbole de Hilbert $\left(\frac{x,y}{\infty}\right)$, à valeurs dans $A_2 = \{-1, 1\}$, nous constatons qu'il existe une famille unique d'endomorphismes $\varphi_p : A_p \to A_2$ tels que

$$\left(\frac{x,y}{\infty}\right) = \prod_p \varphi_p((x,y)_p).$$

Mais, si p est impair, le groupe A_p est cyclique, et il n'y a que deux homomorphismes $A_p \to A_2$: $z \to 1$ et $z \to z^{(p-1)/2}$. Il existe donc ε_p, égal à 0 ou 1, tel que $\varphi_p(z) = z^{\varepsilon_p(p-1)/2}$ pour tout $z \in A_p$. Il en résulte que

$$\varphi_p((x,y)_p) = (((x,y)_p)^{(p-1)/2})^{\varepsilon_p} = \left(\frac{x,y}{p}\right)^{\varepsilon_p}.$$

Si maintenant $p = 2$, il n'y a encore que deux homomorphismes de A_2 dans $A_2 : z \to z^{\varepsilon_2}$ où ε_2 est égal à 0 ou à 1, et l'on a

$$\varphi_2((x,y)_2) = ((x,y)_2)^{\varepsilon_2} = \left(\frac{x,y}{2}\right)^{\varepsilon_2}.$$

D'où la formule du produit :

$$\left(\frac{x,y}{\infty}\right) = \prod_p \left(\frac{x,y}{p}\right)^{\varepsilon_p} \quad \text{où les } \varepsilon_p \text{ valent 0 ou 1.}$$

Comme nous l'avons vu au n° 2.3, démontrer la loi de réciprocité, c'est démontrer que les ε_p sont tous égaux à 1.

3.2. La démonstration.

(a) Détermination de ε_2. On prend $x = y = -1$, et il vient

$$\left(\frac{-1,-1}{\infty}\right) = -1, \quad \left(\frac{-1,-1}{p}\right) = 1$$

pour p premier impair (car toute équation $ax^2 + by^2 = c$ a des racines dans $\mathbb{Z}/p\mathbb{Z}$ si $ab \not\equiv 0$). Par suite, on a $(-1, -1/2)^{\varepsilon_2} = -1$, d'où $\varepsilon_2 = 1$ et $(-1, -1/2) = -1$. Cette dernière affirmation pourrait se vérifier directement par exemple en partant du fait que -1 n'est pas somme de deux carrés dans $\mathbb{Z}/8\mathbb{Z}$.

(b) Détermination de ε_p pour $p = 8k + 5$. Soit $x = 2, y = p$. Pour q premier, $q \neq p, q \neq 2$, on a $(2, p/q) = 1$, d'où

$$\left(\frac{2,p}{\infty}\right) = \left(\frac{2,p}{2}\right)^{\varepsilon_2} \left(\frac{2,p}{p}\right)^{\varepsilon_p}.$$

Or, on a $\dfrac{2,p}{\infty} = 1$. Pour déterminer $\dfrac{2,p}{2}$, on écrit :

$$2 = (-1)^0.2^1.5^0.1 \text{ et } p = (-1)^0.2^0.5^1.\frac{5p}{25}$$

et on applique la formule vue au n° 2.2 (b): il vient $\left(\frac{2,p}{2}\right) = -1$ d'où $(2,p/p)^{\varepsilon_p} = -1$, ce qui implique $(2,p/p) = -1$ et $\varepsilon_p = 1$.

(c) Détermination de ε_p pour $p = 8k-5$. Même déroulement qu'au (b), mais ici on écrit $p = (-1)^1.2^0.5^1.\frac{-p}{5}$ et on en déduit $(2,p/2) = -1$, etc.

(d) Cas où $p = 8k-1$. On prend $x = -1, y = p$, et l'on a $\left(\frac{-1,p}{2}\right) = -1$ etc.

3.3. Cas où $p = 8k+1$.

Dans les cas précédents, nous nous sommes efforcés de trouver des valeurs de a et b telles que $\left(\frac{a,b}{p}\right) = -1$, ce qui correspond à la nécessité, rencontrée dans la "Première démonstration", de prendre p' tel que $\left(\frac{p'}{q}\right) = -1$ (voir n° 1.3).

Mais, de la même manière, ce dernier cas offre des résistances à cette recherche. TATE le dit en ces termes: "I then tried to prove the law of reciprocity using the result on $K_2\mathbb{Q}$, and was surprised to find that there was still a non-trivial lemma needed"[1].

Ce lemme, c'est celui que nous avons exposé plus haut (n° 1.4): il existe $p' < p$ tel que $(p/p') = -1$, ce qui implique $(p,p'/p') = -1$. Dès lors, notre théorème se démontre encore par récurrence sur les nombres premiers: supposons que $\varepsilon_q = 1$ pour tous les nombres premiers $q < p$. Notre dernière "formule de produit" s'écrit alors :

$$\left(\frac{p,p'}{\infty}\right) = \left(\frac{p,p'}{2}\right)\left(\frac{p,p'}{p'}\right)\left(\frac{p,p'}{p}\right)^{\varepsilon_p}.$$

Or, il est clair que $\left(\frac{p,p'}{\infty}\right) = \left(\frac{p,p'}{2}\right) = 1$, et $\left(\frac{p,p'}{p'}\right) = -1$. D'où il découle encore que

$$\left(\frac{p,p'}{p}\right) = -1 \qquad \text{et} \qquad \varepsilon_p = 1.$$

C. Q. F. D.

[1] "Je tentai alors de prouver la loi de réciprocité en utilisant le résultat concernent $K_2\mathbb{Q}$, et je fus surpris de constater qu'un lemme non trivial était encore nécessaire".

Bibliographie

[1] Cuculière R. Histoire d'un théorème d'arithmétique : la loi de réciprocité quadratique, Publication de l'IREM, Paris-Nord, Université Paris-XII, 1930.

[2] Gauss C. F. Disquisitiones arithmeticae, Werke, Band I. Göttingen, 1870. Traduction française de Poullet-Delisle, Paris, 1807. Réédition Librairie Blanchard, 1979. Traduction anglaise de A. Clarke, Yale University Press, 1956.

[3] Lejeune-Dirichlet G. Über den ersten der von Gauss gegebenen Boweise des Reciprocitätsgesetzes in der Theorie der quadratischen Roste. J. für reine und angw. Math., t. 47, 1854, p. 139-150. Werke, Band II, p. 121-138. Berlin, 1897. Reprint Chelsea, 1969. Traduction française de Houel : Sur la première démonstration donnée par Gauss de la loi de réciprocité dans la théorie des résidus quadratiques, J. Math. pures et appl., 2e série, t. 4, 1859, p. 401-420.

[4] Milnor J. Introduction to algebraic K-theory, Princeton, Princeton University Press and University of Tokyo Press, 1971 (Annals of Mathematics Studies, 72).

[5] Serre J.-P. Cours d'arithmétique. Paris, Presses universitaires de France, 1970 (Collection SUP, "Le Mathématicien", 2).

[6] Tate J. Symbols in arithmetic, Actes du Congrès international des Mathématiciens [1970, Nice], Vol 1, p. 201-211. Paris, Gauthier. Villars, 1971.

[7] Tate J. The general reciprocity law, Mathematical developments arising from Hilbert problems, p. 311-322. Providence, American mathematical Society, 1976 (Proceedings of Symposia in pure Mathematics, 28, Part 2).

Résumé de l'article de Lehmer sur le nombre de résidus quadratiques d'un nombre quelconque (Denise Vella-Chemla, mai 2023)

Pour trouver le nombre de résidus quadratiques d'un nombre quelconque, on le factorise, on trouve le nombre des résidus quadratiques de chacune des puissances de premiers intervenant dans sa factorisation, et on multiplie les résultats.

Le nombre de résidus quadratiques de 2 est 2.

Le nombre de résidus quadratiques d'un nombre premier impair p est $\frac{p+1}{2}$.

Le nombre de résidus quadratiques d'une puissance 2^α non nulle de 2 est égal à :

$$\begin{cases} \frac{2^{\alpha-1}+4}{3} & \text{si } \alpha \text{ est pair ;} \\ \frac{2^{\alpha-1}+5}{3} & \text{si } \alpha \text{ est impair.} \end{cases}$$

Le nombre de résidus quadratiques d'une puissance p^α non nulle d'un nombre premier impair p est égal à :

$$\begin{cases} \frac{p^{\alpha+1}-p}{2(p+1)}+1 & \text{si } \alpha \text{ est pair ;} \\ \frac{p^{\alpha+1}-1}{2(p+1)}+1 & \text{si } \alpha \text{ est impair.} \end{cases}$$

Exemple : Pour $98 = 2.7^2$, le nombre de résidus quadratiques est

$$\begin{aligned} \#RQ &= 2 \times \left(\frac{7^3-7}{2(7+1)}+1\right) \\ &= 2 \times \left(\frac{336}{2\times 8}+1\right) \\ &= 2 \times 22 = 44. \end{aligned}$$

Les résidus quadratiques sont : 0, 1, 2, 4, 8, 9, 11, 15, 16, 18, 22, 23, 25, 29, 30, 32, 36, 37, 39, 43, 44, 46, (49), 50, 51, 53, 57, 58, 60, 64, 65, 67, 71, 72, 74, 78, 79, 81, 85, 86, 88, 92, 93, 95.

Observer la récurrence du "motif" de longueur 7 : R R N R N N N (R signifiant Résidu quadratique, et N signifiant non-résidu quadratique, voir les Recherches arithmétiques de Gauss, à l'origine de cette notion).

CERTAINS THÉORÈMES DANS LA THÉORIE DES RÉSIDUS QUADRATIQUES.

D. N. LEHMER
Université de Californie

La définition d'un résidu quadratique est habituellement donnée comme suit : *Si l'on peut trouver un entier X qui satisfasse la congruence,*

$$X^2 \equiv D \pmod{m}$$

où D est premier à m, alors D est dit être un résidu quadratique de m. La restriction que D doive être premier à m simplifie de nombreux résultats. Il y a des théories, pourtant, dans lesquelles cette restriction brouille les résultats et dans cet article, nous ne l'imposerons pas. Commençons, tout d'abord, par déterminer le nombre de résidus d'un entier m donné, en utilisant la définition élargie.

On étudie avant tout le cas où le module m est une puissance d'un nombre premier impair p. Aux premières positions vont surgir $\frac{1}{2}\varphi(p^\alpha)$ résidus distincts de l'élévation au carré des nombres k, qui sont inférieurs à p^α, et premiers à p, $p^\alpha - k$ et k fournissant les mêmes résidus. Considérons ensuite les nombres kp, où k est premier à p. Si deux tels nombres quand on les élève au carré donnent le même résidu, on a :

$$k^2p^2 \equiv k_1^2p^2 \pmod{p^\alpha},$$

d'où,

$$k_1^2 \equiv k_1^2 \pmod{p^{\alpha-2}}$$

ou

$$k \equiv \pm k_1 \pmod{p^{\alpha-2}}.$$

Appelons maintenant k les $\varphi(p^{\alpha-2})$ valeurs inférieures à $p^{\alpha-2}$ et premières à p. Les carrés résultant fournissent $\frac{1}{2}\varphi(p^{\alpha-2})$ résidus distincts. De la même façon, les nombres kp^2 où k est premier à p fournissent $\frac{1}{2}\varphi(p^{\alpha-4})$ des résidus distincts qui sont également différents de ceux obtenus à partir de kp obtenus ci-dessus. En procédant de la sorte, on obtient pour le nombre total de résidus distincts :

$$\frac{1}{2}[\varphi(p^\alpha) + \varphi(p^{\alpha-2}) + \varphi(p^{\alpha-4}) + \varphi(p^{\alpha-6}) + \ldots] + 1$$

Traduction Denise Vella-Chemla, juin 2022.
Référence : https://www.jstor.org/stable/2972413.

l'unité étant ajouté pour le résidu zéro.

Pour α pair, la formule résultante est :

$$\frac{p^{\alpha+1}-p}{2(p+1)}+1 \qquad (p \text{ un nombre premier impair}).$$

Pour α impair :

$$\frac{p^{\alpha+1}-1}{2(p+1)}+1.$$

Pour m une puissance de 2, le résultat est un peu différent. Il y a $2^{\alpha-3}$ résidus distincts résultant des carrés des nombres impairs. Cela est dû à la congruence, $(2^{\alpha-2}-k)^2 \equiv (2^{\alpha-2}+k)^2 \pmod{2^\alpha}$. Il y a $2^{\alpha-5}$ résidus provenant des carrés des nombres $2k$ où k est impair. Cela vient de la congruence, $(2^{\alpha-3}-2k)^2 \equiv (2^{\alpha-3}+2k)^2 \pmod{2^\alpha}$. Similairement, il y a $2^{\alpha-7}$ résidus distincts provenant des carrés des nombres 2^2k où k est impair, et en général, il y a $2^{\alpha-(2\kappa+3)}$ résidus provenant des carrés des multiples impairs de 2^κ. Ainsi dans le cas où α est impair, on a la série $2^{\alpha-3}+2^{\alpha-5}+2^{\alpha-7}+\ldots$, qui se termine par 1, le dernier terme résultant des multiples impairs de 2 où $\lambda=(\alpha-3)/2$. Il reste en outre deux résidus ; l'un résultant de 2^λ où $\lambda=(\alpha-1)/2$, et l'autre de 2^λ où $\lambda=(\alpha+1)/2$. On voit que ce dernier est nul, modulus 2, en raison de la congruence,

$$(2^{\alpha+1/2}\cdot k)^2 \equiv 2^{\alpha+1}\cdot k^2 \equiv 0 \pmod{2^\alpha}.$$

Pour α impair donc, la formule est $(2^{\alpha-1}+5)/3$. Pour α pair le résultat est $(2^{-3}+2^{\alpha-5}+2^{\alpha-7}+2)+2$[1]; c'est-à-dire que $(2^{\alpha-1}+4)/3$.

Comme illustrations des résultats, le nombre de résidus du nombre $81=3^4$, est $(3^5-3)/2\cdot 4+1$ ou 31. Les résidus sont les nombres : 0, 1, 4, 7, 9, 10, 13, 16, 19, 22, 25, 28, 31, 34, 36, 37, 40, 43, 36, 39, 52, 55, 58, 61, 63, 64, 67, 70, 73, 76, 79.

Pour le nombre $27=3^3$ le nombre est $(3^4-1)/2\cdot 4+1$ ou 11. Les résidus sont les nombres : 0, 1, 4, 7, 9, 10, 13, 16, 21, 25.

Pour le nombre $32=2^5$ la formule donne $(2^4+5)/3=7$. Les résidus sont : 0, 1, 4, 9, 16, 17, 25.

Pour le nombre $64=2^6$ on a $(2+4)/3=12$. Les résidus sont : 0, 1, 4, 9, 16, 17, 25, 33, 36, 41, 49, 57.

1. manque un α dans le premier exposant de 2 ?

Pour un module m qui est le produit d'un nombre quelconque de puissances de premiers, le nombre de résidus est obtenu en prenant le produit des nombres de résidus pour les puissances de premiers séparément. Ainsi si $mp_1^{\alpha_1}p_2^{\alpha_2}$, la solution de $X^2 \equiv D \pmod{m}$ est possible si et seulement si les différentes congruences $X^2 \equiv D \pmod{p_1^{\alpha_1}}$ et $X^2 \equiv D \pmod{p_2^{\alpha_2}}$ sont possibles ; et toute solution de la première peut être combinée avec n'importe quelle solution de la seconde pour fournir une solution de la congruence originale. Ainsi si $D \equiv \alpha \pmod{p_1^{\alpha_1}}$ est telle que la congruence $X^2 \equiv D \pmod{p_1^1}$ est résoluble et $D \equiv \beta \pmod{p_2^2}$ telle que la congruence $X^2 \equiv D \pmod{p_2^{\alpha_2}}$ est résoluble, alors comme les modules sont relativement premiers les uns aux autres, une et une seule solution des deux congruences est possible $D \equiv \alpha \pmod{p_1^{\alpha_1}}$ et $D \equiv \beta \pmod{p_2^{\alpha_2}}$ pris simultanément et le D résultat rend $X^2 \equiv D \pmod{p_1^1 p_2^{\alpha_2}}$ résoluble. Ainsi le nombre des résidus du nombre 42 est égal au produit des nombres de résidus de 2, 3 et 7. C'est-à-dire, $2 \cdot 2 \cdot 4$ ou 16. Les résidus sont en fait : 0, 1, 4, 7, 9, 15, 16, 18, 21, 22, 25, 28, 30, 36, 37, 39.

Résidus consécutifs. Certains théorèmes intéressants[2] concernant le nombre de résidus consécutifs pour un nombre premier donné ont été obtenus pour la définition courante du résidu quadratique par M. Aladov[3] et également par M. von Sterneck[4]. Les résultats de M. Aladov - je n'ai pas lu l'article - sont les suivants :

Soient x = le nombre de non-résidus suivis par un non-résidu,
x' = le nombre de non-résidus suivis par un résidu,
y = le nombre de résidus suivis par un non-résidu,
y' = le nombre de résidus suivis par un résidu.

Alors pour p un nombre premier de la forme $4n+1$ on a :

$$x = x' = y = \frac{p-1}{4}\ ; \qquad \text{and} \qquad y' = \frac{p-5}{4}$$

et pour p un nombre premier de la forme $4n+3$ on a :

$$x = x' = y' = \frac{p-3}{4}, \qquad \text{and} \qquad y = \frac{p+1}{4}.$$

M. von Sterneck a étendu ces résultats pour montrer que pour tout nombre premier exceptés 2, 3, 5, 7, 11, and 17, il y a au moins un groupe de quatre résidus consécutifs, ou de quatre non-résidus consécutifs.

2. Ces théorèmes ont été démontrés par Jordan dans son *Traité des Substitutions*, 1870, page 158. Le Professeur Dickson a gentiment attiré mon attention sur la preuve de Jordan, qui est basée sur des principes différents de ceux donnés ici.
3. *Recueil Mathématique*, Société de Moscou, t. XVIII, 1895.
4. *Ibid.*, t. XX, 1898.

Les résultats de M. Aladov ne sont pas difficiles à obtenir en considérant la congruence, $xy \equiv 1 \pmod{p}$. Cette congruence regroupe les $p-1$ nombres, $1, 2, 3, 4, \ldots p-1$, en paires. Pour deux valeurs de x, notamment, ± 1, la valeur de y est égale à x. Pour d'autres valeurs de x la valeur de y est différente. Il y a donc en tout $(p+1)/2$ paires. Appelons x', y', une telle paire. Alors il y a une autre paire $(p-x')(p-y')$, et pour notre but, ces deux paires ne sont pas vraiment distinctes, puisqu'elles fournissent des paires identiques de résidus consécutifs comme suit : si l'on met $a+b \equiv x'$ et $a-b \equiv y'$ on obtient $a^2 - b^2 \equiv 1 \pmod{p}$, ou a et b sont des résidus consécutifs. La paire $(p-x')(p-y')$ donne la même paire de résidus. Le nombre de paires de résidus consécutifs semblerait par conséquent être $(p+1)/4$, et c'est effectivement la bonne formule pour p, un nombre premier de la forme $4n+3$. Pour p un nombre premier de la forme $4n+1$ le nombre de paires sera impair et il y aura une paire dans laquelle $x' = p - y'$, ou bien dans laquelle la paire (x', y') est identique à la paire $(p-y', x')$. Le nombre de paires distinctes de résidus consécutifs pour un tel nombre premier est par conséquent $(p+3)/4$. Dans ces formulæ on a inclus le résidu zéro. Ainsi pour le nombre premier 11, nous avons les paires suivantes de valeurs x, y et les valeurs correspondantes de a et b :

x,	y.	$p-x$,	$p-y$.	Résidus.	
1,	1.	10,	10.	1,	0.
2,	6.	9,	5.	5,	4.
3,	4.	8,	7.	4,	3.

Il y a ainsi trois paires consécutives de résidus pour le nombre premlier 11. Pour le nombre premier 17, on a les paires suivantes :

x,	y.	$p-x$,	$p-y$.	Résidus.	
1,	1.	16,	16.	1,	0.
2,	9.	15,	8.	9,	8.
3,	6.	14,	11.	16,	15.
4,	13.	13,	4.	17,	16.
5,	7.	12,	10.	2,	1.

La formule d'Aladov donnera seulement trois paires parce qu'il n'admet pas le résidu 0. Cela élimine la première et la quatrième paires.

Le reste des résultats de M. Aladov suivent sans trop de difficulté. Ainsi pour un nombre premiler de la forme $4n+1$, si on dénote un résidu par R, et un non-résidu par N, notre formule pour le nombre de séquences RR est $(p+3)/4$. Pour la séquence NN on peut commencer à partir de la congruence $xy \equiv N \pmod{p}$ et par une ligne de raisonnement exactement similaire, on peut dériver la formule $(p-1)/4$ pour le nombre de paires de résidus différant par un non-résidu donné N. Soient R' et R'' deux tels résidus, tels que $R' - R'' \equiv N \pmod{p}$. Multiplions maintenant cette congruence par le non-résidu N' qui est tel que $NN' \equiv 1 \pmod{p}$ et nous obtenons une paire de

non-résidus différant de l'unité. Pour les séquences NR et RN on peut voir qu'elles doivent être égales en nombre, car puisque -1 est résidu de nombres premiers de la forme $4n+1$ la séquence RN implique la séquence $-R, -N$, qui quand on l'écrit $p-N, p-R$ est vue comme étant une séquence NR. Maintenant le nombre total de séquences dans la suite de nombres $0, 1, 2, 3, 4, \ldots, p-1, p$ est égal à p. Parmi ceux-ci, il y a $(p+3)/4$ séquences RR, et $(p-1)/4$, séquences NN. Les $(p-1)/2$ séquences restantes se divisent en séquences NR et séquences RN, et sont donc au nombre de $(p-1)/4$. Avec la notation utilisée pour établir les résultats de M. Aladov, on a, en incluant le résidu zéro,

$$x = x' = y = \frac{p-1}{4}\ ; \qquad \text{et} \qquad y' = \frac{p+3}{4}$$

Le cas où p est de la forme $4n+3$ peut être étudié de la même manière,

$$x' = y' = y = \frac{p+1}{4}, \qquad \text{et} \qquad x = \frac{p-3}{4}.$$

Je ne sais pas si M. Aladov a étendu ces résultats pour les appliquer aux modules composés ou pas. Nous allons faire cela, et d'abord, prenons le cas où le module est une puissance d'un nombre premier impair p. On montrera comment on peut dériver, à partir d'une paire de résidus consécutifs pour le module p^α, p paires de résidus consécutifs pour le module $p^{\alpha+1}$, à moins que l'une des paires de résidus consécutifs pour p^α ne soit congrue à zéro mod p^α.

Soit $x_1^2 - y_1^2 \equiv 1 \pmod{p^\alpha}$ une paire de résidus consécutifs. Alors $(x_1 + kp^\alpha)^2 - (y_1 + lp^\alpha)^2 \equiv 1 \pmod{p^\alpha}$ fournira la même paire pour toutes les valeurs de k et 1. Multiplions et posons $x_1^2 - y_1^2 - 1 = mp^\alpha$, alors

$$mp^\alpha + 2(kx_1 - ly_1)p^\alpha + (k^2 - l^2)p^{2\alpha} \equiv 0 \pmod{p^\alpha}.$$

Le dernier terme sur la gauche est congru à zéro mod $p^{\alpha+1}$ si α est plus grand que l'unité. Les autres termes seront aussi divisibles par $p^{\alpha+1}$ si

$$m + 2(kx_1 - ly_1) \equiv 0 \pmod{p}.$$

Dans cette congruence m, x_1, et y_1 sont connus et k et l sont inconnus. On peut montrer qu'une congruence de la forme $ax + by + c \equiv 0 \pmod{p}$ a exactement p racines, à moins que a et b ne soient divisibles par p, et que c ne le soit pas. Nous différons la preuve de ce théorème et notons que si $y_1 \equiv 0 \pmod{p^\alpha}$ alors la congruence $m + 2kx_1 \equiv 0 \pmod{p}$ fournit seulement une paire effective, car quelle que soit la valeur de 1, l'expression $(y_1 + lp^\alpha)^2$ sera divisible par $p^{\alpha+1}$ pour α plus grand que un. Donc une paire de résidus consécutifs pour le module p^α fournit en général p résidus consécutifs pour le module $p^{\alpha+1}$ excepté la paire consécutive $(1, 0)$ qui amène la paire unique $(1, 0)$. Aussi, si p est de la forme $4n+1$ alors une paire $(0, -1)$ peut

être obtenue qui amène également la paire unique $(0, -1)$ pour le module $p^{\alpha+1}$. Le théorème est ainsi démontré.

Le théorème concernant le nombre de solutions de la congruence $ax + by + c \equiv 0 \pmod{p}$ est un cas particulier du théorème plus général :

La congruence $ax + by + c \equiv 0 \pmod{m}$ a $m\delta$ solutions, ou aucune selon que δ, le plus grand diviseur commun de a, b et m, divise ou ne divise pas c.

La congruence n'a clairement pas de solutions quand δ ne divise pas c. Prenons d'abord le cas où δ est l'unité, et appelons δ' le plus grand commun diviseur de a et m. Alors selon la théorie bien connu des congruences, $ax + b \equiv 0 \pmod{m}$, on voit qu'il y aura δ' valeurs de x pour toute valeur de y satisfaisant la congruence $by + c \equiv 0 \pmod{\delta'}$. Maintenant, b est premier à δ' et donc cette dernière congruence a une et une seule racine β, disons. Les m/δ' nombres inférieurs ou égaux à m et congruents à $\beta \pmod{\delta'}$ serviront de valeurs de y, chacune fournissant les valeurs correspondantes de δ' correspondant aux valeurs de x. D'autres valeurs de y ne donneront aucune valeur du tout de x. Le nombre total de solutions dans ce cas $m/\delta' \cdot \delta'$, ou m. Si maintenant δ n'est pas l'unité, on peut diviser les deux côtés de la congruence par δ et obtenir la congruence $(a/\delta)x + (b/\delta)y + (c/\delta) \equiv 0 \pmod{(m/\delta)}$, qui a par la discussion ci-dessus m/δ solutions. Soit (α, β) l'une de ces solutions. Alors à la place de α on peut prendre n'importe lequel des nombres δ congruents à $\alpha \bmod(m/\delta)$ qui sont inférieurs ou égaux à m. De même pour β. Le nombre total de solutions est donc $(m/\delta) \cdot \delta \cdot \delta$, ou $m\delta$, ce qui prouve le théorème. Une ligne de raisonnement similaire montrera que le nombre de solutions de la congruence $ax + by + cz + d \equiv 0 \pmod{m}$, est $m^2\delta$, ou zéro, selon que δ, le plus grand diviseur commun de a, b, c, et m ne divise pas d. En général aussi, par une induction simple, on peut établir que le nombres de solutions de la congruence $a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + \ldots + a_nx_n + a_{n+1} \equiv 0 \pmod{m}$ is $m^{n-1}\delta$, ou zéro, selon que δ, le plus grand diviseur de $a_1, a_2, a_3, \ldots a_n$ et m divise ou ne divise pas a_{n+1}. Ces théorèmes sont, bien sûr, des cas particuliers du problème général des congruences linéaires simultanées discutées par H. J. S. Smith (*Works*, Vol. II, p. 367).

On peut maintenant écrire les formulæ pour le nombre de résidus consécutifs pour un module qui est la puissance de n'importe quel nombre premier impair p. On a vu que le nombre de résidus consécutifs pour un nombre premier de la forme $4n + 1$ est $(p + 3)/4$, et en éliminant les deux séquences $(0, 1)$ et $(-1, 0)$ il reste $\{(p + 3)/4\} - 2$ séquences ordinaires. Pour le module p^2, on doit multiplier cela par p et les deux séquences finales $(0, 1)$ et $(-1, 0)$ sont ajoutées, ce qui donne pour le module p^2 le nombre total de résidus consécutifs comme étant $\{(p - 5)/4\}p^{\alpha-1} + 2$. En général, pour la puissance p^α le nombre de résidus consécutifs sera $\{(p - 5)/4\}p^{\alpha-1} + 2$. La formule est fausse pour le nombre premier 5, puisque dans le cas de cet nombre pre-

mier $(p+3)/4$ est égal à 2, et rejeter les deux résidus consécutifs finaux donnera zéro. La formule donnerait toujours comme nombre 2. Ceci est correct pour α égale à 1, ou 2, mais pour α plus grand que 2 la formule correcte est $4 \cdot 5^{\alpha-3} + 2$.

L'argument est facile à établir également pour p de la forme $4n-1$ et la formule est $\{(p-3)/4\}p^{\alpha-1} + 1$, pour le nombre de résidus consécutifs pour le module p^α. Le nombre premier 3 est une exception. Pour α égal à 1 ou 2 le nombre est 1. Pour α plus grand que 2 le nombre est $3^{\alpha-3} + 1$.

Pour un module qui est une puissance de 2 la formule se réduit au plus grand entier dans $(2^{\alpha-5}+5)/3$, pour 2^α, où α est plus grand que 4. Pour α inférieur à 4 le nombre de séquences vaut 1.

Pour un module composé général, il est maintenant possible de calculer le nombre de résidus consécutifs. En fait, le nombre de tels résidus pour le produit de deux nombres premier l'un à l'autre est égal au produit des nombres pour chacun de ces facteurs. Supposons que les deux facteurs soient p et q, et que nous ayons trouvé pour chacun une paire de résidus consécutifs, de telle façon que

$$P_1 - P_2 \equiv 1 \pmod{p}$$

et

$$Q_1 - Q_2 \equiv 1 \pmod{q}$$

et que ceux-ci proviennent des carrés,

$$x_1^2 - y_1^2 \equiv 1 \pmod{p}$$

et

$$x_2^2 - y_2^2 \equiv 1 \pmod{q};$$

déterminons maintenant k et l pour satisfaire les congruences :

$$x_1 + kp \equiv x_2 \pmod{q}, y_1 + lp \equiv y_2 \pmod{q};$$

p étant premier à q celles-ci auront une et uniquement une solution chacune. Ainsi le nombre de résidus consécutifs pour le module pq est au moins aussi grand que le produit du nombre deux ceux existant pour le module p par le nombre de ceux existant pour le module q. Mais puisque un résidu de pq doit nécessairement être un résidu de p et de q séparément, toute paire de résidus consécutifs pour pq sera également une paire de résidus consécutifs pour p et pour q.

Comme illustration de la méthode pour trouver les résidus consécutifs pour un module composé, prenons le module $253 = 11.23$. Pour le module 11 on a les résidus consécutifs 3, 4 provenant de 5^2 et 2^2. Pour le module 23, on a les résidus 1, 2 provenant de 1^2 et 5^2. Les congruences $2 + 11k \equiv 5 \pmod{23}$ et $5 + 11l \equiv 1 \pmod{23}$ donnent $k \equiv 17$, et $l \equiv 8 \pmod{23}$. Alors $2+187$, ou 189, et $5+88$ ou 93 doivent fournir une paire de résidus consécutifs pour 253. On trouve que $189^2 \equiv 48$ et $93^2 \equiv 47$. Puisque de plus, il y a 3 résidus consécutifs pour le module 11, et 6 pour le module 23 il y en aura 18 pour le module 253.

En conclusion, on doit dire un mot à propos de la détermination de la possibilité de la congruence $x^2 \equiv D \pmod{m}$ où D n'est pas contraint à être premier à m. En premier lieu, il est nécessaire de ne considérer que le cas où le module est une puissance d'un nombre premier. Car on peut trouver x tel que $x^2 - D$ est divisible par pq, où p et q sont premiers l'un à l'autre, alors $x^2 - D$ sera divisible par p et q, et inversement. Considérons alors le module p^α ; et soit $D = Ap^\lambda$ où A est premier à p.

Si λ est plus grand que α la congruence aura la racine $x \equiv 0$.

I. Supposons que λ est inférieur à α, et supposons d'abord que A est un résidu de p et écrivons $A \equiv y^2 \pmod{p^\alpha}$. Alors si λ est pair, la congruence est possible et a la racine $x \equiv \pm y p^{\lambda/2}$

II. Si A est un résidu de p et λ est impair, la congruence n'a pas de racine. Car en écrivant $x^2 \equiv Ap^\lambda + Mp^\alpha$ alors x contient p^λ comme un facteur. Il doit donc contenir un autre facteur p. Mais le côté droit ne peut pas contenir de tel facteur.

III. Si A est un non-résidu de p et λ est pair, la congruence est impossible. Pour diviser par p^λ nous aurions la congruence impossible

$$x'^2 \equiv A \pmod{p^{\alpha-2}}.$$

IV. Si A est un non-résidu, et λ est impair alors Ap^λ est un non-résidu. La preuve est comme dans le cas II. En général, alors Ap^λ est un résidu de p^α quand λ est supérieur ou égal à α et quand λ est inférieur à α et pair, et A est un résidu de p.

Compter les carrés dans $\mathbb{Z}_n$

Walter D. Stangl
Université Biola La Mirada, CA 90639

Un problème élémentaire de théorie des nombres consiste à déterminer les formes possibles des carrés parmi les entiers positifs. Par exemple, il est facile de voir que tout carré doit être de la forme $3k$ ou $3k+1$. (Puisque tout entier peut s'écrire sous l'une des formes $3q$, $3q+1$, ou $3q+2$, élever simplement au carré ces nombres et simplifier). Reformulée, cette assertion est que 0 et 1 sont les carrés dans $\mathbb{Z}_3$, l'anneau des classes d'équivalence des entiers modulo 3. En général, un carré a la forme $nk+r$ si, et seulement si, r est un carré dans l'anneau $\mathbb{Z}_n$. Combien de carrés y a-t-il dans $\mathbb{Z}_n$?

Notions fondamentales. Un élément a dans $\mathbb{Z}_n$ est un *carré* dans $\mathbb{Z}_n$ si et seulement si $x^2 = a$ a une solution dans $\mathbb{Z}_n$. Les unités de $\mathbb{Z}_n$ sont les éléments qui sont premiers à n. Les unités qui sont des carrés sont habituellement appelées *résidus quadratiques* (ou, plus précisément, les résidus quadratiques mod n dans le système des résidus réduit) [1, p. 84]. Les résidus quadratiques ont été complètement caractérisés [2, p. 201], et les résultats standards seront utilisés dans ce qui suit.

On adoptera la notation suivante : $q(n)$ = le nombre de résidus quadratiques dans $\mathbb{Z}_n$, et $s(n)$ = le nombre des carrés dans $\mathbb{Z}_n$. Par exemple, $q(8) = 1$ puisque $x^2 = 1$ a une solution dans $\mathbb{Z}_8$, (en fait, les quatre unités, notamment 1, 3, 5, et 7, sont toutes solutions), et $x^2 = 3, x^2 = 5$, et $x^2 = 7$ n'ont pas de solutions dans $\mathbb{Z}_8$. Aussi, $s(8) = 3$ puisque $x^2 = 0$ et $x^2 = 4$ ont aussi des solutions dans $\mathbb{Z}_8$, mais $x^2 = 2$ et $x^2 = 6$ n'en ont pas.

Un fonction de théorie des nombres $f(n)$ est *multiplicative* si $\gcd(m, n) = 1$ implique $f(mn) = f(m) \cdot f(n)$. Les fonctions typiques de théorie des nombres qui sont multiplicatives incluent le nombre de diviseurs positifs de n et la somme de ces diviseurs [1, p. 109]. Une fonction de théorie des nombres qui est multiplicative est complètement caractérisée par ses valeurs sur les puissances des nombres premiers. Et $q(n)$ et $s(n)$ sont multiplicatives ; on dérive des formules récursives et en forme fermée pour ces fonctions sur les puissances de nombres premiers. Cela nous permettra de calculer $s(n)$ et $q(n)$ pour tout n, en utilisant la factorisation en nombres premiers de n.

Supposons que $\gcd(m, n) = 1$. Alors $\mathbb{Z}_{mn}$ est isomorphe à $\mathbb{Z}_m \times \mathbb{Z}_n$, selon l'isomorphisme d'anneaux $\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ défini par $h(z) = (z \bmod m, z \bmod n)$ [3, p. 80]. Supposons que a est un carré dans $\mathbb{Z}_{mn}$. Alors il existe un certain b dans $\mathbb{Z}_{mn}$ tel que $b^2 = a$. Puisque h est une fonction de $\mathbb{Z}_{mn}$ dans $\mathbb{Z}_m \times \mathbb{Z}_n$, il existe $(x, y) \in \mathbb{Z}_m \times \mathbb{Z}_n$, tel que $h(b) = (x, y)$. Alors $h(a) = h(b^2) = [h(b)]^2 = (x, y)^2 = (x^2, y^2)$, et donc $h(a)$ est un carré dans $\mathbb{Z}_m \times \mathbb{Z}_n$. Par conséquent $s(mn) \leq s(m) \cdot s(n)$.

D'un autre côté, si u dans $\mathbb{Z}_m$ et v dans $\mathbb{Z}_n$ sont des carrés, alors il existe x dans $\mathbb{Z}_m$ et y dans $\mathbb{Z}_n$, tels que $(x^2, y^2) = (u, v)$ dans $\mathbb{Z}_m \times \mathbb{Z}_n$. Ainsi, $h^{-1}(u, v) = h^{-1}[(x, y)^2] = [h^{-1}(x, y)]^2$, donc $h^{-1}(u, v)$ est un carré dans $\mathbb{Z}_{mn}$. Par conséquent, $s(mn) \geq s(m) \cdot s(n)$.

La combinaison de ces résultats amène l'égalité souhaitée, montrant que $s(n)$ est une fonction multiplicative. Étendre la preuve à $q(n)$ nécessite simplement d'observer que pour tout entier b, $\gcd(b, mn) = 1$ si, et seulement si, $\gcd(b, m) = 1$ et $\gcd(b, n) = 1$.

Formule de récurrence. Notre prochain but est de démontrer une formule générale de récurrence pour le nombre de carrés dans $\mathbb{Z}_{p^n}$ où p est un nombre premier supérieur à 2. Une fois que ceci sera fait, les formules en forme fermée pour les différentes composantes complèteront notre procédure de comptage. On commence par l'observation que les carrés dans $\mathbb{Z}_{p^n}$ qui ne sont pas des résidus quadratiques sont engendrés par les carrés dans $\mathbb{Z}_{p^{n-2}}$, i.e., b est un carré dans $\mathbb{Z}_{p^{n-2}}$ si et seulement si bp^2 est un carré dans $\mathbb{Z}_{p^n}$.

D'abord, supposons qu'il existe c dans $\mathbb{Z}_{p^{n-2}}$ tel que $c^2 = kp^{n-2} + b$ dans $\mathbb{Z}$. Alors $c^2p^2 = kp^n + bp^2$. Maintenant $cp < p^n$, donc $(cp)^2 = bp^2$ est un carré dans $\mathbb{Z}_{p^n}$. Inversement, supposons qu'il existe y dans $\mathbb{Z}_{p^n}$ tel que $y^2 = mp^n + sp^2$ dans $\mathbb{Z}$. Alors p^2 divise y^2, donc p divise y. Ainsi, il existe c tel que $y = cp$. Alors $c^2 = mp^{n-2} + s$ et s est un carré dans $Z_{p^{n-2}}$.

Maintenant on souhaite compter tous les carrés dans $\mathbb{Z}_{p^n}$. On commence par observer que les carrés sont de deux sortes. Puisque $q(p^n)$ compte les carrés dans $\mathbb{Z}_{p^n}$ qui sont des unités, on doit simplement compter les carrés qui ne sont pas des unités, i.e., les multiples de p. Supposons que kp est un carré dans $\mathbb{Z}_{p^n}$. Alors il existe un b tel que $b^2 = cp^n + kp$. Alors p divise b^2, et donc b. Par conséquent, p^2 divise b^2, et donc kp, donc p divise k. Donc les multiples de p qui sont des carrés sont des multiples de p^2. Mais par le résultat précédent, le nombre de ceux-ci est donné par $s(p^{n-2})$.

Ainsi on a démontré la formule de récurrence suivante.

THÉORÈME. Pour $n \geq 3, s(p^n) = q(p^n) + s(p^{n-2})$.

Puissances de nombres premiers impairs. Pour obtenir des formules explicites pour les fonctions $q(p^n)$ et $s(p^n)$, il est utile de traiter le cas $p = 2$ séparément. L'argument pour les puissances d'un nombre premier impair p dépend de l'existence d'une racine primitive pour p^n pour tout n. En langage algébrique, cela dit que les unités de $\mathbb{Z}_{p^*}$ forment un groupe cyclique selon la multiplication et par conséquent ont un générateur [1, p. 62]. Puisque cela n'est pas vrai pour les puissances de 2 supérieures ou égales à 3, notre approche et nos résultats devront être un peu modifiés pour cette situation.

Si p est un nombre premier impair, la fonction indicatrice d'Euler fournit le nombre d'unités de $\mathbb{Z}_{p^n}$, qui est $p^n - p^{n-1}$. Il y a une racine primitive de p^n. Les puissances paires de cette racine primitive sont clairement des résidus quadratiques distincts, et la formule suivante est démontrée.

THÉORÈME. *Si p est un nombre premier impair, alors $q(p^n) = (p^n - p^{n-1})/2$, pour tout $n \geq 1$.*

Dans le but de compter tous les carrés dans $\mathbb{Z}_{p^n}$, il est utile de regarder les deux premiers cas séparément. Puisque 0 est le seul élément non unité dans $\mathbb{Z}_p$, clairement $s(p) = q(p) + 1 = (p + 1)/2$. Dans $\mathbb{Z}_{p^2}$, les non-unités sont des multiples de p, et ont des carrés égaux à 0. Ainsi $s(p^2) = q(p^2) + 1 = (p^2 - p + 2)/2$.

Maintenant, supposons $n \geq 3$ et n pair. Par des applications répétées de la formule de récurrence,

on obtient

$$\begin{aligned} s(p^n) &= \frac{p^n - p^{n-1}}{2} + \frac{p^{n-2} - p^{n-1}}{2} + \ldots + \frac{p^4 - p^3}{2} + \frac{p^2 - p + 2}{2} \\ &= \frac{p^{n+1} - p^n + p^n - p^{n-1} + p^{n-1} - \ldots + p^3 - p^2 + 2p + p^2 - p + 2}{2(p+1)} \\ &= \frac{p^{n+1} + p + 2}{2(p+1)} \end{aligned}$$

Si n est impair, on obtient

$$\begin{aligned} s(p^n) &= \frac{p^n - p^{n-1}}{2} + \frac{p^{n-2} - p^{n-1}}{2} + \ldots + \frac{p^4 - p^3}{2} + \frac{p^2 - p + 2}{2} \\ &= \frac{p^{n+1} - p^n + p^n - p^{n-1} - \ldots + p^2 + 2p + 1}{2(p+1)} \\ &= \frac{p^{n+1} + 2p + 1}{2(p+1)} \end{aligned}$$

Nos résultats sont résumés dans le théorème suivant.

THÉORÈME. *Supposons que p est un nombre premier impair. Alors*

$$s(p) = \frac{p+1}{2} \quad \text{et} \quad s(p^2) = \frac{p^2 - p + 2}{2}$$

Si $n \geq 3$, alors

$$s(p^n) = \begin{cases} \dfrac{p^{n+1} + p + 2}{2(p+1)} & n \ \textit{pair} \\ \dfrac{p^{n+1} + 2p + 1}{2(p+1)} & n \ \textit{impair.} \end{cases}$$

Puissances de deux. Maintenant on procède au cas restant : les puissances de 2. On a besoin d'un résultat préliminaire avant de nous consacrer à notre but principal.

Supposons $n \geq 3$, et $\text{pgcd}(a, 2^n) = 1$. Considérons l'équation $x^2 = a$ dans $\mathbb{Z}_2$. Supposons que b est une solution. Alors, clairement, $-b$ est également une solution. Aussi $b \neq -b$, puisque sinon $2b = 0$, ce qui implique $\text{pgcd}(b, 2^n) \neq 1$ alors qu'on sait que $\text{pgcd}(b^2, 2^n) = 1$. Une autre paire de solutions facilement vérifiable est $2^{n-1} \pm b$. On voit que ces valeurs sont distinctes par l'argument ci-dessus.

Pour montrer que ces quatre solutions sont les seules solutions, supposons que $\text{pgcd}(c, 2^n) = 1$ et que c est une solution en sus de b. Alors $b^2 = a = c^2$ dans $\mathbb{Z}_{2^n}$ implique $b^2 - c^2 = 0$ ou $(b-c)(b+c) = 0$ dans $\mathbb{Z}_{2^n}$. Puisque b et c sont tous les deux impairs, soit $(b-c)$ soit $(b+c)$ doit être de la forme $4m + 2 = 2(2m+1)$. Donc l'autre facteur est un multiple de 2^{n-1} ou bien 0. Par conséquent

$c = 2^{n-1} \pm b$ ou $c = \pm b$.

Ainsi on conclut que si $x^2 = a$ a une solution dans $\mathbb{Z}_{2^n}$, alors l'équation a exactement 4 solutions distinctes dans $\mathbb{Z}_{2^n}$.

On observe que le seul résidu quadratique soit dans $\mathbb{Z}_2$ soit dans $\mathbb{Z}_4$ est 1. Il en découle que $q(2) = q(4) = 1$.

Pour $n \geq 3$, il y a 2^{n-1} unités dans $\mathbb{Z}_{2^n}$, notamment les nombres impairs. Considérons que deux unités sont équivalentes si leurs carrés sont égaux. Alors les unités peuvent être séparés en classes d'équivalence de 4 unités chacune ; par conséquent, il y aura $2^{-2}2^{n-1} = 2^{n-3}$ résidus quadratiques dans $\mathbb{Z}_{2^n}$. Ainsi pour $n \geq 3, q(2^n) = 2^{n-3}$.

On est maintenant prêt à démontrer les dernières formules. Voici le résultat.

THÉORÈME.

$$s(2^n) = \begin{cases} \dfrac{2^{n-1}+4}{3} & n \textit{ pair} \\ \dfrac{2^{n-1}+5}{3} & n \textit{ impair}, n \geq 3. \end{cases}$$

Preuve. L'argument est par induction. En commençant avec $n = 2$, il est clair que $s(2^2) = 2$. Maintenant, supposons que la formule est vérifiée pour $n \leq k$. Il y a deux cas.

Cas I. $k+1$ est pair. Alors

$$\begin{aligned} s(2^{k+1}) &= q(2^{k+1}) + s(2^{k-1}) = 2^{(k+1)-3} + \frac{2^{(k-1)-1}+4}{3} \\ &= 2^{k-2} + \frac{2^{k-2}+4}{3} + \frac{4 \cdot 2^{k-2}+4}{3} = \frac{2^{(k+1)-1}+4}{3} \end{aligned}$$

Cas II. $k+1$ est impair. Alors

$$\begin{aligned} s(2^{k+1}) &= q(2^{k+1}) + s(2^{k-1}) = 2^{(k+1)-3} + \frac{2^{(k-1)-1}+5}{3} \\ &= 2^{k-2} + \frac{2^{k-2}+5}{3} + \frac{4 \cdot 2^{k-2}+5}{3} = \frac{2^{(k+1)-1}+5}{3} \end{aligned}$$

Les formules précédentes sont obtenables directement à partir de la formule de récurrence. Par exemple, si n est impair, des applications répétées amènent

$$\begin{aligned} s(2^n) &= q(2^n) + q(2^{n-2}) + \ldots + q(2^3) + s(2^1) \\ &= 2^{n-3} + 2^{n-5} + \ldots + 1 + 2. \end{aligned}$$

Donc on a besoin d'une formule pour la somme des puissances paires de 2. En posant $x_n =$

$1 + 2^2 + \ldots + 2^{2n}$, on a

$$\begin{aligned} x_n &= (2^2)^0 + (2^2)^1 + \ldots + (2^2)^n \\ &= \frac{(2^2)^{n+1} - 1}{2^n - 1} \end{aligned}$$

Donc $x_n = \dfrac{2^{2n+2} - 1}{3}$, et

$$\begin{aligned} s(2^n) &= x_{(n-3)/2} + 2 \\ &= \frac{2^{n-1} - 1}{3} + 2 = \frac{2^{n-1} + 5}{3}. \end{aligned}$$

Une formule pour la somme des puissances impaires de 2 s'obtient de x_n en factorisant, et alors $s(2^n)$ se calcule facilement.

Références

[1.] Ivan Niven, Herbert Zuckerman, *An Introduction to the Theory of Numbers*, 4ème édition, John Wiley and Sons, Inc., New York, 1980.

[2.] David M. Burton, *Elementary Number Theory*, 3ème édition, Wm. C. Brown, Dubuque, IA, 1994.

[3.] John Fraleigh, *A First Course in Abstract Algebra*, 3ème édition, Addison-Wesley, Reading, MA, 1982.

Tables rondes (Denise Vella-Chemla, 27 août 2023).

Cette petite note pour garder trace de l'implémentation informatique du Snurpf (ou système de numération par les restes dans les parties finies de $\mathbb{N}$) qu'on a en tête depuis longtemps, mais dont on n'avait pas jusque-là trouvé une manière agréable de le représenter.

Chaque nombre est positionné dans le plan complexe, suivant ses restes de division euclidienne par les nombres premiers inférieurs à sa racine. On note l'ensemble des nombres premiers en question $\mathscr{B}$ (pour base). Dans les deux exemples qui seront présentés, on aura comme bases $\mathscr{B} = [2, 3, 5, 7]$ à la recherche des décomposants de Goldbach de $n = 98$ et $\mathscr{B} = [2, 3, 5]$ à la recherche des décomposants de Goldbach de $n = 40$.

Leila Schneps a démontré que la caractérisation (en fait triviale) qu'on avait trouvée identifie bien les décomposants de Goldbach (supérieurs à sa racine) d'un nombre n : les nombres premiers compris entre $\sqrt{n}$ et $n/2$ qui ne partagent aucun reste de division euclidienne avec n sont des décomposants de Goldbach de n. Voir la note là.

Pour que les illustrations soient lisibles, on trace des cercles qui servent de supports au repérage des restes de division dans le plan complexe.

Les nombres pairs seront positionnés sur des cercles du demi-plan réel supérieur (droit), les nombres impairs seront positionnés sur des cercles du demi-plan réel inférieur (gauche).

S'il s'agissait de positionner uniquement des nombres pairs et des nombres impairs, le cercle des pairs et le cercle des impairs ont leur centre sur le cercle-unité, aux positions des deux racines secondes de l'unité qui sont 1 et -1. Ils ont tous les deux un rayon de $1/2$.

Pour positionner les nombres de l'intervalle $[9, 24]$, on va dessiner 3 points sur le cercle des pairs à droite de 0 et sur le cercle à gauche de 0 qui "codent" la divisibilité par 3. Ces 6 points en tout sont sur les 2 cercles présentés au paragraphe précédent, aux positions des trois racines tierces de l'unité qui sont 1 et j et j^2. Ils ont tous un rayon de $1/4$.

Et ainsi de suite : enfin, pour positionner les nombres de l'intervalle $[25, 48]$, on va dessiner 6 cercles qui "codent" la divisibilité par 5. Leur centre sont sur les les 6 cercles présentés au paragraphe précédent, aux positions des cinq racines cinquièmes de l'unité qui sont les $\exp\left(\frac{2\pi i}{5}\right)$ du cercle-unité à translater et réduire adéquatement sur le cercle souhaité, en fonction de la position de son centre et de la taille de son rayon. Ils ont tous un rayon de $1/8$. Sur ces 6 cercles seront positionnés $30 = 6 \times 5$ points aux positions des racines $5^{\text{ièmes}}$ de l'unité.

On a choisi pour les mesures des rayons les inverses des puissances de 4 pour que les nombres pairs n'aillent pas "empiéter" sur les impairs et inversement, et de même à tous les niveaux successifs, pour que les alignements verticaux soient aussi séparés qu'il est possible.

La fonction qui permet de trouver les coordonnées de l'affixe d'un point n pour la base $\mathscr{B} = [2, 3, 5, 7]$

est :

```
def trouvexy(n, c):
    x = r2* cos(2*pi*n/2) + r3* cos(2*pi*n/3) + r5* cos(2*pi*n/5)+r7* cos(2*pi*n/7)
    y = r2* sin(2*pi*n/2) + r3* sin(2*pi*n/3) + r5* sin(2*pi*n/5)+r7* sin(2*pi*n/7)
    plt.plot(x, y, c, marker='o', markersize=4)
    plt.annotate(str(n),xy=(x, y))
    return x,y
```

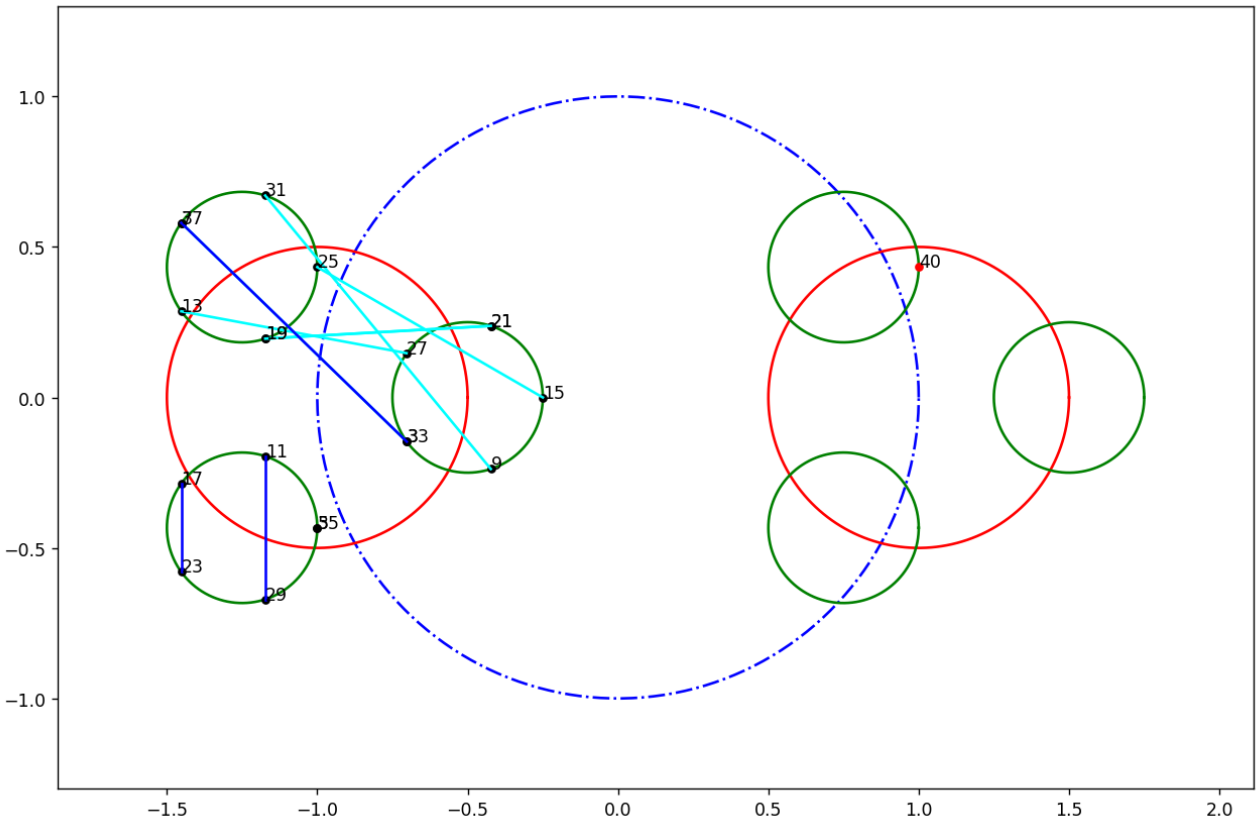


FIGURE 1 : décompositions de Goldbach de $n = 40$ qui sont $3 + 37, 11 + 29, 17 + 23$.
Attention : 3 et 33 sont au même point.

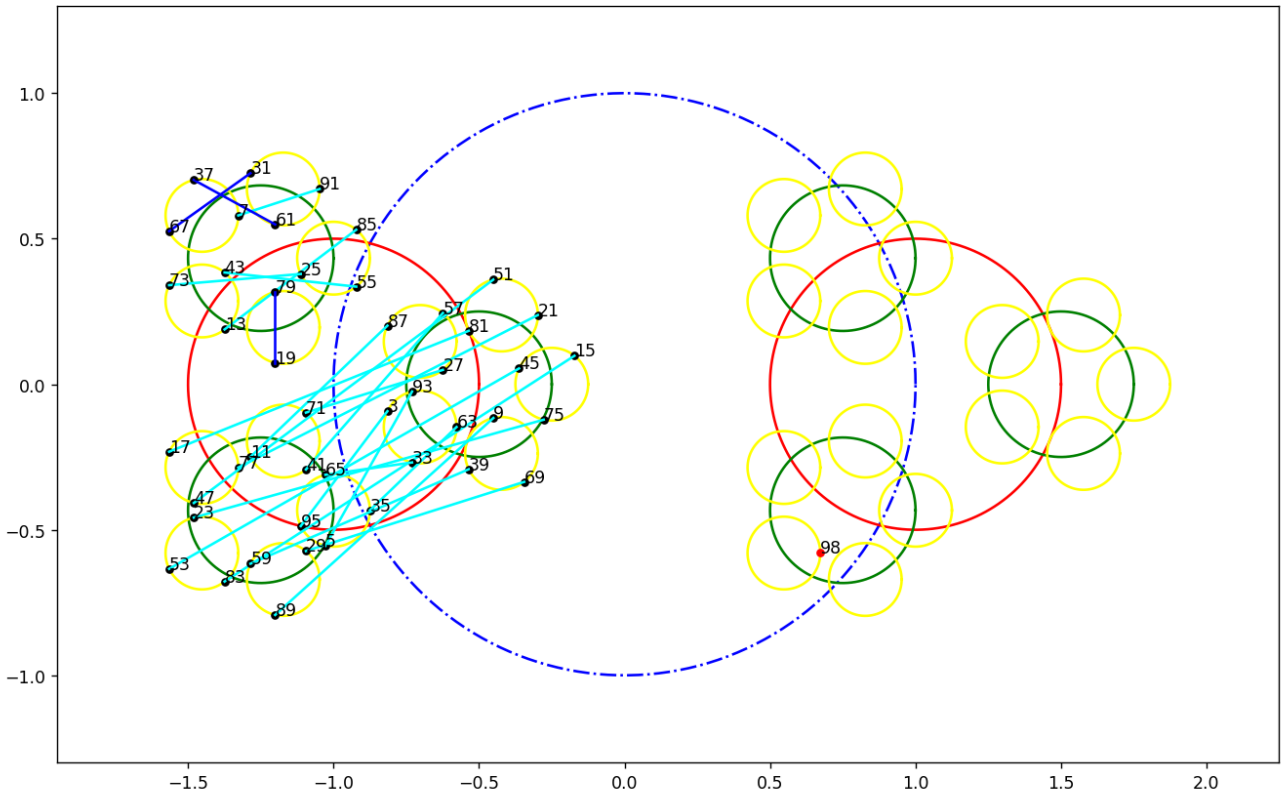


FIGURE 2 : décompositions de Goldbach de $n = 98$ qui sont $19 + 79, 31 + 67, 37 + 61$.

On relie les deux sommants impairs dont la somme vaut n par un segment. On cherche à caractériser les décompositions pour distinguer les décompositions de Goldbach (en somme de deux nombres premiers) des autres décompositions (en somme contenant un nombre composé au moins). On calcule le périmètre des triangles $[n, x, n-x]$, leur aire, et la distance qui sépare l'affixe de n de celle du milieu du segment $[x, n-x]$. On constate que les décompositions de Goldbach, du moins bon nombre d'entre elles, pour le très petit nombre d'exemples étudiés, maximisent cette dernière distance. Ci-dessous les visualisations, le programme et quelques résultats.

```
C:\Users\DENISE_2022\Desktop\conserve-banquet>python3 bodessin26à48.py
3  --> perim =  5.299449151387604 aire =  0.8361734721014444 distmilieu  2.088506694578861 DG.
5  --> perim =  4.358898943540672 aire =  7.177915983922293e-15 distmilieu  2.179449471770332
7  --> perim =  5.299449151387602 aire =  0.8361734721014387 distmilieu  2.0885066945788617
9  --> perim =  4.936769975775583 aire =  0.8978527070498491 distmilieu  1.8107359792910886
11  --> perim =  5.174325755308906 aire =  0.5166010012818898 distmilieu  2.3389792859822323 DG.
13  --> perim =  4.945570679534387 aire =  0.22568376580879224 distmilieu  2.0885066945788617
15  --> perim =  4.18890105931673 aire =  0.4330127018922135 distmilieu  1.6393596310754994
17  --> perim =  5.502637756781938 aire =  0.36034972054872655 distmilieu  2.600682775685266 DG.
19  --> perim =  4.373001009245786 aire =  0.04297380129143002 distmilieu  1.8107359792910895
```

FIGURE 3 : Chercher si les décomposants de Goldbach maximisent une distance (n=40) (on voit que 7 et 13, non décomposants de 40, sont tout de même à grande distance du point 40.

```
C:\Users\DENISE_2022\Desktop\conserve-banquet>python3 bodessin50à120.py
3  --> perim =  3.8474359874237 48 aire =  0.3659990614777857 distmilieu  1.661986965969646
5  --> perim =  3.8170474067801807 aire =  0.45421096531501076 distmilieu  1.578551152375549
7  --> perim =  4.732977894233356 aire =  0.25292128870398106 distmilieu  2.2166026443472537
9  --> perim =  4.110920070470572 aire =  0.5541187174548746 distmilieu  1.5035691982829507
11  --> perim =  4.3175490668800185 aire =  0.5189700472266332 distmilieu  1.8103018041344512
13  --> perim =  4.6972136735633985 aire =  0.5241942714043881 distmilieu  2.0490163078592216
15  --> perim =  4.563054513291625 aire =  0.7349163945668143 distmilieu  1.474727402584816
17  --> perim =  4.8038231555828865 aire =  0.6439091005962185 distmilieu  1.8103018041344487
19  --> perim =  4.304722555442971 aire =  0.22829236393513905 distmilieu  2.0273688601322295 DG.
21  --> perim =  4.445655519213422 aire =  0.6751129958320433 distmilieu  1.585836481861092
23  --> perim =  4.459831057640576 aire =  0.4351742754005213 distmilieu  1.57855115237555
25  --> perim =  4.899858452924814 aire =  0.25114260371506086 distmilieu  2.2200823393022096
27  --> perim =  3.7666636961374698 aire =  0.24317470673992084 distmilieu  1.6299984322491068
29  --> perim =  3.6008008929396746 aire =  0.2125373176080315 distmilieu  1.398215937876957
31  --> perim =  5.192288882003902 aire =  0.37749019342592083 distmilieu  2.4194748168030134 DG.
33  --> perim =  3.459323320571371 aire =  0.0760149816063239 distmilieu  1.5785511523755484
35  --> perim =  3.2904815799185494 aire =  0.24325533915861183 distmilieu  1.4286124166959466
37  --> perim =  5.011263297809169 aire =  0.014536802621137362 distmilieu  2.3463220337758925 DG.
39  --> perim =  4.017618159207392 aire =  0.3040262828095534 distmilieu  1.5880941873437056
41  --> perim =  4.042155567464725 aire =  0.5426766638520251 distmilieu  1.6299984322491152
43  --> perim =  4.556207164120552 aire =  0.16827787117487994 distmilieu  2.0490163078592207
45  --> perim =  4.8378458566454885 aire =  0.7376202830851503 distmilieu  1.6619869659696487
47  --> perim =  4.908287631296902 aire =  0.9147615144 81756 distmilieu  1.7297877941811706
49  --> perim =  3.7741424538073134 aire =  0.0 distmilieu  1.8870712269036567
```

FIGURE 4 : Chercher si les décomposants de Goldbach maximisent une distance (n=98) (on voit que 7, qui divise 98, mais aussi 25, 43, qui ne le divisent, pas sont aussi à grandes distances du point associé à 98.

Résultats pour deux autres nombres :

```
C:\Users\DENISE_2022\Desktop\conserve-banquet>python3 bodessin26à48.py
3  --> perim =  4.9455706795344 aire =  0.22568376580881158 distmilieu  2.0885066945788 66 DG.
5  --> perim =  4.188901059316741 aire =  0.4330127018922235 distmilieu  1.6393596310755028
7  --> perim =  5.502637756781949 aire =  0.3603497205487277 distmilieu  2.6006827756852715 DG.
9  --> perim =  4.37300100924581 aire =  0.04297380129141827 distmilieu  1.8107359792910975
11  --> perim =  4.373001009245799 aire =  0.042973801291405885 distmilieu  1.810735979291095
13  --> perim =  5.502637756781961 aire =  0.36034972054874664 distmilieu  2.60068277568527 DG.
15  --> perim =  4.188901059316738 aire =  0.433012701892218 distmilieu  1.6393596310755032
17  --> perim =  4.945570679534397 aire =  0.22568376580881117 distmilieu  2.0885066945788657
19  --> perim =  5.174325755308915 aire =  0.5166010012818867 distmilieu  2.338979285982239 DG.
21  --> perim =  4.9367699757755865 aire =  0.8978527070498454 distmilieu  1.8107359792910944
23  --> perim =  5.299449151387618 aire =  0.8361734721014473 distmilieu  2.088506694578868
25  --> perim =  4.358898943540679 aire =  0.0 distmilieu  2.1794494717703397
```

FIGURE 5 : Chercher si les décomposants de Goldbach maximisent une distance (n=50)

```
C:\Users\DENISE_2022\Desktop\conserve-banquet>python3 bodessin50à120.py
3  --> perim =  3.3628009449017755 aire =  0.2646120017521994 distmilieu  1.4855798279065868
5  --> perim =  4.541123225738582 aire =  0.3763684992153665 distmilieu  2.0242308010267833 DG.
7  --> perim =  3.8480855571363684 aire =  0.48942070611572874 distmilieu  1.3187532776004725
9  --> perim =  4.0375709909459605 aire =  0.567737344108685 distmilieu  1.4374195364833826
11  --> perim =  3.9185700808569455 aire =  0.1216107825537629 distmilieu  1.8604063151079573 DG.
13  --> perim =  4.171816940287509 aire =  0.6215973127536124 distmilieu  1.5500450176145306
15  --> perim =  4.167385386113514 aire =  0.5342500353786689 distmilieu  1.282791817069301
17  --> perim =  4.587841100098727 aire =  0.49990657280154294 distmilieu  1.9166581196893075
19  --> perim =  3.7850710737352977 aire =  0.41179022488156836 distmilieu  1.5801654358412596
21  --> perim =  3.6573818931747666 aire =  0.3743063714507428 distmilieu  1.2361617634100268
23  --> perim =  4.555705534154152 aire =  0.32048769373295183 distmilieu  2.0710351189923495 DG.
25  --> perim =  3.368002110475985 aire =  0.3173979491105133 distmilieu  1.3696435770789637
```

FIGURE 6 : Chercher si les décomposants de Goldbach maximisent une distance (n=52)

Le programme python initial :

bodessin.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Isearch Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import pi, sin, cos
import math
from math import sqrt

def prime(atester):
    pastrouve = True ; k = 2 ;
    if (atester in [0,1]): return False ;
    if (atester in [2,3,5,7]): return True ;
    while (pastrouve):
        if ((k * k) > atester): return True
        else:
            if ((atester % k) == 0): return False
            else: k=k+1

def cercle(rayon, xcentre, ycentre, c, s):
    theta = np.linspace(0,2*pi,360)
    x = xcentre + rayon * cos(theta)
    y = ycentre + rayon * sin(theta)
    plt.plot(x,y, color=c, ls = s)

def trouvexy(n, c):
    x = r2* cos(2*pi*n/2) + r3* cos(2*pi*n/3) + r5* cos(2*pi*n/5)+r7* cos(2*pi*n
s/7)
    y = r2* sin(2*pi*n/2) + r3* sin(2*pi*n/3) + r5* sin(2*pi*n/5)+r7* sin(2*pi*n
s/7)
    plt.plot(x, y, c, marker='o', markersize=4)
    plt.annotate(str(n),xy=(x, y))
    return x,y

fig = plt.figure(figsize=(15,15))
ax = fig.gca()
ax.set_aspect('equal')
r2 = 1 ; r3 = 1/2 ; r5 = 1/4 ; r7 = 1/8
cercle(r2,0,0,'blue', '-.')
c3d = 1 ; c3g = c3d-2 ; c3y = 0
c5dx = 1 ; c5gx = c5dx-2 ; c5y = 0
c7dx = 1 ; c7gx = c7dx-2 ; c7y = 0
cercle(r3, c3d, c3y, 'red', '-')
cercle(r3, c3g, c3y, 'red', '-')
for m in range(3):
```

-\--- **bodessin.py** Top L28 (Python ElDoc Isearch)

FIGURE 7 : Début du programme

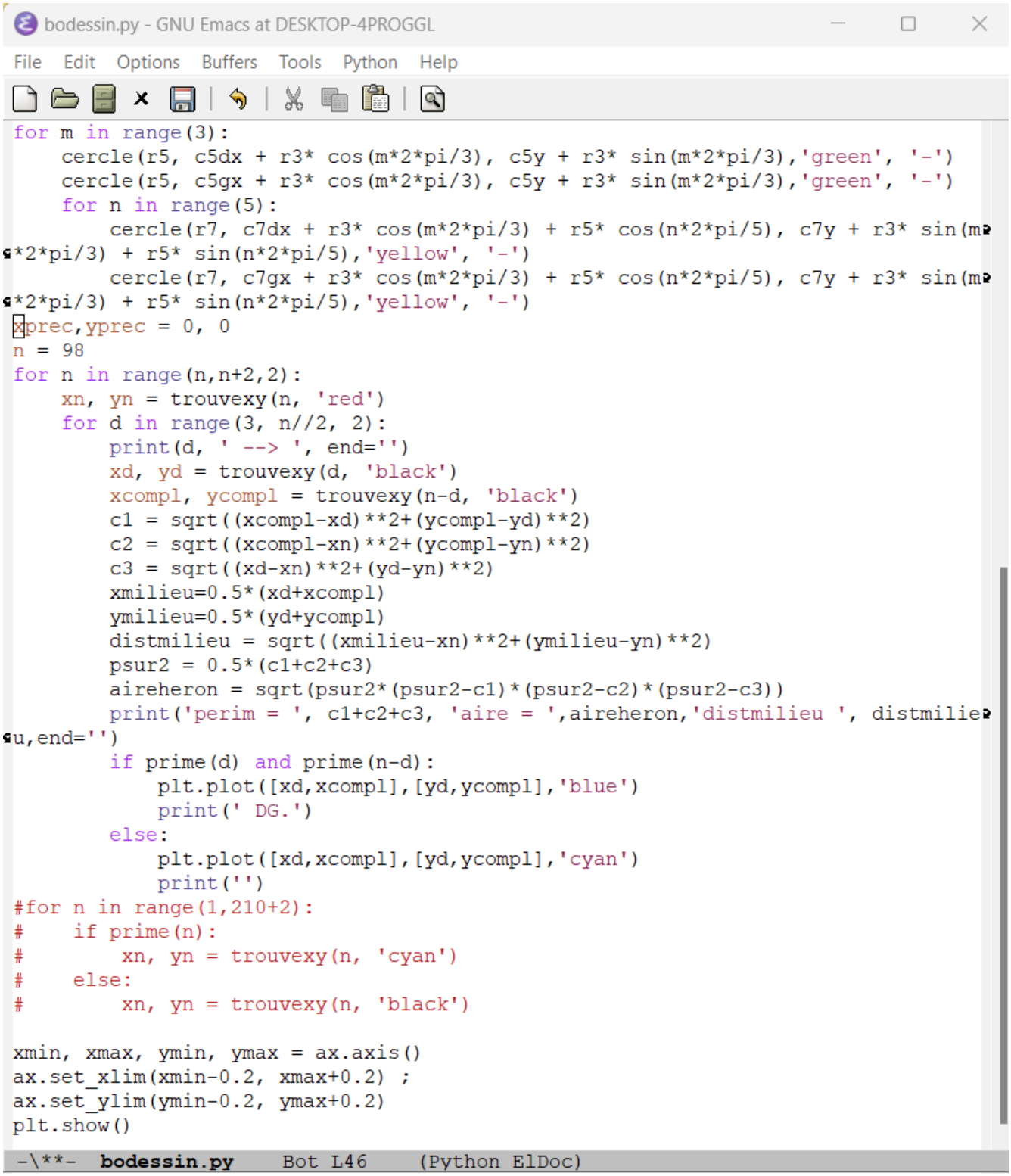


FIGURE 8 : Fin du programme

Ci-après, un programme plus court et le placement obtenu des nombres jusqu'à $2 \times 3 \times 5 \times 7$.

banquet-de-Jacques.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt, numpy as np
from matplotlib.patches import Circle
from itertools import product
from numpy import exp, pi

def primes(n):        # np.array of all primes < n
    is_prime = np.full(n, True)
    is_prime[:2] = False
    for p in range(2, int(round(np.sqrt(n))) + 1):
        if is_prime[p]:
            is_prime[p*p::p] = False
    return np.nonzero(is_prime)[0]

ax = plt.figure(figsize=(16, 16)).subplots(1, 1)
ax.set_aspect('equal')
cmap = plt.colormaps['hsv']
r = 1
p = primes(10)
k = np.arange(len(p))
for n in range(np.prod(p)):
    z = np.sum(r/(2**k)*exp(2j*pi*(n % p)/p))
    plt.plot(z.real, z.imag, 'o', alpha=0.8, markersize=2**2)
    plt.annotate(f'{n}', xy=(z.real, z.imag), textcoords='offset points', xytext
=(2, 2), fontsize=8)
c = [0]
for i in range(len(p)):
    for z in c:
        ax.add_patch(Circle((z.real, z.imag), r/(2**i), fill=False, ec=cmap(i/le
n(p))))
    c = [z + r/(2**i)*exp(2j*pi*j/p[i]) for z in c for j in range(p[i])]
xmin, xmax, ymin, ymax = (1.1*x for x in (-1.6, 1.9, -1.0, 1.0))
ax.set(xlim=(xmin, xmax), ylim=(ymin, ymax))
plt.show()
```

-\--- **banquet-de-Jacques.py** All L25 (Python ElDoc)

Wrote c:/Users/DENISE 2022/Desktop/conserve-banquet/banquet-de-Jacques.py

FIGURE 9 : Programme (numpy)

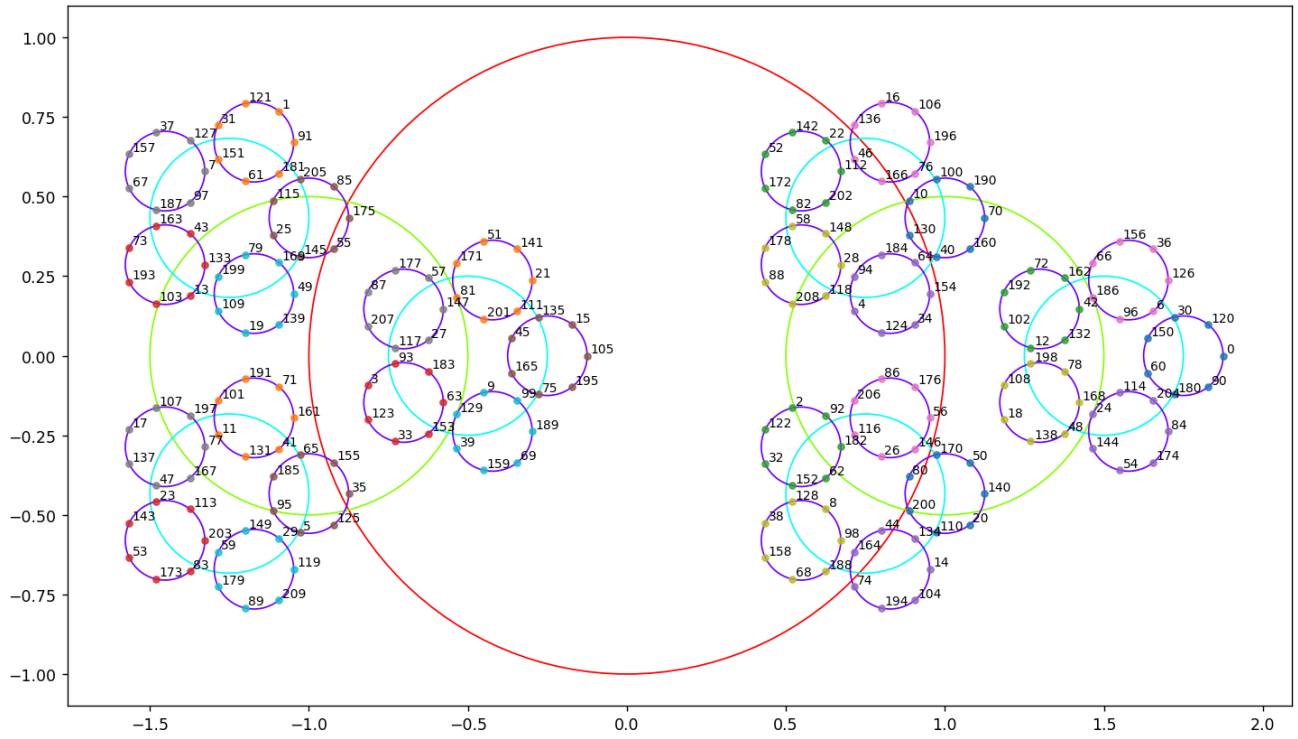


FIGURE 10 : Placement des 210 premiers nombres

Mais il y a quand même un moment où il faut réussir à se détacher des images, parce qu'elles deviennent un peu confuses, même si jolies (ci-dessous, le placement des $2 \times 3 \times 5 \times 7 \times 11$).

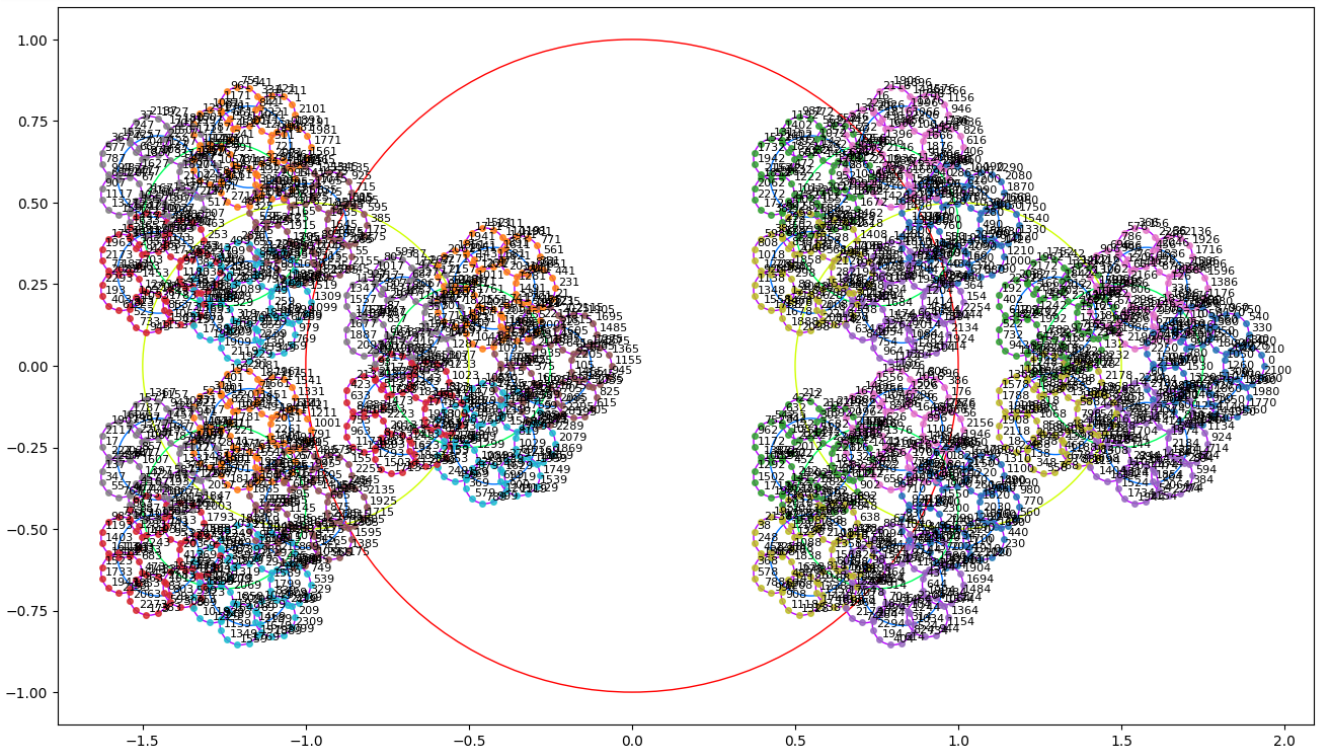


FIGURE 11 : Placement des 2310 premiers nombres

Traduction d'un extrait de l'article Dirac operators and spectral triples for some fractal sets built on curves *d'Erik Christensen, Cristina Ivan et Michel L. Lapidus* [1] *(Denise Vella-Chemla, août 2023)*

2. Triplet spectral pour un cercle

Beaucoup du contenu de cette section est bien connu (voir par exemple [14]) mais n'est habituellement pas présenté dans le langage des triplets spectraux. Il est utile, pourtant, de présenter ce contenu ici parce qu'à notre connaissance, il est seulement disponible dans des références dispersées et non dans la forme dont nous avons besoin. En particulier, on étudiera de façon quelque peu détaillée les domaines de définition des opérateurs non bornés pertinents pour notre objectif et les dérivations.

Soit C_r le cercle dans le plan complexe de rayon $r > 0$ et centré en 0. Comme d'habitude en géométrie non-commutative, on n'étudie pas le cercle directement mais on étudie plutôt une sous-algèbre de l'algèbre des fonctions continues sur le cercle. De ce point de vue, il semble plus facile de regarder l'algèbre des fonctions complexes continues $2\pi r$-périodiques sur la droite réelle. Appelons $\mathcal{A}C_r$ cette algèbre. On notera $(1/2\pi r)\mathfrak{m}$ la mesure de Lebesgue normalisée sur l'intervalle $[-\pi r, \pi r]$ et soit π_r la représentation standard de $\mathcal{A}C_r$ désignant les opérateurs de multiplication sur l'espace de Hilbert H_r qui est définie par $H_r := L([-\pi r, \pi r], (1/2\pi r)\mathfrak{m})$. L'espace H_r a une base orthonormale canonique, notée $(\phi_k^r)_{k\in\mathbb{Z}}$, qui consiste en les fonctions dans $\mathcal{A}C_r$ données par

$$\forall k \in \mathbb{Z}, \quad \phi_k^r(x) \ := \ \exp\left(\frac{ikx}{r}\right).$$

Ces fonctions sont les fonctions propres de l'opérateur différentiel $\frac{1}{i}\frac{\mathrm{d}}{\mathrm{d}x}$ et les valeurs propres correspondantes sont $\{k/r \mid k \in \mathbb{Z}\}$. Le choix naturel pour l'opérateur de Dirac pour cette situation est la fermeture de la restriction de l'opérateur ci-dessus à la portée linéaire de la base $\{\phi_k^r \mid k \in \mathbb{Z}\}$. On notera D_r cet opérateur sur H_r. Il est bien connu que D_r est auto-adjoint et que $\mathrm{dom}(D_r)$, le domaine de définition de D_r, est donné par

$$\forall f \in H_r \ : \quad f \in \mathrm{dom}\ D_r \quad \Longleftrightarrow \quad \sum_{k\in\mathbb{Z}} \frac{k^2}{r^2}\, |\langle f \mid \phi_k^r\rangle|^2 < \infty$$

où $\langle\cdot|\cdot\rangle$ est le produit intérieur de H_r.

Pour un élément $f \in \mathrm{dom}\ D_r$, on a $D_r f = \sum_{k\in\mathbb{Z}} (k/r)\langle f \mid \phi_k^r\rangle\phi_k^r$. L'opérateur auto-adjoint D_r a pour spectre $\{k/r \mid k \in \mathbb{Z}\}$ et chacune de ses valeurs propres a une multiplicité de 1. De plus, toute fonction continument différentiable $2\pi r$-périodique f sur $\mathbb{R}$ satisfait

$$[D_r, \pi_r(f)] = \pi_r(-if'),$$

de telle façon qu'on obtient un triplet spectral associé au cercle C_r de la façon suivante.

[1] Référence : Advances in mathematics 217 vol. 1 (2008) p. 47-48
https://www.sciencedirect.com/science/article/pii/S0001870807001855.

Définition 2.1. *Le triplet spectral naturel,* $\text{TripletSpectral}_n(C_r)$*, pour l'algèbre du cercle* $\mathcal{A}C_r$ *est défini par* $\text{TripletSpectral}_n(C_r) := (\mathcal{A}C_r, H_r, D_r)$.

Un des principaux ingrédients dans les arguments à venir est la possibilité de construire des triplets spectraux *intéressants* comme sommes directes de modules de Fredholm non bornés, chacun d'eux transportant seulement une toute petite quantité de l'information de l'espace total. Dans le cas des triplets naturels pour les cercles, le nombre 0 est toujours une valeur propre et par conséquent, si l'opération somme est exécutée un nombre dénombrable de fois, la valeur 0 sera d'une multiplicité infinie pour l'opérateur de Dirac qui est obtenu par une construction par somme directe. Pour éviter ce problème, on remplacera, pour le cas C_r, l'opérateur de Dirac D_r par un opérateur légèrement modifié, D_r^t qui est le translaté de D_r donné par

$$D_r^t := D_r + \frac{1}{2r} I.$$

L'ensemble des valeurs propres devient maintenant $\{(2k+1)/2r \mid k \in \mathbb{Z}\}$, mais le domaine de définition est le même que pour D_r et, *en particulier*, pour toute fonction $f \in \mathcal{A}C_r$, on a $[D_r^t, \pi_r(f)] = [D_r, \pi_r(f)]$. Par conséquent, la translation ne change pas vraiment l'effet du triplet spectral.

Définition 2.2. Le *triplet spectral translaté*, $\text{TripletSpectral}_t(C_r)$, pour l'algèbre du cercle $\mathcal{A}C_r$ est défini par $\text{TripletSpectral}_t(C_r) = (\mathcal{A}C_r, H_r, D_r^t)$.

La prochaine question est de déterminer pour quelles fonctions f de $\mathcal{A}C_r$ le commutateur $[D_r^t, \pi_r(f)]$ est borné et densément défini. Ceci est fait dans le lemme suivant qui est standard, mais que nous inclurons parce que son assertion particulière ne peut se trouver aisément dans la forme dont nous avons besoin. D'un autre côté, la preuve utilise de l'analyse élémentaire et pour cette raison, elle sera omise.

Lemma 2.3. *Soit* $f \in \mathcal{A}C_r$*. Alors les conditions suivantes sont équivalentes* :

(i) $[D_r^t, \pi_r(f)]$ *est densément défini et borné.*

(ii) $f \in \text{dom}(D_r)$ *et* $D_r f$ *est essentiellement borné.*

(iii) *Il existe une fonction mesurable, essentiellement bornée* g *sur l'intervalle* $[-\pi r, \pi r]$ *telle que*

$$\int_{-\pi r}^{\pi r} g(t)\mathrm{d}t = 0 \;\text{ et }\; \forall x \in [-\pi r, \pi r] \;:\; f(x) = f(0) + \int_0^x g(t)\mathrm{d}t.$$

Si les conditions ci-dessus sont satisfaites, alors $g(x) = (iD_r f)(x)$ *presque partout.*

On terminera cette section en mentionnant quelques propriétés de ce triplet spectral. Nous ne démontrerons aucune de ces assertions car elles sont aisées à vérifier. D'abord, remarquons que toutes les assertions ci-dessous sont vérifiées à la fois par les triplets translatés $\text{TripletSpectral}_t(C_r)$ et par les triplets naturels $\text{TripletSpectral}_n(C_r)$, bien qu'on ne les énonce que pour les triplets naturels $\text{TripletSpectral}_n(C_r)$.

Théorème 2.4. *Soit $r > 0$ et soit $(\mathcal{A}_r C, H_r, D_r)$ le triplet spectral naturel du cercle* $\mathrm{TripletSpectral}_n(C_r)$. *Alors les deux résultats suivants sont vérifiés* :

(i) *La métrique, disons d_r, induite par le triplet spectral naturel* $\mathrm{TripletSpectral}_n(C_r)$ *sur le cercle est la distance géodésique sur C_r.*

(ii) *Le triplet spectral naturel* $\mathrm{TripletSpectral}_n(C_r)$ *est sommable pour tout $s > 1$, mais pas pour $s = 1$. Par conséquent, il a pour dimension métrique 1.*

Références

[5] A. Connes, Compact metric spaces, Fredholm modules, and hyperfiniteness, Ergodic Theory Dynam. Systems 9. (1989) 207–220, https://www.cambridge.org/core/journals/ergodic-theory-and-dynamical-systems/article/compact-metric-spaces-fredholm-modules-and-hyperfiniteness/2ACB2EBA0AA0A40F9D890AA9915500F7.

[6] A. Connes, Noncommutative Geometry, Academic Press, San Diego, 1994, https://alainconnes.org/wp-content/uploads/book94bigpdf.pdf.

[7] A. Connes, Unpublished notes on a Dirac operator associated to the Cantor subset of the unit interval (electronic message to Michel Lapidus, May 2002).

[8] A. Connes, M. Marcolli, A walk in the noncommutative garden, https://arxiv.org/pdf/math/0601054.pdf.

[9] A. Connes, D. Sullivan, Quantized calculus on S1 and quasi-Fuchsian groups, unpublished, 1994, https://www.math.stonybrook.edu/ dennis/publications/PDF/DS-pub-0093.pdf.

[14] R. E. Edwards, Fourier Series. A modern introduction, Vol. 1, Second Edition, Graduate Texts in Mathematics 64, Springer-Verlag, New York (1979).

Traduction d'un extrait de la thèse de Andrea Arauza[1] présentant la notion de triplet spectral (Denise Vella-Chemla, août 2023)

3.2. Triplets spectraux

Dans cette section, on introduit l'outil principal des algèbres d'opérateurs utilisé pour étudier la géométrie fractale - le triplet spectral. On définit également la trace de Dixmier qui sera utilisée pour définir la mesure induite par le triplet spectral. Les exemples incluront des triplets spectraux pour des fractals comme l'ensemble de Cantor dans $\mathbb{R}$, pour des courbes, et pour une certaine classe d'ensembles construits à partir de courbes (comme le triangle de Sierpinski et la courbe étirée de Sierpinski).

3.2.1 Triplets spectraux

On utilise la notation $[A, B] := AB - BA$ pour le commutateur de deux opérateurs A, B sur un espace de Hilbert. En outre, étant donné un espace de Hilbert $\mathscr{H}$ on écrit $\mathscr{B}(\mathscr{H})$ pour l'espace des opérateurs bornés sur $\mathscr{H}$.

Définition 12. *Un* ***triplet spectral*** $(\mathscr{A}, \mathscr{H}, D)$ *est une collection de trois objets*

- $\mathscr{A}$ *une C^*-algèbre unitaire,*
- $\mathscr{H}$ *un espace de Hilbert qui transporte une représentation fidèle unitaire :* $\pi : \mathscr{A} \to \mathscr{B}(\mathscr{H})$, *et*
- *un opérateur, principalement auto-adjoint D de domaine $Dom(D) \subseteq \mathscr{H}$, tel que*
  - *(a) l'ensemble $\{a \in \mathscr{A} : [D, \pi(a)]$ est densément défini et a une extension bornée vers $\mathscr{H}\}$ est dense dans $\mathscr{A}$, et*
  - *(b) l'opérateur $(I + D^2)^{-1}$ est compact.*

La C^*-algèbre $\mathscr{A}$ sera souvent $C(X)$, avec X un espace de Hausdorff compact. L'opérateur $[D, \pi(a)]$, pour $a \in \mathscr{A}$, agira comme la "dérivée" de l'élément a et l'ensemble dense dans la condition (a) agira comme l'ensemble des fonctions C^1 dans $C(X)$. L'opérateur D et ses valeurs propres sera la clef pour retrouver l'information géométrique comme la dimension et la mesure. La condition que l'opérateur $(I + D^2)^{-1}$ soit compact assure que le spectre de l'opérateur D^{-1} ne contient que des valeurs propres et que le seul point d'accumulation possible de ces valeurs propres est 0. On peut alors considérer des sommes infinies de ces valeurs propres.

En utilisant les trois outils d'un triplet spectral, on peut définir les notions de dimension, métrique, et mesure sur un espace de Hausdorff X.

[1] Thèse de Andrea Arauza intitulée *Spectral Triples and Fractal Geometry*, dans le but d'obtenir le titre de Docteur en philosophie des mathématiques, soutenue à Riverside, à l'Université de Californie, en juin 2018.

Définition 13. *Étant donné un triplet spectral* $(C(X), \mathscr{H}, D)$, *le nombre*

$$\mathfrak{d} = \mathfrak{d}(X) := \inf\{p > 0 \ : \ \mathrm{tr}((I + D^2)^{-p/2}) < \infty\}$$

est la ***dimension spectrale*** *(ou* ***dimension métrique****) de l'espace* X.

Notons que la condition (b) dans la définition d'un triplet spectral est nécessaire de telle façon que la trace dans la définition de la dimension spectrale ait la possibilité d'être finie. A priori il n'y a pas de raison que la dimension spectrale $\mathfrak{d}$ soit finie.

On définit ensuite une notion de distance induite par le triplet spectral. La définition semblera familière à ceux qui connaissent les métriques sur des espaces d'états. Pour davantage de détails à ce sujet, voir les travaux de Marc Rieffel dans [30], [31], [32] et d'Alain Connes dans [10].

Définition 14. *Étant donné un triplet spectral* $(C(X), \mathscr{H}, D)$, *définissons la* ***distance spectrale*** *par*

$$d_X(x, y) = \sup\{|f(x) - f(y)| \ : f \in C(X), \ \|[D, \pi(f)]\| \leq 1\}, \qquad \textit{pour } x, y \in X.$$

En utilisant un triplet spectral et une autre notion de géométrie non-commutative, on peut définir la notion de mesure. Pour cela on doit introduire la notion de trace de Dixmier.

3.2.2 La trace de Dixmier

Comme référence à la discussion à venir, on peut se reporter au livre *Noncommutative Geometry* d'Alain Connes [9]. Ce livre est la référence pour la géométrie non-commutative. Pour définir la trace de Dixmier on aura besoin d'extensions de la notion habituelle de limite. Pour cela, on utilisera des limites étendues. Les limites étendues sont des extensions à l^∞ de la fonctionnelle limite habituelle agissant sur c, l'espace des séquences convergentes. Par Hahn Banach la limite classique sur c s'étend à l^∞, notée Lim, et $|\mathrm{Lim}(x)| \leq \|x\|_\infty$ pour tout $x \in l^\infty$.

Définition 3.2.2.1. *Une fonctionnelle linéaire positive* ϕ *sur une algèbre de von Neumann* $\mathcal{N}$ *est un* ***état*** *si* $\phi(1) = 1$.

Les limites étendues sont des états sur l^∞ puisque $\mathrm{Lim}(1) = 1$ et sont caractérisés par le fait qu'ils s'évanouissent sur c_0. En d'autres termes, un état ϕ sur l^∞ s'évanouit sur c_0 si et seulement si ϕ est une extension de la limite classique à l^∞ (i.e. $\phi = \mathrm{Lim}$). Notons que tout état sur l^∞ est continu :

$$|\phi(x)| \leq |\phi(1 \cdot \|x\|_\infty)| \leq \|x\|_\infty$$

où $x = \{x_n\}_{n=1}^\infty \in l^\infty$. Cela signifie qu'il suffit qu'un état s'évanouisse sur des séquences avec un nombre fini d'entrées non nulles pour que l'état puisse être une limite étendue.

Définition 3.2.2.2. *Soit* w *un état sur l'algèbre de von Neumann* l^∞. *Alors* w *est appelé une* ***limite étendue*** *si elle s'évanouit sur toute séquence avec un nombre fini d'entrées non nulles dans* l^∞.

Nous aurons besoin que nos limites étendues satisfassent une certaine propriété de dilatation. Le semi-groupe discret de dilatation $\sigma_k : l^\infty \to l^\infty$ pour $k \in \mathbb{N}$ agit par la formule

$$\sigma_k(x) = (x_0, x_0, \ldots, x_0, x_1, x_1, \ldots, x_1, \ldots)$$

où $x \in l^\infty$ et chaque x_j apparaît k fois. On utilisera des limites étendues invariantes par 2-dilatation. C'est-à-dire des limites étendues, $w : l^\infty \to \mathbb{R}$, qui satisfont

$$w(\sigma_2(x)) = w(x).$$

Le fait que des limites étendues invariantes par dilatation existent découle d'une version du théorème de Hahn Banach invariante par dilatation. La preuve de cette version du théorème de Hahn Banach peut être trouvée dans le texte [11] d'Edwards, Théorème 3.3.1.

Théorème 3.2.2.3. (Théorème de Hahn Banach invariant) *Soit X un espace linéaire et G un semi-groupe commutatif. Étant donnés*

(a) une action $g : x \to g(x)$ de G sur X,
(b) un sous-espace G-invariant Y de X,
(c) une fonctionnelle convexe homogène $p : X \to \mathbb{R}$ telle que $p \circ g \leq p$ pour tout $g \in G$,
(d) une fonctionnelle linéaire invariante G, $w : Y \to \mathbb{R}$ telle que $w \leq p$,

alors il existe une extension invariante G, $w : X \to \mathbb{R}$ telle que $w \leq p$.

Corollaire 3.2.2.4. *Des limites étendues invariantes par dilatation existent sur l^∞.*

L'espace dans la définition qui suit est un idéal dans l'ensemble des opérateurs compacts et servira de domaine de la trace de Dixmier. Pour un opérateur compact T, notons par $\mu_j(T)$ les valeurs propres de $|T|$ ordonnées de telle façon que $0 \leq \mu_{j+1}(T) \leq \mu_j(T)$ pour $j \in \mathbb{N}$.

Définition 3.2.2.5. *Soit $w : l^\infty \to \mathbb{R}$ une fonctionnelle linéaire qui s'évanouit sur c_0 et satisfait pour $x \in l^\infty$, $w(\sigma_2(x)) = w(x)$. Définissons*

$$\mathcal{L}^{(1,\infty)} = \{T \in \mathcal{K} : \|T\|_{(1,\infty)} = \sup_N \frac{1}{\log(1+N)} \sum_{j=1}^{N} \mu_j(T) < \infty\}.$$

*La **trace de Dixmier** de $T \in \mathcal{L}^{(1,\infty)}$ où $T \geq 0$, est donnée par*

$$\mathrm{Tr}_w(T) = w\left\{\frac{1}{\log(1+N)} \sum_{j=1}^{N} \mu_j(T)\right\}.$$

Définissons Tr_w pour les opérateurs auto-adjoints et ensuite pour des opérateurs arbitraires par linéarité.

La séquence

$$\left\{\frac{1}{\log(1+N)} \sum_{j=1}^{N} \mu_j(T)\right\}_{N=1}^{\infty}$$

ne converge pas toujours lorsque $N \to \infty$, donc $\mathrm{Tr}_w(T)$ peut dépendre de la limite étendue w. Dans la plupart des applications on peut montrer l'indépendance de $\mathrm{Tr}_w(T)$ à partir de w. Comme pour la trace des opérateurs habituelle, la trace de Dixmier a de nombreuses propriétés utiles.

Proposition 3.2.2.6. [9]

1. $\mathrm{Tr}_w(\cdot)$ est une fonctionnelle linéaire positive sur l'idéal des opérateurs T pour lesquels $\mu_j(\mathrm{T}) = O(n^{-1})$.
2. $\mathrm{Tr}_w(\mathrm{ST}) = \mathrm{Tr}_w(\mathrm{TS})$ pour tous les opérateurs compacts T avec $\mu_j(\mathrm{T}) = O(n^{-1})$ et $\mathrm{S} \in \mathscr{B}(\mathscr{H})$.
3. $\mathrm{Tr}_w(\cdot)$ s'évanouit sur les opérateurs compacts T avec $\mu_j(\mathrm{T}) = O(n^{-\alpha})$ pour $\alpha > 1$. i.e. $\mathrm{Tr}_w(\mathrm{T}) = 0$ si $n\mu_n \to 0$ lorsque $n \to \infty$.

Un résultat de Connes est que pour un choix adéquat du triplet spectral, l'application $\mathrm{Tr}_w(\pi(f)|D|^{-\mathfrak{d}})$ est une fonctionnelle linéaire positive non triviale sur $C(X)$ et induit par conséquent une mesure ; voir [9]. C'est comme cela qu'on utilisera un triplet spectral pour induire une mesure sur un ensemble fractal. Maintenant que nous avons tous les outils nécessaires, nous pouvons commencer à explorer comment les utiliser pour étudier la géométrie fractale. Voir [28] pour davantage d'éléments sur la théorie des traces singulières comme la trace de Dixmier. Le théorème suivant d'Alain Connes dans [9] est souvent utilisé pour calculer la trace de Dixmier comme résidu d'une certaine série. On utilisera ce théorème dans les sections qui suivent.

Théorème 15.

Pour $\mathrm{T} \geq 0, \mathrm{T} \in \mathcal{L}^{(1,\infty)}$*, les deux conditions suivantes sont équivalentes :*

1. $$(s-1)\sum_{n=0}^{\infty} \mu_n(\mathrm{T})^s \to L \text{ lorsque } s \to 1^+ \ ;$$
2. $$\frac{1}{\log(N+1)} \sum_{n=1}^{N} \mu_n(\mathrm{T}) \to L \text{ lorsque } N \to \infty.$$

Références bibliographiques

[9] A. Connes, *Noncommutative Geometry*, Academic Press, San Diego, 1994.

[10] A. Connes, Compact metric spaces, Fredholm modules, and hypefiniteness, *Ergodic Theory and Dynamical Systems* **9** (1989), 207220.

[11] R. E. Edwards, *Functional Analysis : Theory and Applications*, Dover Publications Inc., New York, 1995.

[28] S. Lord, F. Sukochev, D. Zanin, *Singular Traces: Theory and Applications*, vol. 46. De Gruyter Studies in Mathematics, 2013.

[30] M. A. Rieffel, Metrics on states from actions of compact groups, *Doc. Math.* 3 (1998) 215-229.

[31] M. A. Rieffel, Metrics on state spaces, *Doc. Math.* 4 (1999) 559-600. https://arxiv.org/pdf/math/9906151.pdf.

[32] M. A. Rieffel, Compact quantum metric spaces, in : *Operator Algebras, Quantization, and Non-Commutative Geometry*, Contemp. Math., 365, Amer. Math. Soc., 2004, 315-330.

Transcription en LaTeX d'un article aux Comptes-Rendus de l'Académie des Sciences de Bost et Connes

C. R. Acad. Sci. Paris, t. 315, Série I, p. 279-284, 1992

Analyse mathématique/*Mathematical Analysis*

Produits eulériens et facteurs de type III

Jean-Benoît Bost et Alain Connes

Résumé. Nous établissons un lien précis entre mécanique statistique quantique et théorie des nombres en construisant un système dynamique $(\mathscr{H}, \sigma_1)$ où $\mathscr{H}$ est une C*-algèbre de Hecke non commutative, dont la fonction de partition est la fonction ζ de Riemann. Nous démontrons l'existence d'une transition de phase avec brisure spontanée de symétrie, qui fait intervenir l'action du groupe de Galois de $\overline{\mathbb{Q}}_{ab}/\mathbb{Q}$.

Euler products and type III factors

Abstract. We establish a precise relation between quantum statistical mechanics and number theory by the construction of a C* dynamical system $(\mathscr{H}, \sigma_1)$ where $\mathscr{H}$ is a non-commutative Hecke C*-algebra, whose partition function is the Riemann ζ function. We show the existence of a phase transition with spontaneous symmetry breaking which involves the action of the Galois group of $\overline{\mathbb{Q}}_{ab}/\mathbb{Q}$.

Soit S le foncteur de la catégorie des espaces de Hilbert dans elle-même qui associe à un espace de Hilbert $\mathfrak{h}$ l'espace de Hilbert $\mathrm{S}\mathfrak{h} = \oplus \mathrm{S}^n\mathfrak{h}$ somme directe des puissances symétriques $\mathrm{S}^n\mathfrak{h}$ dotées du produit scalaire tel que :

$$\langle \xi_1\xi_2\ldots\xi_n, \eta_1\eta_2\ldots\eta_n\rangle = \sum_{\sigma} \prod_{j=1}^{n} \langle \xi_j, \eta_{\sigma(j)}\rangle \tag{1}$$

où σ parcourt le groupe des permutations de $\{1, ..., n\}$. Si T est un opérateur non borné autoadjoint dans $\mathfrak{h}$, ST est l'opérateur non borné autoadjoint tel que

$$(\mathrm{ST})(\xi_1\ldots\xi_n) = (\mathrm{T}\xi_1)\ldots(\mathrm{T}\xi_n), \qquad \forall \xi_j \in \text{Domaine T}. \tag{2}$$

Si T est traçable et de norme < 1, alors ST est traçable et l'on a

$$\mathrm{Trace}(\mathrm{ST}) = \det(1-\mathrm{T})^{-1}. \tag{3}$$

Pour tout $\xi \in \mathfrak{h}$ on définit un opérateur $b^*(\xi)$ dans $\mathrm{S}\mathfrak{h}$ comme la fermeture de l'opérateur de multiplication par ξ :

$$b^*(\xi)\eta = \xi\eta, \qquad \forall \in \mathrm{S}^n\mathfrak{h}. \tag{4}$$

Note présentée par Alain Connes.
0764-4442/92/03150279 $2.00
Transcription : Denise Vella-Chemla, août 2023.

Ces opérateurs et leurs adjoints $b(\xi) = (b^*(\xi))^*$ vérifient les relations de commutation canoniques [5] :

$$[b^*(\xi), b(\eta)] = \langle \xi, \eta \rangle, \qquad \forall \xi, \eta \in \mathfrak{h}. \tag{5}$$

En particulier pour $\mathfrak{h}$ de dimension 1 les opérateurs b^* et b correspondants dans $S\mathfrak{h}$ donnent l'unique représentation irréductible de la relation $bb^* - b^*b = 1$. L'opérateur bb^* admet alors $\mathbb{N}^* \subset \mathbb{R}$ comme spectre simple et cette écriture caractérise les opérateurs autoadjoints admettant $\mathbb{N}^*$ comme spectre simple.

Le lemme suivant caractérise les opérateurs autoadjoints admettant pour spectre simple le sous-ensemble $\mathscr{P} \subset \mathbb{R}_+$ formé des nombres premiers. C'est une traduction immédiate du théorème de factorisation d'Euclide.

LEMME 1. *Soit* T *un opérateur autoadjoint dans* $\mathfrak{h}$. *Pour que* T *admette* $\mathscr{P}$ *comme spectre simple, il faut et il suffit que* ST *admette* $\mathbb{N}^*$ *comme spectre simple.*

L'égalité (3) appliquée à T^{-s}, $\mathrm{Re}(s) > 1$, correspond évidemment à la décomposition de la fonction ζ de Riemann en produit eulérien. Le foncteur S et les relations de commutation canoniques (5) sont les ingrédients essentiels de la deuxième quantification des physiciens théoriciens. Ainsi le lemme 1 suggère de remplacer l'étude du sous-ensemble de $\mathbb{R}$ par celle du système dynamique non commutatif constitué par

(a) l'algèbre (des observables) engendrée par les opérateurs $b(\xi), b^*(\eta)$; $\xi, \eta \in l^2(\mathscr{P})$ dans l'espace de Hilbert $l^2(\mathbb{N}^*) = S\, l^2(\mathscr{P})$,

(b) l'évolution σ_t de cette algèbre définie par :

$$\sigma_t(x) = e^{itH_b} x e^{-itH_b}, \quad \forall t \in \mathbb{R} \tag{6}$$

où l'"hamiltonien" H_b, est l'opérateur

$$H_b \varepsilon_n = (\log n)\varepsilon_n \tag{7}$$

dans la base orthonormale canonique ε_n de $l^2(\mathbb{N}^*)$. La définition précise de la C*-algèbre des observables, formée d'opérateurs *bornés* dans $\mathfrak{h}_b = l^2(\mathbb{N}^*)$, ainsi que sa structure sont contenues dans la proposition suivante.

PROPOSITION 2.

1. *Pour tout* $n \in \mathbb{N}^*$ *l'égalité suivante définit une isométrie* μ_n *de* $l^2(\mathbb{N}^*)$ *dans* $l^2(\mathbb{N}^*)$:

$$\mu_n \varepsilon_k = \varepsilon_{kn} \quad \forall k \in \mathbb{N}^*.$$

2. La C*-algèbre $C^*(\mathbb{N}^*)$ engendrée par les opérateurs $\mu_n, n \in \mathbb{N}^*$ est le produit tensoriel infini : $C^*(\mathbb{N}^*) = \bigotimes_{p \in \mathscr{P}} \tau_p$ des C*-algèbres τ_p engendrées par $\mu_p, p \in \mathscr{P}$.

3. Chaque C*-algèbre τ_p est isomorphe à la C*-algèbre de Tœplitz.

4. L'égalité $\sigma_t(x) = e^{itH_b} x e^{-itH_b}, x \in \mathrm{C}^*(\mathbb{N}^*)$ définit un groupe à un paramètre d'automorphismes de $\mathrm{C}^*(\mathbb{N}^*)$.

Les C*-algèbres de Toeplitz sont nucléaires, de sorte que la définition du produit tensoriel $\otimes\tau_p$ est non ambiguë. Pour un tel système dynamique non commutatif, une notion essentielle, issue de la mécanique statistique quantique est la suivante (cf. [4], chap. 1).

Définition 3. Soient (B, σ_t) une C*-algèbre unifère munie d'un groupe à un paramètre d'automorphismes, φ un état sur B et $\beta \in]0, \infty[$. On dit que φ *vérifie la condition* KMS_β *relativement à* σ_t si et seulement s'il existe pour tous $x, y \in \mathrm{B}$ une fonction holomorphe $\mathrm{F}_{x,y}$ bornée continue au bord dans la bande $\{z \in \mathbb{C}, \mathrm{Im}\ z \in [0, \beta]\}$ telle que $\mathrm{F}_{x,y}(t) = \varphi(x\sigma_t(y))$ et $\mathrm{F}_{x,y}(t + i\beta) = \varphi(\sigma_t(y)x)$.

On n'a, en général, ni existence ni unicité d'états KMS_β.

Théorème 4.

(a) *Pour tout $\beta > 0$, il existe un unique état* KMS_β *sur* $\mathrm{C}^*(\mathbb{N}^*)$ *; c'est un produit tensoriel infini* $\varphi_\beta = \bigotimes_{p \in \mathscr{P}} \varphi_{\beta,p}$ *où* $\varphi_{\beta,p}$ *est l'état sur l'algèbre de Tœplitz dont la liste des valeurs propres est* $\{(1 - p^{-\beta})p^{-n\beta}, n \in \mathbb{N}\}$

(b) *Pour $\beta > 1$, l'état φ_β est de type* I_∞ *et donné par*

$$\varphi_\beta(x) = \zeta(\beta)^{-1}\ \mathrm{Trace}\ (e^{-\beta \mathrm{H}_b} x), \quad \forall x \in \mathrm{C}^*(\mathbb{N}^*).$$

(c) *Pour $\beta = 1$, l'état φ_β est factoriel de type* III_1*, et donné par :*

$$\varphi_1(x) = \mathrm{Trace}_\omega(e^{-\mathrm{H}_b} x), \quad \forall x \in \mathrm{C}^*(\mathbb{N}^*)$$

où Trace_ω *est la trace de Dixmier.*

(d) *Pour $0 < \beta \leq 1$, l'état φ_β est factoriel de type* III_1*, et le facteur associé est le facteur d'Araki-Woods* R_∞.

Blackadar [3] avait démontré que φ_1 est factoriel de type III.

Rappelons de plus que la trace de Dixmier d'un opérateur comme $e^{-H}x$ est égale au résidu en $s = 1$, si celui-ci a un sens, de la fonction $s \to \mathrm{Trace}(e^{-sH}x)$ ([1], chap. 5). Nous interprétons maintenant la C*-algèbre $\mathrm{C}^*(\mathbb{N}^*)$ en termes adéliques. Soit P le groupe algébrique des matrices triangulaires de la forme $\begin{bmatrix} 1 & n \\ 0 & h \end{bmatrix}$, h inversible. Considérons l'anneau localement compact commutatif A_f des adèles finies sur $\mathbb{Q}$. Notons R le sous-anneau compact maximal, il est ouvert dans A_f. La proposition suivante identifie $\mathrm{C}^*(\mathbb{N}^*)$ à la C*-algèbre de convolution des fonctions P_R-biinvariantes sur $\mathrm{P}_{\mathrm{A}_f}$. Rappelons que si G est un groupe localement compact moyennable, la C*-algèbre du groupe $\mathrm{C}^*(\mathrm{G})$ est la C*-algèbre engendrée dans l'espace de Hilbert $\mathrm{L}^2(\mathrm{G}, ds)$ de la représentation régulière gauche (ds est une mesure de Haar à gauche sur G) de G par l'action de $\mathrm{L}^1(\mathrm{G})$ par convolution :

$$(\lambda(f)\xi)(s) = \int_{\mathrm{G}} f(t)\xi(t^{-1}s)dt. \tag{8}$$

Soit ds la mesure de Haar à gauche sur $\mathrm{P}_{\mathrm{A}_f}$ normalisée par

$$\int_{\mathrm{P_R}} ds = 1. \tag{9}$$

Proposition 5.

1. *Soient* $p \in \mathscr{P}, \mathrm{K} = \mathbb{Q}_p, \mathrm{R} = \mathbb{Z}_p$. *La fonction caractéristique* $1_{\mathrm{P_R}} = e$ *de l'ouvert* $\mathrm{P_R} \subset \mathrm{P_K}$ *définit un idempotent* $e \in \mathrm{C}^*(\mathrm{P_K})$ *et la* C^**-algèbre réduite* $\mathrm{C}^*(\mathrm{P_K})_e$ *est canoniquement isomorphe à l'algèbre de Tœplitz* τ_p.

2. *La* C^**-algèbre* $\mathrm{C}^*(\mathrm{P}_{\mathrm{A}_f})$ *est le produit tensoriel infini* $\bigotimes_{p\in\mathscr{P}} (\mathrm{C}^*(\mathrm{P}_{\mathbb{Q}_p}), e_p)$.

3. *La fonction caractéristique* $1_{\mathrm{P_R}} = e$ *de l'ouvert* $\mathrm{P_R} \subset \mathrm{P}_{\mathrm{A}_f}$ *définit un idempotent* $e \in \mathrm{C}^*(\mathrm{P}_{\mathrm{A}_f})$ *et la* C^**-algèbre réduite* $\mathrm{C}^*(\mathrm{P}_{\mathrm{A}_f})_e$ *est canoniquement isomorphe à* $\mathrm{C}^*(\mathbb{N}^*)$.

La notion de produit tensoriel infini de couples (B_ν, e_ν) de C^*-algèbres sans unité et idempotents $e_\nu = e_\nu^* \in B_\nu$ se définit comme limite inductive en utilisant les morphismes $x \to x \otimes e_\nu$. L'idéal bilatère J engendré par l'idempotent $e \in \mathrm{C}^*(\mathrm{P}_{\mathrm{A}_f})$ n'est pas dense dans $\mathrm{C}^*(\mathrm{P}_{\mathrm{A}_f})$ et les C^*-algèbres considérées ne sont pas équivalentes au sens de Morita. Rappelons qu'un *poids* φ sur une C^*-algèbre B est une application linéaire de $\mathrm{B}^+ = \{x \in \mathrm{B}\ ;\ \varphi(x^*x) \geq 0\}$ dans $[0, +\infty]$. Un poids est dit *semi-fini* si, et seulement si, $\{x \in \mathrm{B}\ ;\ \varphi(x^*x) < \infty\}$ est dense (en norme) dans B et semi-continu inférieurement (s.c.i.) s'il l'est pour la topologie normique sur B^+.

Si G est un groupe localement compact, on construit un poids canonique φ sur $\mathrm{C}^*(\mathrm{G})$, semi-fini et semi-continu inférieurement (s.c.i.) tel que $\varphi(f) = f(e)$ pour $f \in L^1(\mathrm{G})$ suffisamment régulière. C'est le poids de Plancherel. Quand G n'est pas unimodulaire, ce poids n'est pas une trace. Soit alors Δ le module de G :

$$d(t^{-1}) = \Delta(t)^{-1}dt, \qquad d(ts) = \Delta(s)dt. \tag{10}$$

Le poids de Plancherel vérifie la condition KMS_1 relativement au groupe à un paramètre $\sigma_t \in \mathrm{Aut}(\mathrm{C}^*(\mathrm{G}))$ tel que :

$$\sigma_t(f)(s) = f(s)\Delta(s)^{it}, \qquad \forall s \in \mathrm{G}, \quad t \in \mathbb{R}. \tag{11}$$

Les groupes $\mathrm{P_K}$, K=$\mathbb{Q}_p$ et $\mathrm{P}_{\mathrm{A}_f}$, ne sont pas unimodulaires et le module Δ est donné par l'égalité :

$$\Delta\left(\begin{bmatrix} 1 & n \\ 0 & h \end{bmatrix}\right) = |h|. \tag{12}$$

L'idempotent $e \in \mathrm{C}^*(\mathrm{P}_{\mathrm{A}_f})$ (prop. 5) est invariant par le groupe σ_t d'automorphismes modulaires du poids de Plancherel et la restriction de σ_t à l'algèbre réduite $\mathrm{C}^*(\mathbb{N}^*) \simeq \mathrm{C}^*(\mathrm{P}_{\mathrm{A}_f})_e$ est identique au groupe d'évolution de la proposition 2.4.

THÉORÈME 6.

1. Pour tout $\beta > 0$ il existe (à normalisation près) un unique poids semi-fini semi-continu inférieurement (s.c.i.) et KMS_β sur le système dynamique $(\mathrm{C}^*(\mathrm{P}_{\mathrm{A}_f}), \sigma_t)$.

2. Pour $\beta = 1$, φ_β est le poids de Plancherel. Le poids φ_β est factoriel de type III_1 pour $\beta \in]0, 1]$ et le facteur associé est le facteur d'Araki-Woods R_∞ [1].

3. La C*-algèbre $\mathrm{C}^*(\mathrm{P}_{\mathrm{A}_f})$ est canoniquement isomorphe au produit croisé de $\mathrm{C}_0(\mathrm{A}_f)$ par l'action par homothéties du groupe A_f^* et pour $\beta > 1$, le poids φ_β est le poids dual de la mesure μ_β :

$$\mu_\beta(f) = \zeta(\beta)^{-1} \int_{\mathrm{A}_f^*} |j|^\beta f(j) d^*j$$

où d^*j désigne la mesure de Haar sur A_f^*. Ce poids φ_β est factoriel de type I_∞ ($\beta > 1$).

L'isomorphisme $\mathrm{C}^*(\mathrm{P}_{\mathrm{A}_f}) = \mathrm{C}_0(\mathrm{A}_f) \rtimes \mathrm{A}_f^*$ dépend du choix de l'isomorphisme de Fourier entre A_f et le groupe dual. Pour $f \in \mathrm{C}_0(\mathrm{A}_f)$ suffisamment régulière la fonction $\beta \to \mu_\beta(f)$ se prolonge en une fonction méromorphe dans $\mathbb{C}$ ([8], [9]) et l'égalité $\widehat{\mu}_\beta = \varphi_\beta$ persiste pour $0 < \beta < 1$.

Étudions maintenant la relation entre les C*-algèbres $\mathrm{C}^*(\mathrm{P}_{\mathrm{A}_f}) = \mathrm{B}$ et $\mathrm{C}^*(\mathbb{N}^*) = \mathrm{B}_e$ grâce au bimodule Be des fonctions sur $\mathrm{P}_{\mathrm{A}_f}/\mathrm{P}_{\mathrm{R}}$. Rappelons quelques généralités sur les C*-modules et les représentations associées. Étant donnée une C*-algèbre C et un module à droite $\mathscr{E}$ sur C, muni d'une application sesquilinéaire $\mathscr{E} \times \mathscr{E} \to \mathrm{C}$, notée $\langle \xi, \eta \rangle$; $\xi, \eta \in \mathscr{E}$, on dit que $\mathscr{E}$ est un C*-module sur C si, et seulement si, les conditions suivantes sont vérifiées :

(α) $\langle \xi a, \eta b \rangle = a^* \langle \xi, \eta \rangle b, \ \ \forall a, b \in \mathrm{C}\ ;\ \forall \xi, \eta \in \mathscr{E}$

(β) $\langle \xi, \xi \rangle \in \mathrm{C}^+, \ \ \forall \xi \in E$

(γ) $\mathscr{E}$ est complet pour la norme $\xi \to \|\langle \xi, \xi \rangle\|^{1/2}$.

On note $\mathrm{End}_{\mathrm{C}}(\mathscr{E})$ la C*-algèbre des endomorphismes de $\mathscr{E}$.

LEMME 7. *Soient* C *une* C*-algèbre unifère, $\mathscr{E}$ un* C*-module sur* C, $\sigma_t \in \mathrm{Aut}(\mathrm{C})$ *un groupe à un paramètre d'automorphismes, φ_β un état* KMS_β *sur* C, *et $\mathfrak{h}_{\varphi_\beta}$ l'espace de Hilbert de la représentation* GNS *de* C *associée à φ_β.*

(a) Soit $\mathfrak{h}_\beta$ la complétion de $\mathscr{E}$ pour le produit scalaire : $\langle \xi, \eta \rangle = \varphi_\beta(\langle \xi, \eta \rangle), \ \forall \xi, \eta \in \mathscr{E}$. Alors l'action de $\mathrm{End}_{\mathrm{C}}(\mathscr{E})$ dans $\mathscr{E}$ se prolonge par continuité à $\mathfrak{h}_\beta$.

(b) Il existe une unique représentation unitaire de C^0 dans $\mathfrak{h}_\beta$ telle que $\rho(a)\xi = \xi \sigma_{-i\beta/2}(a), \ \forall \xi \in \mathscr{E}, a \in \mathrm{C}$.

La démonstration résulte de l'identification de $\mathfrak{h}_\beta$ avec le produit tensoriel de C*-modules $\mathscr{E} \otimes_{\mathrm{C}} \mathfrak{h}_{\varphi_\beta}$.

Considérons alors le C*-module sur $\mathrm{C}^*(\mathbb{N}^*)$ obtenu en munissant Be du produit scalaire $\langle \xi, \eta \rangle = \xi^* \eta \in e\mathrm{B}e = \mathrm{C}^*(\mathbb{N}^*), \mathrm{B} = \mathrm{C}^*(\mathrm{P}_{\mathrm{A}_f})$. Pour $\beta \in]0, \infty[$, soit φ_β l'unique état KMS_β sur $\mathrm{C}^*(\mathbb{N}^*)$ et $\mathfrak{h}_\beta$ l'espace de Hilbert associé par le lemme 7 au couple $(\mathscr{E}, \varphi_\beta)$. Le lemme 7 (a) montre que la

C*-algèbre $C^*(P_A)$ et donc le groupe P_A sont représentés unitairement dans $\mathfrak{h}_\beta$.

Par construction $\mathscr{E}$ est un espace de fonctions sur l'espace homogène $\Delta = P_{A_f}/P_R$. Pour toute place finie p le quotient $T_p = P_{\mathbb{Q}_p}/P_{\mathbb{Z}_p}$, est l'arbre de $SL(2,\mathbb{Q}_p)$ avec un bout privilégié et Δ est le produit restreint de ces arbres. L'action de P_A sur Δ préserve cette structure.

Le sous-groupe $P_\mathbb{Q} \subset P_A$ agit transitivement sur Δ que l'on identifie ainsi à $P_\mathbb{Q}/P_\mathbb{Z}$. Pour tout $\alpha \in \Delta$, soit $\varepsilon_\alpha \in \mathscr{E}$ la fonction caractéristique de $\{\alpha\} \subset \Delta$.

LEMME 8. *Soit $\beta \in]0,+\infty[$. Les vecteurs $\varepsilon_\alpha, \alpha \in \Delta$, sont totaux dans l'espace de Hilbert $\mathfrak{h}_\beta$. On $\|\varepsilon_\alpha\| = 1$ et le produit scalaire $\langle \varepsilon_{\alpha'}, \varepsilon_\alpha \rangle$ est déterminé par la fonction de type positif $\Psi_\beta(g) = \langle g\varepsilon_\alpha, \varepsilon_\alpha \rangle_\beta, g \in P_\mathbb{Q}$ donnée par :*

(α) $\Psi_\beta(g) = 0$ si $g \notin N = \left\{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} ; n \in \mathbb{Q} \right\}$

(β) $\Psi_\beta \left(\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \right) = \prod p^{-k_p \beta}(1 - p^{\beta-1})(1-p^{-1})^{-1}$

où $b = \prod p^{k_p}$ est la décomposition facteurs premiers du dénominateur de la fraction en irréductible $n = a/b$.

Pour $\beta = 1$ les vecteurs $\varepsilon_x, x \in \Delta$, forment une base orthonormale de $\mathfrak{h}_\beta$ de sorte que $\mathfrak{h}_1 = l^2(\Delta)$. En général, la décomposition $\Delta = \bigcup \Delta_k, k \in \mathbb{Q}_+^*$ de Δ en orbites de N : $\Delta_k = N \begin{bmatrix} 1 & 0 \\ 0 & k \end{bmatrix} \varepsilon_1$ donne une décomposition de $\mathfrak{h}_\beta$ en sous espaces $\mathfrak{h}_{\beta,k}$ deux à deux orthogonaux.

Nous déterminons le commutant de $P_\mathbb{Q}$ dans $\mathfrak{h}_\beta$ grâce à la C*-algèbre "de Hecke" suivante. Les orbites de l'action de $P_\mathbb{Z}$ à gauche dans $\Delta = P_\mathbb{Q}/P_\mathbb{Z}$ sont finies, leur longueur définit une fonction $\alpha \to l(\alpha)$ de Δ dans $\mathbb{N}^*$. L'algèbre involutive $\mathscr{H}_f$ des fonctions $P_\mathbb{Z}$ biinvariantes sur $P_\mathbb{Q}$, à support fini dans $P_\mathbb{Q}/P_\mathbb{Z}$ est définie par :

(a) $(f_1 * f_2)(g) = \sum_{P_\mathbb{Q}/P_\mathbb{Z}} f_1(g_1) f_2(g_1^{-1} g)$

(b) $f^*(g) = \overline{f}(g^{-1})$.

L'algèbre $\mathscr{H}_f$ contient comme sous-algèbre commutative l'algèbre de Hecke des fonctions $PSL(2,\mathbb{Z})$-biinvariantes sur $PGL^+(2,\mathbb{Q})$, car $PGL^+(2,\mathbb{Q})$ agit transitivement sur Δ qui s'identifie à $PGL^+(2,\mathbb{Q})/PSL(2,\mathbb{Z})$.

Pour toute double classe $\gamma \in P_\mathbb{Z} \backslash P_\mathbb{Q} / P_\mathbb{Z}$, soient $\delta(\gamma) = l(\gamma)/l(\gamma^{-1})$ et $e_\gamma \in \mathscr{H}_f$ la fonction caractéristique de $\{\gamma\}$.

PROPOSITION 9. *Soit $\beta \in]0,+\infty[$.*

1. *L'égalité suivante définit une représentation unitaire ρ_β de l'algèbre opposée $\mathscr{H}_f^o$ dans $\mathfrak{h}_\beta$*

$$\rho_\beta(e_\gamma)\varepsilon_\alpha = \delta(\gamma)^{\beta/2} \sum_{\alpha' \in \alpha \cdot \gamma} \varepsilon_{\alpha'}.$$

2. $\rho_\beta(\mathscr{H}_f^o)$ *engendre le commutant de l'action de* $\mathrm{P}_\mathbb{Q}$ dans $\mathfrak{h}_\beta$.

3. *La norme de* $\rho_\beta(x), x \in \mathscr{H}_f$, *est indépendante de* β *et définit par complétion une* C*-*algèbre* $\mathscr{H}$ *à laquelle* ρ_β *se prolonge.*

4. *Le vecteur* ε_1 *est séparateur pour* $\rho_\beta(\mathscr{H})''$ *et définit un état* $\varphi_\beta(x) = \langle \rho_\beta(x)\varepsilon_1, \varepsilon_1\rangle$ *sur* $\mathscr{H}$ *qui est* KMS_β *relativement au groupe d'automorphismes* $\sigma_t \in \mathrm{Aut}(\mathscr{H}), \sigma_t(e_\gamma) = \delta(\gamma)^{it} e_\gamma$.

Le sous espace cyclique $\mathfrak{h}_\beta^{(1)} = \overline{\rho_\beta(\mathscr{H})\varepsilon_1}$ est l'espace des vecteurs fixes pour le sous groupe $\mathbb{Z} \subset \mathbb{N} \subset \mathrm{P}_\mathbb{Q}$.

Comme $\mathrm{P}_\mathbb{Q}$ commute avec $\rho_\beta(\mathscr{H})$, l'action de $\mathbb{Q}^*$ dans $\mathscr{L}(\mathfrak{h}_\beta)$ par automorphismes intérieurs laisse $\rho_\beta(\mathscr{H})$ invariant point par point, de sorte que l'extension de cette action à $\mathrm{A}_f^* \subset \mathrm{P}_{\mathrm{A}_f}$ définit par passage au quotient une action par automorphismes $\theta_j \in \mathrm{Aut}(\mathscr{H})$, indépendante de β, du groupe compact $\mathrm{C}{=}\mathrm{A}_f^*/\mathbb{Q}^*$ des classes d'idèles finies. L'action de C sur $\mathscr{H}$ commute avec l'action σ_t de $\mathbb{R}$. La C*-algèbre $\mathscr{H}^\mathrm{C} = \{x \in \mathscr{H}\ ; \theta_j(x) = x,\ \forall j \in \mathrm{C}\}$ des points fixes de C est canoniquement isomorphe à la C*-algèbre $\mathrm{C}^*(\mathbb{N}^*)$. La C*-algèbre $\mathscr{H}^\mathbb{R} = \{x \in \mathscr{H}\ ;\ \sigma_t(x) = x, \forall t \in \mathbb{R}\}$ est canoniquement isomorphe à la C*-algèbre $\mathrm{C}^*(\mathbb{Q}/\mathbb{Z})$ du groupe discret $\mathbb{Q}/\mathbb{Z}$. Le théorème suivant, qui est le résultat principal de cette Note, montre l'existence d'une transition de phase pour $\beta = 1$, avec brisure spontanée de symétrie, pour le système dynamique non commutatif $(\mathscr{H}, \sigma_t)$.

Théorème 10.

(a) *Pour* $0 < \beta \leq 1$, *il existe un unique état* KMS_β *sur* $\mathscr{H}$ *(pour l'évolution* σ_t*) ; cet état est factoriel de type* III_1, *invariant par* C *et sa restriction à* $\mathrm{C}^*(\mathbb{Q}/\mathbb{Z})$ *est la fonction de type positif* Ψ_β.

(b) *Pour* $\beta > 1$, *les états* KMS_β *sur* $\mathscr{H}$ *et extrémaux sont de type* I *et paramétrés par les caractères injectifs* $\chi : \mathbb{Q}/\mathbb{Z} \to \mathbb{C}^*$ *; la restriction de* $\varphi_{\beta,\chi}$ *à* $\mathrm{C}^*(\mathbb{Q}/\mathbb{Z})$ *est donnée par l'égalité :*

$$\varphi_{\beta,\chi}(e_\gamma) = \zeta(\beta)^{-1} \sum_{n=1}^{\infty} n^{-\beta} \chi(\gamma)^n.$$

L'action du groupe compact C sur l'ensemble des états extrémaux pour $\beta > 1$ est non triviale et c'est l'action naturelle du groupe de Galois de l'extension abélienne maximale de $\mathbb{Q}$. Pour $\beta = 1$, la représentation de $\mathrm{P}_\mathbb{Q}$ dans $\mathfrak{h}_1$ est la représentation induite de la représentation triviale de $\mathrm{P}_\mathbb{Z}$. Qu'elle soit factorielle et de type III a été démontré indépendamment par Binder ([2]).

Corollaire 11. *Pour* $\beta \in]0, 1]$ *la représentation de* $\mathrm{P}_\mathbb{Q}$ *dans* $\mathfrak{h}_\beta$ *est factorielle de type* III_1. *Elle est réductible et de type* I_∞ *pour* $\beta > 1$.

Bien que l'étude ci-dessus soit limitée à l'aspect "théorie de la mesure" du système dynamique non commutatif $(\mathscr{H}, \sigma_t)$, l'opérateur H_b admet une racine carrée supersymétrique D ([6], [7]) qui permet de définir sur $\mathscr{H}$ un module θ-sommable et d'en définir la géométrie non commutative [4]. Dans une Note ultérieure, nous étudierons cette géométrie ainsi que l'analogue des résultats ci-dessus pour un corps global arbitraire.

Note remise le 6 avril 1992, acceptée le 9 avril 1992.

Références bibliographiques

[1] H. Araki, E. J. Woods, A classification of factors, *Publ. Res. Inst. Math. Sci. Kyoto Univ.*, 4, 1968, p. 51-130.

[2] M. Binder, Induced factor representations of discrete groups and their type, *J. Funct. Anal.* (à paraître).

[3] B. E. Blackadar, The regular representation of restricted direct product groups, J. Funct. Anal., 25, 1977, p. 267-274.

[4] A. Connes, *Géométrie non commutative*, InterEditions, Paris, 1990.

[5] P. A. M. Dirac, The quantum theory of the emission and absorption of radiation, *Proc. Roy. Soc. London, Ser. A*, 114, 1927, p. 243-265.

[6] B. Julia, Statistical theory of numbers, in *Number Theory and Physics, Les Houches Winter School*, J.-M. Luck, P. Moussa et M. Waldschmidt éd., Springer-Verlag, 1990.

[7] D. Spector, Supersymmetry and the Möbius inversion function, *Comm. Math. Phys.*, 127, 1990, p. 239-252.

[8] J. Tate, Fourier analysis in number fields and Hecke's zeta function, in *Algebraic Number Theory*, J. W. S. Cassels et A. Fr{ohlich éd., Academic-Press, 1967.

[9] A. Weil, Fonction zêta et distributions, *Séminaire Bourbaki*, n° 312, juin 1966.

I.H.É.S., 35, route de Chartres, 91440 Bures-sur-Yvette.

Une découverte géométrique concernant certaines décompositions de Goldbach (Denise Vella-Chemla, 17 août 2023).

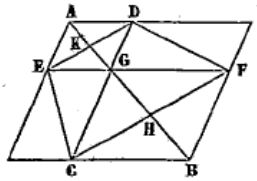
On s'intéresse aux trois décompositions de Goldbach de 98 que sont $19 + 79 = 31 + 67 = 37 + 61$.

On trouve d'abord dans le livre "La géométrie grecque" de Paul Tannery aux éditions Jacques Gabay la figure suivante, vers la toute fin du livre (ce livre de géométrie ne contient que deux figures) :

Ce lemme est la réciproque d'Euclide, I, 43. Il s'agit de prouver que, si un parallélogramme AB est découpé en quatre autres ADGE, DF, FGCB, CE, en sorte que DF et CE soient équivalents, le sommet commun G sera sur la diagonale AB (*fig.* 1).

Pour le prouver, Héron prolonge AG jusqu'à la rencontre en H avec FC, et joint HB. Il s'agit de prouver que HB est dans le prolongement de AH.

Fig. 1.



Les autres lignes de la figure étant tracées, « les aires DF, EC étant égales, les triangles DGF, ECG seront équivalents. Ajoutant à chacun le triangle GCF, les triangles DCF, ECF seront équivalents. Comme ils ont même base CF, d'après (40), CF sera parallèle à DE. Mais, d'après (34), (29) et (26), les triangles AEK, DKG seront égaux : donc EK = KD; donc, d'après le lemme II, CH = HF. Mais (34) BF = CG et les angles BFH = HCG. Donc (4) les triangles sont égaux, BH = HG et les angles BHF = CHG. Ajoutant de part et d'autre l'angle GHF, la somme des angles CHG + GHF = BHF + GHF. Mais la première somme est égale à deux droits, donc aussi la seconde. Ainsi, du point H de la droite CF, on a mené, de part et d'autre de cette droite, HA et HB qui font avec elle et d'un même côté des angles dont la somme est de deux droits. Donc HA et HB sont en ligne droite ».

C. Q. F. D.

FIGURE 1 : *page 172 du livre "Géométrie grecque" de Paul Tannery*

Alors on utilise `GeoGebra`, on reproduit les parallélogrammes de Héron, et on prend quelques mesures.

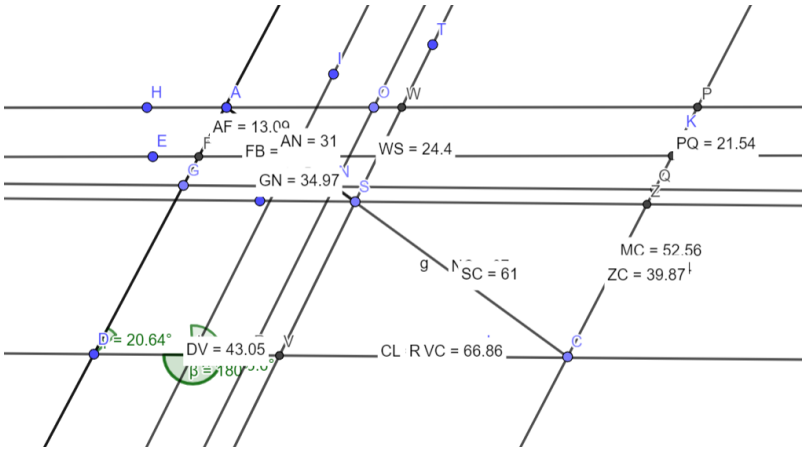


FIGURE 2 : *essai en* `GeoGebra` *avec des parallélogrammes*

Enfin, on "rectangule" pour n'avoir qu'une solution à étudier. Ça donne cette figure un peu brouillonne.

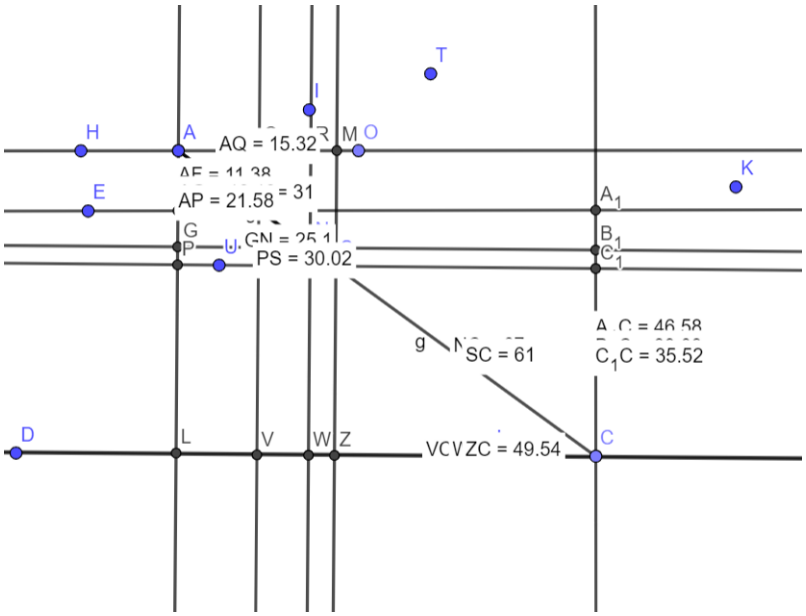


FIGURE 3 : *essai en* `GeoGebra` *avec des rectangles*

Voyons dans un tableau la valeur du nombre premier recherché p, les valeurs a et b proposées par `GeoGebra` pour les côtés du rectangle dont ce nombre premier est la diagonale (dans un premier temps, intéressons-nous aux seuls nombres premiers décomposants de Goldbach de 98) :

p	a	b	c	$98-p$	a	b	c
19	11.38	15.32	19.08	79	46.58	64.24	79.35
31	18.19	25.1	30.998	67	39.03	54.46	67.0017
37	21.58	30.02	36.97	61	35.52	49.54	60.9580

Et là, les nombres, obtenus par la fonctionnalité de recherche de mesure des segments offerte par `GeoGebra`, interpellent, on ne peut pas ne pas constater des coïncidences troublantes au niveau

des parties fractionnaires, alors on approxime les parties fractionnaires des nombres proposés par `GeoGebra` par des parties fractionnaires connues (les demis, les quarts, les huitièmes, les tiers, les neuvièmes, et leurs multiples ...).

Pour obtenir 19, ou avoisinant, on va prendre $11 + \frac{1}{3}$ au lieu de 11.38 (qui est d'ailleurs approximatif) et $15 + \frac{1}{3}$ en place de 15.32.

Pour obtenir 79, son complémentaire, au lieu de 46.58, on va prendre $46 + \frac{1}{2}$ et au lieu de 64.24, on va prendre $64 + \frac{1}{4}$.

Et on réitère pour la décomposition $31 + 67$ et pour la décomposition $37 + 61$.

Voici le tableau qui montre les valeurs des diagonales pour les valeurs de remplacement d, e et f en place des a, b, c[1].

p	d	e	f	$98 - p$	d	e	f
19	$11 + \frac{1}{3}$	$15 + \frac{1}{3}$	19.067	79	$46 + \frac{1}{2}$	$64 + \frac{1}{4}$	79.31149
31	$18 + \frac{1}{9}$	$25 + \frac{1}{9}$	30.96094	67	39	$54 + \frac{1}{2}$	67.0167
37	$21 + \frac{2}{3}$	$30 + \frac{1}{9}$	37.096133	61	$35 + \frac{1}{2}$	$49 + \frac{1}{2}$	60.91387

Ce qui surprend, c'est que pour les largeurs (petits côtés des rectangles), on a utilisé exclusivement des puissances de 3 pour obtenir leur partie fractionnaire, alors que pour les longueurs (grands côtés des rectangles), on a utilisé exclusivement des puissances de 2 pour obtenir leur partie fractionnaire, et on voit qu'ainsi, on a bien approximé les nombres premiers décomposants de Goldbach de 98.

Cet exemple est à relier à la musique : les mélodies qui sont harmonieuses à notre oreille le sont parce qu'il se trouve que $2^{19} \simeq 3^{12}$[2]. Dans l'exemple présenté ci-dessus, ce sont les proportions des rectangles "de Goldbach" qui pourraient être harmonieuses : elles mettraient en rapport des longueurs proportionnelles, les unes à base de puissances de 3 (y compris négatives) et les autres faisant intervenir des puissances de 2.

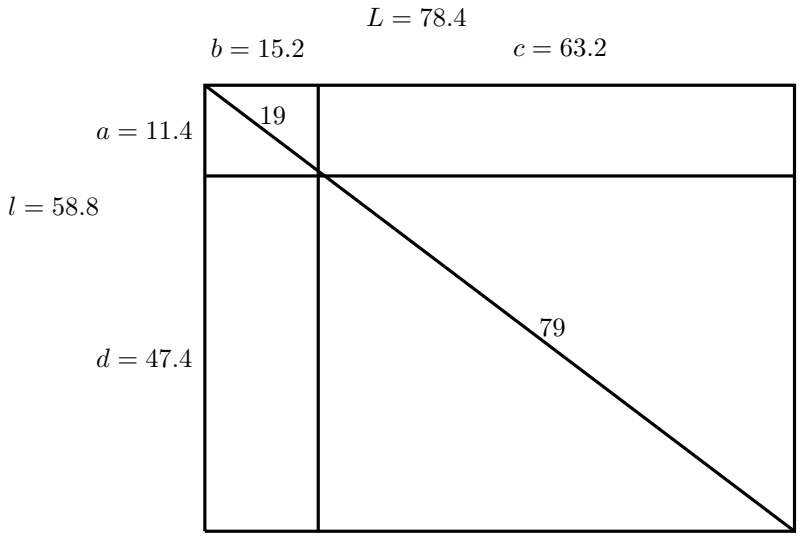
On complète maintenant le tableau par les mesures pour tous les impairs pour voir si les décompositions de Goldbach (i.e. de 98 en somme de deux nombres premiers) se distinguent des autres décompositions (i.e. sommes de deux impairs contenant un nombre composé au moins).

On a linéarisé le problème : la formule d'obtention des largeurs des rectangles est $\frac{3}{5} + \frac{6}{5}k$ et celle d'obtention des longueurs est $\frac{4}{5} + \frac{8}{5}k$.

1. calculées par la formule de Pythagore $\sqrt{l^2 + L^2}$ dans un rectangle de largeur l et de longueur L.
2. On pourra se reporter à , http://denise.vella.chemla.free.fr/transc-AC-dualite.pdf ou encore à l'article de blog *Music of spheres* http://noncommutativegeometry.blogspot.com/2012/, ou bien à la transcription d'une vidéo de Pierre Cartier à laquelle on n'a plus accès http://denise.vella.chemla.free.fr/musique-spheres-PC-EK.pdf et qui était accessible précédemment sur le site de Jean-Michel Kantor.

k	$\frac{3}{5}+\frac{6}{5}k$	$\frac{4}{5}+\frac{8}{5}k$	$n-k$	$a+kb$	$a'+kb'$
1	0.6	0.8	97	58.2	78.6
3	1.8	2.4	95	57	76
5	3	4	93	35.2	74.4
7	4.2	5.6	91	54.6	72.8
9	5.4	7.2	89	53.4	71.2
11	6.6	8.8	87	52.2	69.6
13	7.8	10.4	85	51	68
15	9	12	83	49.8	66.4
17	10.2	1.6	81	48.6	64.8
19	11.4	15.2	79	47.4	63.2
21	12.6	16.8	77	46.2	61.6
23	13.8	18.4	75	45	60
25	15	20	73	43.8	58.4
27	16.2	21.6	71	42.6	56.8
29	17.4	12.2	69	41.4	55.2
31	18.6	24.8	67	40.2	53.6
33	19.8	26.4	65	39	52
35	21	28	63	37.8	50.4
37	22.2	29.6	61	36.6	48.8
39	23.4	31.2	59	35.4	47.2
41	24.6	32.8	57	34.2	45.6
43	25.8	34.4	55	33	44
45	27	36	53	31.8	42.4
47	28.2	37.6	51	30.6	40.8
49	29.4	39.2	49		

Trouver les longueurs c et d en fonction de a et b est un peu prise de tête, on a ce dessin-là :



et ces formules-là :

$$\begin{aligned} 98^2 &= (a+d)^2 + (b+c)^2 \\ &= a^2 + 2ad + d^2 + b^2 + 2bc + c^2 \end{aligned}$$

On connaît les valeurs de a et b et leurs formules linéaires de calcul, on arrive à une formule telle que celle ci-dessous, on doit se débrouiller...

$$98 - a^2 - b^2 = d^2 + \left(\tfrac{6}{5} + \tfrac{12}{5}k\right) d + c^2 + \left(\tfrac{8}{5} + \tfrac{16}{5}k\right) c$$

Il s'agira maintenant de voir avec ce qu'on a réalisé si les décompositions de Goldbach n'ont pas un comportement particulier (de minimisation ou maximisation par exemple) des distances aux nombres de parties fractionnaires en lien avec 3 pour les largeur et longueur du rectangle supportant le petit sommant, et en lien avec 2 pour les largeur et longueur du rectangle supportant le grand sommant.

(poursuite du travail, 19.8.2023)
On utilise d'abord google, puis python pour voir l'allure des surfaces $z = x^2+y^2-\sqrt{2}xy$ et $z = 98$ qu'on a parcourues sans trop le réaliser ci-dessus.

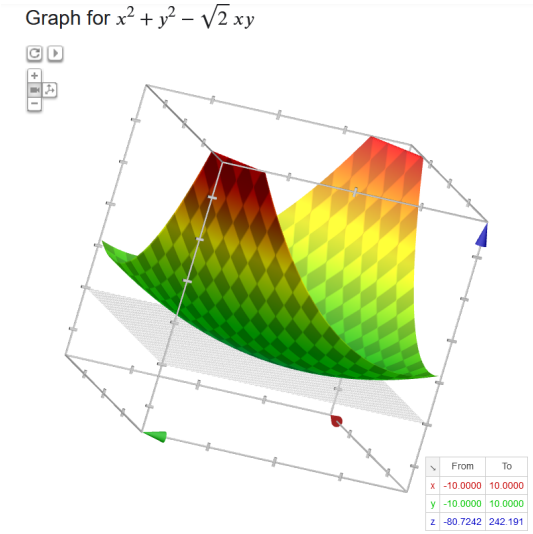


FIGURE 4 : *essai avec le grapheur de fonctions google*

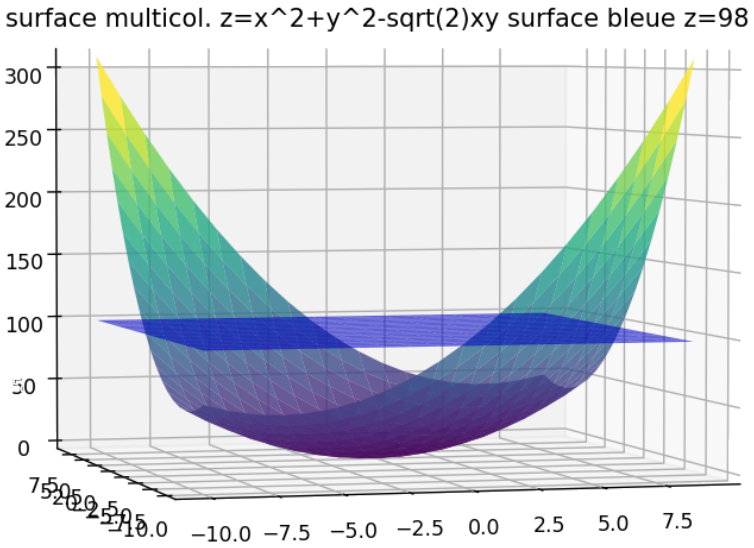


FIGURE 5 : *essai en python*

Programme d'obtention de la surface (dite "hamac" !) :

```
import numpy as np
from mpl_toolkits.mplot3d import Axes3D
import matplotlib.pyplot as plt
import math
from numpy import sqrt
from matplotlib import cm

def f(x, y):
   return x**2 + y**2 - sqrt(2)*x*y

def g(x,y):
   return x*0 + 98

x = np.arange(-10, 10)
y = np.arange(-10, 10)
X, Y = np.meshgrid(x, y)
Z = f(X, Y)

xp = np.arange(-10, 10)
yp = np.arange(-10, 10)
XP, YP = np.meshgrid(xp, yp)
ZP = g(XP,YP)

fig = plt.figure()
ax = plt.axes(projection = '3d')
ax.set_title('surface multicol. z=x^2+y^2-sqrt(2)xy   surface bleue z=98')
ax.plot_surface(X, Y, Z, alpha = 0.8, cmap = 'viridis')
ax.plot_surface(XP, YP, ZP, alpha = 0.6, color='blue')
plt.show()
```

FIGURE 6 : *Héron à la lunette astronomique*

On trouve sur la frise de certains mathématiciens ici https://fr.mathigon.org/timeline une courte biographie de Héron d'Alexandrie.

Héron d'Alexandrie (Ἥρον ὁ Ἀλεξανδρξυς, premier siècle après J. C.) était un mathématicien grec et un ingénieur. Il vécut dans la ville d'Alexandrie en Égypte, et est l'un des plus grands "expérimentateurs" de l'Antiquité.

Ses inventions incluent un orgue hydraulique, des moulins à vent, des pantographes[3], ainsi qu'une turbine à vapeur radiale appelée éolipile, sphère de vent ou moteur de Héron.

La formule de Héron permet de calculer l'aire d'un triangle quelconque, en utilisant juste les longueurs de ses côtés a, b, c :

$$\text{Aire} = \sqrt{\frac{\text{Périmètre}}{2}\left(\frac{\text{Périmètre}}{2} - a\right)\left(\frac{\text{Périmètre}}{2} - b\right)\left(\frac{\text{Périmètre}}{2} - b\right)}$$

3. un *pantographe* est un instrument composé de tiges articulées, qui sert à reproduire mécaniquement un dessin.

Petite remarque sur les écritures en base, (Denise Vella-Chemla, août 2023).

Dans l'article de Connes et Consani https://arxiv.org/pdf/2208.08339.pdf, sont utilisés (page 8) des polynômes de la forme

$$P(X) = \sum_{j=0}^{k} a_j X^j, \quad a_j \in \{-1, 0, 1\}, \forall j,$$

avec $X = 3$. Il y a une subtilité pour l'addition des polynômes car ajouter deux coefficients égaux à -1 ou $+1$ "fait sortir" de l'ensemble des coefficients possibles. Une preuve est fournie de l'isomorphisme entre cet ensemble de polynômes muni de l'addition telle que définie et de la multiplication et l'anneau $\mathbb{Z}$.

Ce qui m'étonne, plus loin, c'est le rôle "spécial" de $\mathbb{F}_3$. Les auteurs écrivent :

> *Conceptually, one sees that the above construction is described by the addition rule of two Witt vectors over* $\mathbb{F}3$. *The number 3 is the only prime for which the Witt vectors with only finitely many non-zero components form an additive subgroup of the Witt ring.*

Cela vient après la proposition page 9 :

> *We obtain the following intriguing conclusion*
>
> > Proposition 5.2. *The set of polynomials as in (5.1), under the addition stated in Proposition 5.1, and the unique associated product, forms a ring isomorphic to* $\mathbb{Z}$.

Et cela m'étonne car j'aurais vraiment cru que "ça marchait" pour toute base impaire $b = 2k + 1$ avec les coefficients à prendre dans $[-k, \ldots, -1, 0, 1, \ldots, k]$.

Pour illustrer un peu le propos, la table 1 ci-après donne quelques exemples de la bijection de $\mathbb{Z}$ vers les n-uplets de coefficients lorsque les polynômes sont considérés jusqu'au degré 4 pour la base $X = 3$. ($81 = 3^4$) Les nombres de $-40 = -\frac{3^4-1}{2}$ à $40 = \frac{3^4-1}{2}$ sont bien tous couverts. Pour bien voir la symétrie, lire les $3^{\text{ièmes}}$ et $4^{\text{ièmes}}$ ensembles de colonnes de bas en haut !

La table 2 illustre la bijection de $\mathbb{Z}$ vers les coefficients des polynômes de degré 2 au plus, jusqu'à $15^2 = 225$ pour la base 15 (un impair composé). On a démarré l'écriture à l'entier relatif -13 et jusqu'à 400, histoire de voir entrer 2 en scène en tant que troisième coefficient.

TABLE 1 : écriture en base 3 avec coefficients dans $[-1, 0, 1]$

n	3^0	3^1	3^2	3^3	n	3^0	3^1	3^2	3^3	n	3^0	3^1	3^2	3^3	n	3^0	3^1	3^2	3^3
−40	−1	−1	−1	−1	−20	1	−1	1	−1	20	−1	1	−1	1	40	1	1	1	1
−39	0	−1	−1	−1	−19	−1	0	1	−1	19	1	0	−1	1	39	0	1	1	1
−38	1	−1	−1	−1	−18	0	0	1	−1	18	0	0	−1	1	38	−1	1	1	1
−37	−1	0	−1	−1	−17	1	0	1	−1	17	−1	0	−1	1	37	1	0	1	1
−36	0	0	−1	−1	−16	−1	1	1	−1	16	1	−1	−1	1	36	0	0	1	1
−35	1	0	−1	−1	−15	0	1	1	−1	15	0	−1	−1	1	35	−1	0	1	1
−34	−1	1	−1	−1	−14	1	1	1	−1	14	−1	−1	−1	1	34	1	−1	1	1
−33	0	1	−1	−1	−13	−1	−1	−1	0	13	1	1	1	0	33	0	−1	1	1
−32	1	1	−1	−1	−12	0	−1	−1	0	12	0	1	1	0	32	−1	−1	1	1
−31	−1	−1	0	−1	−11	1	−1	−1	0	11	−1	1	1	0	31	1	1	0	1
−30	0	−1	0	−1	−10	−1	0	−1	0	10	1	0	1	0	30	0	1	0	1
−29	1	−1	0	−1	−9	0	0	−1	0	9	0	0	1	0	29	−1	1	0	1
−28	−1	0	0	−1	−8	1	0	−1	0	8	−1	0	1	0	28	1	0	0	1
−27	0	0	0	−1	−7	−1	1	−1	0	7	1	−1	1	0	27	0	0	0	1
−26	1	0	0	−1	−6	0	1	−1	0	6	0	−1	1	0	26	−1	0	0	1
−25	−1	1	0	−1	−5	1	1	−1	0	5	−1	−1	1	0	25	1	−1	0	1
−24	0	1	0	−1	−4	−1	−1	0	0	4	1	1	0	0	24	0	−1	0	1
−23	1	1	0	−1	−3	0	−1	0	0	3	0	1	0	0	23	−1	−1	0	1
−22	−1	−1	1	−1	−2	1	−1	0	0	2	−1	1	0	0	22	1	1	−1	1
−21	0	−1	1	−1	−1	−1	0	0	0	1	1	0	0	0	21	0	1	−1	1
										0	0	0	0	0					

Le programme python à tester[1] :

```
mu = [-1,0,1]
nu = [1,3,9,27]
for k4 in mu:
   for k3 in mu:
      for k2 in mu:
         for k1 in mu:
            print(k1*1+k2*3+k3*9+k4*27,' ',k1, ' ', k2, ' ', k3, ' ', k4)
```

[1] dans google colab, par exemple, ;-).

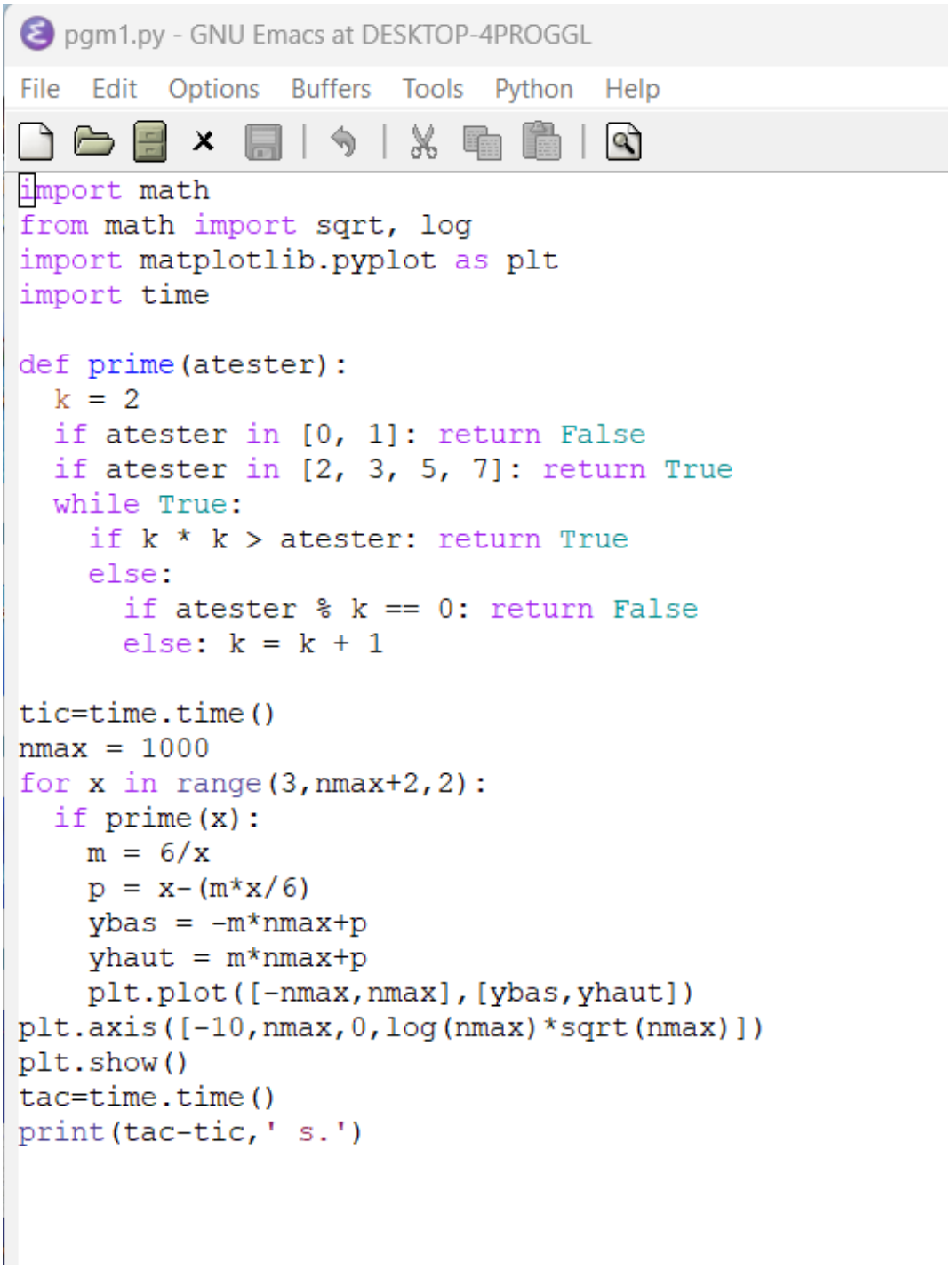
TABLE 2 : écriture en base 15 avec coefficients entiers dans $[-7, \ldots, -1, 0, 1, \ldots, 7]$

n	15^0	15^1	15^2	n	15^0	15^1	15^2	n	15^0	15^1	15^2	n	15^0	15^1	15^2
-13	2	-1	0	21	6	1	0	54	-6	4	0	88	-2	6	0
-12	3	-1	0	22	7	1	0	55	-5	4	0	89	-1	6	0
-11	4	-1	0	23	-7	2	0	56	-4	4	0	90	0	6	0
-10	5	-1	0	24	-6	2	0	57	-3	4	0	91	1	6	0
-9	6	-1	0	25	-5	2	0	58	-2	4	0	92	2	6	0
-8	7	-1	0	26	-4	2	0	59	-1	4	0	93	3	6	0
-7	-7	0	0	26	-4	2	0	60	0	4	0	94	4	6	0
-6	-6	0	0	27	-3	2	0	61	1	4	0	95	5	6	0
-5	-5	0	0	28	-2	2	0	62	2	4	0	96	6	6	0
-4	-4	0	0	29	-1	2	0	63	3	4	0	97	7	6	0
-3	-3	0	0	30	0	2	0	64	4	4	0	98	-7	7	0
-2	-2	0	0	31	1	2	0	65	5	4	0	99	-6	7	0
-1	-1	0	0	32	2	2	0	66	6	4	0	100	-5	7	0
0	0	0	0	33	3	2	0	67	7	4	0				
1	1	0	0	34	4	2	0	68	-7	5	0				
2	2	0	0	35	5	2	0	69	-6	5	0				
3	3	0	0	36	6	2	0	70	-5	5	0				
4	4	0	0	37	7	2	0	71	-4	5	0				
5	5	0	0	38	-7	3	0	72	-3	5	0				
6	6	0	0	39	-6	3	0	73	-2	5	0				
7	7	0	0	40	-5	3	0	74	-1	5	0				
8	-7	1	0	41	-4	3	0	75	0	5	0				
9	-6	1	0	42	-3	3	0	76	1	5	0				
10	-5	1	0	43	-2	3	0	77	2	5	0				
11	-4	1	0	44	-1	3	0	78	3	5	0				
12	-3	1	0	45	0	3	0	79	4	5	0				
13	-2	1	0	46	1	3	0	80	5	5	0				
14	-1	1	0	47	2	3	0	81	6	5	0				
15	0	1	0	48	3	3	0	82	7	5	0				
16	1	1	0	49	4	3	0	83	-7	6	0				
17	2	1	0	50	5	3	0	84	-6	6	0				
18	3	1	0	51	6	3	0	85	-5	6	0				
19	4	1	0	52	7	3	0	86	-4	6	0				
20	5	1	0	53	-7	4	0	87	-3	6	0				

Petite remarque personnelle : je préfère définitivement, même sans aucune démonstration à la clef, l'écriture multi-bases par les restes modulaires que j'avais appelée SNURPF (pour Système de Numération par les Restes dans les Parties Finies de $\mathbb{N}$), ou encore Snur∞ (si on utilise des restes modulaires selon tous les nombres premiers comme bases, dans l'ensemble infini des nombres premiers donc), les restes "tournant" dans les corps premiers, ce système de numérotation ayant également une représentation équivalente merveilleuse dans le langage des matrices ∞-dimensionnelles, avec plein de petites rotations sur les diagonales, et une somme de diviseurs d'Euler, qui était infernale à programmer en 2006, et qui s'avère être une bébête élévation d'une matrice à une certaine puissance, bref, un truc d'une simplicité limpide.

Rappel de programmes pour envelopper le log par des droites (Denise Vella-Chemla, août 2023).

On écrit des programmes dans le style de l'article de blog ici : https://www.cantorsparadise.com/the-twin-prime-conjecture-3671e604818e qui permettent de voir les courbes de la racine carrée ou du logarithme enveloppées par des droites de pentes de plus en plus faibles.

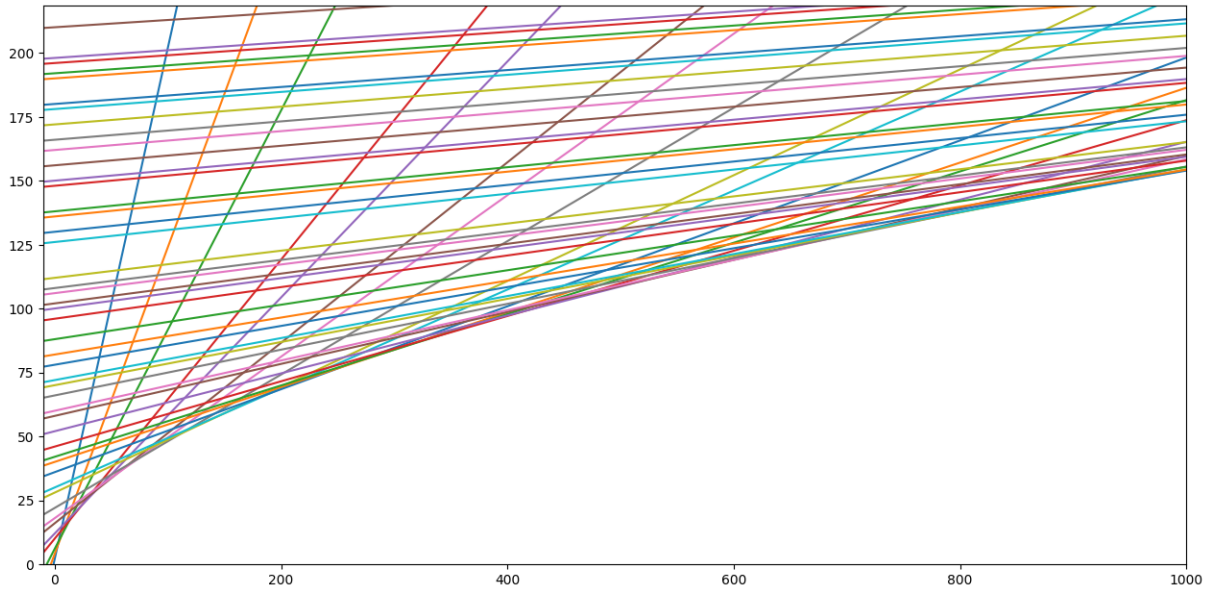


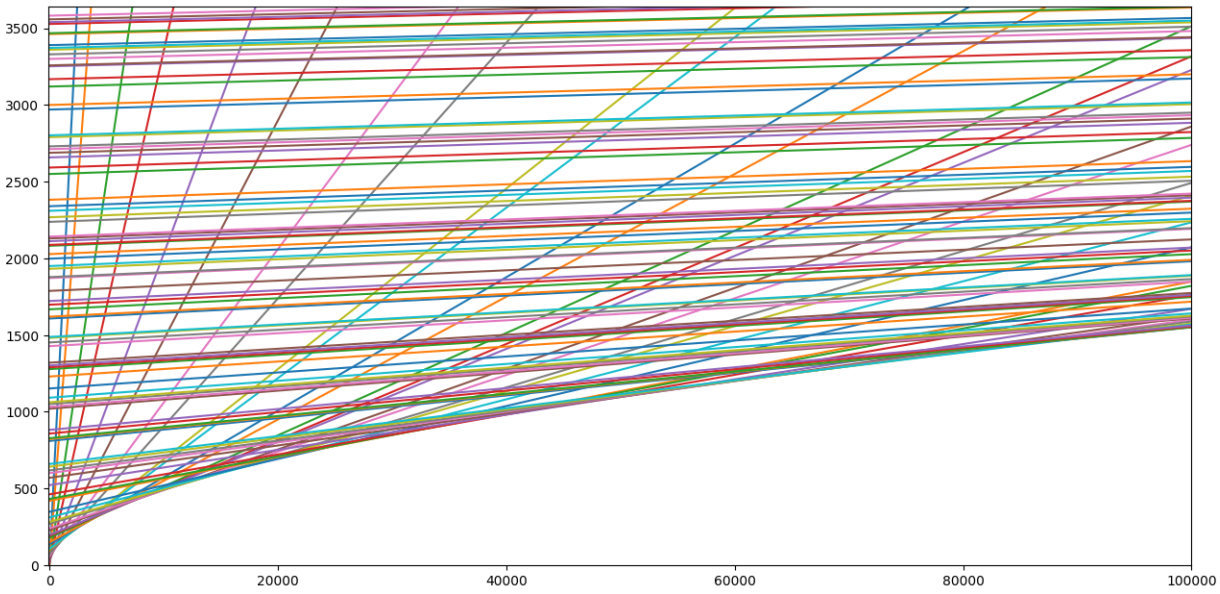

```
import math
from math import sqrt, log
import matplotlib.pyplot as plt
import time

def prime(atester):
  k = 2
  if atester in [0, 1]: return False
  if atester in [2, 3, 5, 7]: return True
  while True:
    if k * k > atester: return True
    else:
      if atester % k == 0: return False
      else: k = k + 1

tic=time.time()
nmax = 1000
for x in range(3,nmax+2,2):
  if prime(x):
    m = 6/x
    p = x-(m*x/6)
    ybas = -m*nmax+p
    yhaut = m*nmax+p
    plt.plot([-nmax,nmax],[ybas,yhaut])
plt.axis([-10,nmax,0,log(nmax)*sqrt(nmax)])
plt.show()
tac=time.time()
print(tac-tic,' s.')
```

pgm2.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Isearch Help

```
import math
from math import sqrt, log
import matplotlib.pyplot as plt
import time

def prime(atester):
  k = 2
  if atester in [0, 1]: return False
  if atester in [2, 3, 5, 7]: return True
  while True:
    if k * k > atester: return True
    else:
      if atester % k == 0: return False
      else: k = k + 1

tic=time.time()
nmax=100000
for n in range(4,nmax+2,2):
  if prime(n-1) and prime(n+1):
    m = 6/n
    p = n+1-(m*n/6)
    ybas = -m*nmax+p
    yhaut = m*nmax+p
    plt.plot([-nmax,nmax],[ybas,yhaut])
plt.axis([-100,nmax,0,log(nmax)*sqrt(nmax)])
plt.show()
tac=time.time()
print(tac-tic,' s.')
```


0
25
50
75
100
125
150
175
200
0
200
400
600
800
1000


0
500
1000
1500
2000
2500
3000
3500
0
20000
40000
60000
80000
100000

Transcription d'un extrait de *Men of mathematics* de Eric Temple Bell, pages 64 et suivantes du chapitre *Descartes, Gentleman, soldat et mathématicien*

Depuis l'automne 1641, Descartes vivait dans un petit village tranquille près de La Haye en Hollande, où habitait la princesse Elisabeth[1], qui était alors une jeune femme ayant un penchant pour l'étude, exilée à la campagne avec sa mère. La princesse semble en effet avoir été une prodige intellectuelle. Après avoir maîtrisé six langues et lu beaucoup de littérature, elle s'était tournée vers les mathématiques et les sciences, espérant trouver là des sujets plus nourrissants. Une théorie pour expliquer l'appétit inhabituel de cette remarquable jeune femme attribue sa soif de savoir à une déception amoureuse. Mais ni les mathématiques ni les sciences ne la satisfaisaient. Puis elle a découvert le livre de Descartes et elle a su qu'elle y avait trouvé ce dont elle avait besoin pour combler son vide existentiel. Une entrevue fut organisée avec le philosophe quelque peu réticent.

Il est très difficile de comprendre exactement ce qui s'est passé par la suite. Descartes était un gentleman, avec toute les craintes et la révérence d'un gentleman en ces temps galants et royaux, même pour le prince ou la princesse les moins puissants. Ses lettres sont des modèles de discrétion courtoise, mais d'une manière ou d'une autre, elles ne sonnent pas toujours tout à fait juste. Une petite remarque malveillante, citée dans un instant, en dit probablement plus sur ce qu'il pensait vraiment de la capacité intellectuelle de la princesse Elisabeth, que toutes les pages de flatteries subtiles qu'il écrivit à son élève passionnée ou à propos d'elle, en ayant un œil sur son style et l'autre sur ce qui fut publié après sa mort.

Elisabeth a insisté pour que Descartes lui donne des leçons. Officiellement, il déclara "de tous mes disciples, elle seule a parfaitement compris mon œuvre". Il ne fait aucun doute qu'il l'aimait sincèrement d'une façon paternelle, comme un chat regardant la femme d'un roi, mais croire qu'il voulait dire ce qu'il a dit comme s'il s'agissait d'une déclaration scientifique, c'est étirer la crédulité jusqu'à sa limite, à moins, bien sûr, qu'il ne l'ait entendu comme un commentaire ironique sur sa propre philosophie. Elisabeth a peut-être trop compris, car il semble être un fait que seul un philosophe comprend à fond sa propre philosophie, bien que n'importe quel imbécile puisse le penser. Quoi qu'il en soit, il ne lui a pas proposé ses leçons ni, autant que l'on sache, elle ne le lui a proposé.

Entre autres parties de sa philosophie qu'il lui exposait, il y avait la méthode de la géométrie analytique. Or il y a un certain problème de géométrie élémentaire qui peut être résolu tout simplement par la géométrie pure, et qui paraît assez facile, mais qui est un diable parfait pour que la géométrie analytique le traite sous sa stricte forme cartésienne. II s'agit de construire un cercle qui doit toucher (être tangent à) trois cercles quelconques donnés au hasard dont les centres ne se trouvent pas tous sur une ligne droite. Il y a huit solutions possibles. Le problème est un beau spécimen du genre qui n'est pas adapté à la force brute de la géométrie cartésienne élémentaire. *Elisabeth l'a résolu par les méthodes de Descartes.* C'était plutôt cruel de sa part de la laisser faire. Son commentaire en voyant sa solution est un spectacle pour n'importe quel mathématicien. Elle était assez fière de son exploit, la pauvre fille. Descartes a déclaré qu'il n'entreprendrait pas de mettre en œuvre sa solution et de construire réellement le cercle tangent requis en un mois. Si cela

éditions Touchstone et Simon & Schuster.

Traduction (assistée de google traduction) : Denise Vella-Chemla, août 2023.

[1]Fille de Frédéric, Électeur Palatin du Rhin, roi de Bohême, et petite-fille de Jacques ier d'Angleterre.

ne traduit pas son estimation de l'aptitude mathématique d'Elisabeth, il est impossible de poser question plus simple. C'était une chose méchante à dire, d'autant plus qu'elle n'avait pas compris et qu'il savait qu'elle le ferait.

Quand Elisabeth quitta la Hollande, elle correspondit avec Descartes presque jusqu'au jour de sa mort. Ses lettres contiennent beaucoup de beauté et de sincérité, mais on aurait pu souhaiter qu'il n'ait pas été aussi ébloui par l'aura de la royauté.

En 1646, Descartes vivait une retraite heureuse à Egmond, en Hollande, méditant, jardinant dans un petit terrain, et entretenant une correspondance d'une ampleur incroyable avec les intellectuels d'Europe. Son plus grand travail mathématique était derrière lui, mais il continuait à penser aux mathématiques, toujours avec pénétration et originalité. Un problème auquel il accorda une certaine attention est celui d'Achille et de la tortue de Zénon. Sa solution du paradoxe ne serait pas universellement acceptée aujourd'hui mais elle était ingénieuse pour son époque. Il avait maintenant cinquante ans et était mondialement connu, bien plus célèbre en fait qu'il n'aurait jamais voulu l'être. Le repos et la tranquillité qu'il avait désirés toute sa vie lui échappaient encore. Il continuait de faire un grand travail, mais il ne devait pas être laissé en paix pour mettre en œuvre toutes les idées qu'il avait en tête. La reine Christine de Suède avait entendu parler de lui.

Cette jeune femme un peu masculine avait alors dix-neuf ans, c'était déjà une dirigeante douée, une classiciste réputée (de cela, plus tard), une athlète nerveuse avec l'endurance physique de Satan lui-même, une chasseuse impitoyable, une cavalière experte qui ne pensait à rien d'autre qu'à être dix heures en selle sans descendre une seule fois, et enfin un morceau de féminité coriace aussi endurci au froid qu'un bûcheron suédois. À tout cela, elle combinait une certaine obtusté épaisse envers les fragilités des êtres moins épais. Elle pouvait sauter des repas ; il en était de même de ceux de ses courtisans. Comme une grenouille en hibernation, elle pouvait rester assise pendant des heures dans une bibliothèque non chauffée au beau milieu de l'hiver suédois ; ses acolytes la suppliaient à travers leurs claquements de dents d'ouvrir toutes grandes les fenêtres et de laisser entrer la joyeuse neige. Son cabinet, nota-t-elle sans scrupule, était toujours d'accord avec elle. Elle savait tout ce qu'il y avait à savoir ; ses ministres et tuteurs le lui avaient dit. Comme elle ne dormait que cinq heures par nuit, elle faisait sauter ses crapauds dans le cerceau dix-neuf heures par jour. Au moment même où cette sainte terreur a vu la philosophie de Descartes, elle a décidé qu'elle devait annexer le pauvre diable endormi comme son instructeur privé. Toutes ses études jusque-là l'avaient laissée vide et avide de davantage. Comme l'érudite Élisabeth, elle savait que seules de copieuses douches philosophiques du philosophe lui-même pouvaient assouvir sa soif de savoir et de sagesse.

Sans cette fâcheuse pointe de snobisme dans son maquillage, Descartes aurait pu résister aux flatteries de la reine Christine jusqu'à l'âge de quatre-vingt-dix ans et la laisser finir sa vie sans dents, sans cheveux, sans philosophie, sans tout. Descartes tint bon jusqu'à ce qu'elle envoie l'amiral Fleming au printemps de 1649 avec un navire pour le chercher. L'ensemble fut généreusement mis à la disposition du philosophe réticent. Descartes temporisa jusqu'en octobre. Puis, avec un dernier regard de regret à son petit jardin, il ferma la serrure et quitta Egmond pour toujours.

Sa réception à Stockholm fut bruyante, pour ne pas dire royale. Descartes n'habitait pas au Palais ;

cela lui fut épargné. Des amis importunément gentils, cependant, les Chanute, brisèrent son dernier espoir de se réserver un peu d'intimité. Ils insistèrent pour qu'il vive avec eux. Chanute était un compatriote, en fait l'ambassadeur de France. Tout aurait pu bien se passer, car les Chanute étaient vraiment très prévenants, si l'obtuse Christine ne s'était pas mis dans la tête inébranlable que cinq heures du matin était l'heure appropriée pour une jeune femme occupée et dure comme elle pour étudier la philosophie. Descartes aurait volontiers troqué toutes les reines têtues de la chrétienté contre un mois de rêverie couché à La Flèche avec l'éclairé Charlet discrètement proche pour veiller à ce qu'il ne se lève pas trop tôt. Cependant, il rampa consciencieusement hors de son lit à cette heure impie dans l'obscurité, il monta dans la voiture envoyée pour le chercher et il traversa la place la plus sombre et la plus venteuse de Stockholm jusqu'au palais où Christine était assise dans la bibliothèque glacée attendant impatiemment que sa leçon de philosophie commence à cinq heures A.M précises..

Les habitants les plus anciens déclarèrent plus tard que Stockholm n'avait jamais, de mémoire, subi un hiver aussi rigoureux. Christine semble avoir manqué d'une peau humaine normale ainsi que de nerfs. Elle ne s'apercevait de rien, mais maintenait son horrible rendez-vous avec Descartes qui y assistait sans broncher. Il essayait de rattraper son repos en se couchant l'après-midi. Elle l'en empêcha bientôt. Une académie royale suédoise des sciences était en gestation dans son activité prolifique ; Descartes fut tiré hors du lit pour la délivrer.

Il devint bientôt évident pour les courtisans que Descartes et leur reine discutaient bien plus que de philosophie lors de leurs discussions interminables. Le philosophe fatigué réalisa bientôt qu'il avait mis les deux pieds dans un nid de frelons populeux et occupé. Ils le piquaient chaque fois qu'ils le pouvaient et partout où ils le pouvaient. Soit la reine était trop épaisse pour remarquer ce qui arrivait à son nouveau favori, soit elle était assez intelligente pour piquer ses courtisans à travers son philosophe. Quoi qu'il en soit, pour faire taire les chuchotements malveillants de "l'influence étrangère", elle résolut de faire de Descartes un Suédois. Un domaine lui fut réservé par arrêté royal. Chaque mouvement désespéré qu'il faisait pour sortir du désordre ne faisait que l'enliser plus profondément. Le 1er janvier 1650, il était en Suède jusqu'au cou avec seulement un miracle qui pourrait venir de sa grossièreté, comme son seul faible espoir de se libérer un jour. Mais avec son respect inné pour la royauté, il ne pouvait se résoudre à prononcer les mots magiques qui le renverraient en Hollande, bien qu'il en ait dit beaucoup, avec une politesse courtoise, dans une lettre à sa dévouée Elisabeth. Il avait par hasard interrompu une des leçons de grec. À sa grande surprise, Descartes apprit que Christine, la célèbre classiciste, luttait contre des puérilités grammaticales qu'il avait, dit-il, maîtrisées par lui-même lorsqu'il était petit garçon. Son opinion sur sa mentalité par la suite semble avoir été respectueuse mais basse. Elle n'a pas été soulevée par son insistance pour qu'il produise un ballet pour le plaisir de ses invités lors d'une réception à la cour lorsqu'il a résolument refusé de se faire un saltimbanque en tentant à son âge de maîtriser les cabrioles majestueuses des lanciers suédois.

Bientôt Chanute tomba désespérément malade d'une inflammation des poumons. Descartes le soigna. Chanute récupéra ; Descartes tomba malade de la même maladie. La reine, alarmée, envoya des médecins. Descartes les fit sortir de la chambre. Son état s'aggrava régulièrement. Incapable dans sa maladie de distinguer l'ami de la peste, il consentit enfin à être saigné par le plus obstiné des médecins, un ami personnel qui, tout le temps, rôdait en attendant sa chance. Cela

l'acheva presque, mais pas tout à fait.

Ses bons amis les Chanute, voyant qu'il était très malade, lui proposèrent de recevoir le dernier sacrement. Il avait exprimé le désir de voir son conseiller spirituel. Recommandant son âme à la miséricorde de Dieu, Descartes fit face à sa mort calmement, disant que le sacrifice volontaire qu'il faisait de sa vie pourrait peut-être expier ses péchés. La Flèche le serra dans ses bras jusqu'au bout. Le conseiller lui demanda d'exprimer s'il souhaitait recevoir l'extrême onction. Descartes ouvrit les yeux et les ferma. Il reçut la bénédiction. C'est ainsi qu'il mourut le 11 février 1650, âgé de 54 ans, en sacrifice à la vanité démesurée d'une fille têtue", déplore Christine. Dix-sept ans plus tard, alors qu'elle avait depuis longtemps renoncé à sa couronne et à sa foi, les ossements de Descartes furent restitués à la France (tous sauf ceux de la main droite, qui furent conservés par le Trésorier général français en souvenir de son talent d'ingénieur). Sa dépouille a été réinhumée à Paris dans l'actuel Panthéon. Il devait y avoir une oraison publique, mais cela fut interdit à la hâte par ordre de la couronne, car les doctrines de Descartes étaient jugées comme encore trop récentes pour être manipulées devant le peuple. Commentant le retour de la dépouille de Descartes dans sa France natale, Jacobi remarqua qu'"il est souvent plus commode de posséder les cendres des grands hommes que de posséder les hommes eux-mêmes de leur vivant".

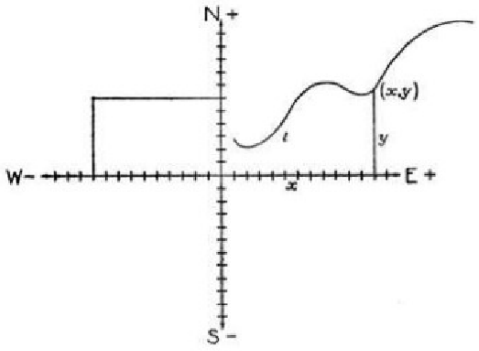
Peu de temps après sa mort, les livres de Descartes furent inscrits à l'Index de cette Église qui, acceptant la suggestion éclairée du cardinal de Richelieu du vivant de l'auteur, avait autorisé leur publication. "Cohérence, tu es un bijou !" Mais les fidèles n'étaient pas troublés par la cohérence, "l'épouvantail des petits esprits" - et le fléau des fanatiques incohérents.

⋆ ⋆ ⋆

Il ne s'agit pas ici de passer en revue les apports monumentaux que Descartes a apportés à la philosophie. Son rôle brillant dans l'aube de la méthode expérimentale ne peut pas non plus nous retenir. Ces choses sont bien en dehors du domaine des mathématiques pures dans lequel réside peut-être son plus grand travail. Il n'est donné qu'à peu d'hommes de rénover tout un pan de la pensée humaine. Descartes fut l'un de ces rares hommes. Pour ne pas occulter la brillante simplicité de sa plus grande contribution, nous la décrirons brièvement seule et laisserons de côté les nombreuses belles choses qu'il a faites en algèbre et particulièrement en notation algébrique et en théorie des équations. Cette seule chose est du plus haut ordre d'excellence, marquée par la simplicité sensible de la demi-douzaine de plus grandes contributions de tous les temps aux mathématiques. Descartes a refait la géométrie et il a rendu possible la géométrie moderne.

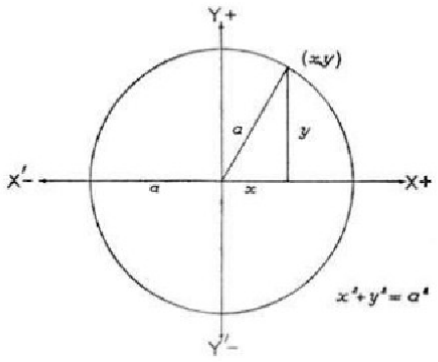
L'idée de base, comme toutes les grandes choses en mathématiques, est simple au point d'être évidente. Étendez deux lignes qui se croisent sur un plan. Sans perte de généralité, nous pouvons supposer que les lignes sont perpendiculaires les unes aux autres. Imaginez maintenant une ville tracée sur le plan américain, avec des avenues au nord et au sud, des rues à l'est et à l'ouest. L'ensemble du plan sera disposé par rapport à une avenue et une rue, appelées les axes, qui se coupent dans ce qu'on appelle l'origine, à partir de laquelle les numéros de rue-avenue sont lus consécutivement. Ainsi on voit clairement sans schéma où se trouve le 1002-Ouest-126-Street, si l'on note que les dix avenues résumées dans le nombre 1002 sont décalées vers l'ouest, c'est-à-dire, sur la carte, à gauche de l'origine. Ceci est si familier que nous visualisons instantanément la position de n'importe quelle adresse particulière. Le numéro d'avenue et le numéro de rue, avec les

compléments nécessaires de chiffres plus petits (comme dans le "2" de "1002" ci-dessus) permettent de fixer définitivement et uniquement la position d'un point quelconque par rapport aux axes, en donnant le couple de nombres qui mesurent son est ou son ouest et son nord ou son sud à partir des axes, ce couple de nombres est appelé les coordonnées du point (par rapport aux axes).



Supposons maintenant qu'un point se promène sur la carte. Les coordonnées (x, y) de tous les points de la courbe sur lesquels elle se déplace seront reliées par une équation (cela doit être pris pour acquis par le lecteur qui n'a jamais tracé de graphique pour ajuster les données), qui s'appelle *l'équation de la courbe*. Supposons maintenant pour simplifier que notre courbe soit un cercle. Nous avons son équation. Que peut-on faire avec ? Au lieu de cette équation particulière, on peut écrire la plus générale du même genre (par exemple, ici, du second degré, sans terme de produit vectoriel, et avec les coefficients des puissances les plus élevées des coordonnées égales), puis on peut procéder à la manipulation algébrique de cette équation. Enfin nous reportons les résultats de toutes nos manipulations algébriques dans leurs équivalents en termes de coordonnées de points sur le schéma que, tout ce temps, on a délibérément oublié. Il est plus facile de voir à travers l'algèbre que de voir, à la manière grecque de la géométrie élémentaire, à travers les lignes d'une toile d'araignée. Ce que nous avons fait a été *d'utiliser l'algèbre pour découvrir et rechercher des théorèmes géométriques concernant les cercles.*

Pour les lignes droites et les cercles, cela peut ne pas sembler très excitant ; nous savions tout faire auparavant d'une autre façon, à la grecque. Vient maintenant le véritable pouvoir de la méthode. Nous commençons avec des équations de n'importe quel degré de la complexité souhaitée ou suggérée et nous interprétons géométriquement leurs propriétés algébriques et analytiques. Ainsi, nous n'avons pas seulement abandonné la géométrie comme pilote ; nous avons attaché un sac de briques à son cou avant de le jeter par-dessus bord. L'algèbre et l'analyse seront désormais nos pilotes vers les mers inexplorées de "l'espace" et de sa "géométrie". Tout ce que nous avons fait peut être étendu, d'un seul coup, à l'espace d'un nombre quelconque de dimensions ; pour le plan il faut deux coordonnées, pour l'espace "solide" ordinaire trois, pour la géométrie de la mécanique et de la relativité, quatre coordonnées, et enfin, pour "l'espace" comme les mathématiciens l'aiment, il faut n coordonnées, soit autant de coordonnées qu'il y a de nombres 1, 2, 3,..., ou autant qu'il y a de points sur une ligne, une infinité. C'est battre Achille et la tortue dans leur propre course.



Descartes n'a pas révisé la géométrie ; il l'a créée.

Il semble approprié qu'un éminent compatriote mathématicien vivant de Descartes ait le dernier mot, nous citerons donc Jacques Hadamard. Il remarque d'abord que la simple invention des coordonnées n'était pas le plus grand mérite de Descartes, car cela avait déjà été fait "par les anciens" - affirmation qui n'est exacte que si l'on lit l'intention non exprimée dans l'acte inaccompli. L'enfer est pavé d'idées à moitié cuites d'"anciens"

"C'est tout autre chose que de reconnaître [dans l'usage des coordonnées] une méthode générale et de suivre jusqu'au bout l'idée qu'elle représente. C'est précisément ce mérite, dont tout vrai mathématicien connaît l'importance, qui fut par excellence celui de Descartes en géométrie ; c'est ainsi qu'il fut conduit à ce qui est sa véritable grande découverte en la matière ; à savoir, l'application de la méthode des coordonnées non seulement pour traduire en équations des courbes déjà définies géométriquement, mais, en considérant la question d'un point de vue exactement opposé, à la définition a priori de courbes de plus en plus compliquées et, partant, de plus en plus et plus générales...

"Directement, avec Descartes lui-même, plus tard, indirectement, dans le retour que le siècle suivant a fait en sens inverse, c'est toute la conception de l'objet de la science mathématique qui a été révolutionnée. Descartes avait bien compris à fond la portée de ce qu'il avait fait, et il avait raison de se vanter d'avoir surpassé toute la géométrie avant lui comme la rhétorique de Cicéron surpasse l'ABC".

Traduction d'un extrait du livre "Redécouvrons la géométrie" de Harold Scott MacDonald Coxeter, sur l'axe radical de deux cercles, page 35.

2.2. Axe radical de deux cercles

Dans l'un de ses livres[1], E. T. Bell a raconté l'anecdote suivante. Pendant son exil hors de la Bohême, la jeune princesse Elisabeth avait, un jour, abordé avec succès un problème de géométrie élémentaire en utilisant les coordonnées. Et Bell écrit : "ce problème est un bel exemple du genre qui ne se prête pas à l'emploi direct et sans nuances de la géométrie cartésienne élémentaire". La princesse avait pour maître René Descartes (auquel les coordonnées cartésiennes doivent leur nom[2]), et celui-ci déclara "qu'il n'entreprendrait pas d'achever la solution... en un mois !"

La leçon à tirer est claire : si elle est possible avec une certaine méthode, une solution peut très bien n'être pas, pour autant, la meilleure ou la plus rapide. Voici, en tout cas, un théorème dont la démonstration analytique, sans être en rien plus difficile que la démonstration synthétique habituelle, a quelques conséquences intéressantes :

Théorème 2.21. - *Le lieu géométrique des points ayant même puissance par rapport à deux cercles non concentriques est une droite perpendiculaire à la ligne des centres de ces cercles.*

Exprimé en coordonnées cartésiennes, le carré de la distance d entre deux points (x, y) et (a, b) est

$$d^2 = (x - a)^2 + (y - b)^2.$$

La puissance du point (x, y) par rapport au cercle dont le centre est le point (a, b) et le rayon r est donc :

$$d^2 - r^2 = (x - a)^2 + (y - b)^2 - r^2.$$

En particulier, étant le lieu des points (x, y) de puissance nulle, le cercle lui-même a pour équation

$$(x - a)^2 + (y - b)^2 - r^2 = 0. \tag{2.22}$$

Mise sous la forme $(x - a)^2 + (y - b)^2 = r^2$, cette même équation exprime que le cercle est le lieu des points dont les distances au point (a, b) ont la valeur constante r.

Si, maintenant, on écrit l'équation du cercle sous la forme

$$x^2 + y^2 - 2ax - 2by + c = 0, \tag{2.23}$$

Aux éditions Jacques Gabay, 1971.

Denise Vella-Chemla, août 2023.

[1] *Men of mathematics.*

[2] Certains affirment qu'en fait c'est Pierre Fermat (1601-1665) qui inventa la géométrie analytique parce que, dans une lettre à Descartes, il en donna le principe essentiel.
Voir Pierre Fermat, *Précis des Œuvres mathématiques et de l'Arithmétique de Diophante*, 1853, réédition Jacques Gabay, 1989.

(avec $c = a^2 + b^2 - r^2$), le premier membre de cette équation c'est-à-dire

$$x^2 + y^2 - 2ax - 2by + c$$

exprime encore la puissance d'un point quelconque (x, y).

Un autre cercle, de même centre (a, b) mais de rayon différent, aura une équation de même forme, c étant naturellement différent ; tandis que tout cercle n'ayant pas le même centre aura une équation de la forme

$$x^2 + y^2 - 2a'x - 2b'y + c' = 0, \tag{2.24}$$

dans laquelle $a' \neq a$, ou $b' \neq b$, ou les deux à la fois. Pour les deux cercles non concentriques dont il est question dans le théorème 2.21, nous pouvons donc utiliser les équations (2.23) et (2.24). Ainsi, le lieu des points (x, y) ayant même puissance par rapport à ces deux cercles sera défini par l'égalité

$$x^2 + y^2 - 2ax - 2by + c = x^2 + y^2 - 2a'x - 2b'y + c'$$

qui, après simplification, s'écrit

$$(a' - a)x + (b' - b)y = 1/2(c' - c).$$

Le lieu est donc une *droite*.

Si l'on adopte un système de référence où l'axe des x est la ligne des centres, les équations des cercles se simplifient comme suit :

$$x^2 + y^2 - 2ax + c = 0, \qquad x^2 + y^2 - 2a'x + c' = 0, \tag{2.25}$$

avec $a' \neq a$, et l'équation du lieu devient

$$x = \frac{c' - c}{2(a' - a)}.$$

On a donc une droite *perpendiculaire* à l'axe des x, c'est-à-dire à la ligne des centres. Or, du fait qu'elle représente l'ensemble de tous les points d'égale puissance, cette droite peut être définie géométriquement en fonction des cercles : nous aurions donc pu la prendre comme axe des y, comme sur la figure 2.2A. Les équations de deux cercles non concentriques peuvent, ainsi, se simplifier encore et s'écrire

$$x^2 + y^2 - 2ax + c = 0, \qquad x^2 + y^2 - 2a'x + c = 0 \tag{2.26}$$

Le lieu est alors $x = 0$. Réciproquement, tout point $(0, y)$ de la droite $x = 0$ a la *même* puissance $y^2 + c$ par rapport aux deux cercles.

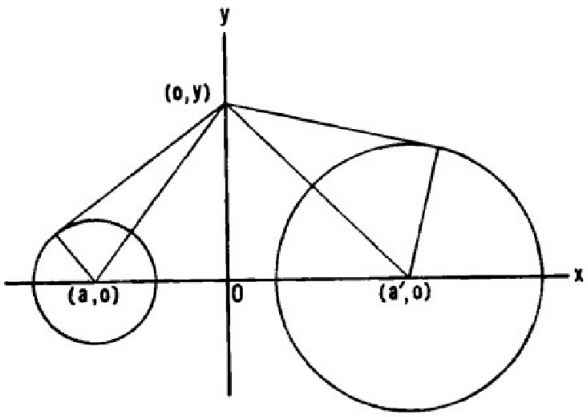


Fig. 2.2A

La remarque précédente achève la démonstration. Nous aurions pu, naturellement, abréger cette dernière en écrivant immédiatement les équations des deux cercles sous la forme (2.25) ; mais, dans ce cas, nous aurions omis le beau lemme suivant lequel, pour tout cercle exprimé sous la forme générale (2.23), *la puissance d'un point quelconque* (x, y) *est représentée par le premier membre de l'équation.*

Le lieu géométrique des points ayant même puissance par rapport à deux cercles non concentriques s'appelle *l'axe radical* de ces derniers. Dans le cas particulier où les deux cercles se coupent en deux points A et A' (fig. 2.2B), chacun de ces points a une puissance nulle par rapport aux deux cercles dont l'axe radical est alors la droite AA'. De même, lorsque deux cercles sont tangents (fig. 2.2C), leur axe radical est leur tangente commune au point de contact.

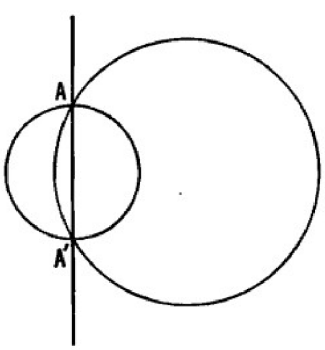


Fig. 2.2B

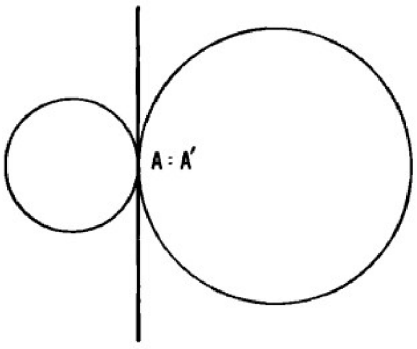


Fig. 2.2C

Explication pour une question qu'on s'était posée (Denise Vella-Chemla, juin 2023)

L'inverse complexe du cercle unité (parcouru dans un sens) est le cercle unité (parcouru dans l'autre sens) tandis que l'inverse d'un cercle de rayon unité mais décalé à droite (i.e. de diamètre [0,2] au lieu de [-1,1]) est une droite, pourquoi ?

Texte du programme python utilisé "pour voir".

```
import numpy as np
import matplotlib.pyplot as plt
from cmath import *

fig, ax = plt.subplots(1)
cercle unite
theta = np.linspace(0, 2*np.pi/3, 360)
r = 1.0
a = r*np.cos(theta)
b = r*np.sin(theta)
z = a+1j*b
ax.plot(a,b,color='black')
zprime = 1/z
aprime = zprime.real
bprime = zprime.imag
ax.plot(aprime,bprime,color='green')

theta = np.linspace(0, 2*np.pi, 360)
r = 1.0
a = r*np.cos(theta)+1
b = r*np.sin(theta)
z = a+1j*b
print(z)
zprime = 1/z
aprime = zprime.real
bprime = zprime.imag
ax.plot(a,b, color='red')
ax.plot(aprime,bprime,color='yellow')
ax.set_aspect(1)
plt.grid(linestyle = '--')
plt.xlim(-1,3)
plt.ylim(-5,5)
plt.grid(linestyle='--')
plt.title('Dans le plan complexe, un cercle de rayon 1 qui passe par (0,0) et (2,0)
a pour inverse la droite de partie reelle 1/2.', fontsize=8)
plt.show()
```

Explication du phénomène :

$$\begin{aligned}
\frac{1}{1+e^{i\theta}} &= \frac{1+e^{-i\theta}}{(1+e^{i\theta})(1+e^{-i\theta})} \\
&= \frac{1+e^{-i\theta}}{(1+\cos\theta)^2+\sin^2\theta} \\
&= \frac{1+e^{-i\theta}}{2+2\cos\theta} \\
&= \frac{1}{2}\frac{(1+\cos\theta)-i\sin\theta}{(1+\cos\theta)} \\
&= \frac{1}{2}-i\frac{\sin\theta}{1+\cos\theta} \\
&= \frac{1+e^{-it}}{2+2\cos t} \\
&= \frac{1}{2}\frac{(1+\cos t)-i\sin t}{1+\cos t} \\
&= \frac{1}{2}\left(1-i\frac{\sin t}{1+\cos t}\right) \\
&= \frac{1}{2}\left(1-i\tan\left(\frac{t}{2}\right)\right)
\end{aligned}$$

en utilisant, à la dernière étape, les identités trigonométriques $\sin(2x) = 2(\sin x)(\cos x)$ et $\cos(2x) = 2\cos^2(x) - 1$.
Pour t variant de $0 \to 2\pi$, et donc $\frac{t}{2}$ de $0 \to \pi$, la partie imaginaire de l'inverse, $-\frac{1}{2}\tan\left(\frac{t}{2}\right)$, varie de $0 \to +\infty$ puis de $-\infty \to 0$, parcourant ainsi l'ensemble de la droite réelle.

La partie réelle de l'inverse étant fixe, l'ensemble $\mathcal{C}^{-\infty}$ est la droite verticale d'abscisse $\frac{1}{2}$.

Transcription de l'extrait (pages 44 à 47) de l'Encyclopédie des sciences mathématiques pures et appliquées de Jules Molk, volume 3, tome 1 de théorie des nombres, consacré aux imaginaires de Galois.

24. Imaginaires de Galois. L'étude des congruences des degrés supérieurs est facilitée par l'introduction des *imaginaires de Galois*.

Lorsque $F(x)$ est une fonction-première (mod. p), de degré $\pi > 1$, la congruence irréductible

$$F(x) \equiv 0 \text{ (mod. } p),$$

n'a aucune solution entière. Dans ce cas, *E. Galois*[1] introduit un symbole i auquel s'appliquent, par définition, les mêmes règles de calcul qu'aux nombres naturels et qui est, en outre, supposé tel que l'on ait

$$F(i) \equiv 0 \text{ (mod. } p).$$

On peut dire que i est une *solution imaginaire* de la congruence irréductible $F(x) \equiv 0$ (mod. p) ; rien n'empêche d'imaginer par exemple que i est une des racines de l'équation irréductible $F(x) = 0$. *E. Galois* a d'ailleurs mis en pleine lumière les avantages que l'on peut tirer de cette façon de parler, dans la théorie des congruences[2].

Une congruence de la forme

$$\varphi(x) \equiv \psi(x) \text{ (modd. } p, F(x)),$$

est complètement équivalente à la congruence

$$\varphi(i) \equiv \psi(i) \text{ (mod. } p).$$

On appelle *imaginaire de Galois*, toute fonction rationnelle entière de i, à coefficients entiers ; la condition nécessaire et suffisante pour qu'une imaginaire de Galois $f(i)$ soit $\equiv 0$ (mod. p), est que $f(x)$ soit $\equiv 0$ (modd. $p, F(x)$). Si l'on envisage comme égales deux imaginaires de Galois congrues (mod. p), il n'y a qu'un nombre limité p^π d'imaginaires de Galois distinctes, parmi lesquelles une seule est nulle tandis que $(p-1)$ sont congrues (mod. p) aux $(p-1)$ premiers nombres naturels ; chacune de ces p^π imaginaires de Galois peut être mise sous la forme

$$f(i) = a_0 + a_1 i + a_2 i^2 + \ldots + a_{n-1} i^{n-1} \text{ (mod. } p),$$

où $a_0, a_1, a_2, \ldots, a_{n-1}$ sont des nombres entiers que l'on peut choisir parmi les nombres $0, 1, 2, ..., p-1$.

Le produit de plusieurs imaginaires de Galois ne peut être $\equiv 0$ (mod. p) que si l'une de ces imaginaires est $\equiv 0$ (mod. p). A chaque imaginaire de Galois différente de 0 (mod. p), correspond une imaginaire associée $f_1(i)$ telle que l'on ait

$$f(i) f_1(i) \equiv 1 \text{ (mod. } p).$$

Réédition aux éditions Jacques Gabay de volumes édités de 1904 à 1916 par Gauthier-Villars et B.G.Teubner.
Transcription : Denise Vella-Chemla, août 2023.

[1] Cf. *P. Bachmann*, Niedere Zahlentheorie 1, p. 393, in *P. Bachmann, W. F. Meyer*, (eds) Encyklopädie der Mathematischen Wissenschaften mit Einschluss ihrer Anwendungen.

[2] Cf. *É. Borel* et *J. Drach*, Introd. à l'étude de la théorie des nombres, d'après des conférences de *J. Tannery*, Paris 1895, p. 58.

Lorsqu'on introduit les imaginaires de Galois, aux théorèmes démontrés pour les congruences prises suivant un système de modules $p, F(x)$, correspondent les théorèmes suivants concernant les congruences prises suivant un module p.

Chacune des p^π imaginaires de Galois $f(i)$ est racine de la congruence

$$x^{p^\pi} \equiv x \text{ (mod. } p),$$

en sorte que cette congruence a autant de racines que l'indique son degré.

Les racines de la *congruence fundamentale* $F(x) \equiv 0 \text{ (mod } p)$ sont $i, i^p, i^{p^2}, \ldots, i^{p^{\pi-1}}$.

Quelle que soit la congruence fondamentale $F(x) \equiv 0 \text{ (mod. } p)$ servant à définir les imaginaires de Galois, le nombre des racines (imaginaires de Galois) d'une congruence quelconque $\Phi(x) \equiv 0 \text{ (mod. } p)$ est au plus égal au degré de cette congruence.

Toute imaginaire de Galois $f(i)$ *appartient à un exposant* n qui divise $p^n - 1$; à chaque diviseur n de $p^n - 1$ appartiennent $\varphi(n)$ nombres $f(i)$; la congruence $x^{p^\pi} - x \equiv 0 \text{ (mod. } p)$ a $\varphi(p^\pi - 1)$ *racines primitives* $f(i)$ qui sont incongrues et *appartiennent* à l'exposant $p^\pi - 1$.

Chacune de ces $\varphi(p^\pi - 1)$ racines primitives est, comme i elle-même, racine d'une congruence irréductible de degré π, et ses puissances donnent toutes les racines de la congruence

$$x^{p^\pi} \equiv x \text{ (mod. } p),$$

c'est à dire des quantités $f(i)$ toutes incongrues. Ainsi les racines de la congruence[3]

$$x^{i^3} \equiv x \text{ (mod. } 7)$$

peuvent toutes, puisque $i^3 \equiv 2 \text{ (mod. } 7)$ est irréductible, se mettre sous la forme

$$a_0 + a_1 i + a_2 i^2 \text{ (mod. } 7);$$

on trouve comme racine primitive

$$j = i - i^2$$

c'est à dire une racine de la congruence irréductible

$$j^3 - j + 2 \equiv 0 \text{ (mod. } 7),$$

et toutes les racines de la congruence $x^{343} \equiv x \text{ (mod. } 7)$ sont aussi de la forme

$$a_0 + a_1 j + a_2 j^2 \text{ (mod. } 7).$$

Si m est le nombre auquel *convient* $f(i)$, c'est-à-dire le plus petit nombre naturel pour lequel $[f(i)]^{p^m-1} \equiv 1 \text{ (mod. } p)$, m est un diviseur de π, et si $a_1, a_2, a_3, \ldots, a_k$ sont les nombres premiers inégaux qui divisent m, le nombre naturel

$$p^m + \sum_{(i)} p^{\frac{m}{a_i}} + \sum_{(i<k)} p^{\frac{m}{a_i a_k}} - \sum_{(i<k<l)} p^{\frac{m}{a_i a_k a_l}} + \ldots \pm p^{\frac{m}{a_1 a_2 \ldots a_k}},$$

[3] *E. Galois*, Œuvres, publiées par É. Picard, Paris, 1897, p. 19 ; cf. *J. A. Serret*, Alg. sup. (5e éd.), 2, Paris 1885, p. 181.

où les sommes sont formées comme il a été expliqué plus haut, in-dique combien, parmi les nombres incongrus $f(i)$, il y en a qui *conviennent* à m.

Les puissances

$$f(i), [f(i)]^p, [f(i)]^{p^2}, ..., [f(i)]^{p^{m-1}},$$

sont les racines d'une congruence irréductible $\Phi(x) \equiv 0 \pmod{p}$ de degré m, en sorte que toute fonction symétrique entière de ces puissances, à coefficients entiers, est congrue (mod. p) à un nombre entier ; réciproquement, toute congruence entière à coefficients entiers, à laquelle satisfait $f(i)$, a, en même temps, ces puissances pour racines.

Si π est le degré de la congruence fondamentale $F(x) \equiv 0 \pmod{p}$ au moyen de laquelle on introduit les imaginaires de Galois, toute congruence *irréductible* $\Phi(x) \equiv 0 \pmod{p}$, dont le degré est un diviseur de π, a un nombre de racines égal à son degré, tandis que toute congruence *irréductible* $\Phi(x) \equiv 0 \pmod{p}$ dont le degré n'est pas diviseur de π n'admet pas de racine (imaginaire de Galois).

Si $\Psi(x) \equiv 0 \pmod{p}$ est une congruence quelconque, entière à coefficients entiers, si $f(x), f_1(x), ...$ sont les fonctions premières de degrés respectifs $\mu, \mu_1, \ldots$ dont $\Psi(x)$ est le produit (mod. p), si enfin π désigne le p.p.c.m. de $\mu, \mu_1, \ldots$, il existe une fonction-première $F(x)$ de degré π ; si l'on introduit l'imaginaire de Galois i définie par la relation

$$F(i) \equiv 0 \pmod{p},$$

la congruence $\Psi(x) \equiv 0 \pmod{p}$ aura un nombre de racines (imaginaires de Galois) égal à son degré.

Il suffit de rapprocher ce théorème du théorème fondamental de l'Algèbre pour avoir nettement conscience de l'utilité de l'introduction des imaginaires de Galois dans la Théorie des nombres. Ce théorème a d'ailleurs donné lieu à mainte application, notamment dans la Théorie des substitutions[4].

[4]Voir à ce sujet *C. Jordan*, Traité des substitutions, Paris 1870 ; cf I. 8.

Traduction d'un extrait de "A History of Algebra" de Bartel L. van der Waerden concernant Galois (p. 105 à 111) (Denise Vella-Chemla, août 2023).

Le mémoire de 1831

Pour nous, qui avons appris la théorie de Galois d'un livre ou de séances d'un cours, il n'est pas aussi difficile de comprendre le mémoire de Galois que cela l'a été pour Poisson.

Galois commence avec une équation $f(x) = 0$. Les coefficients sont supposés connus, par exemple, ce sont des nombres rationnels ou irrationnels ou juste des lettres. Toutes les fonctions rationnelles de ces coefficients sont dites rationnelles. On peut aussi *adjoindre* d'autres quantités, par exemple les racines m-ièmes de quantités rationnelles, et considérer comme rationnel au sens plus large toutes les fonctions rationnelles de ces quantités, dit Galois. En terminologie moderne, on dirait qu'un certain "corps de base" est présupposé, qui peut être étendu par des adjonctions au cours des recherches.

Si un polynôme $f(x)$ peut être factorisé sans quitter le corps de base, on le dit *réductible*, sinon il est dit *irréductible*.

Souvent, mais pas régulièrement, Galois utilise les mots *permutation* et *substitition* dans le même sens que Cauchy. Une permutation est un ordre d'un ensemble fini, et une substitution est un passage d'un ordre à un autre (ou au même).

Galois considère maintenant des *groupes* de substitutions ayant la propriété : si S et T appartiennent au groupe, ST y appartient aussi.

Si un polynôme f a une racine en commun avec un polynôme irréductible g, alors f est divisible par g. Ceci est le premier lemme de Galois. C'est aussi le premier théorème du mémoire de 1829 d'Abel. Le lemme implique que l'extension de corps $K(V)$ obtenue en adjoignant une racine V d'un polynôme irréductible $g(x)$ est complètement connue dès que le corps de base K et le polynôme g sont connus. En terminologie moderne, le corps $K(V)$ est isomorphe à l'anneau des classes résiduelles $K[x]/(g)$.

Galois prouve ensuite : si une équation $g(x) = 0$ n'a pas de racine multiple et si $a, b, c, \ldots$ sont ses racines, on peut toujours former une fonction V des racines telle que toutes les valeurs de V obtenues en permutant les racines soient différentes.

Par exemple, on peut prendre

$$V = Aa + Bb + Cc + \ldots \tag{1}$$

avec des entiers convenablement choisis A, B, C,..., dit Galois.

De ce lemme, Galois déduit un cas particulier de ce qu'on appelle maintenant le "théorème de l'élément primitif" :

Lemme 3. Si V est choisi comme précédemment, toutes les racines $a, b, c, \ldots$ sont exprimables comme des fonctions rationnelles de V.

Pour prouver ce lemme important, Galois pose

$$V = \varphi(a, b, c, ...).$$

Il permute maintenant les racines b, c, de toutes les manières possibles, en gardant seulement l'une des racines fixe a, et il forme le produit

$$[V - \varphi(a, b, c, ...)] \cdot [V - \varphi(a, c, b, ...)].....$$

Ceci est une fonction symétrique de $b, c, \ldots$ qui sont les racines du polynôme

$$g(x)/(x - a),$$

par conséquent elle peut être exprimée comme une fonction rationnelle de a. On a donc une équation

$$F(V, a) = 0. \tag{2}$$

Cett équation et

$$g(a) = 0 \tag{3}$$

ont seulement une racine a en commun, car il ne peut pas advenir, par exemple, que $F(V, b)$ soit nul, dit Galois.

Maintenant, si deux équations comme (2) et (3) ont seulement une racine a en commun, cette racine peut être calculée rationnellement. Donc a est une fonction rationnelle de V.

Galois a raison de dire que $F(V, b)$ ne peut être nul, car $F(V, b)$ est un produit de facteurs

$$[V - \varphi(b, a, c, ...)] \cdot [V - \varphi(b, c, a, ...)] \cdot ...$$

dans lequel les permutations $(b, a, c, ...)$ etc. sont toutes les permutations de $(a, b, c, ...)$ dans lesquelles b est en première position, alors que les autres $(a, c, ...)$ sont permutées de toutes les façons possibles. Cela découle de la définition de $F(V, a)$, comme l'a remarqué H. M. Edwards dans son livre "Galois Theory" (Springer-Verlag 1984), p. 44-45. Notamment : puisque toutes les expressions $\varphi(b, a, c, ...)$ etc. sont supposées être différentes de $V = \varphi(a, b, ...)$, il en découle que les $F(V, b)$ sont différents de zéro, et il en est de même des $F(V, c)$, etc.

Poisson a écrit une note dans la marge du lemme 3, disant : "La preuve de ce lemme est insuffisante, mais le lemme est vrai par l'article 100 du mémoire de Lagrange." Il est facile de comprendre l'attitude de Poisson. La preuve de Galois est seulement une esquisse, et il ne démontre pas l'assertion que $F(V, b)$ est non nul. La dernière phrase de Poisson "Il est vrai par l'article 100 de Lagrange" est correcte, car dans l'article 100 des "Réflexions" de Lagrange, une preuve complète

du lemme est fournie.

Selon moi, Galois avait raison de dire que sa preuve est essentiellement correcte, mais Poisson avait raison de déclarer qu'elle était incomplète.

En notation moderne, on peut maintenant écrire

$$K(a, b, c, ...) = K(V) \tag{4}$$

où K est le corps de base. L'"élément primitif" V est une racine d'une équation irréductible. Appelons

$$V, V', V'', ...V^{(n-1)}$$

les racines de cette équation. Le lemme 4 dit : si $a = \varphi(V)$ est une racine de l'équation originale, $\varphi(V')$ sera aussi une racine. La preuve est aisée.

Ensuite vient le théorème principal :

Proposition I. Il y a un groupe de permutations des lettres $a, b, c, \ldots$, tel que

1° Toute fonction des racines, invariable selon les substitutions du groupe, est connue rationnellement ;

2° inversement, toute fonction des racines connue est invariable selon le groupe.

La terminologie de Galois n'est pas consistante. Il parle d'abord des "permutations" et ensuite des "substitutions" formant le groupe, mais ce qu'il veut dire est complètement clair.

Pour prouver ce théorème, Galois exprime les racines comme des fonctions rationnelles de V :

$$\varphi V, \varphi_1 V, ..., \varphi_{m-1} V.$$

Il écrit ensuite les permutations

$$\begin{array}{llll} \varphi V, & \varphi_1 V, & \varphi_2 V, & \ldots, \ \varphi_{m-1} V \\ \varphi V', & \varphi_1 V', & \varphi_2 V', & \ldots, \ \varphi_{m-1} V' \\ \ldots & \ldots & \ldots & \ldots \ \ \ldots \\ \varphi V^{(n-1)}, & \varphi_1 V^{(n-1)}, & \varphi_2 V^{(n-1)}, & \ldots, \ \varphi_{m-1} V^{(n-1)} \end{array}$$

et il énonce que le "groupe des permutations" (signifiant le groupe correspondant des substitutions) satisfait les conditions requises. La preuve est très courte, mais il n'est pas difficile pour un lecteur moderne d'en compléter les étapes.

Galois recherche ensuite comment le groupe de l'équation change quand le corps de base est étendu par l'adjonction d'une racine ou de toutes les racines d'une équation auxiliaire. Il est clair qu'après l'adjonction le groupe de Galois sera un sous-groupe H du groupe original G. Si H est un sous-groupe propre, G peut être décomposé comme suit :

(5) $$G = H + HS + HS' + ...$$

ou, alternativement, comme

(6) $$G = H + TH + T'H + ...$$

Ces deux décompositions sont plus clairement expliquées dans la lettre à Chevalier (Œuvres de Galois, 1897, p. 25-32).

Les deux décompositions ne coïncident pas toujours, dit Galois. Si elles coïncident, la décomposition est dite "propre". En terminologie moderne, c'est le cas quand H est un "sous-groupe invariant", ou un "diviseur normal" de G. En particulier, si *toutes* les racines d'une équation auxiliaire sont adjointes, les deux décompositions coïncideront. Ceci est la proposition III de Galois. La preuve est omise ("On trouvera la démonstration").

Galois en vient maintenant à son principal problème : dans quel cas une équation est-elle résoluble par radicaux ?

On peut, bien sûr, se restreindre aux radicaux de degré premier p. À chaque fois qu'une racine p-ième est extraite, Galois suppose que les racines p-ièmes de l'unité sont adjointes au préalable. Ceci n'est pas une restriction essentielle, parce que Gauss avait déjà démontré que les racines p-ièmes de l'unité peuvent s'exprimer au moyen de radicaux de degrés moindres que p.

Supposons maintenant que l'adjonction d'un radical r, racine d'une équation

(7) $$x^p - s = 0,$$

amène à une réduction du groupe de Galois. Parce que les racines p-ièmes de l'unité

$$\alpha, \alpha^2, ..., \alpha^p = 1$$

sont dans le corps de base, la même réduction est obtenue en adjoignant *toutes* les racines de l'équation (7). Par la proposition III, la décomposition (5) sera une décomposition propre, c'est-à-dire que le sous-groupe H est un diviseur normal. Galois a affirmé, mais n'a pas démontré, que le nombre de termes dans la décomposition (5) (qu'on appelle l'indice de H dans G) est juste un nombre premier p. Inversement, si G a un diviseur normal H d'indice premier p, on peut réduire le groupe de Galois G au sous-groupe H en adjoignant un radical de degré p. Ceci est démontré comme dans nos livres en prenant une fonction invariante selon le groupe H et en formant un "résolvant de Lagrange"

(8) $$z = \theta + \alpha\theta_1 + \alpha^2\theta_2 + \ldots + \alpha^{p-1}\theta_{p-1}$$

où α est une racine p-ième de l'unité, alors que $\theta_1, \theta_2, \ldots$, les substitutions sont obtenues à partir de θ par les substitutions

$$S, S^2, ..., S^{p-1}$$

représentant les cosets dans la décomposition (5).

Il en découle qu'une équation $g(x) = 0$ est résoluble par radicaux si et seulement si une séquence de sous-groupes

$$G \supset H_1 \supset H_2 \supset ... \supset H_m = E$$

existe, telle que tout H_k est un diviseur normal du précédent H_{k-1} ou G, alors que tous les indices sont des nombres premiers. Si tel est le cas, on dit que le groupe G est *résoluble*.

Galois suppose ensuite que l'équation $f(x) = 0$ est irréductible et de degré premier n. Il démontre : l'équation peut être résolue par radicaux si et seulement si chacune des substitutions de G transforme x_k en $x_{k'}$ par une transformation linéaire de k modulo n :

$$k' = ak + b \pmod{n}.$$

Le groupe de Galois de l'équation générale quintique n'est pas de cette forme, par conséquent son équation ne peut être résolue par radicaux. Ainsi le résultat d'Abel découle de la théorie de Galois.

Dans la dernière version de son mémoire de l'Académie, Galois a cité Abel, mais au moment où il a envoyé sa première version à l'Académie, il ne connaissait même pas le nom d'Abel. Ses sources principales étaient les travaux de Lagrange, Gauss, et Cauchy.

Les corps de Galois

À la fois Abel et Galois avaient une notion claire de ce que l'on appelle maintenant un "corps". Galois énonce bien au début de son grand mémoire :

"On peut s'accorder à considérer comme rationnelle toute fonction rationnelle d'un certain nombre de quantités regardées comme connues a priori", et il continue en expliquant ce qu'il veut dire par adjoindre une certaine quantité au corps des quantités considérées comme connues.

Les corps considérés par Abel et Galois dans leurs articles sur la résolution des équations contiennent tous le corps des nombres rationnels. En terminologie moderne, ce sont des corps de caractéristique zéro. Si la caractéristique était p, l'équation

$$x^p - 1 = 0$$

aurait seulement une racine $x = 1$, alors que Abel et Galois supposent toujours que les racines p-ièmes de l'unité sont toutes différentes.

Pourtant, dans son article "Sur la théorie des nombres", qui fut publié en 1830 dans le Bulletin des Sciences de Férussac (Œuvres de Galois, Paris 1897, p. 15-23) Galois construit des corps finis, ce qu'on appelle les *corps de Galois*. Il énonce dès le tout début que son objectif est de considérer les structures algébriques dans lesquelles toutes les quantités, multipliées par p, sont considérées comme nulles. Dans ses propres termes, il dit :

> Si l'on s'accorde à regarder comme nulles toutes les quantités qui, dans des calculs algébriques sont multipliées par p, et si on essaie de trouver, selon cette convention, la solution d'une équation algébrique $Fx = 0$, que Mr. Gauss désigne par la notation $Fx \equiv 0$, l'habitude est de considérer les solutions entières seulement. Ayant été amené, par mes propres recherches, à considérer des solutions incommensurables, j'ai atteint certains résultats que je considère comme nouveaux.

En lisant ces mots, il est clair que le point de départ de Galois était le calcul des congruences modulo un nombre premier p, initié par Gauss. Il était connu que des classes résiduelles modulo p peuvent être ajoutées, multipliées, et que la congruence

$$ax \equiv b \text{ (modulo } p)$$

peut toujours être résolue par des solutions rationnelles, en supposant que a n'est pas congru à zéro. En d'autres termes, les classes résiduelles modulo p forment un corps.

Gauss avait aussi considéré les congruences de degrés plus élevés telles que

$$x^2 \equiv a \text{ (modulo } p),$$

mais il admettait seulement des solutions rationnelles. Galois se demande alors si on peut introduire des solutions irrationnelles, c'est-à-dire si on peut élargir le corps de classe résiduelle par l'adjonction de racines non contenues dans le corps original.

Galois suppose que le polynôme Fx est irréductible modulo p. Il se demande si on peut résoudre la congruence $Fx \equiv 0$ en introduisant de nouveaux "symboles", qui peuvent être juste aussi utiles que l'unité imaginaire i en analyse ordinaire.

Galois appelle i l'une des racines de la congruence $Fx \equiv 0$ de degré ν. Il forme les p^ν expressions

$$\text{(A)} \qquad a + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1},$$

où $a, a_1, a_2, ..., a_{\nu-1}$ sont les entiers modulo p. Ces p^ν éléments forment ce que nous appelons aujourd'hui un "corps de Galois" $\mathrm{GF}(p^\nu)$.

Il est facile de montrer que les expressions (A) forment un corps, c'est-à-dire qu'elles satisfont les règles bien connues d'addition, soustraction, multiplication, et division.

Galois prend maintenant un élément α de la forme (A), dans lequel les coefficients $a, a_1, \ldots, a_{\nu-1}$ ne sont pas tous nuls. Les puissances $\alpha, \alpha^2, ...$ ne peuvent pas être toutes différentes, par conséqueent une puissance α^n doit être égale à 1. Si n est le plus petit entier pour lequel α^n est égal à 1, les expressions

$$1, \alpha, \alpha^2, ..., \alpha^{n-1}$$

doivent être toutes différentes. En terminologie moderne, elles forment un sous-groupe du groupe multiplicatif du corps de Galois.

En multipliant ces nombres par un autre élément $\beta \neq 0$, on obtient un coset du sous-groupe. En continuant de la même façon, on trouve que tous les cosets ensemble forment le sous-groupe

multiplicatif dans son entièreté d'ordre $p^\nu - 1$, et que l'exposant n est un diviseur de $p^\nu - 1$. Par conséquent, on a

$$\alpha^{p^\nu - 1} = 1.$$

Ensuite on démontre, dit Galois, comme dans la théorie des classes résiduelles modulo p, qu'il existe des "racines primitives" pour lesquelles n est exactement $p^\nu - 1$. Tous les autres éléments non nuls du corps de Galois sont des puissances d'un élément primitif α. La preuve de l'existence d'un tel élément, donnée par Gauss pour le cas d'un corps de classes résiduelles modulo p, marche juste aussi bien que dans le cas de $\mathrm{GF}(p^\nu)$.

On voit maintenant que tous les éléments du corps de Galois, incluant zéro, sont des racines du polynôme

(B) $$x^{p^\nu} - x$$

et que tout polynôme irréductible Fx de degré ν est un diviseur du polynôme (B). Si α est une des racines d'un tel polynôme, les autres sont

$$\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{\nu-1}}.$$

Cela découle de la congruence bien connue

$$(Fx)^p \equiv F(x^p).$$

À la fin de son traité, Galois inverse la situation. Il commence avec une extension quelconque de corps de $\mathrm{GF}(p)$ dans laquelle le polynôme (B) peut être complètement factorisé. Se restreignant lui-même au sous-corps engendré par les racines, il prend un "élément primitif" i du sous-corps. Un tel élément existe toujours selon un théorème connu d'Abel, dit Galois. Tout tel i est une racine d'un polynôme irréductible (mod p) Fx. Le choix du polynôme irréductible ν qui est choisi n'a pas d'importance, on obtient toujours le même corps $\mathrm{GF}(p^\nu)$. Dans la plupart des cas, la façon la plus simple d'obtenir un tel polynôme est de le faire "par tatônnement", dit Galois, par essai et erreur. Comme exemple, il prend $p = 7$ et $\nu = 3$. Le polynôme $x^3 - 2$ est irréductible (mod 7), et une racine i de ce polynôme engendre le corps $\mathrm{GF}(7^3)$.

Traduction d'un extrait de "A History of Algebra" de Bartel L. van der Waerden concernant Gauss (p. 89 à 102) (Denise Vella-Chemla, août 2023).

Chapitre 5

Carl Friedrich Gauss

Les contributions les plus importantes de Gauss à la théorie des équations algébriques sont :

1° la solution complète de l'"équation cyclotomique"

(1) $$x^m - 1 = 0$$

au moyen de radicaux,

2° la preuve que tout polynôme en une variable à coefficients réels est un produit de facteurs linéaires ou quadratiques. Ce théorème implique ce que nous appelons maintenant le "théorème fondamental de l'algèbre" : tout polynôme $f(x)$ à coefficients complexes est un produit de facteurs linéaires. Nous allons maintenant discuter de ces deux contributions extrêmement intéressantes.

L'équation cyclotomique

L'équation (1) est appelée cyclotomique, parce que sa solution est très liée à la construction d'un polygone régulier à n côtés inscrit dans un cercle donné.

Pour voir cela, on a juste à noter que l'équation (1) a n racines complexes

(2) $$\cos(2\pi k/n) + i\sin(2\pi k/n) \quad k = 0, 1, 2, ..., n-1.$$

Cette solution trigonométrique était connue de de Moivre et Euler longtemps avant Gauss. Maintenant, si on représente les nombres complexes $a + ib$ par des points dans le plan complexe de coordonnées (a, b), il est clair que les nombres complexes (2) sont représentés par les sommets d'un n-gone régulier inscrit dans le cercle-unité. Par conséquent, si on réussit à résoudre l'équation (1) au moyen de racines carrées, on peut construire le n-gone régulier à la règle et au compas.

Les pythagoriciens savaient déjà comment construire des polygones réguliers de 3, 4, 5, et 6 côtés. On peut trouver leurs constructions dans le Livre 4 des Éléments d'Euclide. Pour l'attribution de ce livre aux pythagoriciens, se reporter à mon livre "Die Pythagoreer" (Artemis-Verlag, Zürich 1979), p. 348-351.

Lagrange résolut l'équation

(3) $$x^5 - 1 = 0$$

comme suit. Une racine est $x = 1$. Les autres sont les racines de l'équation

$$x^4 + x^3 + x^2 + x + 1 = 0,$$

qui peut s'écrire

$$(x^2 + x^{-2}) + (x + x^{-1}) + 1 = 0. \tag{4}$$

En posant

$$x + x^{-1} = y \tag{5}$$

on obtient

$$y^2 + y - 1 = 0. \tag{6}$$

Cette équation quadratique peut être résolue pour y, et ensuite, (5) peut être résolue pour x. Il en découle, une fois de plus, que le pentagone régulier peut être construit à la règle et au compas.

La construction d'Euclide est aussi basée sur la solution d'une équation quadratique. On lit dans la traduction de Heath du Livre 2 des Éléments d'Euclide la proposition 11 :

> *Couper une droite donnée de telle façon que le rectangle contenu par le tout et l'un des segments soit égal au carré du segment restant.*

Si la droite donnée est appelée a et le second segment y, le problème d'Euclide est de résoudre l'équation

$$a(a - y) = y^2. \tag{7}$$

Dans sa solution du problème II, 11, Euclide résout d'abord l'équation équivalente

$$y^2 + ay = a^2 \tag{8}$$

et ensuite, il soustrait le rectangle ay des deux côtés, obtenant ainsi la solution de (7). Si le segment donné a est pris comme unité de longueur, on voit que (8) est la même équation que l'équation (6) de Lagrange.

Dans le livre 4, Euclide utilise la solution de (7) dans sa construction du pentagone régulier. Juste ainsi, Lagrange utilise la solution de (6) pour la solution de l'équation cyclotomique (3).

Lagrange applique ensuite la même méthode à l'équation

$$x^{11} - 1 = 0 \tag{9}$$

(Œuvres III, p. 246). En divisant par $x - 1$ et ensuite par x^5, Lagrange obtient

(10) $$(x^5 + x^{-5}) + (x^4 + x^{-4}) + (x^3 + x^{-3}) + (x^2 + x^{-2}) + (x + x^{-1}) + 1 = 0.$$

En posant à nouveau

(11) $$x + x^{-1} = y$$

on obtient une équation quintique pour y.

Lagrange l'a laissée ainsi, mais Vandermonde a réussi à résoudre l'équation quintique par radicaux, comme on l'a vu au chapitre 4.

Alors qu'il avait presque 19 ans, Gauss découvrit que le polygone régulier à 17 côtés peut être construit à la règle et au compas. Dans le chapitre 7 du fameux travail de Gauss intitulé les "Disquisitiones arithmeticae", la preuve complète de la résolubilité de l'équation (1) par radicaux est donnée. L'équation

(12) $$x^{17} - 1 = 0$$

est traitée comme un cas particulier. Puisqu'on ne sait pas comment le jeune Gauss a trouvé la solution de (12) et donc la construction du 17-gone, on n'a d'autre choix que de suivre Gauss et de traiter le cas général en premier.

Gauss montre d'abord que l'équation générale (1) peut se réduire au cas particulier dans lequel n est un nombre premier, en écrivant n comme un produit de puissances de nombres premiers. Un cas particulier, notamment $n = 15$, était déjà connu d'Euclide. Euclide montre : si on peut inscrire dans un cercle un triangle régulier et un pentagone régulier, on peut aussi inscrire un polygone régulier à 15 côtés.

En divisant (1) par $x - 1$, on obtient l'équation

(13) $$X = x^{n-1} + x^{n-2} + \ldots + x + 1 = 0.$$

En supposant que n est un nombre premier, Gauss montre d'abord que le polynôme X est *irréductible rationnellement*. Ensuite, il annonce son résultat principal : si $n - 1$ est un produit de facteurs $\alpha\beta\gamma...$, l'équation (1) peut être résolue en résolvant des équations de degrés $\alpha, \beta, \gamma, \ldots$. Par exemple, si n est égal à 17, on a

$$n - 1 = 2^4,$$

et alors l'équation (12) peut être résolue en résolvant quatre équations quadratiques, et par conséquent le 17-gone peut être construit à la règle et au compas. Plus généralement, si $n-1$ est une puissance de 2, ce qui arrive pour

(14) $$n = 3, 5, 17, 257, 65537,$$

le n-gone régulier peut être construit à la règle et au compas.

Les nombres premiers mentionnés dans (14) étaient connus de Gauss. Les autres nombres premiers de la forme $2^m + 1$ ne sont pas connus à ce jour (3 décembre 1982).

En supposant toujours n comme étant un nombre premier, Gauss dénote par r n'importe quelle racine de (13). Maintenant les racines sont

$$r, r^2, \ldots, r^{n-1}. \tag{15}$$

Deux puissances r^λ et r^μ sont multipliées en ajoutant les exposants et en réduisant la somme $\lambda + \mu$ modulo n.

Gauss note ensuite que toute fonction rationnelle des racines peut être réécrite ainsi

$$A + A'r + A''r^2 + ... + A^{(n-1)}r^{n-1}. \tag{16}$$

Pour simplifier la notation, Gauss écrit $[\lambda]$ à la place de r^λ. Ainsi, les racines (15) sont réécrites comme

$$[1], [2], ..., [n-1]. \tag{17}$$

Dans le chapitre III des Disquisitiones, Gauss a démontré : si n est un nombre premier, le groupe multiplicatif des entiers modulo n est cyclique, i.e. il existe un "élément primitif" g tel que toutes les puissances d'exposants non divisibles par n sont congrues à des puissances de g. Donc les racines (17) peuvent être réordonnées et écrites comme

$$[1], [g], [g^2], \ldots [g^{n-2}]. \tag{18}$$

Ce réordonnancement est un point essentiel dans la théorie de Gauss. les exposants de g sont appelés des *indices*. Ils jouent le rôle des logarithmes : deux puissances de g sont multipliées en ajoutant leurs indices (mod $n-1$).

Maintenant soit e n'importe quel diviseur de $n-1$. En posant

$$n - 1 = ef$$

$$g^e = h,$$

Gauss considère l'ensemble des racines

$$[\lambda], [\lambda h], [\lambda h^2], \ldots, [\lambda h^{f-1}],$$

où λ est un entier arbitraire congru à zéro (mod n), et il forme la somme

$$(f, \lambda) = [\lambda] + [\lambda h] + [\lambda h^2] + \ldots + [\lambda h^{f-1}]. \tag{19}$$

Ces sommes sont indépendantes du choix de g. On les appelle des *périodes*.

Gauss élucide la formation des périodes en étudiant l'exemple $n = 19$. Je préfère donner l'exemple $n = 17$, élaboré par Gauss dans la section 354 (Werke, Vol. I, p. 437). Comme élément primitif (mod 17) Gauss choisit $g = 3$. Ainsi les indices (mod 16)

$$i = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15$$

donnent les puissances de 3 (mod 17)

$$\mu = g^i = 1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6$$

et les racines

$$[\mu] = r^\mu = r, r^3, r^9, r^{10}, ..., r^6.$$

Les diviseurs de $n - 1 = 16$ sont

$$e = 1, 2, 4, 8, 16$$

correspondant à

$$f = 16, 8, 4, 2, 1.$$

Il y a seulement une période (16, 1), notamment la somme de toutes les racines. Il y a deux périodes avec $f = 8$, notamment

$$(8, 1) = [1] + [9] + [13] + [15] + [16] + [8] + [4] + [2]$$

et

$$(8, 3) = [3] + [10] + [5] + [11] + [14] + [7] + [12] + [6].$$

Il y a quatre périodes avec $f = 4$, notamment

$$(4, 1), (4, 3), (4, 9), (4, 10).$$

Il y a huit périodes avec $f = 2$, notamment

$$(2, 1) = [1] + [16] = r + r^{-1},$$

et il y a 16 périodes avec $f = 16$, notamment les racines uniques.

Gauss considère aussi la période $(f, 0)$, qui est une somme de f unités et est par conséquent égale à f.

Dans la section 345 Gauss prouve le théorème général qui énonce qu'un produit

$$(f, \lambda) \cdot (f, \mu)$$

peut être exprimé comme une somme de périodes ainsi :

$$(f, \lambda) \cdot (f, \mu) = (f, \lambda + \mu) + (f, \lambda' + \mu) + (f, \lambda'' + \mu) + \ldots. \tag{20}$$

Maintenant, appliquons la formule (20) au cas $n = 17$. La somme

$$(8, 1) + (8, 3)$$

est la somme de toutes les racines et par conséquent elle est égale à -1. Le produit

$$(8,1)\cdot(8,3)$$

peut être calculé par (20) : il est égal à -4. Donc (8, 1) et (8,3) sont les racines de l'équation quadratique

$$y^2+y-4=0. \tag{21}$$

En résolvant cette équation, on obtient (8, 1) et (8,3). Ensuite (4, 1) et (4,9) peuvent être calculés par la même méthode. Leur somme est (8,1) et leur produit est -1, donc ce sont les racines de l'équation quadratique

$$x^2-(8,1)x-1=0. \tag{22}$$

Juste ainsi, (4,3) et (4,10) sont les racines de l'équation

$$x^2-(8,3)x-1=0. \tag{23}$$

Par la même méthode, les périodes $(2,\lambda)$ et finalement les racines $[\mu]$ peuvent être obtenues comme racines des équations quadratiques.

Dans le cas général, on doit factoriser $n-1$

$$n-1=\alpha\beta\gamma...$$

et résoudre des équations de degrés α,β,γ,.... Dans la section 359, Gauss montre que ces équations peuvent être résolues par radicaux.

Je suppose que ces exemples sont suffisants pour expliquer les idées principales de Gauss au sujet de l'équation cyclotomique.

Le "théorème fondamental"

Dans la notation de Gauss, toute équation algébrique de degré m peut s'écrire

$$x^m+Ax^{m-1}+Bx^{m-2}+\ldots+M=0 \tag{24}$$

ou $X=0$. Le "théorème fondamental de l'algèbre" comme on l'appelle, dit que tout polynôme X avec des coefficients réels ou complexes peut être factorisé en facteurs linéaires dans le corps des nombres complexes.

Il est suffisant de démontrer le théorème pour les polynômes à coefficients réels, car si X a des coefficients complexes, le produit $X\overline{X}$ est réel, et sa factorisation implique la factorisation des facteurs X et $\overline{X}$. Ainsi on a la justification du fait que Gauss se restreigne aux polynômes réels X.

Dans sa première démonstration, Gauss n'introduit pas les nombres complexes. Il démontre le théorème fondamental sous la forme suivante :

Tout polynôme X à coefficients réels peut être factorisé en facteurs linéaires et quadratiques.

Gauss a considéré que ce théorème était si important qu'il en a donné quatre démonstrations. Les principes, sur lesquels la première preuve est basée, ont été découverts par Gauss en octobre 1797. La première démonstration a été publiée en 1799, la seconde et la troisième en 1816, et la quatrième en 1849. La quatrième preuve est basée sur les mêmes principes que la première. Je me restreindrai ici aux trois premières démonstrations.

Les quatre preuves ont été traduites du latin à l'allemand par E. Netto et publiées sous le titre "Die vier Gauss'schen Beweise für die Zerlegung ganzer algebraischer Funktionen in reelle Faktoren ersten oder zweiten Grades", Ostwald's Klassiker der exakten Wissenschaften[1], Vol. 14 (Leipzig 1913).

La première démonstration

La première preuve de Gauss a été publiée dans sa thèse (Werke III, p. 1-30). Avant d'exposer sa propre preuve, Gauss critique des démonstrations antérieures données par d'Alembert, Euler, Fontenex, et Lagrange. Sa principale objection est que dans toutes ces preuves, l'existence de racines est présupposée. Il est montré que des racines complexes peuvent être obtenues, en supposant qu'elles existent d'une manière ou d'une autre. Il y a d'autres objections à chacune des preuves individuelles qui ne seront pas discutées ici.

Gauss commence avec un polynôme réel.

$$X = x^m + Ax^{m-1} + B^{m-2} + ... + Lx + M, \tag{25}$$

dans lequel x est une indéterminée ("unbestimmte Größe"). Ce qu'il veut démontrer c'est qu'un facteur linéaire ou quadratique de X existe. Un facteur réel linéaire implique l'existence d'une racine réelle $\pm r$, où r est positif ou nul. Un facteur irréductible quadratique implique l'existence de deux racines complexes

$$r(\cos\varphi + i\sin\varphi), \tag{26}$$

par conséquent, les facteurs quadratiques peuvent s'écrire

$$x^2 - 2xr\cos\varphi + r^2 \qquad (r > 0). \tag{27}$$

En substituant l'une des racines (26) dans l'équation $X = 0$ et en séparant les parties réelle et imaginaire, on obtient une paire d'équations réelles pour r et φ :

[1] "Les quatre preuves de Gauss de la décomposition de toute fonction algébrique en facteurs réels du premier et second degrés", Les classiques des sciences exactes de Ostwald.

(28) $$r^m \cos m\varphi + Ar^{m-1} \cos(m-1)\varphi + ... + Lr \cos \varphi + M = 0$$
(29) $$r^m \sin m\varphi + Ar^{m-1} \sin(m-1)\varphi + ... + Lr \sin \varphi = 0.$$

Gauss note qu'Euler a obtenu cette paire d'équations en utilisant les nombres complexes. Gauss évite les nombres complexes : il dérive (28) et (29) directement de la supposition que le polynôme X a un facteur linéaire $x \pm r$ ou un facteur quadratique (27).

Gauss interprète (28) et (29) comme des équations de courbes algébriques en coordonnées polaires, et il réussit à prouver que ces courbes s'intersectent en un point au moins. Si ceci est démontré, il en découle que X a un facteur linéaire ou quadratique, et en continuant le processus, on obtient une factorisation de X en facteurs linéaires et quadratiques.

L'équation (28) est notée $U = 0$, et (29) est notée $T = 0$. Pour illustrer la preuve, j'ai dessiné les courbes $U = 0$ et $T = 0$ dans le cas d'une équation quadratique

$$x^2 + 1 = 0.$$

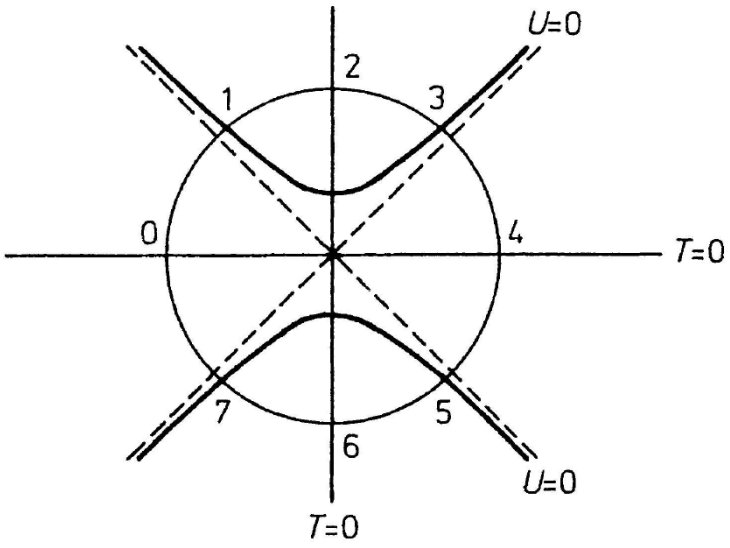


FIG. 23

En coordonnées orthogonales x et y, on a deux courbees d'ordre m. L'axe $y = 0$ est toujours une partie de la seconde courbe $T = 0$.

Gauss étudie maintenant les intersections des deux courbes avec un cercle de rayon R, et il démontre :

Pour un rayon suffisamment large R, il y a exactement $2m$ intersections du cercle avec $T = 0$ et $2m$ intersections avec $U = 0$, et tout point d'intersection du second type est entre deux points du premier type.

Gauss présente une preuve complète de ce lemme. Il note ensuite que les $4m$ points changent seulement très peu si R est rendu un peu plus grand ou un peu plus petit. En terminologie moderne, on dirait que les $4m$ points sont des fonctions continues de R. Gauss ne démontre pas

cette continuité : il dit seulement qu'elle est "facile à voir". Ensuite, Gauss étudie le comportement des branches des courbes $U = 0$ et $T = 0$ à l'intérieur du cercle, et il affirme : il existe un point d'intersection d'une branche de la première courbe avec une branche de la seconde courbe. Pour cette conclusion, il donne une preuve intuitive, géométrique. Il dénote le point d'intersection du cercle avec l'axe des x par 0, le prochain point voisin sur le cercle par 1, et etc., comme dans la figure Fig. 23. Les nombres impairs dénotent des points sur $U = 0$, les nombres pairs des points sur $T = 0$. Maintenant il dit : si une branche d'une courbe algébrique entre dans un certain domaine, elle doit aussi quitter le même domaine quelque part. Dans une note de bas de page, il ajoute :

> *Il semble bien démontré qu'une courbe algébrique ne se termine jamais abruptement (comme cela arrive dans le cas de la courbe transcendante $y = 1/\log x$), ni ne se perd jamais après un nombre infini d'enroulements en un point (comme une spirale logarithmique). Aussi loin que je m'en souvienne, personne n'a jamais douté de cela, mais si quelqu'un le nécessite, je prends sur moi de présenter de cela, à une autre occasion, une preuve indubitable.*

Si ce point de départ est accepté, il en découle que tout "point pair" est relié à (au moins) un autre point pair par une branche de la courbe $T = 0$, et que tout "point impair" est relié à un autre point impair par une branche de la courbe $U = 0$. Maintenant, aussi compliquées que ces relations puissent être, on peut montrer qu'un point d'intersection existe toujours. Cela se démontre comme suit.

Supposons qu'aucun point d'intersection n'existe. Le point 0 est relié au point $2m$ par l'axe des x. Le point 1 ne peut pas être relié à un point quel qu'il soit de l'autre côté de cet axe sans intersecter l'axe. Donc, si le point 1 est relié au point impair n, on doit avoir $n < 2m$. Juste ainsi, si 2 est relié à n', on doit avoir $n' < n$. Notons que la différence $n' - 2$ est paire, parce que 2 et n' sont tous les deux pairs. En continuant de cette manière, on trouve finalement un point h relié à $h + 2$. Mais maintenant la branche qui entre dans le cercle au point $h + 1$ doit nécessairement intersecter la branche reliant h et $h+2$, contrairement à notre hypothèse. Par conséquent, il existe un point d'intersection.

De cet exposé, on voit que la première démonstration de Gauss est basée sur des suppositions à propos des branches de courbes algébriques, qui semblent plausibles à notre intuition géométrique, mais qui ne sont strictement pas démontrées par Gauss. Alexander Ostrowski a montré dans un article très intéressant "Über den ersten und vierten Gauss'schen Beweis des Fundamentalsatzes der Algebra", que toutes les suppositions faites par Gauss peuvent être justifiées par des démonstrations indubitables. L'article d'Ostrowski a été d'abord publié dans les Nachrichten der Gesellschaft der Wissenschaften Göttingen 1920, et réimprimé dans les Travaux de Gauss X, 2.

La seconde preuve

La seconde preuve est purement algébrique. Les seules suppositions faites à propos du corps des nombres réels sont :

1° que toute équation réelle de degré impair a une racine réelle,

2° que toute équation quadratique à coefficients complexes a deux racines complexes.

L'idée sous-tendant la seconde preuve est simple, mais la mise en œvre est assez difficile. Gauss commence avec un polynôme réel de degré m

(30) $$Y = x^m - L'x^{m-1} + \check{L}''x^{m-2} - ... + ...$$

Si on suppose un instant que Y peut être factorisé en facteurs linéaires

(31) $$Y = (x-a)(x-b)(x-c)...$$

dans une certaine extension de corps, alors une combinaison linéaire

(32) $$(a+b)t - ab$$

peut être formée avec une nouvelle indéterminée t. Si les racines $a, b, c, ...$ sont permutées, la fonction linéaire (32) prend

$$m' = \tfrac{1}{2}m(m+1)$$

valeurs, par conséquent, elle est racine d'une équation de degré m'. Les racines de cette équation auxiliaire sont des fonctions linéaires de t de la forme (32). Dès qu'une racine de l'équation auxiliaire est connue, $a+b$ et ab sont connus, donc a et b peuvent être exprimés au moyen de racines carrées. Cela reste vrai si l'indéterminée t est spécialisée de telle façon que des fonctions linéaires différentes (32) restent différentes après la spécialisation.

Maintenant si m est un nombre de la forme

(33) $$m = 2^\mu k$$

où k est impair, le degré de l'équation auxiliaire est de la forme

(34) $$m' = 2^{\mu-1}k'$$

où k' est à nouveau impair.

Dès qu'une racine complexe de cette équation auxiliaire est connue, deux racines a et b de l'équation originale peuvent être calculées qui sont des nombres complexes en extrayant une racine carrée.

En continuant de cette manière, on arrive finalement à une équation de degré impair. Les coefficients de cette équation sont des fonctions symétriques des racines $a, b, ...$ avec coefficients réels, donc ce sont des nombres réels connus. Puisque le degré est impair, cette équation a au moins une racine réelle. En revenant à travers la séquence des équations auxiliaires, on peut calculer au moins une racine complexe de l'équation originale.

Dans cette forme simplifiée, la preuve fonctionne si on sait que l'équation $Y = 0$ a m racines $a, b, ...$ dans une certaine extension du corps des nombres réels. L'existence d'une telle extension peut être démontrée par la méthode de Kronecker de l'"adjonction symbolique" : on peut en trouver la démonstration dans n'importe quel livre d'algèbre moderne. Pourtant, Gauss ne suit pas cette voie. Il construit ses équations auxiliaires sans supposer l'existence des racines. Par exemple, il construit l'équation auxiliaire de degré m' comme suit :

D'abord, le polynôme spécial (30) est remplacé par un polynôme y, dont les racines sont les indéterminées $a, b, c, ...$

$$y = (x - a)(x - b)(x - c)....\tag{35}$$

Gauss forme ensuite un polynôme auxiliaire en une nouvelle variable u, définissant ζ comme le produit des m' expressions

$$u - (a + b)t + ab\tag{36}$$

obtenues en permutant les racines. Ce polynôme ζ est symétrique en les indéterminées $a, b, c, ...$, donc il peut être exprimé de manière unique comme un polynôme en u et t et les coefficients de y, qui sont les fonctions élémentaires symétriques de $a, b, c, ...$ Après ça, les coefficients de y sont remplacés par les coefficients $L', L'', ...$ du polynôme donné (30), et ainsi le polynôme auxiliaire Z est obtenu.

8. Le plan de Riemann pour prouver le théorème des nombres premiers

8.1. Une méthode pour estimer précisément le nombre de nombres premiers. Jusqu'au milieu du dix-neuvième siècle, toutes les approches pour estimer $\pi(x) = \#\{\text{nombrespremiers} \leq \text{x}\}$ étaient relativement directes, basées sur la théorie élémentaire des nombres et des principes combinatoires, ou la théorie des formes quadratiques. En 1859, pourtant, le grand géomètre Riemann releva le défi de compter les nombres premiers d'une façon différente. Il écrivit juste un article qu'on pourrait dire de "théorie des nombres", mais ce court mémoire eut un impact qui a duré presque un siècle et demi, et ses idées ont défini le sujet que l'on appelle désormais *théorie analytique des nombres*.

Le mémoire de Riemann décrivait une approche surprenante du problème, une approche utilisant la théorie de l'analyse complexe, qui était en ce temps-là un sujet encore en développement[1]. Cette nouvelle approche de Riemann semblait éloignée du royaume dans lequel vivait le problème original. Pourtant elle avait deux caractéristiques clefs :

- c'était un moyen pratique de régler la question une bonne fois pour toutes ;
- elle faisait des prédictions qui étaient similaires à la prédiction de Gauss, bien que différentes.

En effet, elle suggère même un terme secondaire pour compenser l'erreur que l'on a vu dans les données de la table en section 2.10[2].

La méthode de Riemann est la base de notre démonstration principale du théorème des nombres premiers, et dans ce chapitre, nous donnerons une introduction tranquille aux idées clefs qu'elle contient. Commençons par extraire la prédiction clef du mémoire de Riemann et énonçons-la en langage complètement élémentaire :

$$\text{ppcm}[1, 2, 3, \ldots, x] \text{ est environ égal à } e^x.$$

En utilisant les données pour tester sa précision, on obtient :

x	Entier le plus proche de $\ln(\text{ppcm}[1, 2, 3, \ldots, x])$	Différence
100	94	-6
1000	997	-3
10000	10013	13
100000	100052	57
1000000	999587	-413

Chapitre trouvé dans la page de cours d'Andrew Granville ici https://dms.umontreal.ca/ andrew/Courses/Chapter8.pdf.

Traduction Denise Vella-Chemla, août 2023.

[1] En effet, le mémoire de Riemann a été un élément significatif dans le développement de la théorie des fonctions analytiques, notamment dans leurs aspects globaux.

[2] Fournissons ici les valeurs de la section 2.10 de $\text{Li}(x) - \pi(x)$ pour x de 10^3 à 10^{23} : 10, 17, 38, 130, 339, 754, 1701, 3104, 11588, 38263, 108971, 314890, 1052619, 3214632, 7956589, 21949555, 99877775, 222744 597394254, 1932355208, 7236148412.

La prédiction de Riemann peut être exprimée précisément et explicitement par

$$|\log(\text{ppcm}[1,2,\dots,x]) - x| \le 2\sqrt{x}(\log x)^2 \quad \text{pour tout } x \ge 100. \tag{8.1.1}$$

Puisque la puissance d'un nombre premier p qui divise $\text{ppcm}[1,2,3,\dots,x]$ est précisément la plus grande puissance de p n'excédant pas x, on a que

$$\left(\prod_{p\le x} p\right) \times \left(\prod_{p^2\le x} p\right) \times \left(\prod_{p^3\le x} p\right) \times \dots = \text{ppcm}[1,2,3,\dots,x].$$

En combinant cela avec la prédiction de Riemann et en prenant les logarithmes, on déduit que

$$\left(\sum_{p\le x} \log p\right) \times \left(\sum_{p^2\le x} \log p\right) \times \left(\sum_{p^3\le x} \log p\right) \times \dots \text{ est environ } x.$$

Les nombres premiers dans la première somme ici sont précisément les nombres premiers comptés par $\pi(x)$, les nombres premiers dans la seconde somme sont ceux comptés par $\pi(x^{1/2})$, et etc. Par sommation partielle, on en déduit que

$$\pi(x) + \tfrac{1}{2}(x^{1/2}) + \tfrac{1}{3}(x^{1/3}) + \dots \approx \int_2^x \frac{dt}{\ln t} = \text{Li}(x).$$

Si on résout pour $\pi(x)$ de manière convenable, on trouve la forme équivalente

$$\pi(x) \approx \text{Li}(x) - \tfrac{1}{2}\text{Li}(x^{1/2}) + \dots.$$

Par conséquent, la méthode de Riemann amène plus ou moins la même prédiction que celle de Gauss, mais avec un supplément, le second terme qui, on l'espère, compensera l'excès qu'on a constaté avec la prédiction de Gauss. En revoyant les données (où "excès de Riemann" représente $\text{Li}(x) - \frac{1}{2}\text{Li}(\sqrt{x}) - \pi(x)$, alors que "excès de Gauss" représente $\text{Li}(x) - \pi(x)$ comme précédemment), on a :

x	{nombres premiers $\le$ x}	excès de Gauss	excès de Riemann
10^8	5761455	753	131
10^9	50847534	1700	−15
10^{10}	455052511	3103	−1711
10^{11}	4118054813	11587	−2097
10^{12}	37607912018	38262	−1050
10^{13}	346065536839	108970	−4944
10^{14}	3204941750802	314889	−17569
10^{15}	29844570422669	1052618	76456
10^{16}	279238341033925	3214631	333527
10^{17}	2623557157654233	7956588	−585236
10^{18}	24739954287740860	21949554	−3475062
10^{19}	234057667276344607	99877774	23937697
10^{20}	2220819602560918840	222744643	−4783163
10^{21}	21127269486018731928	597394253	−86210244
10^{22}	201467286689315906290	1932355207	−126677992

TABLE 6. Nombre de nombres premiers jusqu'à différentes valeurs de x, et prédictions de Gauss et Riemann.

La prédiction de Riemann ne semble pas mieux s'en sortir que celle de Gauss, ou du moins elle ne s'en sort pas beaucoup mieux. Pourtant, le fait que l'erreur de la prédiction de Riemann prenne des valeurs à la fois positives et négatives suggère qu'elle pourrait être le mieux qui puisse être fait.

8.2. Relier la théorie des nombres et l'analyse complexe. Riemann a montré que le nombre de nombres premiers jusqu'à x peut être obtenu en fonction des zéros complexes de la fonction

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \dots.$$

étudiée par Euler, qu'on appelle maintenant la *fonction zeta de Riemann*. Dans cette définition s est un nombre complexe, qu'on écrit $s = \sigma + it$ quand on veut faire référence à ses parties réelle et imaginaire σ et t séparément. Si s était un nombre réel, on saurait depuis les cours de calcul des premières années que la série dans la définition de $\zeta(s)$ converge si et seulement si $s > 1$; c'est-à-dire qu'on peut sommer une série infinie et obtenir comme résultat une valeur unique finie. De façon similaire, on peut montrer que la série converge seulement pour les nombres complexes tels que $\sigma > 1$. Mais qu'en est-il lorsque $\sigma \leq 1$? Comment contournons-nous le fait que la série ne peut se sommer (c'est-à-dire ne converge pas) ? Comme on l'a montré en section 7.7, on peut "prolonger analytiquement" $\zeta(s)$ de telle façon qu'elle soit bien définie dans la totalité du plan complexe. Plus que ça, $\zeta(s) - \frac{1}{s-1}$ est analytique, de telle façon que ζ est méromorphe, analytique en effet partout ailleurs qu'en son unique pôle en $s = 1$, qui est un pôle simple de résidu 1.

Riemann a montré que confirmer la conjecture de Gauss concernant le nombre de nombres premiers jusqu'à x est *équivalent* à obtenir une bonne compréhension des zéros de la fonction $\zeta(s)$, donc on va maintenant commencer à esquisser les étapes clefs de l'argument qui lie ces sujets qui sembleraient non reliés. Le point de départ est de prendre la dérivée du logarithme de l'identité d'Euler (2.2.1)

$$\zeta(s) = \sum_{\substack{n \geq 1 \\ n \text{ un entier positif}}} \frac{1}{n^s} = \prod_{p \text{ premier}} \left(1 - \frac{1}{p^s}\right)^{-1}, \tag{8.2.1}$$

pour obtenir

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p \text{ premier}} \frac{\log p}{p^s - 1} = \sum_{p \text{ premier}} \sum_{m \geq 1} \frac{\log p}{p^{ms}}.$$

La formule de Perron (7.6.2) permet de décrire une "fonction en escalier" en fonction d'une fonction continue de telle façon que si x n'est pas une puissance de nombre premier alors on obtient

$$\begin{aligned} \Psi(x) &:= \sum_{\substack{p^m \leq x \\ p \text{ premier} \\ m \geq 1}} \log p = \frac{1}{2\pi i} \sum_{\substack{p \text{ premier} \\ m \geq 1}} \log p \int_{s \,:\, \mathfrak{Re}(s) = c} \left(\frac{x}{p^m}\right)^s \frac{ds}{s} \\ &= -\frac{1}{2\pi i} \int_{s \,:\, \mathfrak{Re}(s) = c} \frac{\zeta'(s)}{\zeta(s)} \, \frac{x^s}{s} ds. \end{aligned} \tag{8.2.2}$$

Ici on peut justifier d'échanger l'ordre de la somme et de l'intégrale si c est suffisamment grand puisqu'alors, tout converge absolument. Notons qu'on ne compte pas le nombre de nombres premiers jusqu'à x mais plutôt la version "pondérée", $\Psi(x)$.

L'étape suivante est peut-être la plus difficile. L'idée est de remplacer la droite $\mathfrak{Re}(s) = c$ le long de laquelle l'intégrale a été prise par une droite loin à gauche, sur laquelle on peut montrer que l'intégrale est petite, en fait plus petite plus on va vers la gauche. La différence entre les valeurs le long de ces deux intégrales est donnée par une somme de résidus, comme décrit dans les sections 7.5 et 7.6. Maintenant pour toute fonction méromorphe f, les pôles de $f'(s)/f(s)$ sont donnés par les zéros et les pôles de f, tous d'ordre 1, et le résidu est simplement l'ordre de ce zéro, ou moins l'ordre de ce pôle. De cette façon, on peut obtenir la *formule explicite*

$$\Psi(x) = \sum_{\substack{p \text{ premier} \\ m \geq 1 \\ p^m \leq x}} \log p = x - \sum_{\rho \,:\, \zeta(\rho)=0} \frac{x^\rho}{\rho} - \frac{\zeta'(0)}{\zeta(0)}, \tag{8.2.3}$$

où, si ρ est un zéro de $\zeta(s)$ d'ordre k, alors il y a k termes pour ρ dans la somme. On peut se demander comment on ajoute la (potentiellement) infinie somme sur les zéros ρ de $\zeta(s)$? Simple, il suffit de les ajouter par ordre de valeurs de $|\rho|$ croissantes et cela marchera. Il est difficile de croire qu'une telle formule, fonction des zéros d'une fonction compliquée, peut fournir une expression exacte du nombre de nombres premiers jusqu'à x. On peut voir pourquoi le travail de Riemann a étiré l'imagination des gens et a eu un impact incroyable.

8.3. L'équation fonctionnelle. On a vu en section 7.7 comment prolonger analytiquement $\zeta(s)$ à tous les s pour lesquels $\mathfrak{Re}(s) > 0$. Riemann a fait une incroyable observation qui nous permet de déterminer facilement les valeurs de $\zeta(s)$ du côté gauche du plan complexe (où la fonction n'est pas définie naturellement) en fonction du côté droit. L'idée est de multiplier $\zeta(s)$ par une fonction simple de telle façon que ce nouveau produit $\xi(s)$ satisfasse l'*équation fonctionnelle*

$$\xi(s) = \xi(1-s) \quad \text{pour tous les nombres complexes } s. \tag{8.3.1}$$

Riemann a déterminé que l'on peut faire cela en prenant $\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s)$. Ici, $\Gamma(s)$ est une fonction qui est égale à la fonction factorielle pour les entiers positifs (c'est-à-dire que $\Gamma(n) = (n-1)!$) ; et elle est bien définie et continue pour tous les autres s.

8.4. Les zéros de la fonction zeta de Riemann. Une analyse du côté droit de (8.2.1) révèle qu'il n'y a pas de zéros de $\zeta(s)$ avec $\mathfrak{Re}(s) > 1$. Donc, en utilisant (8.3.1) et (7.9.4), on en déduit que les seuls zéros de $\zeta(s)$ avec $\mathfrak{Re}(s) < 0$ sont les entiers négatifs pairs -2, -4,..., ceux qu'on appelle les *zéros triviaux*. Par conséquent, pour pouvoir utiliser (8.2.3), on doit déterminer les zéros de $\zeta(s)$ à l'intérieur de la bande critique $0 \leq \mathfrak{Re}(s) \leq 1$. Après quelques calculs, Riemann a fait encore une autre observation extraordinaire qui, si elle était vraie, nous permettrait une compréhension perspicace formidable de virtuellement tous les aspects de la distribution des nombres premiers :[3]

L'HYPOTHÈSE DE RIEMANN : Si $\zeta(s) = 0$ avec $0 \leq \mathfrak{Re}(s) \leq 1$ alors $\mathfrak{Re}(s) = \dfrac{1}{2}$.

Des personnes intelligentes ont calculé littéralement des billions de zéros de $\zeta(s)$[4], et tout zéro unique dans la bande critique qui a été calculé a effectivement une partie réelle de 1/2. Par ex-

[3] Aucune référence à ces calculs de Riemann n'est apparue dans la littérature jusqu'à ce que Siegel les découvre dans les notes personnelles, non publiées de Riemann longtemps après sa mort.

[4] Au moins les dix billions de zéros de hauteurs les plus petites ; c'est-à-dire avec $|\mathfrak{Im}(s)|$ les plus petites.

emple, les zéros non triviaux les plus proches de l'axe réel sont $s = 1/2 + \gamma_1$ et $s = 1/2 - i\gamma_1$, où $\gamma_1 \approx 14.1347...$. Notons que si l'hypothèse de Riemann était vraie, alors on pourrait écrire tous les zéros non triviaux sous la forme $\rho = \frac{1}{2} + i\gamma$ (avec leur conjugué $\frac{1}{2} - i\gamma$, puisque $\zeta(1/2 + i\gamma) = 0$ si et seulement si $\zeta(1/2) - i\gamma = 0$), où γ est un nombre positif réel. On croit que les nombres positifs qui apparaissent dans les zéros non triviaux semblent plus ou moins aléatoires, au sens où aucun d'entre eux n'est relié aux autres par de simples équations linéaires à coefficients entiers (ou même par des équations polynomiales plus complexes avec des nombres algébriques comme coefficients). Pourtant, rien selon ces directions n'a jamais pu être prouvé, en effet tout ce qu'on sait faire c'est d'approximer ces zéros non triviaux numériquement jusqu'à une certaine précision.

On va démontrer qu'il y a une infinité de zéros $\beta+i\gamma$ de $\zeta(s)$ dans la bande critique, en effet environ $\frac{T}{2\pi}\log(\frac{T}{2e})$ avec $0 \le \gamma \le T$. Il n'est pas difficile de trouver tous les zéros jusqu'à une certaine hauteur T. On peut montrer que l'hypothèse de Riemann est vérifiée par au moins quarante pour cent de tous les zéros, et cela s'accorde joliment avec de nombreuses autres assertions heuristiques à propos de la distribution des nombres premiers et d'autres séquences de nombres, mais cela reste encore une hypothèse non démontrée, peut-être la plus célèbre et tentante de toutes les mathématiques.

8.5. Compter les nombres premiers. Au premier regard, il semble sensé d'utiliser une sommation partielle sur (8.2.3) pour obtenir une expression exacte pour $\pi(x)$, telle que

$$\pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \ldots = \mathrm{Li}(x) - \sum_{\rho\,:\,\zeta(\rho)=0} \mathrm{Li}(x^\rho) + \mathrm{Petit}(x) - \log 2,$$

où $\mathrm{Petit}(x) = \int_x^\infty \frac{dt}{(t^3-t)\log t}$[5]. Pourtant, celle-ci est beaucoup plus compliquée que (8.2.3), donc il sera plus facile de faire la sommation partielle à la fin des calculs plutôt qu'au début.

Puisque $\zeta(s)$ a une infinité de zéros dans la bande critique, (8.2.3) est une formule difficile à utiliser en pratique. En effet, on ne devrait pas s'attendre à utiliser une infinité d'ondes sinusoïdales à partir de la formule (7.2.1) pour approximer $\{x\} - \frac{1}{2}$ en pratique, mais à la place on pourrait utiliser un nombre fini d'ondes sinusoïdales, comme dans notre discussion là, vraisemblablement ceux avec les amplitudes les plus grandes. De façon similaire, on modifie (8.2.3) pour seulement inclure un nombre fini de zéros, en particulier ceux jusqu'à une certaine hauteur, T, qui sont dans la boîte

$$\mathcal{B}(T) = \{\rho \ : \zeta(\rho) = 0, 0 \le \mathfrak{Re}(\rho) \le 1, -T \le \mathfrak{Im}(\rho) \le T\}.$$

Ceci pourtant est une approximation, non une formule exacte, et cela vient au prix d'un terme d'erreur, qui dépend de la hauteur T : pour $1 \le T \le x$ on a[6]

$$\Psi(x) = x - \sum_{\substack{\rho\,:\,\zeta(\rho)=0 \\ 0<\mathfrak{Re}(\rho)<1 \\ |\mathfrak{Im}(\rho)|<T}} \frac{x^\rho}{\rho} + O\left(\frac{x\log x\log T}{T}\right). \tag{8.5.1}$$

Notre but est de montrer que $\Psi(x) \sim x$, donc on sélectionne $T \ge (\log x)^2$, et par conséquent, on a seulement besoin de borner la somme sur les zéros de $\zeta(s)$. Chaque terme dans cette somme est

[5]Cette expression apparaît dans l'article de Riemann. L'expression plus simple (8.2.3) est due von Mangoldt.

[6]Les zéros triviaux sont -2,-4,-6,... et ainsi contribuent pour $\sum_{m\le 1} 1/(2mx^{2m}) = -\frac{1}{2}\log(1-\frac{1}{x^2})$ au total dans (8.2.3), qui est en $O(1)$ pour $x \ge 1$.

un nombre complexe et consiste donc en une grandeur et une direction et on peut deviner qu'il y a beaucoup d'annulations parmi ces termes, résultant des différentes directions pointées. Pourtant on est incapable de démontrer quoi que ce soit dans cette direction-là, ce qui désappointe plutôt, on borne simplement chaque terme en valeur absolue :

$$\left|\sum_{\rho\in\mathcal{B}(T)}\frac{x^\rho}{\rho}\right| \le \sum_{\rho\in\mathcal{B}(T)}\left|\frac{x^\rho}{\rho}\right| \le \max_{\rho\in\mathcal{B}(T)} x^{\mathfrak{Re}(\rho)}\sum_{\rho\in\mathcal{B}(T)}\frac{1}{|\rho|} \ll x^{\beta(T)}(\log T)^2,$$

en utilisant le fait qu'il y a environ $\frac{T}{2\pi}\log\left(\frac{T}{2e}\right)$ zéros dans $\mathcal{B}(T)$ pour tout T, où $\beta(T)$ est la plus grande partie réelle d'un zéro quelconque dans $\mathcal{B}(T)$.

L'étape finale pour prouver le théorème des nombres premiers est alors de produire des *régions sans zéros* pour $\zeta(s)$: c'est-à-dire des régions du plan complexe, proches de la droite $\mathfrak{Re}(s) = 1$, sans zéros de $\zeta(s)$. Par exemple, dans la section 9.6, on montre qu'on peut prendre $\beta(T) = 1 - c/\log T$ pour une certaine constante $c > 0$. Par conséquent, en choisissant T de telle façon que $\log T = (\log x)^{1/2}$ on déduit que

$$\Psi(x) = x + O\left(x/e^{c'(\log x)^{1/2}}\right)$$

pour une certaine constante $c' > 0$, ce qui implique le théorème des nombres premiers,

$$\pi(x) = \mathrm{Li}(x) + O\left(x/e^{c'(\log x)^{1/2}}\right).$$

On peut voir que n'importe quelle amélioration dans la région sans zéros pour $\zeta(s)$ apportera immédiatement des améliorations dans le terme d'erreur du théorème des nombres premiers. Par exemple, si l'hypothèse de Riemann est vraie, de telle façon que $\beta(T) = \frac{1}{2}$ pour tout T, alors en prenant $T = \sqrt{x}$ dans (8.5.1), on obtient que $\Psi(x) = x + O(x^{1/2}(\log x)^2)$,[7] et donc

$$\pi(x) = \int_2^x \frac{\mathrm{d}t}{\log t} + O(\sqrt{x}\log x) \tag{8.5.2}$$

On montrera que ceci n'est pas seulement impliqué par l'hypothèse de Riemann, mais également que cela implique l'hypothèse de Riemann. Avec davantage de soin, on peut démontrer que la borne plus précise

$$|\pi(x) - \mathrm{Li}(x)| \le \sqrt{x}\log x \quad \text{pour tout } x \ge 3, \text{ est équivalente à l'hypothèse de Riemann.}$$

8.6. La formule révolutionnaire de Riemann. La formule de Riemann (8.2.3) est un peu difficile à apprécier au premier regard. Si on suppose que l'hypothèse de Riemann est vraie, alors tout zéro non trivial peut être écrit comme $1/2 + i\gamma$ et par conséquent contribue à hauteur de $x^{1/2+i\gamma}/(\frac{1}{2} + i\gamma)$. Maintenant au fur et à mesure qu'on change de zéro de $\zeta(s)$ la valeur de γ augmente et $\frac{1}{2}+i\gamma$ sera dominé par la valeur de $i\gamma$. Donc $x^{1/2+i\gamma}/(\frac{1}{2}+i\gamma)$ est à peu près $x^{1/2+i\gamma}/(i\gamma)$. En ajoutant cela au terme pour $\frac{1}{2} - i\gamma$, on obtient, à peu près, $x^{1/2+i\gamma}/(i\gamma) - x^{1/2-i\gamma}/(i\gamma) = 2x^{1/2}\sin(\gamma\log\ x)/\gamma$. En combinant cette information, (8.2.3) devient

$$\Psi(x) \text{ est à peu près } x - 2x^{1/2}\sum_{\gamma>0\,:\,\zeta(\frac{1}{2}+i\gamma)=0}\frac{\sin(\gamma\log\ x)}{\gamma} + O(1).$$

[7] ce qui est une forme faible de (8.1.1) puisque $\Psi(x) = \log(\mathrm{ppcm}[1, 2, \dots, x])$.

On veut convertir cela en information à propos du nombre de nombres premiers jusqu'à x. Si on procède par sommation partielle alors $\Psi(x)$ devrait être remplacé par $\pi(x) + \frac{1}{2}\pi(x^{1/2}) + ...$, comme dans la section 8.1, et $x^{1/2}$ par $x^{1/2}/\log x$. Par conséquent, après quelques ré-arrangements,

$$\boxed{\frac{\int_2^x \frac{\mathrm{d}t}{\ln t} - \#\{\text{nombres premiers} \le x\}}{\sqrt{x}/\ln x} \approx 1 + 2 \sum_{\substack{\text{tous les nombres réels } \gamma>0 \\ \text{tels que } \frac{1}{2}+i\gamma \\ \text{est un zéro de } \zeta(s)}} \frac{\sin(\gamma \log x)}{\gamma}.} \tag{8.6.1}$$

Le numérateur du côté gauche de cette formule est le terme excédentaire quand on compare à la prédiction de Gauss $\mathrm{Li}(x)$ avec le nombre effectif $\pi(x)$ de nombres premiers jusqu'à x. Le dénominateur, étant à peu près de taille $\sqrt{x}$, correspond à la grandeur de l'excès comme on l'a observé précédemment dans nos données. Le côté droit de la formule a beaucoup en commun avec notre formule pour $\{x\} - 1/2$. C'est la somme de fonctions sinus, avec les nombres γ employés de deux façons différentes à la place de $2\pi n$: chaque γ est utilisé à l'intérieur du sinus (comme la "fréquence"), et l'inverse de chacun forme le coefficient du sinus (comme l'"amplitude"). On obtient même le même facteur de 2 dans chaque formule. Pourtant, les nombres γ ici sont beaucoup plus subtils que les nombres évidents $2\pi n$ dans la formule correspondante pour $x - 1/2$. Cette formule peut peut-être être paraphrasée par

Les nombres premiers peuvent être comptés comme une somme d'ondes.

On devrait noter que cette formule est valide si et seulement si l'hypothèse de Riemann est vraie et on croit donc grandement qu'elle est correcte. Il y a une formule similaire si l'hypothèse de Riemann est fausse, mais elle est plutôt compliquée et techniquement beaucoup moins agréable. La principale difficulté provient des coefficients, $1/\gamma$, qui sont remplacés par des fonctions de x. Donc on souhaiterait que l'hypothèse de Riemann soit vraie car elle amène à la formule plus simple (8.6.1), et que cette formule est un délice. En effet, cette formule est assez similaire aux formules pour les ondes sonores et certains experts, pour affirmer cette formule (8.6.1), disent que "*les nombres premiers ont la musique en eux.*"

Sur l'article de Riemann, "Sur le nombre de nombres premiers inférieurs à une grandeur donnée"

W. Dittrich
Institut de physique théorique
Université de Tübingen
Auf der Morgenstelle 14
D-72076 Tübingen
Allemagne

Résumé : Cet article est dédié à l'un des trois membres du triumvirat de Göttingen, Gauß, Dirichlet et Riemann. C'est au dernier que je souhaiterais rendre honneur, et particulièrement à son article de 1859, qu'il présenta en personne à l'Académie de Berlin lors de son élection comme membre correspondant. Son article intitulé "Über die Anzahl der Primzahlen unter einer gegebenen Größe" ("Sur le nombre de nombres premiers inférieurs à une grandeur donnée") a révolutionné les mathématiques mondiales. Dans le présent article, on mène une analyse détaillée de l'article de Riemann, incluant des concepts nouveaux comme le prolongement analytique dans le plan complexe ; la formule du produit pour les fonctions entières ; et, en dernier lieu mais non des moindres, une étude détaillée des zéros et de celle qu'on appelle la fonction zeta de Riemann et de sa relation proche à la détermination du nombre de nombres premiers jusqu'à une certaine grandeur, i.e. une formule explicite pour la fonction de décompte des nombres premiers.

Courte biographie de Bernhard Riemann (1826 - 1866)

Bernhard Riemann est né à Breselenz près de Dannenberg en Basse-Saxe en 1826. Comme son père, il était d'abord supposé devenir pasteur, mais déjà au lycée, le talent extraordinaire de Riemann en mathématiques attira l'attention du Principal. On dit que Riemann lut le livre de Legendre de théorie des nombres de 859 pages qui lui avait été prêté par le Principal en une semaine. Il commença à étudier les mathématiques à Göttingen, où il assista aux cours de Gauß, bien qu'ils soient fermés aux étudiants de premier semestre. Riemann fut alors transféré à Berlin auprès de Jacobi et Dirichlet qui tous deux le soutinrent et l'encouragèrent ; il retourna alors à Göttingen. Sa thèse doctorale portait sur la théorie des fonctions. Pour avoir le droit d'enseigner comme professeur privé à Göttingen,

Référence : https://arxiv.org/pdf/1609.02301.pdf.
Traduction : Denise Vella-Chemla, août 2023.

les candidats devaient proposer trois sujets pour leur exposé d'habilitation, et normalement le chef du département choisissait le premier sujet de la liste. Le troisième sujet de Riemann était "Les bases de la géométrie", et quand il lut cela, Gauß, en tant que chef du département, choisit ce sujet pour l'exposé d'habilitation de Riemann. Très surpris, Riemann mit toutes ses recherches sur le sujet "Électricité, magnétisme, lumière et gravitation" de côté et deux mois avant sa leçon test, il créa les fondements de la géométrie différentielle. Gauß était content ! En 1855 Gauß mourut et Dirichlet lui succéda. Quand Dirichlet mourut quatre ans plus tard, Riemann prit en charge la chaire de mathématiques à l'Université de Göttingen. En 1862, il épousa Elise Koch, avec qui il eut une fille. Riemann attrapa la tuberculose et il chercha à améliorer sa santé dans le climat plus doux du Tessin, où il mourut au jeune âge de seulement 39 ans au Lac Majeur.

En plus de fonder la géométrie différentielle, Riemann fit d'autres contributions majeures ; son travail dans la théorie des fonctions a été particulièrement important ; son article "Über die Anzahl der Primzahlen unter einer gegebenen Größe" (Sur le nombre de nombres premiers inférieurs à une grandeur donnée), communiqué dans le Monatsberichte der Berliner Akademie, en novembre 1859, avec des découvertes sur la fonction zeta ; ses travaux sur la théorie de l'intégration, la transformée de Fourier, l'équation différentielle hyper-géométrique, et les équations différentielles hyperboliques et les problèmes de stabilité des solutions des équations différentielles partielles en physique mathématique. Riemann était influencé par les recherches en géométrie algébrique et topologie de ses collègues mathématiciens italiens Betti et Beltrami. La théorie de la relativité générale d'Einstein aurait été impensable sans la géométrie riemanienne.

Tous ces sujets ont occupé les mathématiciens et les physiciens théoristes pendant de nombreuses années et continueront de le faire pour de longues années encore. Aujourd'hui, exactement 150 ans après la mort de Riemann, le problème non résolu le plus grand en mathématiques pures est ce qu'on appelle l'hypothèse de Riemann, une conjecture énoncée par Riemann en 1859 dans son article sur le nombre de nombres premiers inférieurs à un certain entier positif donné x.

Les mathématiciens réalisèrent plus tard que l'hypothèse de Riemann gouverne la distribution des nombres premiers à un degré extraordinaire, ce pourquoi sa preuve est si avidement recherchée. Puisque tous les efforts de quelques-uns des meilleurs mathématiciens ont échoué jusque là, peut-être faudrait-il un autre Riemann.

Ceci est également vrai pour de nombreux modèles en théorie quantique des champs des particules élémentaires, où les résultats de Riemann sont de la plus haute importance pour

gérer les infinis à l'aide de sa régularisation de la fonction zeta. En mécanique quantique non relativiste, on a besoin de l'hamiltonien riemanien qui devient diagonalisé dans la base des nombres premiers. Le processus de mesure, i.e. l'opérateur agissant sur un objet qui nous fournira un ensemble de valeurs propres qui soit l'ensemble des nombres premiers est encore à trouver. On peut se demander quelle sorte de structure de symétrie se cache derrière un tel système physique.

N'oublions pas que le peu d'articles que Riemann a publié tout au long de sa vie traitent de problèmes physiques. De plus, du temps de Gauß, Dirichlet et Riemann, la distinction entre les disciplines mathématique et physique n'existait pas. En particulier, Riemann approchait les problèmes mathématiques et physiques non pas comme un analyste mais il les éclairait plutôt globalement d'un point de vue géométrique et topologique, ceci signifiant qu'il rendit de nombreux résultats de l'analyse plus compréhensibles en utilisant les nouvelles méthodes de la théorie des fonctions et du prolongement analytique au plan complexe dans sa totalité, simplifiant ainsi de nombreux problèmes de l'analyse réelle.

1 Vers la formule du produit d'Euler et l'extension de Riemann de la fonction zeta

Il y a une connexion très forte entre les sommes des inverses des entiers élevés à une puissance variable qu'Euler écrivit en 1737, et qu'on appelle maintenant la fonction zeta,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots, \qquad s > 1 \tag{1}$$

et les nombres premiers - qui, comme entiers, sont la véritable signature de la discontinuité. Euler considérait s comme une variable vraiment entière avec $s > 1$ pour assurer la convergence de la somme. En multipliant la définition de $\zeta(s)$ par $1/2^s$, on obtient

$$\frac{1}{2^s}\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{(2n)^s} = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \cdots \tag{2}$$

et en soustrayant cela de $\zeta(s)$, on obtient

$$\zeta(s) - \frac{1}{2^s}\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} - \sum_{n=1}^{\infty} \frac{1}{(2n)^s}$$

$$\text{ou} \qquad \left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \frac{1}{11^s} + \cdots. \tag{3}$$

Par conséquent tous les multiples du nombre premier $n = 2$ disparaissent de la somme originale de la définition de $\zeta(s)$. En bref, on trouve

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = \sum_{\substack{n=1 \\ \Lambda n \neq 2k}}^{\infty} \frac{1}{n^s}\,. \tag{4}$$

Ensuite, on multiplie ce dernier résultat par $1/3^s$ pour obtenir

$$\frac{1}{3^s}\left(1 - \frac{1}{2^s}\right)\zeta(s) = \sum_{\substack{n=1 \\ \Lambda n \neq 2k}}^{\infty} \frac{1}{(3n)^s} = 1 + \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \frac{1}{21^s} + \cdots \tag{5}$$

et ainsi, en soustrayant cela de $(1 - 1/2^s)\zeta(s)$, on a

$$\begin{aligned}\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right)\zeta(s) &= 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \cdots \\ &= \sum_{\substack{n=1 \\ \Lambda n \neq 2k \\ \Lambda n \neq 3k}}^{\infty} \frac{1}{n^s}\,.\end{aligned} \tag{6}$$

Maintenant, on multiplie ce résultat par $1/5^s$ et etc. Comme on répète ce processus encore et encore, multipliant notre dernier résultat par $1/p^s$, où p dénote les nombres premiers successifs, on soustrait tous les multiples des nombres premiers. Par conséquent, puisque tous les entiers sont composés des nombres premiers (théorème fondamental d'Euclide de la théorie des nombres), on a enlevé tous les nombres du côté droit de la somme définissant $\zeta(s)$ - excepté pour le nombre 1. Ainsi notre résultat final est le produit

$$\left\{\Pi_{p\,\text{premier}}\left(1 - p^{-s}\right)\right\}\zeta(s) = 1 \tag{7}$$

ou

$$\boxed{\zeta(s) = \Pi_{p\,\text{premier}}\frac{1}{1 - p^{-s}} = \sum_{n=1}^{\infty}\frac{1}{n^s}\,, \qquad s > 1}\,. \tag{8}$$

L'assertion exacte d'Euler est : "Si ex serie numerorum primorum sequens formetur expressio $\prod\limits_{p} \frac{p^s}{(p^s-1)}$ erit eius valor aequalis summae huius seriei $\sum\limits_{n=1} \frac{1}{n^s}$."
Maintenant on va étendre la fonction zeta d'Euler dans le plan complexe C, ce qui est une découverte majeure de Riemann. Donc à partir de maintenant, s est une valeur complexe et on écrit

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots \qquad \text{mais avec} \quad \mathfrak{Re}(s) > 1\,. \tag{9}$$

Ceci est une série infinie absolument convergente, qui est également vérifiée par le produit de tous les nombres premiers dans

$$\zeta(s) = \Pi_{p\,\text{premier}} \frac{1}{1-p^{-s}} = \left(\frac{1}{1-2^{-s}}\right)\cdot\left(\frac{1}{1-3^{-s}}\right)\cdot\left(\frac{1}{1-5^{-s}}\right)\cdots\left(\frac{1}{1-p^{-s}}\right)\cdots . \quad (10)$$

$\zeta(s)$ n'a pas de zéros dans la région $\mathfrak{Re}(s) > 1$, puisqu'aucun de ses facteurs n'a de zéros. Pourtant, avec l'extension de Riemann de zeta à tout le plan complexe, on sera capable de localiser les zéros aussi bien que les pôles. Pour montrer cela, on doit prolonger analytiquement la fonction zeta originale d'Euler à tout le plan complexe s. Un premier résultat dans cette direction sera obtenu à l'aide des séries qu'on dit de Dirichlet qui adviennent quand on calcule

$$\begin{aligned}(1-2^{1-s})\zeta(s) &= \sum_{n=1}^{\infty} n^{-s} - 2^{1-s}\sum_{n=1}^{\infty} n^{-s} = \sum_{n=1}^{\infty} n^{-s} - 2\sum_{n=1}^{\infty}(2n)^{-s} \\ &= 1 - \frac{2}{2^s} + \frac{1}{2^s} - \frac{2}{4^s} + \cdots = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \frac{1}{5^s} - \frac{1}{6^s} + \cdots \\ &= \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s} =: \eta(s)\,, \qquad \text{série de Dirichlet}\,. \end{aligned} \quad (11)$$

Cette série est convergente pour tout $s \in C$ avec $\mathfrak{Re}(s) > 0$. Donc on peut définir

$$\boxed{\zeta(s) = \frac{1}{1-2^{1-s}} \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s} \qquad \text{pour} \quad \mathfrak{Re}(s) > 0 \quad \text{et} \quad 1 - 2^{1-s} \neq 0\,.} \quad (12)$$

Quand on écrit

$$\begin{aligned}\eta(s) + \frac{2}{2^s}\zeta(s) &= \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s} + \frac{2}{2^s}\sum_{n=1}^{\infty}\frac{1}{n^s} \\ &= \sum_{n=1}^{\infty}\left(\frac{1}{(2n-1)^s} - \frac{1}{(2n)^s} + \frac{2}{(2n)^s}\right) \\ &= \sum_{n=1}^{\infty}\frac{1}{n^s} = \zeta(s)\,, \end{aligned} \quad (13)$$

on peut rassembler les résultats obtenus jusque-là en la suite d'égalités

$$\zeta(s) = \frac{1}{1-2^{1-s}}\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n^s} = \frac{\eta(s)}{1-2^{1-s}} = \frac{1}{s-1}\sum_{n=1}^{\infty}\left(\frac{n}{(n+1)^s} - \frac{n-s}{n^s}\right)\,. \quad (14)$$

Plus important, on peut prolonger $\zeta(s)$ dans le domaine de la bande critique $0 < \mathfrak{Re}(s) < 1$. Bien sûr, les zéros dans le dénominateur de la représentation donnée ci-dessus doivent être exclus, i.e. de

$$1 - 2^{1-s} = 0 \quad (15)$$

découle

$$1 = e^{(1-s)\log 2} \tag{16}$$

signifiant que

$$2\pi i n = (1-s)\log 2 \tag{17}$$

ou

$$s = 1 - \frac{2\pi i n}{\log 2}\,, \qquad n \in \mathbb{Z}\,. \tag{18}$$

Ayant montré que la fonction zeta peut être prolongée analytiquement dans le demi-plan $\{s \in C | \mathfrak{Re}(s) > 0, s \neq 1\}$, on doit encore démontrer que $\zeta(s)$ a un pôle en $s = 1$:

$$\begin{aligned}\lim_{s\to 1}\zeta(s) &= \lim_{s\to 1}\frac{(s-1)}{1-2^{1-s}}\sum_{n=1}^{\infty}(-1)^{n+1}n^{-s} = \lim_{s\to 1}\frac{(s-1)}{1-2^{1-s}}\log 2 \\ &= \lim_{s\to 1}\frac{1}{-\log 2\cdot 2^{1-s}\cdot(-1)}\log 2 = \lim_{s\to 1}\frac{1}{2^{1-s}} = 1\,,\end{aligned} \tag{19}$$

où on utilise le théorème d'Abel $\lim_{x\to 1^-}\log(x+1) = \log 2$ et la continuité de $\log(x+1)$. Combien d'arguments environ de la fonction zeta sont égaux ou inférieurs à zéro ? Plus tard on montrera que la fonction zeta satisfait l'équation fonctionnelle

$$\zeta(s) = 2^s\pi^{s-1}\sin\left(\frac{\pi s}{2}\right)\Gamma(1-s)\zeta(1-s)\,. \tag{20}$$

Cela définit $\zeta(s)$ dans la totalité du plan complexe s. Notons que le côté gauche passe par-dessus en changeant juste $s \to 1-s$ dans $\zeta(1-s)$, donc on peut calculer $\zeta(1-s)$, étant donné $\zeta(s)$, par exemple $\zeta(-15)$ en fonction de $\zeta(16)$.

Si s est un entier négatif pair, alors $\zeta(s) = 0$ parce que le facteur $\sin(\pi s/2)$ s'évanouit. Ce sont les zéros triviaux de la fonction zeta. Ainsi, tous les zéros non triviaux sont dans la bande critique de partie réelle comprise entre 0 et 1.

Voici une première curiosité qui nécessite davantage d'interprétation. Si on substitue dans l'équation fonctionnelle $s = -1$, on obtient

$$\zeta(-1) = 2^{-1}\pi^{-2}(-1)\Gamma(2)\zeta(2) = \frac{1}{2}\cdot\frac{1}{\pi^2}(-1)\cdot 1\cdot\frac{\pi^2}{6} = -\frac{1}{12}\,, \tag{21}$$

ce qui signifie que $\zeta(-1) = -1/12$.

Cette valeur de $\zeta(-1)$ régularisée n'a absolument rien à voir avec la représentation dans l'espace réel de $\zeta(-1)$ par la série divergente $\zeta(-1) = \sum_{n=1}^{\infty}\frac{1}{n^{-1}} = 1+2+3+4+\cdots$, qui nous

dit que la même fonction peut avoir différentes interprétations. Quelques mathématiciens très savants entretiennent l'opinion que la régularisation de la fonction zeta a balayé les laides divergences vers l'infini et a produit une "noisette dorée" de séries qui sont tout le contraire de non-convergentes. En théorie quantique, on observe le même phénomène, où la régularisation de la fonction zeta fait disparaître les infinis (effet Casimir, électrodynamique quantique, chromodynamique quantique et production de particules à proximité des trous noirs). Nous reviendrons sur ce point vers la fin de cet article.

2 Fonction de comptage des puissances de nombres premiers

Sur le chemin pour montrer la significativité des zéros de zeta pour compter les nombres premiers, Riemann a introduit une importante fonction pondérée de comptage des nombres premiers $f(x)$. On l'appellera $\Pi(x)$ alors que d'autres utilisent $J(x)$. Puisque cette fonction est de la plus haute importance, on commencera par l'introduire au moyen d'exemples.

D'abord, la définition de $\Pi(x)$ est donnée ainsi

$$\Pi(x) = \sum_{\substack{p^n < x \\ p \text{ premier}}} \frac{1}{n}\,, \tag{22}$$

i.e. pour toute puissance de premier p^n qui est plus petite que x, on somme ses fractions ; par exemple,

$$\begin{aligned}\Pi(20) = &\underbrace{\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}\right)}_{2^1,2^2,2^3,2^4<20} + \underbrace{\left(\frac{1}{1}+\frac{1}{2}\right)}_{3^1,3^2<20} + \underbrace{\left(\frac{1}{1}\right)}_{5^1<20} + \underbrace{\left(\frac{1}{1}\right)}_{7^1<20} + \underbrace{\left(\frac{1}{1}\right)}_{11^1<20} + \underbrace{\left(\frac{1}{1}\right)}_{13^1<20} \\ &+ \underbrace{\left(\frac{1}{1}\right)}_{17^1<20} + \underbrace{\left(\frac{1}{1}\right)}_{19^1<20}\end{aligned} \tag{23}$$

Les crochets peuvent aussi être réorganisés ainsi :

$$\begin{aligned}\Pi(20) = &\left(\frac{1}{1}+\frac{1}{1}+\frac{1}{1}+\frac{1}{1}+\frac{1}{1}+\frac{1}{1}+\frac{1}{1}+\frac{1}{1}\right) \\ &+ \frac{1}{2}\left(\frac{1}{1}+\frac{1}{1}\right) + \frac{1}{3}\left(\frac{1}{1}\right) + \frac{1}{4}\left(\frac{1}{1}\right)\,.\end{aligned} \tag{24}$$

La première paire de crochets compte le nombre de nombres premiers inférieurs à $x = 20$; la seconde paire compte les nombres premiers qui sont plus petits que la racine carrée de x, etc. Par conséquent, en notant $\Pi(x)$ le nombre de nombres premiers jusqu'à x, on obtient la formule de Riemann,

$$\Pi(x) = \sum_{n=1}^{\infty} \frac{1}{n} \pi(x^{1/n}) \,, \tag{25}$$

qui contient un nombre fini de termes, ce qui devient évident en regardant l'exemple suivant :

$$\begin{aligned} \Pi(x) &= \pi(x) + \frac{1}{2}\pi(\sqrt[2]{x}) + \frac{1}{3}\pi(\sqrt[3]{x}) + \frac{1}{4}\pi(\sqrt[4]{x}) + \cdots \\ x &= 100 : \\ \sqrt[2]{x} &= 10, \sqrt[3]{x} = 4.6415 \,, \sqrt[4]{x} = 3.1622, \sqrt[5]{x} = 2.51188 \,, \\ \sqrt[6]{x} &= 2.15 \ldots, \sqrt[7]{x} = 1.930 \ldots < 2 \,. \end{aligned} \tag{26}$$

Si l'argument de Π est inférieur à 2, alors $\Pi(x) = 0$. Donc notre résultat pour $\Pi(100)$ est donné par

$$\begin{aligned} \Pi(100) = \pi(100) &+ \frac{1}{2}\pi(10) + \frac{1}{3}\pi(4.6415) + \frac{1}{4}\pi(3.1622) \\ &+ \frac{1}{5}\pi(2.5118) + \frac{1}{6}\pi(2.15) + 0 + 0 + \cdots \,. \end{aligned} \tag{27}$$

En comptant les nombres premiers, on obtient

$$\begin{aligned} \Pi(100) &= 25 + \frac{1}{2} \cdot 4 + \frac{1}{3} \cdot 2 + \frac{1}{4} \cdot 2 + \frac{1}{5} \cdot 1 + \frac{1}{6} \cdot 1 \\ &= 28\frac{8}{15} = 28.533 \,. \end{aligned} \tag{28}$$

Donc, pour n'importe quel argument $x > 1$, la valeur $\Pi(x)$ peut être calculée par une somme finie. Jusque là, on a appris que $\Pi(x)$ compte les nombres premiers. Évidemment, $\Pi(x)$ est une fonction en escalier qui commence en $\Pi(0) = 0$ et augmente pour certains entiers positifs, i.e. le saut est de 1 pour les premiers, 1/2 pour les carrés de premiers, 1/3 pour les cubes de premiers. Donc nos équations définissant $\Pi(x)$ peuvent aussi s'écrire comme

$$\Pi(x) = \sum_{p} \sum_{n=1}^{\infty} \frac{1}{n} \Theta(x - p^n) \,, \tag{29}$$

où $\Theta(x)$ est la fonction en escalier de Heaviside donnée par $\Theta(x) = \begin{cases} 1 & , \quad x > 0 \\ \frac{1}{2} & , \quad x = 0 \\ 0 & , \quad x < 0 \end{cases}$.

Il y a encore une autre fonction de la théorie analytique des nombres dont on a besoin. On l'appelle la fonction de Möbius, elle définit l'inverse de la fonction zeta :

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1 - \frac{1}{2^s} - \frac{1}{3^s} - \frac{1}{5^s} + \frac{1}{6^s} - \frac{1}{7^s} + \cdots . \tag{30}$$

En utilisant la représentation originale

$$\frac{1}{\zeta(s)} = \left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{5^s}\right)\left(1 - \frac{1}{7^s}\right)\cdots , \tag{31}$$

on peut calculer la multiplication des différents facteurs et terminer ainsi à nouveau avec

$$1 - \frac{1}{2^s} - \frac{1}{3^s} - \frac{1}{5^s} + \frac{1}{6^s} - \frac{1}{7^s} + \frac{1}{10^s} - \cdots , \tag{32}$$

qui identifie les valeurs suivantes de μ :

$$\begin{aligned} &\mu(1) = 1, \mu(2) = -1, \mu(3) = -1, \mu(4) = 0, \mu(5) = -1 , \\ &\mu(6) = 1, \mu(7) = -1, \mu(8) = 0, \mu(9) = 0, \mu(5) = 1, etc. \end{aligned} \tag{33}$$

Voici la règle :

$$\mu(n) = \begin{cases} -1 & \text{si } n \text{ contient un nombre impair de nombres premiers} \\ 1 & \text{si } n \text{ contient un nombre pair de nombres premiers} \\ 0 & \text{si } n \text{ contient comme facteur un nombre premier au carré} \end{cases} \tag{34}$$

Par exemple:

$$\begin{array}{lll} \mu(7) = -1; & 7 & \text{est un nombre premier} \\ \mu(66) = -1; & 66 = 2 \cdot 3 \cdot 11, & \text{contient un nombre impair de nombres premiers} \\ \mu(18) = 0; & 18 = 2 \cdot 3^2, & \text{contient un carré de premier} \end{array} \tag{35}$$

Pour l'usage ultérieur, on liste les nombres de Möbius en début de liste :

$\mu(n) = -1$	2	3	5	7	11	13	17	19	23	29	30	31	37		
$\mu(n) = 0$	4	8	9	12	16	18	20	24	25	27	28	32	36		
$\mu(n) = +1$	1	6	10	14	15	21	22	26	33	34	35	38	39		

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\mu(n)$	1	−1	−1	0	−1	1	−1	0	0	1	−1	0	−1	1	1	0	−1	0	−1	0

La relation entre $\Pi(x)$ et $\pi(x)$ est inversée par Riemann au moyen de la formule d'inversion de Möbius pour obtenir

$$\pi(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \Pi(x^{1/n}) = \Pi(x) - \frac{1}{2}\Pi(x^{1/2}) - \frac{1}{3}\Pi(x^{1/3}) - \frac{1}{5}\Pi(x^{1/5}) + \frac{1}{6}\Pi(x^{1/6}) + \cdots . \quad (36)$$

Dans la partie finale de cette section, je souhaite discuter brièvement d'une certaine transformation intégrale qui sera d'un grand secours dans la prochaine section. Cette transformation de noyau $K(z, \xi) = \xi^{z-1}$ est appelée transformation de Mellin, bien que Riemann l'ait connue quarante ans avant qu'elle ne devienne connue sous ce nom.

Commençons par

$$g(z) = \int_0^{\infty} d\xi \xi^{z-1} f(\xi) \,, \quad (37)$$

par exemple, avec le côté gauche donné par $\Gamma(s), \mathfrak{Re}(s) > 0$ et $f(x) = e^{-x}$:

$$\Gamma(s) = \int_0^{\infty} dx e^{-x} x^{s-1} \text{ avec inverse } e^{-x} = \frac{1}{2\pi i} \int_{a-i_\infty}^{a+i_\infty} ds \frac{\Gamma(s)}{x^s} \,. \quad (38)$$

Maintenant remplaçons x par $nx (n = 1, 2, 3...)$, alors multiplions les équations par des constantes c_n et sommons sur n:

$$\sum_{n=1}^{\infty} \frac{c_n}{n^s} = \frac{1}{\Gamma(s)} \int_0^{\infty} x^{s-1} \left\{ \sum_{n=1}^{\infty} c_n (e^{-x})^n \right\} dx \,,$$

$$\sum_{n=1}^{\infty} c_n (e^{-x})^n = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} \frac{\Gamma(s)}{x^s} \left\{ \sum_{n=1}^{\infty} \frac{c_n}{n^s} \right\} ds \,. \quad (39)$$

On peut voir que la transformation de Mellin change la série de puissances $\Sigma c_n (e^{-x})^n$ en une série de Dirichlet $\Sigma c_n / n^s$ et l'inverse de la transformation de Mellin change une série de Dirichlet en série de puissances.

En particulier, si on note $c_n = 1$ pour tout n, alors avec $\Sigma (e^{-x})^n = 1/(e^x - 1)$ on obtient une représentation intégrale de la fonction zeta de Riemann :

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^{\infty} \frac{x^{s-1}}{e^x - 1} dx \,, \qquad \mathfrak{Re}(s) > 1 \quad (40)$$

dont l'inverse est donné par

$$\frac{1}{e^x-1}=\frac{1}{2\pi i}\int\limits_{a-i\infty}^{a+i\infty}\frac{\Gamma(s)\zeta(s)}{x^x}ds\quad(a>1)\,. \tag{41}$$

Une des plus importantes formules dans l'article de Riemann est

$$\frac{\log\zeta(s)}{s}=\int\limits_0^\infty\Pi(x)x^{-s-1}dx\,. \tag{42}$$

Ici on reconnaît pour la première fois la forte connexion entre les zéros de zeta et la fonction $\Pi(x)$. Pour mieux comprendre la formule ci-dessus, prenons le logarithme des deux côtés de

$$\zeta(s)=\prod_p\frac{1}{1-p^{-s}} \tag{43}$$

et en utilisant $\log(1-x)=-x-1/2\,x^2-1/3\,x^3\cdots$ on obtient

$$\log\zeta(s)=-\sum_p\log(1-p^{-s})=\sum p^{-s}+\frac{1}{2}\sum p^{-2s}+\frac{1}{3}\sum p^{-3s}+\cdots\,. \tag{44}$$

Ici on utilise les identités ($\mathfrak{Re}(s)>1$)

$$p^{-s}=s\int\limits_p^\infty x^{-s-1}ds\,,\qquad p^{-2s}=s\int\limits_{p^2}^\infty x^{-s-1}dx\,,\qquad\cdots\,,\qquad p^{-ns}=s\int\limits_{p^n}^\infty x^{-s-1}dx\,,\cdots \tag{45}$$

pour écrire

$$\begin{aligned}\log\zeta(s)&=\sum_p\sum_n\frac{1}{n}p^{-ns}=\sum_p\sum_n\frac{1}{n}\cdot s\int\limits_{p^n}^\infty x^{-s-1}dx\\&=s\int\limits_0^\infty\Pi(x)x^{-s-1}dx\,.\end{aligned} \tag{46}$$

Pour expliquer la dernière ligne, écrivons

$$\begin{aligned}s\int\limits_0^\infty\Pi(x)x^{-s-1}dx&=s\left\{\cancel{\left[\Pi(x)(-1)\frac{1}{2}x^{-s}\right]_0^\infty}-\int\limits_0^\infty dxd\Pi\frac{x^{-s}}{-s}\right\}\\&=\int\limits_0^\infty x^{-s}d\Pi(x)\quad\text{(intégrale de Stieltjes)}\,,\end{aligned} \tag{47}$$

où la mesure $d\Pi$ a été écrite comme la densité fois dx ; plus précisément :

$$d\Pi = \left(\frac{d\Pi}{dx}\right) dx\,, \tag{48}$$

où $d\Pi/dx$ est la densité des nombres premiers plus la 1/2-densité des carrés de nombres premiers, plus la 1/3-densité des cubes de nombres premiers, etc.

N'oublions pas que la version calculatoire de la "formule dorée"

$$\frac{\log\zeta(s)}{s} = \int_0^\infty \Pi(x) x^{-s-1} dx \tag{49}$$

trouve son origine dans le produit de nombres premiers d'Euler-Riemann pour la fonction zeta et dans l'invention intelligente de la fonction en escalier $\Pi(x)$. Ce nom est justifié parce que quand x est l'exact carré d'un nombre premier, par exemple quand $x = 9 = 3^2, \Pi(x)$ saute d'un demi, puisque $\pi(\sqrt{x}) = \pi(3)$ saute de 1, et etc. Notons qu'au point effectif où le saut a lieu, la fonction est à mi-hauteur du saut.

Donc on a dérivé la merveilleuse formule donnée ci-dessus, qui devrait nous amener directement au résultat central de l'article de Riemann. Mais quelle est l'expression inverse, i.e. comment exprimer $\Pi(x)$ en fonction de $\zeta(x)$? On discutera de cela dans la prochaine section.

3 Riemann, un expert de la transformée de Fourier

Plus tôt on a introduit la paire d'équations

$$\begin{aligned} \frac{\log\zeta(s)}{s} &= \int_0^\infty \Pi(x) x^{-s-1} dx \qquad (\mathfrak{Re}(s) > 1)\,, \\ \text{et} \quad \Pi(x) &= \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} \log\zeta(s) x^s \frac{ds}{s} \qquad (a > 1)\,, \end{aligned} \tag{50}$$

quand on a discuté de la transformée de Mellin. Voyons comment Riemann a atteint le même résultat bien plus tôt en utilisant la formule d'inversion de Fourier :

$$\varphi(x) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \left[\int_{-\infty}^{+\infty} \varphi(\lambda) e^{i(x-\lambda)\mu} d\lambda \right] d\mu\,. \tag{51}$$

Quand on écrit

$$\varphi(x) = \int_{-\infty}^{+\infty} \phi(\mu) e^{i\mu x} d\mu \,, \tag{52}$$

on peut considérer $\phi(\mu)$ comme les coefficients d'une expansion définie par

$$\phi(\mu) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \varphi(\lambda) e^{-i\lambda\mu} d\lambda \,. \tag{53}$$

Maintenant notons $s = a + i\mu, a = const. > 1$ et μ une variable réelle.
Alors avec $\lambda = \log x$ and $\varphi(x) = 2\Pi(e^x)e^{-ax}$, on obtient

$$\begin{aligned} \begin{matrix} x = e^\lambda \\ \frac{dx}{x} = d\lambda \end{matrix} : \frac{\log\zeta(a+i\mu)}{a+i\mu} &= \int_{-\infty}^{+\infty} \Pi(e^\lambda) e^{-(a+i\mu)\lambda} d\lambda \\ &=: \phi(\mu) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \varphi(\lambda) e^{-i\mu\lambda} d\lambda \,. \end{aligned} \tag{54}$$

Donc on peut continuer à écrire

$$(\varphi(x)) = 2\pi\Pi(e^x)e^{-ax} = \int_{-\infty}^{+\infty} \frac{\log\zeta(a+i\mu)}{a+i\mu} e^{i\mu x} d\mu \tag{55}$$

et en utilisant $e^x = y$, alors $y \to x, s = a+i\mu, ds = id\mu, d\mu = 1/i \cdot ds$ on obtient finalement

$$\Pi(x) = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} \log\zeta(s) x^s \frac{ds}{s} \qquad (a > 1) \,, \tag{56}$$

qui est le résultat souhaité.
À partir de là, on peut directement arriver au résultat principal de l'article de 1859 de Riemann. Pourtant, pour le moment, on doit accepter deux nouvelles quantités de Riemann (des détails seront fournis ultérieurement) : la fonction entière $\xi(s)$ ($\zeta(s)$ n'est pas une fonction entière) et la formule du produit pour la fonction ξ :

$$\begin{aligned} \xi(s) &= \frac{1}{2} s(s-1)\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) \,, \qquad \Gamma\left(\frac{s}{2}\right) = \frac{2}{s}\Gamma\left(1+\frac{s}{2}\right) \\ &= (s-1)\pi^{-\frac{s}{2}} \Gamma\left(1+\frac{s}{2}\right) \zeta(s) \end{aligned} \tag{57}$$

et

$$\xi(s) = \frac{1}{2} \prod_\rho \left(1 - \frac{s}{\rho}\right) \,, \tag{58}$$

avec ρ les zéros de la fonction zeta (égaux aux zéros de ξ).
Ainsi, en prenant le logarithme des deux côtés, on obtient

$$-\log 2+\sum_p \log\left(1-\frac{s}{\rho}\right)=\log(s-1)-\frac{s}{2}\log\pi+\log\Gamma\left(1+\frac{s}{2}\right)+\log\zeta(s)$$

$$\text{ou}\quad \log\zeta(s)=\sum_\rho \log\left(1-\frac{s}{\rho}\right)-\log 2-\log\Gamma\left(1+\frac{s}{2}\right)+\frac{s}{2}\log\pi-\log(s-1)\,. \tag{59}$$

Le premier terme du côté droit nous donne la connexion recherchée entre les zéros non triviaux de zeta et $\Pi(x)$. Cela devient évident quand on écrit

$$\Pi(x)=\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\frac{\log\zeta(s)}{s}x^s ds \tag{60}$$

avec $\log\zeta(s)$ pris ci-dessus. Voici, alors, le résultat de Riemann :

$$\boxed{\Pi(x)=\mathrm{Li}(x)-\sum_\rho \mathrm{Li}(x^\rho)+\log\left(\frac{1}{2}\right)+\int_x^\infty \frac{dt}{t(t^2-1)\log t}\,,\qquad x>1\,.} \tag{61}$$

La somme sur ρ doit être comprise comme

$$\sum_{\mathrm{Im}\rho>0}\left(\mathrm{Li}(x^\rho)+\mathrm{Li}(x^{1-\rho})\right) \tag{62}$$

et $\mathrm{Li}(x)$ dénote le logarithme intégral (voir ci-dessous).
Cette expression calculée pour $\Pi(x)$ est alors utilisée dans la formule

$$\pi(x)=\sum_{n=1}^\infty \frac{\mu(n)}{n}\Pi(x^{1/n})=\Pi(x)-\frac{1}{2}\Pi(x^{1/2})-\frac{1}{3}\Pi(x^{1/3})-\frac{1}{5}\Pi(x^{1/5})+\frac{1}{6}\Pi(x^{1/6})+\cdots\,. \tag{63}$$

Ceci est la grande prouesse de Riemann, le calcul explicite, exact, de la fonction de comptage des nombres premiers $\pi(x)$.
Réécrivons le résultat de Riemann plus explicitement :

$$\Pi(x)=\mathrm{Li}(x)-\sum_{\mathrm{Im}\rho>0}\left(\mathrm{Li}(x^\rho)+\mathrm{Li}(x^{1-\rho})\right)-\log 2+\int_x^\infty \frac{dt}{t(t^2-1)\log t}\,,\qquad x>1 \tag{64}$$

avec

$$\mathrm{Li}(x)=\lim_{\epsilon\to 0}\left[\int_0^{1-\epsilon}\frac{dt}{\log t}+\int_{1+\epsilon}^x\frac{dt}{\log t}\right]\,. \tag{65}$$

Si on différencie $\Pi(x)$ on obtient

$$d\Pi = \left[\frac{1}{\log x} - \sum_{Re\alpha>0} \frac{2\cos(\alpha \log x)}{x^{1/2}\log x} - \frac{1}{x(x^2-1)\log x}\right] dx \qquad x > 1\,. \tag{66}$$

α parcourt toutes les valeurs telles que $\rho = 1/2 + i\alpha$; en d'autres termes, $\alpha = -i(\rho - 1/2)$ où ρ parcourt toutes les racines de telle façon que

$$x^{\rho-1} + x^{-\rho} = x^{-\frac{1}{2}}\left[x^{i\alpha} + x^{-i\alpha}\right] = 2x^{-\frac{1}{2}}\cos(\alpha \log x)\,. \tag{67}$$

L'hypothèse de Riemann dit que tous les α sont réels.
À nouveau, par définition de Π, la mesure $d\Pi$ est dx fois la densité des nombres premiers plus $1/2$ la densité des carrés de nombres premiers, plus $1/3$ fois la densité des cubes de nombres premiers, etc. Donc $1/(\log x)$ tout seul ne devrait pas être considéré comme une approximation de la seule densité des nombres premiers comme Gauß le suggérait, mais plutôt comme $d\Pi/dx$, i.e. la densité des nombres premiers plus $1/2$ fois la densité des carrés de nombres premiers, plus, etc.
Une assez bonne approximation néglige le dernier terme dans $d\Pi$. C'est le nombre de α qui est significatif dans $d\Pi$ que Riemann se destinait à étudier empiriquement pour voir l'influence des "termes périodiques" sur la distribution des nombres premiers. Avec les équations ci-dessus, on a atteint la fin du célèbre article de Riemann de 1859.
On a pourtant, laissé de côté un certain nombre de résultats révolutionnaires vers lesquels on souhaite se tourner maintenant.

4 Sur le chemin vers la fonction entière de Riemann $\xi(s)$

Commençons avec la représentation intégrale de la fonction Γ d'Euler :

$$\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}dx\,,$$

$$s \to \frac{s}{2}: \quad \Gamma\left(\frac{s}{2}\right) = \int_0^\infty x^{\frac{s}{2}-1}e^{-x}dx\,,$$

$$x = \pi t n^2: \quad \Gamma\left(\frac{s}{2}\right) = \int_0^\infty (\pi t n^2)^{\frac{s}{2}-1}e^{-\pi t n^2}\pi n^2 dt\,,$$

$$\Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}\frac{1}{n^s}=\int_0^\infty e^{-\pi t n^2}t^{\frac{s}{2}}\frac{dt}{t}\,,$$

Prenons $\displaystyle\sum_{n=1}^{\infty}:\qquad \Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}\zeta(s)=\int_0^\infty \psi(t)t^{\frac{s}{2}}\frac{dt}{t}\,,\qquad \mathfrak{Re}(s)>1\,,$

$$\psi(t)=\sum_{n=1}^{\infty}e^{-\pi t n^2}\,. \tag{68}$$

La dernière équation définit l'une des fonctions ϑ de Jacobi :

$$\Theta(x):=\vartheta_3(0,ix)=\sum_{n=-\infty}^{+\infty}e^{-\pi x n^2}\,,\qquad \psi(x)=\sum_{n=1}^{\infty}e^{-\pi x n^2}\,,\qquad \Theta(x)=2\psi(x)+1\,. \tag{69}$$

Également, mentionnons l'identité de Jacobi sans démonstration :

$$\Theta(x)=\frac{1}{\sqrt{x}}\Theta\left(\frac{1}{x}\right)\,,\qquad x>0\,. \tag{70}$$

On peut facilement vérifier que

$$\frac{1+2\psi(x)}{1+2\psi\left(\frac{1}{x}\right)}=\frac{1}{\sqrt{x}}\,, \tag{71}$$

de telle façon que

$$\psi\left(\frac{1}{x}\right)=\frac{1}{2}\Theta\left(\frac{1}{x}\right)-\frac{1}{2}=\frac{1}{\sqrt{2}}\sqrt{x}\Theta(x)-\frac{1}{2}=\sqrt{x}\psi(x)+\frac{\sqrt{x}}{2}-\frac{1}{2}\,. \tag{72}$$

Maintenant, on va calculer l'intégrale suivante, qui nous donnera l'un des merveilleux résultats de Riemann.

En utilisant $\Psi(x)=x^{-1/2}\Psi(1/x)-1/2+1/2x^{-1/2}$ et en séparant l'intégrale en deux parties en 1, on obtient

$$\int_0^\infty \Psi(x)x^{s/2}\frac{dx}{x}=\int_1^\infty \Psi(x)x^{s/2}\frac{dx}{x}+\int_0^1 \Psi\left(\frac{1}{x}\right)x^{\frac{s-1}{2}}\frac{dx}{x}+\frac{1}{2}\int_0^1\left(x^{\frac{s-1}{2}}-x^{\frac{s}{2}}\right)\frac{dx}{x}\,. \tag{73}$$

Dans les deux dernières intégrales, on substitue $x\to 1/x$ et donc on obtient

$$\int_0^\infty \Psi(x)x^{\frac{s}{2}}\frac{dx}{x}=\int_1^\infty \Psi(x)\left[x^{\frac{s}{2}}+x^{\frac{1}{2}(1-s)}\right]\frac{dx}{x}+\frac{1}{2}\int_1^\infty\left[x^{\frac{1}{2}(1-s)}-x^{-\frac{s}{2}}\right]\frac{dx}{x}$$

$$\int_1^\infty dx\left[x^{-\frac{s}{2}-\frac{1}{2}}\right]=-\frac{2}{s-1}\,,$$

$$\int_1^\infty dx \left[x^{-\frac{s}{2}-1}\right] = \frac{2}{s}\,,$$

$$= \int_1^\infty \Psi(x)\left(x^{\frac{s}{2}-1} + x^{-\frac{s}{2}-\frac{1}{2}}\right) dx = \frac{1}{s} + \frac{1}{s-1}\,. \tag{74}$$

On a alors ici la formule importante de l'article de Riemann :

$$\Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}\zeta(s) = \int_1^\infty \Psi(x)\left(x^{\frac{s}{2}-1} + x^{-\frac{s}{2}-\frac{1}{2}}\right) dx - \frac{1}{s(1-s)}\,. \tag{75}$$

$$\begin{matrix} \text{pôle}\,\Gamma : s = 0 \\ \text{pôle}\,\zeta : s = 1 \end{matrix}$$

Notons qu'il n'y a pas de changement du côté droit selon $s \to 1 - s$!
$\pi^{-s/2}\Gamma(s/2)\zeta(s)$ a des pôles simples en $s = 0$ et $s = 1$. Pour supprimer ces pôles, on multiplie par $1/2s(s-1)$. C'est la raison pour laquelle Riemann définit

$$\xi(s) = \frac{1}{2}s(s-1)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)\,, \tag{76}$$

qui est une fonction entière ($\zeta(s)$ est une fonction méromorphe). De façon évidente, on a $\xi(s) = \xi(1-s)$ et l'équation fonctionnelle

$$\Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}\zeta(s) = \Gamma\left(\frac{1-s}{2}\right)\pi^{-\frac{1}{2}(1-s)}\zeta(1-s)\,. \tag{77}$$

On obtient le côté droit par le côté gauche en remplaçant s par $(1-s)$.
Maintenant on continue à écrire pour $\xi(s)$

$$\begin{aligned}
\xi(s) &= \frac{1}{2} - \frac{s(1-s)}{2}\int_1^\infty \Psi(x)\left(x^{\frac{s}{2}} + x^{\frac{1}{2}(1-s)}\right)\frac{dx}{x} \\
&= \frac{1}{2} - \frac{s(1-s)}{2}\int_1^\infty \frac{d}{dx}\left\{\Psi(x)\left[\frac{x^{\frac{s}{2}}}{\frac{s}{2}} + \frac{x^{\frac{1}{2}(1-s)}}{\frac{1}{2}(1-s)}\right]\right\} dx \\
&+ \frac{s(1-s)}{2}\int_1^\infty \Psi'(x)\left[\frac{x^{\frac{s}{2}}}{\frac{s}{2}} + \frac{x^{\frac{1}{2}(1-s)}}{\frac{1}{2}(1-s)}\right] ds \\
&= \frac{1}{2} + \frac{s(1-s)}{2}\Psi(1)\left[\frac{2}{3} + \frac{2}{1-s}\right] \\
&+ \int_1^\infty \Psi'(x)\left[(1-s)x^{\frac{s}{2}} + sx^{\frac{1}{2}(1-s)}\right] dx
\end{aligned}$$

$$= \frac{1}{2} + \Psi(1) + \int_1^\infty x^{\frac{s}{2}} \Psi'(x) \left[(1-s) x^{\frac{1}{2}(s-1)-1} + s x^{-\frac{s}{2}-1} \right] dx$$

$$= \frac{1}{2} + \Psi(1) + \int_1^\infty \frac{d}{dx} \left[x^{\frac{3}{2}} \Psi'(x) \left(-2x^{\frac{1}{2}(s-1)} - 2x^{-\frac{s}{2}} \right) \right] dx$$

$$- \int_1^\infty \frac{d}{dx} \left[x^{\frac{3}{2}} \Psi'(x) \right] \left[-2x^{\frac{1}{2}(s-1)} - 2x^{-\frac{s}{2}} \right] dx$$

$$= \frac{1}{2} + \Psi(1) - \Psi'(1)[-2-2] + \int_1^\infty \frac{d}{dx} \left[x^{\frac{3}{2}} \Psi'(x) \right] \left(2x^{\frac{1}{2}(s-1)} + 2x^{-\frac{s}{2}} \right) dx \,. \tag{78}$$

La différentiation de

$$2\Psi(x) + 1 = x^{-\frac{1}{2}} \left[2\Psi\left(\frac{1}{x}\right) + 1 \right] \tag{79}$$

donne facilement

$$\frac{1}{2} + \Psi(1) + 4\Psi'(1) = 0 \tag{80}$$

et utiliser cela permet de mettre la formule dans sa forme finale :

$$\xi(s) = 4 \int_1^\infty \frac{d}{dx} \left[x^{\frac{3}{2}} \Psi'(x) \right] x^{-\frac{1}{4}} \cosh \left[\frac{1}{2} \left(s - \frac{1}{2} \right) \log x \right] dx \,, \tag{81}$$

ou, comme Riemann l'écrit ($s = 1/2 + it; 1/2$ est l'hypothèse de Riemann !):

$$\Xi(t) = \xi\left(\frac{1}{2} + it\right) = 4 \int_1^\infty \frac{d}{dx} \left[x^{\frac{3}{2}} \psi'(x) \right] x^{-\frac{1}{4}} \cos\left(\frac{t}{2} \log x \right) dx \,. \tag{82}$$

Avec

$$\frac{d}{dx} \left[x^{3/2} \psi'(x) \right] = \sum_{n=1}^\infty \left(n^4 \pi^2 x - \frac{3}{2} n^2 \pi \right) x^{1/2} \exp(-n^2 \pi x) \tag{83}$$

et

$$v = \frac{1}{2} \log x \tag{84}$$

et alors $v = 2u$, on peut aussi écrire $\Xi\left(\frac{t}{2}\right)$ comme une transformée de Fourier

$$\Xi\left(\frac{t}{2}\right) = 8 \int_0^\infty du \Phi(u) \cos(ut) \tag{85}$$

avec

$$\Phi(u) = \sum_{n=1}^\infty \pi n^2 \left(2n^2 \pi \exp(4u) - 3 \right) \exp(5u - n^2 \pi \exp(4u)) \,. \tag{86}$$

Si $\cosh[1/2(s-1/2)\log x]$ est développé dans la série habituelle de puissances

$$\cos hy = \frac{1}{2}\left(e^{y}+e^{-y}\right) = \sum \frac{y^{2n}}{(2n)!}\,, \tag{87}$$

on peut écrire

$$\xi(s) = \sum_{n=0}^{\infty} a_{2n}\left(s-\frac{1}{2}\right)^{2n}\,, \tag{88}$$

où

$$a_{2n} = 4\int_{1}^{\infty}\frac{d}{dx}\left[x^{3/2}\Psi'(x)\right]x^{-\frac{1}{4}}\frac{\left(\frac{1}{2}\log x\right)^{2n}}{(2n)!}dx\,. \tag{89}$$

Revenons à

$$\xi(s) = \frac{1}{2}s(s-1)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)\,, \tag{90}$$

avec

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \frac{1}{s(s-1)} + \int_{1}^{\infty}\Psi(x)\left(x^{\frac{s}{2}-1}+x^{-\frac{s}{2}-\frac{1}{2}}\right)dx\,, \tag{91}$$

et écrivons le côté droit en fonction de $s = 1/2+it$, ce qui utilise la conjecture de Riemann $\mathfrak{Re}(s) = 1/2$. Puisque les détails de la substitution sont évidents, on donne simplement le résultat suivant :

$$\begin{aligned}\xi\left(\frac{1}{2}+it\right) &= \frac{1}{2}\left(\frac{1}{2}+it\right)\left(it-\frac{1}{2}\right)\pi^{-\frac{1}{4}-i\frac{t}{2}}\Gamma\left(\frac{1}{4}+i\frac{t}{2}\right)\zeta\left(\frac{1}{2}+it\right)\\ &= \frac{-\left(t^2+\frac{1}{4}\right)}{\left[2(\sqrt{\pi})^{\frac{1}{2}+it}\right]}\Gamma\left(\frac{1}{4}+\frac{it}{2}\right)\zeta\left(\frac{1}{2}+it\right)\,.\end{aligned} \tag{92}$$

En particulier,

$$\xi\left(\frac{1}{2}\right) = \frac{-1}{(8\pi^{1/4})}\Gamma\left(\frac{1}{4}\right)\zeta\left(\frac{1}{2}\right) \tag{93}$$

avec

$$\zeta\left(\frac{1}{2}\right) = -1.4603545088\,,\quad \Gamma\left(\frac{1}{4}\right) = \sqrt{2\varpi 2\pi} = 3.6256099082\,, \tag{94}$$

où la constante de la lemniscate de Gauß est égale à

$$\varpi = 2.62205755429\,. \tag{95}$$

Tout ça mis ensemble :

$$\xi\left(\frac{1}{2}\right) = 0.4971207781 = a_0\,, \tag{96}$$

qui est le minimum pour la valeur réelle $\xi(s)$ en $s = 1/2$. D'ailleurs $\xi(0) = \xi(1) = -\zeta(0) = 1/2$. Le résultat ci-dessus peut aussi s'écrire

$$\Xi(t) := \xi\left(\frac{1}{2} + it\right) = \frac{1}{2} - \left(t^2 + \frac{1}{4}\right) \int_1^\infty \Psi(x) x^{-\frac{3}{4}} \cos\left(\frac{t}{2} \log x\right) dx \,. \tag{97}$$

Le côté droit de cette équation nous dit cela parce que $t \in R_e, x \in R_e$ et $\log x \in R_e$, on a

$$\mathrm{Im}\xi\left(\frac{1}{2} + it\right) = 0 \,, \qquad i.e. \quad \xi\left(\frac{1}{2} + it\right) \equiv \Xi(t) \in R_e \,. \tag{98}$$

Puisque $\Xi(t) = \xi(1/2 + it)$ change de signe infiniment souvent lorsque $t \to \infty$, $\xi(s)$ (et $\zeta(s)$) doivent avoir une infinité de zéros sur $\mathfrak{Re}(s) = 1/2$.
Il y a une autre forme utile de $\xi(s)$ qu'on obtient en commençant par sa définition originale

$$\begin{aligned} \xi(s) &= \frac{s(s-1)}{2} \Gamma\left(\frac{s}{2}\right) \pi^{-\frac{s}{2}} \zeta(s) \\ &= e^{\ln \Gamma\left(\frac{s}{2}\right)} \pi^{-\frac{s}{2}} \frac{s(s-1)}{2} \zeta(s) \,. \end{aligned} \tag{99}$$

Alors en posant $s = 1/2 + it$, on a

$$\begin{aligned} \xi\left(\frac{1}{2} + it\right) &= e^{\ln \Gamma \frac{\left(\frac{1}{2} + it\right)}{2}} \pi^{-\frac{\frac{1}{2} + it}{2}} \frac{1}{2} \left(\frac{1}{2} + it\right) \left(\frac{1}{2} + it - 1\right) \zeta\left(\frac{1}{2} + it\right) \\ &= \left[e^{R_e \ln \frac{\left(\frac{1}{2} + it\right)}{2}} \pi^{-\frac{1}{4}} \cdot \frac{-t^2 - \frac{1}{4}}{2}\right] \left[e^{i \,\mathrm{Im} \ln \Gamma \frac{\left(\frac{1}{2} + it\right)}{2}} \pi^{-\frac{it}{2}} \zeta\left(\frac{1}{2} + it\right)\right] \\ &= \left[-e^{R_e \ln \Gamma\left(\frac{\frac{1}{2} + it}{2}\right)} \pi^{-\frac{1}{4}} \frac{t^2 + \frac{1}{4}}{2}\right] \left[e^{i \,\mathrm{Im} \ln \Gamma\left(\frac{\frac{1}{2} + it}{2}\right)} \pi^{-\frac{it}{2}} \zeta\left(\frac{1}{2} + it\right)\right] . \end{aligned} \tag{100}$$

Notons que le premier facteur entre crochets est négatif. Pour le second facteur on a

$$Z(t) = e^{i\vartheta(t)} \zeta\left(\frac{1}{2} + it\right) , \qquad \vartheta(t) = \mathrm{Im} \ln \Gamma\left(\frac{\frac{1}{2} + it}{2}\right) - \frac{t}{2} \ln \pi \,. \tag{101}$$

Ainsi, $Z(t)$ et ξ sont toujours de signes opposés.
Maintenant, on doit calculer $\vartheta(t)$ et $\zeta(1/2+it)$. Pour l'analyse numérique, il suffit d'utiliser

$$\vartheta(t) \sim \frac{t}{2} \log \frac{t}{2\pi} - \frac{t}{2} - \frac{\pi}{8} + \frac{1}{48t} \,, \tag{102}$$

qu'on peut appliquer pour calculer les racines de $\xi(s)$ sur la droite critique.

5 La représentation par un produit de $\xi(s)$ et $\zeta(s)$ par Riemann (1859) et Hadamard (1893)

Le but de Riemann (avant Weierstrass !) était de démontrer que $\xi(s)$ peut être développé en un produit infini

$$\xi(s) = \xi(0) \prod_{\rho} \left(1 - \frac{s}{\rho}\right) , \tag{103}$$

où ρ parcourt toutes les racines de $\xi(\rho) = 0$. Il n'a pas démontré effectivement cette formule mais il avait raison, comme cela a été montré plus tard par Hadamard. Mais l'on doit admettre que Riemann devait avoir une forte idée de la formule du produit que Weierstrass allait bientôt introduire comme une représentation essentielle en théorie des fonctions, ici les fonctions entières, i.e. les fonctions qui peuvent être déterminées par leurs zéros.

Comme bref rappel, voici la représentation en produit de Weierstrass de la fonction Γ :

$$\Gamma(x) = e^{-\gamma x} \frac{1}{x} \prod_{k=1}^{\infty} \frac{e^{\frac{x}{k}}}{\left(1 + \frac{x}{k}\right)} , \tag{104}$$

où γ est la constante d'Euler-Mascheroni,

$$\gamma = \lim_{n\to\infty} \left[\sum_{k=1}^{n} \frac{1}{k} - \log n\right] \simeq 0.5772157 . \tag{105}$$

De cette formule produit découle, avec l'aide de

$$\Gamma(x)\Gamma(1-x) = \Gamma(x)(-x)\Gamma(-x) = \frac{\pi}{\sin(\pi x)} , \tag{106}$$

la représentation en produit de $\sin(\pi x)$:

$$\begin{aligned} \sin(\pi x) &= -\frac{\pi}{x} \frac{1}{\Gamma(x)\Gamma(-x)} = -\frac{\pi}{x} \left(e^{\gamma x} x \prod_{k=1}^{\infty} \frac{\left(1 + \frac{x}{k}\right)}{e^{\frac{x}{n}}}\right) \left(e^{-\gamma x}(-x) \prod_{k>1}^{\infty} \frac{\left(1 - \frac{x}{k}\right)}{e^{-\frac{x}{k}}}\right) \\ &= \pi x \prod_{k=1}^{\infty} \left(1 - \frac{x^2}{k^2}\right) , \end{aligned} \tag{107}$$

un polynôme de degré infini. De façon similaire, Euler voyait $\sin(\pi x)$ comme un polynôme de degré infini quand il conjectura, et finalement démontra, la formule de $\sin(\pi x)$.

Aussi, pourquoi ne pas penser à $\xi(s)$ comme à un polynôme de degré infini et ne pas écrire une formule de produit déterminée par son infinité de zéros ρ ? C'est ce qu'Hadamard a fait

en 1893 dans un article dans lequel il a étudié les fonctions entières et leurs représentations comme produits infinis – comme Weierstrass. Il a pu démontrer que la formule de produit de Riemann était correcte :

$$\xi(s) = \xi(0) \prod_{\rho} \left(1 - \frac{\xi}{\rho}\right) . \tag{108}$$

$\xi(s)$ est une fonction entière. Le produit infini est compris comme devant être pris dans un ordre qui apparie chaque racine à la racine correspondante $1 - \rho$. La démonstration de Hadamard de la formule produit pour ξ a été désignée par von Mangoldt comme "la première réelle avancée dans le domaine en 34 ans", c'est-à-dire la première avancée depuis Riemann.

Hadamard a montré qu'il était possible de construire la fonction ζ comme un produit infini, étant donnés ses zéros

$$\zeta(s) = f(s) \prod_{\zeta(\rho)=0} \left(1 - \frac{s}{\rho}\right) e^{\frac{s}{\rho}} , \qquad f(s) = \frac{1}{2(s-1)} \left(\frac{2\pi}{e}\right)^{s} . \tag{109}$$

Par conséquent, en incluant les zéros triviaux et non triviaux, il obtint

$$\zeta(s) = \frac{1}{2(s-1)} \left(\frac{2\pi}{e}\right)^{s} \prod_{n=1}^{\infty} \left(1 + \frac{s}{2n}\right) e^{-\frac{s}{2n}} \cdot \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{\frac{s}{\rho}} . \tag{110}$$

Pour le premier produit, on utilise la représentation par produit fournie par Weierstrass :

$$\frac{1}{\Gamma(1+s)} = e^{\gamma s} \prod_{n=1}^{\infty} \left(1 + \frac{s}{n}\right) e^{-\frac{s}{n}} , \tag{111}$$

et ainsi on obtient la formule du produit de Hadamard, qui est convergente dans $C \setminus \{1\}$:

$$\zeta(s) = \frac{e^{\left(\log 2\pi - 1 - \frac{\gamma}{2}\right)s}}{2(s-1)\Gamma\left(1 + \frac{s}{2}\right)} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) e^{\frac{s}{\rho}} . \tag{112}$$

Une forme légèrement simplifiée du produit de Hadamard est

$$\zeta(s) = \frac{\pi^{s/2}}{2(s-1)\Gamma\left(1 + \frac{s}{2}\right)} \prod_{\rho} \left(1 - \frac{s}{\rho}\right) . \tag{113}$$

Ici on prend les paires de racines ρ et $-\rho$ ensemble de telle façon que les exposants $e^{-s/\rho}$ s'annulent.

La dernière expression montre que la fonction ζ peut être complètement construite par ses racines (une spécialité de Riemann) et la singularité en $s = 1$. Pourtant, pour obtenir une convergence absolue, on doit introduire ρ et $-\rho$ par paire dans le produit.

Maintenant, on rappelle la fonction entière de Riemann $\xi(s)$ et la façon dont elle est reliée à la fonction (non entière) ζ :

$$\xi(s) = \frac{s(s-1)}{2}\Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}\zeta(s)\,. \tag{114}$$

Alors

$$\frac{s(s-1)}{2}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\cdot\frac{\pi^{s/2}}{2(s-1)\Gamma\left(1+\frac{s}{2}\right)}\prod_{\rho}\left(1-\frac{s}{\rho}\right), \qquad \Gamma\left(1+\frac{s}{2}\right) = \frac{s}{2}\Gamma\left(\frac{s}{2}\right) \tag{115}$$

ou

$$\xi(s) = \frac{1}{2}\prod_{\rho}\left(1-\frac{s}{\rho}\right) \tag{116}$$

et en utilisant $\xi(0) = \frac{1}{2}$, on a en effet

$$\xi(s) = \xi(0)\prod_{\rho}\left(1-\frac{s}{\rho}\right), \tag{117}$$

qui est le résultat de Riemann de 1859 !
Puisque les zéros de $\zeta(s)$ et de $\xi(s)$ dans la bande critique coïncident, on peut également écrire

$$\begin{aligned}\zeta(s) &= \frac{\pi^{s/2}}{2(s-1)\Gamma\left(1+\frac{s}{2}\right)}\prod_{\rho}\left(1-\frac{s}{\rho}\right)\left(1-\frac{s}{1-\rho}\right)\\ &= \frac{\pi^{s/2}}{2(s-1)\Gamma\left(1+\frac{s}{2}\right)}\left(1-\frac{s}{\frac{1}{2}+14.134i}\right)\left(1-\frac{s}{\frac{1}{2}-14.134i}\right)\left(1-\frac{s}{\frac{1}{2}+21.022i}\right)(\cdots)\,,\end{aligned} \tag{118}$$

où on a utilisé les premiers zéros sur l'axe $\mathfrak{Re}(s) = 1/2$.

6 Dérivation de la formule de Von Mangoldt pour $\Psi(x)$

Il y a une autre version, plus moderne, de la formule de Riemann pour $\Pi(x)$, i.e.

$$\Pi(x) = \mathrm{Li}(x) - \sum_{\rho}\mathrm{Li}(x^{\rho}) + \log\xi(0) + \int_{x}^{\infty}\frac{dt}{t(t^2-1)\log t} \quad (x>1)\,. \tag{119}$$

C'est la formule de von Mangoldt pour $\Psi(x)$, qui contient essentiellement la même information que la formule $\Pi(x)$ de Riemann. Sur le chemin de la formule explicite pour

$\Psi(x)$, on a besoin d'une représentation particulière de la fonction de discontinuité. Donc commençons simplement par vérifier

$$\begin{aligned}
\frac{1}{s-\beta} &= \int_1^\infty x^{-s}x^{\beta-1}dx\,, \qquad \mathfrak{Re}(s-\beta)>0\,,\\
x=e^\lambda :&= \int_0^\infty e^{-\lambda s}e^{\lambda(\beta-1)}e^\lambda d\lambda = \int_0^\infty e^{-\lambda s}e^{\lambda\beta}d\lambda\,,\\
s=a+i\mu &= \int_0^\infty e^{-\lambda(a+i\mu)}e^{\lambda\beta}\alpha\lambda\,,\\
\frac{1}{a+i\mu-\beta} &= \int_0^\infty e^{-i\lambda\mu}e^{\lambda(\beta-a)}d\lambda\,, \qquad a>Re\beta\,,\\
\int_{-\infty}^{+\infty}\frac{1}{a+i\mu-\beta}e^{i\mu x}d\mu &= \int_{-\infty}^{+\infty}e^{i\mu x}d\mu\int_0^\infty e^{-i\lambda\mu}e^{\lambda(\beta-a)}d\lambda\\
&= \int_{-\infty}^{+\infty}\left[\int_0^\infty e^{i(x-\lambda)\mu}d\mu\right]e^{\lambda(\beta-a)}d\lambda\\
&= \int_{-\infty}^{+\infty}2\pi\delta(x-\lambda)e^{\lambda(\beta-a)}d\lambda\\
&= \begin{cases} 2\pi e^{x(\beta-a)} & , \quad x>0\\ 0 & , \quad x<0\end{cases}\,. \qquad (120)
\end{aligned}$$

Jusque là on a

$$\frac{1}{2\pi}\int_{-\infty}^{+\infty}\frac{1}{a+i\mu-\beta}e^{x(a+i\mu)}d\mu = \begin{cases} e^{x\beta} & , \quad x>0\\ 0 & , \quad x<0\end{cases}\,. \qquad (121)$$

Avec $e^x=y$ et $s=a+i\mu$, on obtient le facteur de discontinuité (fonction en escalier)

$$\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\frac{1}{s-\beta}y^s ds = \begin{cases} y^\beta & , \quad y>1\\ 0 & , \quad y<1\end{cases} \overset{\beta=0}{=} \begin{cases} 1 & , \quad y>1\\ \frac{1}{2} & , \quad y=0\\ 0 & , \quad y<1\end{cases} \qquad a>0\,. \qquad (122)$$

Maintenant on revient à la fonction zeta d'Euler-Riemann,

$$\zeta(z)=\prod_{p\in P}\frac{1}{1-p^{-z}}\,, \qquad \mathfrak{Re}(z)>1 \qquad (123)$$

et on prend le logarithme :

$$\log\zeta(z) = -\sum_p \log(1-p^{-z}) = -\sum_p \log\left(1-e^{-z\log p}\right)\,,$$

$$\frac{d}{dz}\log\zeta(z) = -\sum_p \frac{1}{1-p^{-z}}\frac{d}{dz}\left(1-e^{-z\log p}\right) = -\sum_p \frac{1}{1-p^{-z}}\log p\cdot p^{-z}$$

$$= -\sum_p \frac{p^{-z}}{1-p^{-z}}\log p = -\sum_p\sum_{\nu=1}^{\infty} p^{-\nu z}\log p$$

$$= \frac{\zeta'(z)}{\zeta(z)}\,.$$

$$\cdot\frac{x^z}{z}\ :\ \frac{x^z}{z}\sum_{\substack{p\\ \nu=1}}^{\infty}\frac{\log p}{p^{\nu z}} = \sum_{\substack{p\\ \nu=1}}^{\infty}\left(\frac{x}{p^\nu}\right)\frac{\log p}{z} = -\frac{\zeta'(z)}{\zeta(z)}\cdot\frac{x^z}{z}\,,$$

$$\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\sum_{p,\nu=1}^{\infty}\left(\frac{x}{p^\nu}\right)^z\frac{\log p}{z} = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} -\frac{\zeta'(x)}{\zeta(z)}\frac{x^z}{z}dz$$

$$\text{ou}\quad \sum_{\substack{p\\ \nu=1}}^{\infty}\log p\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\left(\frac{x}{p^\nu}\right)^z\frac{1}{z}dz = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} -\frac{\zeta'(z)}{\zeta(z)}\frac{x^z}{z}dz$$

$$y=\frac{x}{p^\nu}:\quad \sum_{\substack{p\\ \nu=1}}^{\infty}\log p\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\frac{y^z}{z}dz = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} -\frac{\zeta'(z)}{\zeta(z)}\frac{x^z}{z}dz\,. \tag{124}$$

Ici on utilise le 1 du facteur de discontinuité du côté gauche et ainsi, on obtient la fonction de Chebyshev $\Psi(x)$:

$$\Psi(x) = \sum_{p^\nu<x}\log p = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} -\frac{\zeta'(z)}{\zeta(z)}\frac{x^z}{z}dz\,. \tag{125}$$

On doit donc sommer le logarithme de tous les nombres premiers jusqu'à x.
$p^\nu > x$ devrait signifier $y<1$, mais pour ce cas, la formule de discontinuité donne zéro.
L'intégrale du côté droit peut être évaluée à l'aide du théorème des résidus. Les contri-

butions aux résidus de $\zeta'(z)/\zeta(z) \cdot x^z/z$ viennent de

Singularité	Raison	Résidu
0	$\frac{x^z}{z}$	$\frac{\zeta'(0)}{\zeta(0)} = \frac{-\frac{1}{2}\log 2\pi}{-\frac{1}{2}} = \log(2\pi)$
1	pôle de ζ $\quad \frac{\zeta'(z)}{\zeta(z)} = -\frac{1}{z-1} + \gamma + \cdots$	$\lim_{z\to 1}(z-1)\left(\frac{-1}{z-1} + \mathcal{O}(1)\right)\frac{x^z}{z} = \frac{-x^1}{1} = -x$
$-2, -4, -6, \cdots$	zéros triviaux de $\zeta(z)$	$\frac{1}{2}x^{-2}, \frac{1}{4}x^{-4}, \frac{1}{6}x^{-6}, \cdots$ $\sum_{n=1}^{\infty} \frac{x^{-2n}}{2n} = \frac{1}{2}\log\left(1-\frac{1}{x^2}\right)$
ρ	zéros non triviaux de $\zeta(z)$	$\frac{x^\rho}{\rho}$

(126)

ce qui amène à la formule explicite exacte

$$\Psi(x) = x - \log(2\pi) - \frac{1}{2}\log\left(1 - \frac{1}{x^2}\right) - \sum_{\zeta(\rho)=0} \frac{x^\rho}{\rho}\,. \tag{127}$$

On appelle cette formule la formule de von Mangoldt (1895) et c'est une des formules les plus importantes de la théorie analytique des nombres. $\Psi(x)$ est réelle et donne les sauts pour les puissances de nombres premiers x. Bien que le dernier terme ait l'air complexe, il ne l'est pas, puisque les zéros entrent par paires et donc c'est aussi un nombre réel.
$\Psi(x)$ est équivalent à la fonction $\Pi(x)$ de Riemann et on doit admettre que la formule pour $\Psi(x)$ a été déduite beaucoup plus aisément que la formule pour $\Pi(x)$, avec laquelle on avait commencé cette section. Il n'est pas étonnant qu'on l'ait considérée entre-temps comme préférable à $\Pi(x)$.

7 Le nombre de racines dans la bande critique

Le théorème suivant a originellement été formulé par Riemann – mais non démontré. Ce n'est qu'en 1905 que von Mangoldt a démontré que le nombre de zéros de ζ dans la bande critique $0 < \mathfrak{Re}(s) < 1, 0 < t < T$ est donné par

$$N(T) = \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi}\,. \tag{128}$$

Pour prouver cette assertion, supposons que $T \geq 3$ et que $\zeta(s) \neq 0$ pour $t = T$.

Considérons alors la zone rectangulaire R_T dans le plan complexe :

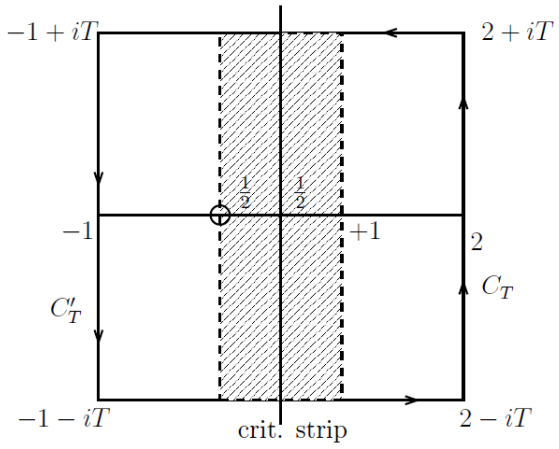


Figure 1: Limites de R_T

Les zéros de la fonction ξ sont identiques à ceux de la fonction ζ dans la zone critique. La symétrie par rapport à l'axe $\mathfrak{Re}(s) = 1/2$ amène (rappelons-nous du résidu logarithmique)

$$2N(T) = \frac{1}{2\pi i} \int\limits_{\partial R_T} \frac{\xi'(s)}{\xi(s)} ds \,. \tag{129}$$

De l'équation fonctionnelle de ξ on obtient

$$\begin{aligned} \xi(1-s) &= \xi(s) \\ -\frac{\xi'(1-s)}{\xi(1-s)} &= \frac{\xi'(s)}{\xi(s)} \,. \end{aligned} \tag{130}$$

$C'_T(C_T)$ est la limite du côté gauche (droit) de R_T:

$$\begin{aligned} \int\limits_{C'_T} \frac{\xi'(s)}{\xi(s)} ds = \int\limits_{C_T} \frac{\xi'(1-s)}{\xi(1-s)} d(1-s) = \int\limits_{C_T} \frac{\xi'(s)}{\xi(s)} ds \\ > \qquad N(T) = \frac{1}{2\pi i} \int\limits_{C_T} \frac{\xi'(s)}{\xi(s)} ds \,. \end{aligned} \tag{131}$$

Maintenant, en utilisant la représentation suivante de la fonction ξ,

$$\xi(s) = \frac{s(s-1)}{2} \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s) \tag{132}$$

on prend le logarithme

$$\log \xi(s) = -\log 2 + \log s + \log(s-1) - \frac{s}{2} \log \pi + \log \Gamma\left(\frac{s}{2}\right) + \log \zeta$$

$$> \frac{d}{ds}\log\xi(s) = \frac{\xi'(s)}{\xi(s)} = \frac{1}{s} + \frac{1}{s-1} - \frac{1}{2}\log\pi + \frac{1}{2}\frac{\Gamma'\left(\frac{s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)} + \frac{\zeta'(s)}{\zeta(s)}$$

$$> 2\pi i N(T) = \underbrace{\int_{C_T}\left(\frac{1}{s} + \frac{1}{s-1}\right)ds}_{①} - \underbrace{\int_{C_T}\frac{1}{2}\log\pi ds}_{②} + \underbrace{\frac{1}{2}\int_{C_T}\frac{\Gamma'\left(\frac{s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}ds}_{③} + \int_{C_T}\frac{\zeta'(s)}{\zeta(s)}ds \quad (133)$$

$$① \qquad \int_{C_T}\left(\frac{1}{s} + \frac{1}{s-1}\right)ds = \frac{1}{2}\int_{\partial R_T}\left(\frac{1}{s} + \frac{1}{s-1}\right)ds \overset{\text{resid}}{=} \frac{1}{2}2\pi i(1+1) = 2\pi i$$

$$② \qquad \int_{C_T}\frac{1}{2}\log\pi ds = \frac{1}{2}\log\pi\left(\left(\frac{1}{2} + iT\right) - \left(\frac{1}{2} - iT\right)\right) = iT\log\pi$$

$$③ \qquad \int_{C_T}\frac{1}{2}\frac{\Gamma'\left(\frac{s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}ds = \log\Gamma\left(\frac{s}{2}\right)\Big|_{\frac{1}{2}-iT}^{\frac{1}{2}+iT}$$

$$= \log\Gamma\left(\frac{1}{4} + i\frac{T}{2}\right) - \log\Gamma\left(\frac{1}{4} - i\frac{T}{2}\right) \quad (134)$$

$$\log\Gamma(\bar{s}) = \overline{\log\Gamma(s)} := 2i\,\mathrm{Im}\log\Gamma\left(\frac{1}{4} + i\frac{T}{2}\right)$$

$$\overset{\text{Développons}}{\underset{T\geq 3}{=}} 2i\,\mathrm{Im}\left(\log\sqrt{2\pi} + \left(-\frac{1}{4} + i\frac{T}{2}\right)\log\left(i\frac{T}{2}\right) - i\frac{T}{2} + \mathcal{O}\left(\frac{1}{T}\right)\right)$$

$$= 2i\,\mathrm{Im}\left(\log\sqrt{2\pi} + \left(-\frac{1}{4} + i\frac{T}{2}\right)\left(\log\frac{T}{2} + i\frac{\pi}{2}\right) - i\frac{T}{2} + \mathcal{O}\left(\frac{1}{T}\right)\right)$$

$$= 2i\pi\left(\frac{T}{2\pi}\log\frac{T}{2} - \frac{T}{2\pi}\right) - \frac{1}{8} + \mathcal{O}\left(\frac{1}{T}\right). \quad (135)$$

Notre résultat immédiat est alors

$$2\pi i N(T) = 2\pi i - iT\log\pi + 2\pi i\left(\frac{T}{2\pi}\log\frac{T}{2} - \frac{T}{2\pi} - \frac{1}{8} + \mathcal{O}\left(\frac{1}{T}\right)\right) + \int_{C_T}\frac{\zeta'(s)}{\zeta(s)}ds\,. \quad (136)$$

$$\boxed{N(T) = 1 - \frac{T}{2\pi}\log\pi + \frac{T}{2\pi}\log\frac{T}{2} - \frac{T}{2\pi} - \frac{1}{8} + \mathcal{O}\left(\frac{1}{T}\right) + \frac{1}{2\pi i}\int_{C_T}\frac{\zeta'(s)}{\zeta(s)}\,.} \quad (137)$$

Le dernier terme peut être séparé en deux parties, dont les résultats sont fournis sans détailler davantage les calculs :

$$\int_{2-iT}^{2+iT}\frac{\zeta'(s)}{\zeta(s)}ds = \mathcal{O}(1)\,, \qquad \text{pour} \quad T \geq 3 \quad (138)$$

et en utilisant

$$\int_{\frac{1}{2}-iT}^{2-iT} \frac{\zeta'(s)}{\zeta(s)} ds = \int_{1/2}^{2} \frac{\zeta'(\sigma - iT)}{\zeta(\sigma - iT)} d\sigma = \overline{\int_{1/2}^{2} \frac{\zeta'(\sigma - iT)}{\zeta(\sigma + iT)} ds}$$

$$= \overline{\int_{\frac{1}{2}+iT}^{2+iT} \frac{\zeta'(s)}{\zeta(s)} ds}$$

$$> \quad \frac{1}{2\pi i} \Big(\int_{\frac{1}{2}-iT}^{2-iT} \frac{\zeta'(s)}{\zeta(s)} ds + \int_{2+iT}^{\frac{1}{2}+iT} \frac{\zeta'(s)}{\zeta(s)} ds \Big) = \frac{1}{\pi} \operatorname{Im} \left(\int_{2+iT}^{\frac{1}{2}+iT} \frac{\zeta'(s)}{\zeta(s)} ds \right) . \tag{139}$$

Jusque-là, on a trouvé

$$N(T) = \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + \frac{7}{8} + \mathcal{O}\left(\frac{1}{T}\right) + \frac{1}{\pi} Im \left(\int_{2+iT}^{\frac{1}{2}+iT} \frac{\zeta'(s)}{\zeta(s)} ds \right) . \tag{140}$$

En utilisant

$$\int_{2+iT}^{\frac{1}{2}+iT} \frac{\zeta'(s)}{\zeta(s)} ds = \log \zeta \left(\frac{1}{2} + iT \right) - \log \zeta(2 + iT)$$

$$> \operatorname{Im} \left(\int_{2+iT}^{\frac{1}{2}+iT} \frac{\zeta'(s)}{\zeta(s)} ds \right) = \arg \left(\zeta \left(\frac{1}{2} + iT \right) \right) - \arg \left(\zeta(2 + iT) \right) . \tag{141}$$

On peut montrer que le module de la dernière expression est $\mathcal{O}(\log T)$.

Par conséquent, notre résultat final pour le nombre de zéros dans la bande critique avec $0 < T$ est donné par

$$\boxed{N(T) = \frac{T}{2\pi} \left(\log \frac{T}{2\pi} - 1 \right) + \mathcal{O}(\log T) .} \tag{142}$$

Comme mentionné ci-dessus, cette formule a été donnée par Riemann en 1859, mais seulement démontrée par von Mangoldt en 1905.

D'ailleurs, on peut aussi approximer $\operatorname{Im} \log \Gamma(1/4 + it/2)$ et ainsi obtenir

$$\operatorname{Im} \left\{ \log \Gamma \left(\frac{1}{4} + \frac{it}{2} \right) \right\} = \frac{t}{2} \log \left(\frac{t}{2} \right) - \frac{t}{2} - \frac{\pi}{8} - \frac{t}{2} \log \pi + \mathcal{O}(t^{-1})$$

$$\text{i.e.} \quad \vartheta(t) = \frac{t}{2} \log \left(\frac{t}{2\pi} \right) - \frac{t}{2} - \frac{\pi}{8} + \mathcal{O}(t^{-1}) . \tag{143}$$

Cela nous amène au résultat utile

$$N(T) = \frac{1}{\pi}\vartheta(T) + 1 + \frac{1}{\pi}\arg\,\zeta\left(\frac{1}{2} + iT\right)\,, \tag{144}$$

avec

$$\frac{1}{\pi}\arg\,\zeta\left(\frac{1}{2} + iT\right) = \mathcal{O}(\log T) \quad \text{pour} \quad T \to \infty\,. \tag{145}$$

On peut ainsi conclure pour le nombre de zéros de ζ dans la bande critique :

$$\begin{aligned} &1. \quad N(T) \overset{T\to\infty}{\longrightarrow} \infty \\ &2. \quad N(T) \sim \frac{T}{2\pi}\log T\,. \end{aligned} \tag{146}$$

Cela découle de

$$N(T) = \frac{T}{2\pi}\log\frac{T}{2\pi} + \mathcal{O}(\log T)\,, \tag{147}$$

qui quand on le divise par $T/2\pi\log T$, amène à

$$\frac{N(T)}{\frac{T}{2\pi}\log T} = \frac{\log T - \log 2\pi}{\log T} + \frac{C}{T/2\pi} \underset{T\to\infty}{\longrightarrow} 1\,. \tag{148}$$

Ce résultat devrait être comparé au théorème des nombres premiers (Gauß 1796, alors qu'il avait 15 ans)

$$\pi(x) \sim \frac{x}{\log x} \quad \text{ou} \quad \lim_{x\to\infty}\left(\frac{\pi(x)}{\frac{x}{\log x}}\right) = 1\,. \tag{149}$$

Von Koch a démontré en 1901 : si l'hypothèse de Riemann $\left(\mathfrak{Re}(s) = \frac{1}{2}\right)$ est vraie, alors

$$\pi(x) = \mathrm{Li}(x) + \mathcal{O}\left(\sqrt{x}\log x\right)\,, \tag{150}$$

i.e. l'erreur dans l'approximation $\pi(x) \sim \mathrm{Li}(x)$ est de l'ordre de $\sqrt{x}\log x$.

8 Régularisation de la fonction zeta de Riemann

Dans cette dernière section, on souhaite introduire le concept de la fonction zeta en lien avec la régularisation de certains problèmes en physique quantique dans lesquels interviennent des quantités infinies. Pour cette raison, on considère un opérateur A avec des valeurs propres positives, réelles discrètes $\{a_n\}$, i.e. $Af_n(x) = a_n f(x)$ et on définit sa fonction de zeta associée par

$$\zeta_A(s) = \sum_n a_n^{-s} = \sum_n e^{-s\ln a_n}\,, \tag{151}$$

où n parcourt toutes les valeurs propres. Si on choisit pour A l'opérateur de Hamilton de l'oscillateur harmonique, par exemple, on obtient (à part le point d'énergie nulle) exactement la fonction zeta. Par différentiation normale, il découle maintenant :

$$\zeta_A'(0) = -\sum_n \ln a_n e^{-s \ln a_n}\Big|_{s=0} = -\ln\left(\prod_n a_n\right) . \tag{152}$$

Cela suggère la définition

$$\det A = \exp\left[-\zeta_A'(0)\right] , \tag{153}$$

que nous utiliserons exclusivement dans la suite. L'avantage de cette méthode est que $\zeta_A'(0)$ n'est pas singulier pour de nombreux opérateurs présentant un intérêt physique. Comme exemple des nombreuses applications à des problèmes aussi bien relativistes que non relativistes en théorie quantique des champs, on choisira l'effet Casimir.
Cet effet est une force de répulsion non classique électromagnétique, attractive ou répulsive qui advient entre des conducteurs électriquement neutres dans le vide. La grandeur de cette force a d'abord été calculée par Casimir pour le cas de la conduction idéale, infiniment étendue dans des plaques parallèles ; son résultat a été une force

$$F = -\frac{\pi^2}{240} \cdot \frac{\hbar c}{a^4} , \tag{154}$$

où a est la distance entre les plaques et le signe négatif indique que les plaques s'attirent l'une l'autre. Cette force dépend apparemment seulement des constantes fondamentales $\hbar$ et c en dehors de la distance entre les plaques ; elle ne dépend pas, pourtant, de la constante de couplage α entre les champs de Maxwell et de matière. Son caractère propre à la mécanique quantique est révélé par le fait que F s'évanouit dans la limite classique $\hbar \to 0$.

La dérivation par Casimir de F était basée sur le concept de vide (de particules) en électrodynamique quantique représentant les oscillations au point zéro d'un nombre infini d'oscillateurs harmoniques. Comme résultat, on obtient l'énergie totale du vide en sommant sur les énergies au point nul $1/2\hbar\omega_{\vec{k}}$ de tous les modes autorisés avec un vecteur de nombre d'onde $\vec{k}$ et de polarisation σ,

$$E = \sum_{\vec{k},\sigma} \frac{1}{2} \hbar \omega_{\vec{k}} . \tag{155}$$

Si on évalue cette équation pour le cas de deux plaques parallèles à distance a l'une de l'autre, on obtient effectivement une énergie totale divergente $E(a)$, mais la différence

d'énergie $E(a) - E(a + \delta a)$ est finie (δa = changement infinitésimal dans la distance entre les plaques), amenant aussi à une force finie par unité d'aire,

$$F = -\frac{\partial E(a)}{\partial a}\,. \tag{156}$$

Pour calculer cette différence d'énergie ou force, on introduit en général un UV-cut-off, i.e. l'énergie E est remplacée par

$$\sum_{\vec{k},\sigma} \frac{1}{2}\hbar\omega_{\vec{k}} e^{-\frac{b}{\pi c}\omega_{\vec{k}}} \tag{157}$$

et dans le résultat final, la limite $b \to 0$ est considérée.

La dérivation de F, pourtant, peut donner l'impression que l'apparence de la force de Casimir est liée à l'existence de fluctuations au point zéro du champ électromagnétique quantifié.

Pour éviter le problème de l'énergie du vide divergente, dans la suite, on considérera le problème selon Hawking du point de vue de la quantisation de l'intégrale de chemin et de la régularisation de la fonction zeta. Ici, il est à nouveau non nécessaire de faire référence à l'oscillation du vide. Pour des raisons de simplicité, on souhaite considérer l'effet Casimir seulement pour la théorie d'un champ réel, scalaire qui est définie par ($\hbar = c = 1$!)

$$\mathcal{L}(\phi) = -\frac{1}{2}\partial_\mu\phi\partial^\mu\phi - \frac{1}{2}m^2\phi^2 - V(\phi)\,, \tag{158}$$

avec le potentiel arbitraire V.

D'abord, on associe le champ ϕ à une source externe J,

$$\mathcal{L}(\phi) \to \mathcal{L}(\phi) + J\phi\,. \tag{159}$$

On peut alors écrire l'amplitude du vide $\langle 0_+|0_-\rangle^J$ ou l'action $W[J]$ sous la forme

$$\langle 0_+|0_-\rangle^J = e^{iW[J]} = \int [d\phi] e^{i\int d^4x\{\mathcal{L}(\phi)+J\phi\}}\,, \tag{160}$$

où on garantit la convergence de l'intégrale de chemin par la substitution $m^2 \to m^2 - i\epsilon\,, \epsilon > 0$. On a supposé que $|0_-\rangle$ or $|0_+\rangle$ décrit un vide qui n'est pas "perturbé" par la présence de certaines géométries, i.e. l'intégrale de chemin est, sans restrictions par des conditions aux bornes, à prendre sur tous les champs ϕ. Cela change dès qu'on introduit

les deux plaques dans le vide, par exemple, perpendiculairement à l'axe des z (points d'intersection : $z = 0$ et $z = a$) et cela a pour conséquence que seuls ces champs devraient contribuer à l'intégrale de chemin qui devrait s'évanouir sur la surface des plaques, i.e. pour lequel il est vérifié que

$$\phi(x_0, x_1, x_2, 0) = \phi(x_0, x_1, x_2, a) = 0 \tag{161}$$

pour des (x_0, x_1, x_2) arbitraires. On obtient alors

$$\begin{aligned} \langle 0_+|0_-\rangle_a^J &= e^{iW(a,[J])} \\ &= \int\limits_{\mathcal{F}_a} [d\phi] \exp\left[i \int d^4x \left\{ -\frac{1}{2}\partial_\mu\phi\partial^\mu\phi - \frac{1}{2}(m^2 - i\epsilon)\phi^2 - V(\phi) - J\phi \right\} \right] , \end{aligned} \tag{162}$$

où $\int_{\mathcal{F}_a}$ suggère que l'intégrale de chemin doit seulement être prise sur l'espace réduit des fonctions $\mathcal{F}_a$ définies par les conditions aux bornes. Avec ça, on a représenté l'amplitude du vide ou l'action pour le cas plus général comme une fonction du paramètre géométrique a et comme une fonctionnelle de la source externe J. Pour approcher les conditions de l'effet Casimir en électrodynamique quantique, on choisit maintenant $J = 0$ ainsi qu'un champ libre ϕ ($V = 0$), sans masse ($m = 0$). Selon l'intégration partielle

$$\langle 0_+|0_-\rangle_a = e^{iW(a)} = \int\limits_{\mathcal{F}_a} [d\phi] e^{-\frac{i}{2}\int d^4x \phi\{-\partial^2 - i\epsilon\}\phi} . \tag{163}$$

L'intégrale de Gauß donne

$$\langle 0_+|0_-\rangle_a = e^{iW(a)} = \int\limits_{\mathcal{F}_a} [d\phi] e^{-\frac{1}{2}\int d^3x d\tau \phi\{-\Box_E\}\phi} . \tag{164}$$

Ici, N est une constante (divergente) qu'on posera $= 1$, puisqu'elle contribue seulement comme constante non physique additionnelle à $W(a)$. En écrivant $\Box_E/\mathcal{F}_a$, on veut dire que les seules valeurs propres avec fonctions propres dans $\mathcal{F}_a$ peuvent être utilisées pour évaluer le déterminant. De plus (en accord avec la contrainte), une rotation de Wick $t \to i\tau$ a été faite, i.e. $\Box_E = \partial_\tau^2 + \Delta$.

De la définition originale du déterminant, il découle que

$$\begin{aligned} \langle 0_+|0_-\rangle_a = e^{iW(a)} &= \left[\exp\left\{-\zeta'_{-\Box_E/\mathcal{F}_a}(0)\right\}\right]^{-\frac{1}{2}} \\ &= \exp\left[\frac{1}{2}\zeta'_{-\Box_E/\mathcal{F}_a}(0)\right] . \end{aligned} \tag{165}$$

L'opérateur $-\Box_E/\mathcal{F}_a$ a pour spectre

$$\left\{k_0^2+k_1^2+k_2^2+\left(\frac{\pi n}{a}\right)^2 | k_0,k_1,k_2\in\mathbb{R}, n\in\mathbb{N}\right\} \tag{166}$$

et ainsi, la fonction zeta

$$\zeta_{-\Box_E/\mathcal{F}_a}(s)=2\frac{A}{(2\pi)^2}\frac{T_E}{2\pi}\int\limits_{-\infty}^{\infty}\int dk_0dk_1dk_2\sum_{n=1}^{\infty}\left[k_0^2+k_1^2+k_2^2+\left(\frac{n\pi}{a}\right)^2\right]^{-s}. \tag{167}$$

Ici, le facteur 2 permet les deux possibilités de polarisation du photon, qui, dans notre modèle simple, n'a pas d'analogue. De plus, AT_E est un volume de normalisation dans un espace trois-dimensionnel $(0,1,2)$, où le temps euclidien T_E est lié à un intervalle de temps de normalisation (de Minkowski) T par $T_E=iT$. Éliminer le terme indépendant d'un $(n=0)$ dans la dernière équation amène simplement à soustraire une constante (infinie) de $W(a)$.

Une évaluation plus avancée de $\zeta_{-\Box_E/\mathcal{F}_a}(s)$ prend maintenant la forme

$$\begin{aligned}\zeta_{-\Box_E/\mathcal{F}_a}(s)&=2AT_E\frac{4\pi}{(2\pi)^3}\sum_{n=1}^{\infty}\int\limits_0^{\infty}dkk^2\left[k^2+\left(\frac{n\pi}{a}\right)^2\right]^{-s}\\&=\frac{8\pi}{(2\pi)^3}AT_E\left(\frac{\pi}{a}\right)^{3-2s}\sum_{n=1}^{\infty}n^{3-2s}\frac{1}{2}\frac{\Gamma\left(\frac{3}{2}\right)\Gamma\left(s-\frac{3}{2}\right)}{\Gamma(s)}\\&=\frac{4\pi}{(2\pi)^3}AT_E\left(\frac{\pi}{a}\right)^{3-2s}\zeta(2s-3)\frac{\Gamma\left(\frac{3}{2}\right)\Gamma\left(s-\frac{3}{2}\right)}{\Gamma(s)}.\end{aligned} \tag{168}$$

La dérivée est

$$\begin{aligned}\zeta'_{-\Box_E/\mathcal{F}_a}(0)&=\frac{4\pi}{(2\pi)^3}AT_E\left(\frac{\pi}{a}\right)^3\zeta(-3)\Gamma\left(\frac{3}{2}\right)\Gamma\left(-\frac{3}{2}\right)\frac{d}{ds}\frac{1}{\Gamma(s)}\bigg|_{s=0}\\&=\frac{\pi^2}{360a^3}AT_E.\end{aligned} \tag{169}$$

Finalement, on obtient

$$\langle 0_+|0_-\rangle=e^{iW(a)}=e^{-\epsilon(a)T_E}=e^{-i\epsilon(a)T}, \tag{170}$$

avec

$$\epsilon(a)=-\frac{\pi^2}{720a^3}A. \tag{171}$$

L'apparence du facteur de phase $e^{-i\epsilon(a)T}$ dans l'amplitude du vide nous permet d'identifier $\epsilon(a)$ comme le déplacement de l'énergie du vide et d'écrire, pour la force par unité de surface

$$F = -\frac{1}{A}\frac{\partial \epsilon}{\partial a}\,, \tag{172}$$

ce qui amène à

$$F = -\frac{\pi^2}{240}\cdot\frac{1}{a^4} \tag{173}$$

ou, après avoir remis $\hbar$ et c

$$F = -\frac{\pi^2}{240}\cdot\frac{\hbar c}{a^4}\,. \tag{174}$$

Ceci est précisément le résultat de Casimir que nous avons maintenant complètement dérivé à l'aide de la régularisation de la fonction de Riemann, qui a complètement éliminé l'énergie divergente au point zéro. La même procédure trouve des applications en électrodynamique quantique et en chromodynamique quantique, et peut être étudiée dans la liste de références (i.e. voir [9,10,11]).

Remerciements

Je souhaite exprimer ma gratitude aux bibliothécaires du "Handschriftenabteilung" (le Département des documents manuscrits) à l'Université de Göttingen pour m'avoir permis d'accéder aux manuscrits originaux de Riemann, et en particulier aux originaux concernant les nombres premiers.

Appendice : Suppléments

La fonction ζ de Riemann peut être étendue méromorphiquement à la région $\{s : \mathfrak{Re}(s) > 0\}$ dans et à droite de la bande critique $\{s : 0 \leq \mathfrak{Re}(s) < 1\}$. C'est une région suffisante de prolongement méromorphe pour de nombreuses applications en théorie analytique des nombres. Les zéros de la fonction ζ dans la bande critique sont connus sous le nom de zéros non triviaux de ζ.

Il est remarquable que ζ vérifie une équation fonctionnelle en établissant une symétrie autour de la droite critique $\{s : \mathfrak{Re}(s) = \frac{1}{2}\}$ plutôt qu'autour de l'axe réel. Une conséquence de cette symétrie est que la fonction ζ peut être étendue méromorphiquement à tout le plan complexe avec un pôle simple en $s = 1$ et aucun autre pôle. Pour toute la région

$\mathbb{C} \setminus \mathfrak{Re}(s) = 1$ incluant la bande critique on a l'équation fonctionnelle :

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{s\pi}{2}\right) \Gamma(1-s)\zeta(1-s), \quad \mathfrak{Re}(s) < 0 \tag{175}$$

ou, de façon équivalente, l'identité entre les fonctions méromorphes $\zeta(s)$:

$$\zeta(1-s) = \frac{2}{(2\pi)^s} \cos\left(\frac{s\pi}{2}\right) \Gamma(s)\zeta(s). \tag{176}$$

Le prolongement analytique donné ici permet de relier $\zeta(s)$ pour les valeurs positives de $\mathfrak{Re}(s)$ avec les valeurs aux nombres négatifs, par exemple :

$$\zeta(-1) = 2^{-1}\pi^{-2}(-1)\Gamma(2)\zeta(2) = \frac{1}{2} \cdot \frac{1}{\pi^2} \cdot (-1) \cdot 1 \cdot \frac{\pi^2}{6} = -\frac{1}{12}\ , \tag{177}$$

i.e.

$$\zeta_R(-1) = -\frac{1}{12} \quad , \tag{178}$$

où l'indice R est ajouté pour distinguer la fonction ζ de Riemann de celle d'Euler, dont elle est une extension, i.e.

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x} = \prod_{p \text{ premier}} \frac{1}{1-p^{-x}} \quad \text{convergeant pour } x > 1$$

$$\frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \ldots = \prod_{p \text{ premier}} \frac{p^x}{p^x - 1} = \left(\frac{2^x}{2^x-1}\right)\left(\frac{3^x}{3^x-1}\right)\left(\frac{5^x}{5^x-1}\right)\ldots$$

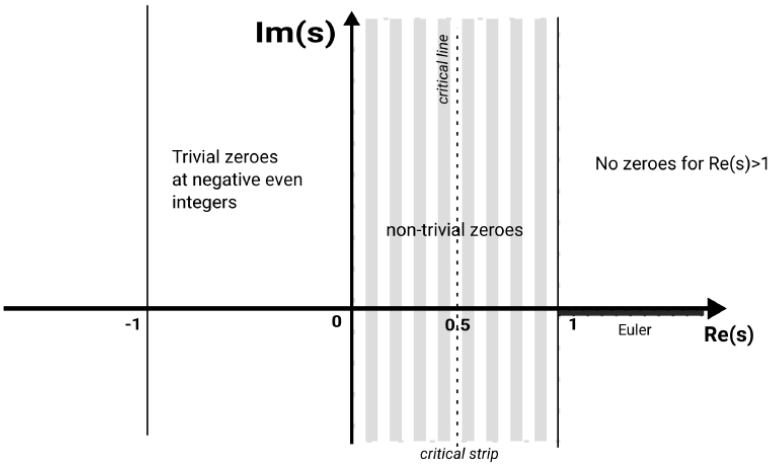


Figure 2: Les différents domaines de définition de la fonction ζ de Riemann de (179)

Quand on étend cette fonction au plan complexe complet s, alors la fonction ζ de Riemann vient en trois représentations différentes :

$$\zeta(s) = \begin{cases} \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ premier}} \frac{p^s}{p^s-1} \ , & \mathfrak{Re}(s) > 1 \\ (1-2^{1-s}) \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s} \ , & 0 < \mathfrak{Re}(s) < 1 \\ 2^s \pi^{s-1} \sin\left(\frac{s\pi}{2}\right) \Gamma(1-s) \zeta(1-s) \ , & \mathfrak{Re}(s) < 0 \end{cases} \tag{179}$$

Où $\zeta(s)$ est-elle égale à 0 ?

1. Il n'y aucun zéro pour $\mathfrak{Re}(s) > 1$ puisque là, $\zeta(s) > 0$.
2. il n'y a pas de zéros non triviaux dans la bande $0 < \mathfrak{Re}(s) < 1$, symétrique autour de $\mathfrak{Re}(s) = \frac{1}{2}$.
3. il y a des zéros triviaux pour $s = -2, -4, \ldots$, donc pour $\mathfrak{Re}(s) < 0$.

Il y a un pôle en $s = 1$.

L'origine de l'équation fonctionnelle pour la fonction η de Dirichlet

Euler dans son article "Remarques sur un beau rapport entre les séries des puissances tant directes que réciproques" écrit les équations fonctionnelles suivantes

$$\frac{1-2^{n-1}+3^{n-1}-4^{n-1}+5^{n-1}-6^{n-1}+\ldots}{1-2^{-n}+3^{-n}-4^{-n}+5^{-n}-6^{-n}+\ldots} = -\frac{1\cdot 2\cdot 3\cdot \ldots (n-1)(2^n-1)}{(2^{n-1}-1)\pi^n} \cos\left(\frac{n\pi}{2}\right)$$
$$\frac{1-3^{n-1}+5^{n-1}-7^{n-1}+\ldots}{1-3^{-n}+5^{-n}-7^{-n}+\ldots} = \frac{1\cdot 2\cdot 3\cdot \ldots (n-1)(2^n)}{\pi^n} \sin\left(\frac{n\pi}{2}\right) \quad .$$

Il finit alors son travail en démontrant que les assertions ci-dessus sont vraies pour des nombres entiers positifs et négatifs ainsi que pour les valeurs fractionnaires de n.
De nos jours, on écrit avec $s \in \mathbb{C}$:

$$\eta(1-s) = -\frac{(2^s-1)}{\pi^s(2^{s-1}-1)} \cos\left(\frac{\pi s}{2}\right) \Gamma(s)\eta(s) \tag{180}$$

qui est l'équation fonctionnelle de la fonction η de Dirichlet.

Hardy a donné une démonstration pour le cas où s est remplacé par $s+1$ dans la dernière équation :

$$\eta(-s) = 2\frac{(1-2^{-s-1}}{1-2^{-s}}\pi^{-s-1}s\ \sin\left(\frac{\pi s}{2}\right)\Gamma(s)\eta(s+1) \quad . \tag{181}$$

De la relation $\eta(s) = (1-2^{1-s})\,\zeta(s)$ on peut montrer que η a des zéros en les points $s_k = 1 + \frac{2\pi i k}{\ln 2}$ pour tout $k \in \mathbb{Z} \setminus \{0\}$, par exemple $s_1 = 1 + 9.0647i$. Pour $k = 0$ on trouve plutôt $\eta(1) = \ln 1 = 0.69315$. Rappelons que $\zeta(1) = \infty$.

Quand on écrit

$$\zeta(s) = \frac{\eta(s)}{1-2^{1-s}}$$

on réalise que $\eta(s)$ ainsi que $(1-2^{1-s})$ ont les mêmes zéros s_k avec $k = 1, 2, 3, \ldots$. $\eta(s)$ est également nulle aux points où $\zeta(s)$ est nulle. Ce sont les zéros triviaux $s = -2, -4, -6, \ldots$ tels que

$$\eta(-2) = \eta(-4) = \eta(-6) = \cdots = 0 \quad .$$

Finalement, η, comme ζ, présente les zéros non triviaux dans la bande critique $\{s \in \mathbb{C} | 0 < \mathfrak{Re}(s) < 1\}$. La célèbre hypothèse de Riemann non démontrée stipule que tous les zéros non triviaux de ζ sont sur l'axe $\mathfrak{Re}(s) = \frac{1}{2}$.

$\zeta(s)$ est une fonction méromorphe. Plus tard on rencontrera la fonction ξ de Riemann, $\xi(s) = \frac{1}{2}s(s-1)\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$. $\xi(s)$ est une fonction entière, elle a des zéros non triviaux, pourtant elle n'a ni zéros triviaux, ni pôles. On a également : $\xi(s) = \xi(1-s)$.

Les tables (1) indiquent que la fonction Γ et les facteurs trigonométriques dans l'équation fonctionnelle ((175), (176), resp.) sont liés aux zéros triviaux et aux pôles de la fonction ζ, mais n'ont pas d'incidence directe sur la distribution des zéros non triviaux, ce qui est la caractéristique la plus importante de la fonction ζ pour les buts de la théorie analytique des nombres, au-delà du fait qu'ils sont symétriques autour de l'axe réel et de la droite critique $x = \frac{1}{2}$. Les fonctions exponentielles telles que 2^{s-1} ou π^{-s} n'ont ni zéros ni pôles. En particulier, l'hypothèse de Riemann ne va pas être résolue juste par une analyse plus poussée de la fonction Γ.

Un remarquable fait historique : Euler, en 1749 (110 ans avant Riemann !) a découvert que la série suivante est convergente :

$$\phi(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s} \tag{182}$$

On appelle aussi cela la fonction η de Dirichlet. Cette série est reliée à ζ par

$$\phi(s) = (1-2^{1-s})\zeta(s) \tag{183}$$

s	$\zeta(s)$
$-2\mathbb{N}$	0
$-\mathbb{N}$	$\frac{-B_{n+1}}{n+1}$
-7	$\frac{1}{240}$
-5	$\frac{-1}{252}$
-3	$\frac{1}{20}$
-1	$\frac{-1}{12}$
0	$-\frac{1}{2}$
$\frac{1}{2}$	-1.46035450
1	∞
$\frac{3}{2}$	2.6123753486
2	$\frac{\pi^2}{2} \approx 1.6449340$ (Euler, Bâle)
$\frac{5}{2}$	1.3414872572
3	1.2020569
$\frac{7}{2}$	1.1267338673
4	$\frac{\pi^4}{90} \approx 1.082323233$

(a) Quelques valeurs de $\zeta(s)$

Fonction	zéros non triviaux	zéros triviaux	Pôles
$\zeta(s)$	Oui	$-2, -4, -6, \ldots$	1
$\zeta(1-s)$	Oui	$3, 5, \ldots$	0
$\sin \frac{\pi s}{2}$	Non	$2\mathbb{N}$	Non
$\cos \frac{\pi s}{2}$	Non	$2\mathbb{N}+1$	Non
$\sin \pi s$	Non	$\mathbb{N}$	Non
$\Gamma(s)$	Non	Non	$0, -1, -2, \ldots$
$\Gamma\left(\frac{s}{2}\right)$	Non	Non	$0, -2, -4, \ldots$
$\Gamma(1-s)$	Non	Non	$1, 2, 3, \ldots$
$\Gamma\left(\frac{1-s}{2}\right)$	Non	Non	$1, 3, 5, \ldots$
$\xi(s)$	Oui	Non	Non

(b) Propriétés de quelques fonctions

Table 1: Propriétés et valeurs particulières de la fonction ζ de Riemann.

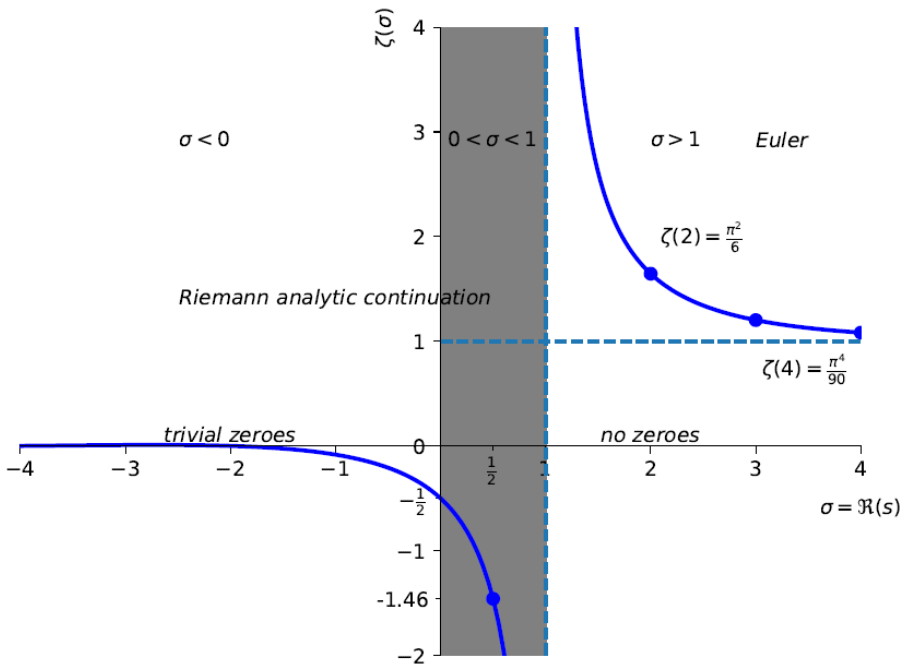


Figure 3: Comportement de la fonction ζ de Riemann pour les arguments réels.

Dans la bande critique $0 < s < 1$, on a :

$$\begin{aligned}\zeta(s) &= \frac{2^{s-1}}{2^{s-1}-1}\phi(s) = \frac{1}{1-2^{1-s}}\phi(s) \\ &= \frac{1}{1-2^{1-s}}\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n^s}, \quad \mathfrak{Re}(s) > 0, 1-2^{1-s} \neq 0\ . \end{aligned} \tag{184}$$

D'Euler, on a

$$\frac{\phi(1-n)}{\phi(n)} = \frac{-(n-1)!(2^n-1)}{(2^{n-1}-1)\pi^n}\cos\left(\frac{n\pi}{2}\right)\ , \tag{185}$$

et il dit de plus : "je hasarderais que la conjecture suivante :

$$\frac{\phi(1-s)}{\phi(s)} = -\frac{\Gamma(s)(2^s-1)\cos\left(\frac{\pi s}{2}\right)}{(2^{s-1}-1)\pi^s} \tag{186}$$

est vraie pour tout s". On sait que $(\eta(s) =)\phi(s) = (1-2^{1-s})\zeta(s)$, ce qui amène directement de (186) à

$$\zeta(1-s) = \frac{2}{(2\pi)^s}\Gamma(s)\zeta(s)\cos\left(\frac{\pi s}{2}\right), \quad \forall s \in \mathbb{C}\setminus 1 \tag{187}$$

et ceci est la célèbre équation fonctionnelle qui a été démontrée par Riemann en 1859 (mais elle avait été conjecturée par Euler en 1749 !). Il est probablement correct de supposer que Riemann était très familier de la contribution d'Euler.

Avec la série alternée de Dirichlet en main, on peut déjà énoncer une assertion importante par rapport aux zéros de la fonction ζ dans la bande critique $0 < \mathfrak{Re}(s) = \sigma < 1$, qui est importante pour l'hypothèse de Riemann, et qui énonce que tous les zéros non triviaux de ζ sont sur la droite $\mathfrak{Re}(s) = \frac{1}{2}$.
Pour montrer cela, on commence par

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s := \sigma + it \tag{188}$$

qui est convergente pour $\mathfrak{Re}(s) > 1$, est une fonction méromorphe et a un pôle en $s = 1$. Ensuite soit

$$n^s = n^{\sigma+it} = n^\sigma n^{it} = n^\sigma e^{it \ln n} = |n|^\sigma \left(\cos(t \ln n) + i \sin(t \ln n)\right) \tag{189}$$

d'où il suit immédiatement que

$$\zeta(s) = \mathfrak{Re}(\zeta(s)) + i\mathfrak{Im}(\zeta(s)) = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} \left[\cos(t \ln n) - i \sin(t \ln n)\right] \tag{190}$$

$$\Rightarrow \mathfrak{Re}(\zeta(s)) = \sum_{n=1}^{\infty} n^{-\sigma} \cos(t \ln n) \tag{191}$$

$$\mathfrak{Im}(\zeta(s)) = \sum_{n=1}^{\infty} n^{-\sigma} \sin(t \ln n) \tag{192}$$

qui sont convergentes pour $\sigma > 1, t \in \mathbb{R}$. Ensuite considérons la fonction ϕ d'Euler comme donnée dans (182), qui est également connue sous le nom de fonction η de Dirichlet. Une extension du domaine de ζ à la région $0 < \sigma < 1$, i.e. dans la bande critique, est obtenue en réécrivant (183) comme

$$\zeta(s) = \frac{1}{1 - 2^{1-s}} \eta(s) \; . \tag{193}$$

Notons que seule la bande critique est importante pour l'hypothèse de Riemann. Notons de plus que η est convergente pour $\sigma = \mathfrak{Re}(s) > 0$ et que la série harmonique alternée suivante,

$$\eta(1) = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots = \ln 2 \approx 0.69315 \; , \tag{194}$$

s'obtient à partir de

$$\ln(x + 1) = x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \ldots \quad -1 < x \leq 1 \; , \tag{195}$$

où x est supposée être réelle. On peut réécrire la fonction η de Dirichlet de la façon suivante :

$$\eta(s) = \sum_{n=1}^{\infty} \left(\frac{1}{(2n-1)^s} - \frac{1}{(2n)^s} \right) \quad . \tag{196}$$

De là, on obtient d'une façon simple (c.f. (191), (192)):

$$\mathfrak{Re}(\eta(s)) = \sum_{n=1}^{\infty} \left[(2n-1)^{-\sigma}\cos(t\ln(2n-1)) - (2n)^{-\sigma}\cos(t\ln(2n))\right] \tag{197}$$

$$\mathfrak{Im}(\eta(s)) = \sum_{n=1}^{\infty} \left[(2n)^{-\sigma}\sin(t\ln(2n)) - (2n-1)^{-\sigma}\sin(t\ln(2n-1))\right] \quad . \tag{198}$$

En utilisant $\cos x - \sin x = \sqrt{2}\sin\left(x + \frac{3}{4}\pi\right)$, on obtient alors

$$\mathfrak{Re}(\eta(s)) + \mathfrak{Im}(\eta(s)) = \sqrt{2}\sum_{n=1}^{\infty}\left[(2n-1)^{-\sigma}\sin\left(t\ln(2n-1) + \frac{3}{4}\pi\right)\right.$$
$$\left. -(2n)^{-\sigma}\sin\left(t\ln(2n) + \frac{3}{4}\pi\right)\right] \neq 0 \quad \forall\sigma \in (0, \frac{1}{2}), \forall t \quad , \tag{199}$$

i.e. η ne possède pas de racine sur la moitié gauche de la bande critique, et à cause de la formule de réflexion (176), cela est aussi vrai du côté droit, i.e. les zéros peuvent seulement être sur la droite critique $\sigma = \frac{1}{2}$, ce qui est l'**hypothèse de Riemann**.

Théorème. Si $\mathfrak{Re}(s) = \sigma > 0$, on a

$$(1 - 2^{1-s})\zeta(s) = \eta(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s} \ , \tag{200}$$

qui implique que $\zeta(s) < 0$ si s est réel et $0 < s < 1$.

Preuve. D'abord supposons que $\sigma > 1$ (Euler : $\mathfrak{Re}(s) > 1$). Alors on a

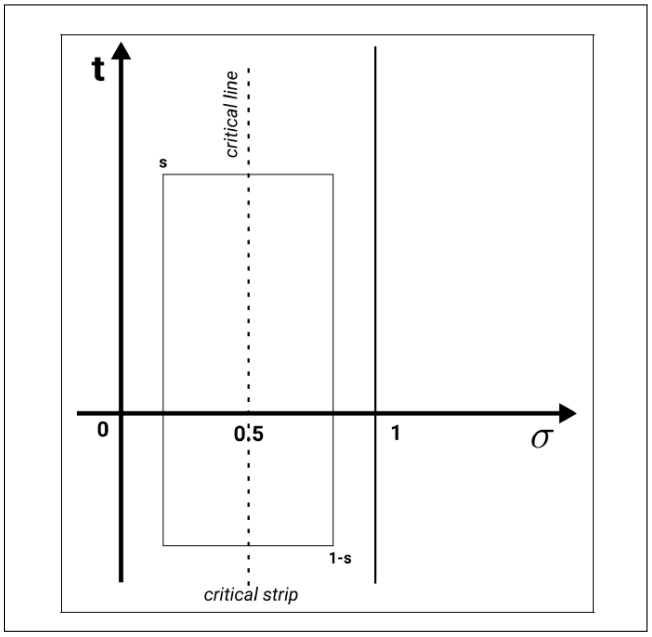
$$\begin{aligned}(1 - 2^{1-s})\zeta(s) &= \sum_{n=1}^{\infty}\frac{1}{n^s} - 2\sum_{n=1}^{\infty}\frac{1}{(2n)^s} \\ &= (1 + 2^{-s} + 3^{-s} + \dots) - 2(2^{-s} + 4^{-s} + 6^{-s} + \dots) \\ &= 1 - 2^{-s} + 3^{-s} - 4^{-s} + \cdots = \text{fonction } \zeta \text{ alternée},\end{aligned}$$

ce qui prouve (200) pour $\mathfrak{Re}(s) = \sigma > 1$. Pourtant, si $\sigma > 0$ la série du côté droit converge, ainsi (200) est aussi vérifiée pour $\sigma > 0$ par prolongement analytique, i.e. quand s est réel alors la somme dans (200) est une série alternée avec une limite positive.

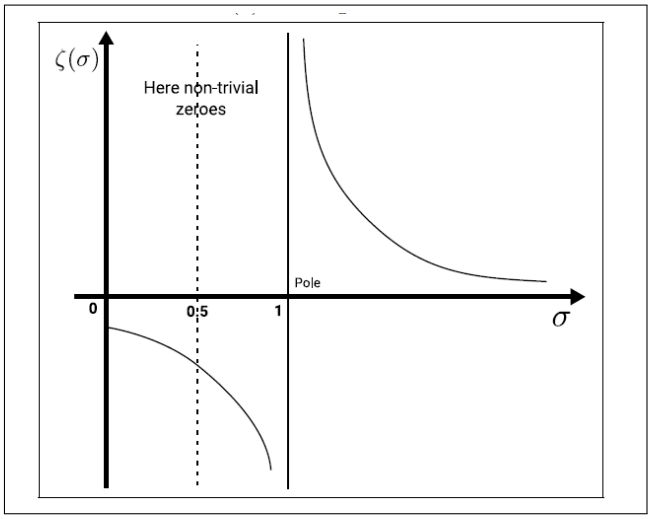
Si $0 < s < 1$, alors le facteur $1-2^{1-s}$ devient négatif. Par conséquent $\zeta(s)$ est aussi négative (n'a pas de zéros !) dans $0 < s < 1$. □

Notons que $\eta(1) = \cdots = \ln 2 \approx 0.69315$ (c.f. (194)) alors que $\zeta(1) = \infty$, c'est-à-dire que $s = 1$ est un pôle de la fonction méromorphe ζ. De plus on a

$$\zeta(0) = -\frac{1}{2} \quad . \tag{201}$$



(a) L'argument



(b) La fonction

Figure 4: Un regard plus attentif au comportement de ζ. En se référant à 4b, on a $|\zeta(\frac{1}{2}-\sigma)| > |\zeta(\frac{1}{2}+\sigma)|$ or $|\zeta(\frac{1}{2}-\sigma)| > |\zeta(\frac{1}{2})|$. Aucun zéro de ζ sur la moitié gauche et sur la moitié droite de la bande critique ce qui est équivalent à l'hypothèse de Riemann.

Preuve. En commençant par l'équation fonctionnelle

$$\Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}\zeta(s) = \Gamma\left(\frac{1-s}{2}\right)\pi^{-\frac{1-s}{2}}\zeta(1-s) \tag{202}$$

on résout $\zeta(s)$ pour obtenir

$$\begin{aligned}\zeta(s) &= \pi^{\frac{s}{2}}\pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\frac{\zeta(1-s)}{\Gamma\left(\frac{s}{2}\right)}\\ s\to 0\ :\ \zeta(0) &= \pi^{-\frac{1}{2}}\Gamma\left(\frac{1}{2}\right)\lim_{s\to 0}\frac{\zeta(1-s)}{\Gamma\left(\frac{s}{2}\right)}\ .\end{aligned}$$

Puisque les résidus de ζ en $s=1$ et de Γ en $s=0$ sont tous les deux égaux à 1, i.e.

$$\zeta(s) = \frac{1}{s-1}+\ldots,\quad \Gamma(s) = \frac{1}{s}+\ldots\quad , \tag{203}$$

on a

$$\zeta(1-s) = -\frac{1}{s}+\ldots,\quad \Gamma(\frac{s}{2}) = \frac{2}{s}+\ldots \tag{204}$$

et donc

$$\lim_{s\to 0}\frac{\zeta(1-s)}{\Gamma(\frac{s}{2})} = \lim_{s\to 0} -\frac{\frac{1}{s}+\ldots}{\frac{2}{s}+\ldots} = -\frac{1}{2} \tag{205}$$

d'où il découle, en utilisant $\Gamma\left(\frac{1}{2}\right)$

$$\zeta(0) = \pi^{-\frac{1}{2}}\pi^{\frac{1}{2}}\left(-\frac{1}{2}\right) = -\frac{1}{2} \implies \zeta(0) = -\frac{1}{2}\ . \tag{206}$$

□

Des équations eqs. (98), (99), on a

$$t, x, \psi(x), \ln(x) \in \mathbb{R}\ .$$

Donc $\mathfrak{Im}\xi(\frac{1}{2}+it) = 0$, i.e. $\xi(\frac{1}{2}+it) \equiv \Xi(t) \in \mathbb{R}$ et par conséquent

$$\begin{aligned}\Xi(t) = \xi(\frac{1}{2}+it) &= -\frac{t^2+\frac{1}{4}}{2\left(\sqrt{\pi}\right)^{\frac{1}{2}+it}}\Gamma\left(\frac{1}{4}+\frac{it}{2}\right)\zeta\left(\frac{1}{2}+it\right)\\ \xi(\frac{1}{2}) &= -\frac{1}{8\pi^{\frac{1}{4}}}\Gamma(\frac{1}{4})\zeta(\frac{1}{2}) \approx 0.4971207781 =: a_0\\ \zeta(\frac{1}{2}) &\approx -1.4603545088\\ \Gamma(\frac{1}{4}) &= \sqrt{2\bar{\omega}2\pi} \approx 3.6256099082\end{aligned}$$

où dans la dernière équation $\bar{\omega}$ est ce qu'on appelle la constante de la lemniscate de Gauss.

Quelques valeurs particulières :

$$\xi(0) = \xi(1) = -\zeta(0) = \frac{1}{2} \quad . \tag{207}$$

Preuve. En utilisant $\xi(s) = \frac{1}{2}s(s-1)\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$ ainsi que $\Gamma(1+\frac{s}{2}) = \frac{s}{2}\Gamma(\frac{s}{2})$ on obtient

$$\xi(s)|_{s=0} = (s-1)\pi^{-\frac{s}{2}}\Gamma(1+\frac{s}{2})\zeta(s)|_{s=0} \Leftrightarrow \xi(s) = -1\cdot 1\cdot\Gamma(1)\cdot\zeta(0) = \frac{1}{2} \tag{208}$$

Donc

$$\xi(0) = \frac{1}{2} \quad .$$

De façon similaire, utiliser la propriété de réflexion $\xi(s) = \xi(1-s)$ amène :

$$\begin{aligned} \xi(s) = (-s)\pi^{-\frac{1}{2}(1-s)}\Gamma(\frac{3}{2}-\frac{s}{2})\zeta(1-s) & \\ \Rightarrow \xi(1) = -1\cdot 1\cdot\Gamma(1)\cdot\zeta(0) = \frac{1}{2} & \\ \Longrightarrow \xi(1) = \frac{1}{2} & \end{aligned} \tag{209}$$

□

Équation fonctionnelle de Riemann

$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma(\frac{1-s}{2})\zeta(1-s)\,, \tag{210}$$

dont la symétrie est évidente quand $s \to 1-s$ est remplacé des deux côtés de l'équation.

Preuve. En commençant avec la fonction Γ d'Euler

$$\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt\,. \tag{211}$$

En utilisant $s \to \frac{s}{2}$, le résultat ci-dessus devient

$$\Gamma(\frac{s}{2}) = \int_0^\infty t^{\frac{s}{2}-1}e^{-t}dt\,. \tag{212}$$

Ensuite, on peut utiliser la substitution $t = \pi n^2 x$ $(dt = \pi n^2 dx)$ pour obtenir

$$\begin{aligned} \Gamma(\frac{s}{2}) &= \int_0^\infty (\pi n^2 x)^{\frac{s}{2}-1}e^{-\pi n^2 x}\pi n^2 dx \\ \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\frac{1}{n^s} &= \int_0^\infty x^{\frac{s}{2}-1}e^{-\pi n^2 x}dx\,. \end{aligned}$$

La sommation sur n amène

$$\sum_{n=1}^{\infty} \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\frac{1}{n^s} = \sum_{n=1}^{\infty}\int_0^{\infty} x^{\frac{s}{2}-1}e^{-\pi n^2 x}dx$$

$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\sum_{n=1}^{\infty}\frac{1}{n^s} = \int_0^{\infty} x^{\frac{s}{2}-1}\sum_{n=1}^{\infty}e^{-\pi n^2 x}dx$$

$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \int_0^{\infty} x^{\frac{s}{2}-1} \underbrace{\sum_{n=1}^{\infty}e^{-\pi n^2 x}}_{\text{fortement relié à la fonction } \vartheta \text{ de Jacobi.}} dx$$

$$\vartheta(x) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 x} = 1 + 2\sum_{n=1}^{\infty} e^{-\pi n^2 x} = 1 + 2\psi(x),\ x > 0\ .$$

$$\Rightarrow \int_0^{\infty} x^{\frac{s}{2}-1}\sum_{n=1}^{\infty}e^{-\pi n^2 x}dx = \int_0^{\infty} x^{\frac{s}{2}-1}\psi(x)dx\ .$$

On sépare l'intégrale du côté droit en deux parties :

$$\int_0^{\infty} x^{\frac{s}{2}-1}\psi(x)dx = \int_1^{\infty} x^{\frac{s}{2}-1}\psi(x)dx + \int_0^{1} x^{\frac{s}{2}-1}\psi(x)dx\,. \tag{213}$$

Regardons $\vartheta(x) = \frac{1}{\sqrt{x}}\vartheta(\frac{1}{x})$ or $2\psi(x)+1 = \frac{1}{\sqrt{x}}(1+\psi(\frac{1}{x}))$. Les équations (72) dans le corps de l'article sont

$$\psi(x) = \frac{1}{\sqrt{x}}\psi(\frac{1}{x}) - \frac{1}{2} + \frac{1}{2\sqrt{x}}$$

$$\begin{aligned}
\int_0^1 x^{\frac{s}{2}-1}\psi(x)dx &= \int_0^1 x^{\frac{1}{2}-1}\left(\frac{1}{\sqrt{x}}\psi(\frac{1}{x}) + \frac{1}{2\sqrt{x}} - \frac{1}{2}\right)dx \\
&= \int_0^1 \left(x^{\frac{s}{2}-\frac{3}{2}}\psi(\frac{1}{x}) + \frac{1}{2}\left(x^{\frac{s}{2}-\frac{3}{2}} - x^{\frac{s}{2}-1}\right)\right)dx \\
&= \int_0^1 x^{\frac{s-3}{2}}\psi(\frac{1}{x})dx + \frac{1}{2}\left[\frac{1}{\frac{s}{2}-\frac{1}{2}}x^{\frac{s}{2}-\frac{1}{2}} - \frac{1}{\frac{s}{2}}x^{\frac{s}{2}}\right]_0^1 \\
&= \int_0^1 x^{\frac{s}{2}-\frac{3}{2}}\psi(\frac{1}{x})dx + \frac{1}{s(s-1)} \\
&\overset{(*)}{=} \int_{\infty}^1 \left(\frac{1}{y}\right)^{\frac{s}{2}-\frac{3}{2}}\psi(y)\left(-\frac{1}{y^2}\right)dy + \frac{1}{s(s-1)} \\
&\overset{y\to x}{=} \int_1^{\infty}\left(\frac{1}{x}\right)^{\frac{s}{2}-\frac{3}{2}}\psi(x)\frac{dx}{x^2} + \frac{1}{s(s-1)}
\end{aligned}$$

$$\Rightarrow \int_0^1 x^{\frac{s}{2}-1}\psi(x)dx = \int_1^{\infty} x^{-\frac{s}{2}-\frac{1}{2}}\psi(x)dx + \frac{1}{s(s-1)}$$

$$\int_0^{\infty} x^{\frac{s}{2}-1}\psi(x)dx = \int_1^{\infty} x^{\frac{s}{2}-1}\psi(x)dx + \int_0^1 x^{\frac{s}{2}-1}\psi(x)dx$$

$$= \int_1^\infty x^{\frac{s}{2}-1}\psi(x)dx + \int_1^\infty x^{-\frac{s}{2}-\frac{1}{2}}\psi(x)dx + \frac{1}{s(s-1)}$$
$$= \int_1^\infty \left(x^{\frac{s}{2}-1} + x^{-\frac{s}{2}-\frac{1}{2}}\right)\psi(x)dx + \frac{1}{s(s-1)}\,,$$

où dans $(*)$ la substitution $x = \frac{1}{y}, dx = -\frac{1}{y^2}dy, \int_0^1 \to \int_\infty^1$ a été utilisée. Rappelons qu'on a commencé avec $\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_0^\infty x^{\frac{s}{2}-1}\psi(x)dx$ et que l'on est parvenu à

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_1^\infty \left(x^{\frac{s}{2}} + x^{\frac{1-s}{2}}\right)\frac{\psi(x)}{x}dx - \frac{1}{s(s-1)}\,. \tag{214}$$

Notons que le dernier terme amène le pôle de Γ en $s = 0$ et de ζ en $s = 1$. Notons également que le côté droit ne change pas selon $s \to 1 - s$, ce qui implique l'équation fonctionnelle de Riemann

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)\,.$$

Riemann a utilisé 4-5 lignes pour dériver cette relation ! □

Dans (214) on a utilisé

$$x^{\frac{s}{2}} = x^{\frac{\sigma+it}{2}} = e^{\frac{\sigma\ln(x)}{2}+i\frac{t}{2}\ln(x)} = e^{\frac{\sigma\ln(x)}{2}}\left[\cos\left(\frac{t}{2}\ln(x)\right) + i\sin\left(\frac{t}{2}\ln(x)\right)\right]$$
$$x^{\frac{1-s}{2}} = e^{\frac{(1-\sigma)\ln(x)}{2}}\left[\cos\left(\frac{t}{2}\ln(x)\right) - i\sin\left(\frac{t}{2}\ln(x)\right)\right]$$
$$x^{\frac{s}{2}} + x^{\frac{1}{2}(1-s)} = \left(e^{\frac{\sigma\ln(x)}{2}} + e^{\frac{(1-\sigma)\ln(x)}{2}}\right)\cos\left(\frac{t}{2}\ln(x)\right)$$
$$\overset{y=\frac{t}{2}\ln(x)}{=} \left(e^{\sigma\frac{y}{2}} + e^{(1-\sigma)\frac{y}{2}}\right)\cos(y)$$
$$\overset{R.H.:\sigma=\frac{1}{2}}{=} \left(e^{\frac{y}{2t}} + e^{\frac{y}{2t}}\right)\cos(y) = 2e^{\frac{y}{2t}}\cos(y)$$
$$= 2e^{\frac{1}{4}\ln(x)}\cos(y) = 2x^{\frac{1}{4}}\cos\left(\frac{t}{2}\ln(x)\right)$$

et dont la partie imaginaire s'évanouit pour $\sigma = \frac{1}{2}$. Donc

$$\Xi(t) := \xi\left(\frac{1}{2}+it\right) = \frac{1}{2} + \frac{1}{2}s(s-1)\int_1^\infty \psi(x)\cdot 2\cdot e^{\frac{1}{4}\ln(x)}\cos\left(\frac{t}{2}\ln(x)\right)\frac{dx}{x} \tag{215}$$

est une fonction réelle, qui est mentionnée dans l'article de Berlin de Riemann à la page 147 comme

$$\Xi(t) = \frac{1}{2} - (t^2 + \frac{1}{4})\int_1^\infty \psi(x)x^{-\frac{3}{4}}\cos\left(\frac{t}{2}\ln(x)\right)dx\,; \tag{216}$$

de plus,

$$\mathfrak{Im}\xi\left(\frac{1}{2}+it\right) = 0, \Rightarrow \xi\left(\frac{1}{2}+it\right) = \Xi(t) \in \mathbb{R}\,. \tag{217}$$

Qu'est-ce qu'une fonction ?

Pourquoi $1+2+3+4+\cdots=-\frac{1}{12}$ est-elle une valeur régularisée ? Une réaction normale à cette assertion est : ce n'est pas un résultat vrai. C'est de la foutaise que de dire que $1+2+3+\ldots$ a une valeur finie, tant qu'on ne spécifie pas ce qu'est une fonction (le concept de fonction) et comment on la calcule, i.e. quelle représentation est choisie, quel est son domaine de définition, etc.
Les deux assertions suivantes sont, pourtant, vraies :

$$1+2+3+4+\ldots\to\infty, \quad \text{i.e. diverge,}$$
$$\zeta_{\text{Riemann}}(-1)=-\frac{1}{12} \quad .$$

Question: Dans quelle représentation cette dernière assertion est-elle vraie ? On a besoin d'une compréhension plus générale d'une fonction ainsi que d'une représentation dans laquelle la valeur de la fonction est calculée.
Il est bien connu qu'une fonction peut avoir différentes représentations, par exemple, en prenant la fonction sinus :

$$f(z)=\begin{cases}\sin(z) & \\ \frac{e^{iz}-e^{-iz}}{2i} & \text{Euler} \\ z-\frac{z^3}{3!}+\frac{z^5}{5!}-\ldots & \text{développement de Taylor} \\ z\prod_{n=1}^{\infty}\left(1-\frac{z^2}{\pi^2n^2}\right) & \text{développement en produit}\end{cases} \tag{218}$$

Le développement de Taylor est un développement en somme infinie de la fonction sinus, on a seulement besoin des puissances de z. Le développement en produit de la fonction sinus nécessite toute l'infinité des zéros de la fonction sinus. On voit qu'il y a de nombreuses manières différentes d'écrire une seule fonction (par exemple sinus), i.e. de nombreuses expressions différentes pour effectuer différents calculs !
Qu'est-ce que tout cela signifie-t-il pour la fonction zeta ? Commençons par la définition d'Euler (1737):

$$\begin{aligned}\zeta(s)&=\sum_{n=1}^{\infty}\frac{1}{n^s}, \quad s>1\\ &=1+\frac{1}{2^s}+\frac{1}{3^s}+\ldots, \quad s>1 \text{ pour avoir la convergence,}\end{aligned}$$

qui est la somme des inverses des puissances des entiers. Substituer de façon évidente des nombres négatifs pour s n'est pas autorisé, même $s=1$ n'est pas permis.

Si on ignore la condition de convergence $s > 1$, alors on peut écrire

$$\zeta_{\text{Euler}}(-1) = 1 + \frac{1}{2^{-1}} + \frac{1}{3^{-1}} + \cdots = 1 + 2 + 3 + 4 + \ldots \quad , \tag{219}$$

qui est un pur non-sens, parce que ça n'est pas correctement défini. $s = -1$ est simplement non autorisé dans la définition (représentation) d'Euler de la fonction zeta, qui est seulement définie sur l'axe réel $1 < x \equiv s$. Mais il y a une autre représentation attribuée à Riemann, qui peut être étendue à tout le plan complexe, $s \in \mathbb{C} \setminus \{0, 1\}$, i.e. incluant la valeur $\mathfrak{Re}(s) = -1$.

$$\zeta(s) = \begin{cases} \zeta_E(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} & \mathfrak{Re}(s) > 1, \text{Euler (1797)} \\ \zeta_R(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s) & s \in \mathbb{C} \setminus \{0,1\}, \text{Riemann (1859)} \end{cases} \tag{220}$$

Notons que cette dernière fonction n'est pas donnée comme une série mais comme une fonction méromorphe.

Dans la représentation de Riemann on obtient

$$\begin{aligned} \zeta_R(-1) &= 2^{-1}\pi^{-2} \sin\left(\frac{-\pi}{2}\right) \Gamma(1-(-1))\zeta(1-(-1)) \\ &= 2^{-1}\pi^{-2}(-1)\Gamma(2)\zeta(2) \\ &= 2^{-1}\pi^{-2}(-1) \cdot 1 \cdot \frac{\pi^2}{6} = -\frac{1}{12} \quad , \end{aligned}$$

où dans la troisième égalité, on a utilisé $\Gamma(2) = (2-1)! \cdot 1 = 1$, $\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$. Ceci est une assertion vraie dans la représentation de la fonction zeta de Riemann

$$-\frac{1}{12} = \zeta_R(-1) \neq \zeta_E(-1) = \sum_{n=1}^{\infty} \frac{1}{n^s}\Big|_{s=-1} \equiv 1 + 2 + 3 + 4 + \ldots \tag{221}$$

alors que la représentation d'Euler n'est pas définie pour $s = -1$.

La fonction de comptage des nombres premiers $\pi(x)$.

Assertion:

$$\begin{aligned} \frac{\ln \zeta(s)}{s} &= \int_2^{\infty} \frac{\pi(x)}{x(x^s - 1)} dx, \quad s > 1 \\ \zeta(s) &= \prod_{p \in \text{Premiers}} \frac{1}{1 - p^{-s}}, \quad s > 1 \\ \ln \zeta(s) &= \ln \prod_{p \in \text{Premiers}} \frac{1}{1 - p^{-s}} = \sum_{p \in \text{Premiers}} \ln \frac{1}{1 - p^{-s}} \end{aligned} \tag{222}$$

où $\pi(x)$ est le nombre de nombres premiers inférieurs à x. Remplacer la sommation sur les nombres premiers par une sommation sur tous les entiers amène

$$\ln \zeta(s) = \sum_{n=2}^{\infty} \{\pi(n) - \pi(n-1)\} \ln \frac{1}{1-n^{-s}} \tag{223}$$

où

$$\pi(n) - \pi(n-1) = \begin{cases} 1, & n \text{ un nombre premier} \\ 0, & \text{sinon.} \end{cases}$$

projections en dehors des nombres premiers, par exemple

$$\begin{aligned} \pi(2) - \pi(1) &= 1 - 0 = 1 \\ \pi(3) - \pi(2) &= 2 - 1 = 1 \\ \pi(4) - \pi(3) &= 2 - 2 = 0 \\ &\vdots \\ (223) \Rightarrow \ln \zeta(s) &= \sum_{n=2}^{\infty} \pi(n) \ln \frac{1}{1-n^{-s}} - \sum_{n=2}^{\infty} \pi(n-1) \ln \frac{1}{1-n^{-s}} \\ &= \sum_{n=2}^{\infty} \pi(n) \ln \frac{1}{1-n^{-s}} - \sum_{n=2}^{\infty} \pi(n) \ln \frac{1}{1-(n+1)^{-s}} \\ &= \sum_{n=2}^{\infty} \pi(n) \left(\ln(1-(n+1)^{-s}) - \ln(1-n^{-s}) \right). \end{aligned} \tag{224}$$

Maintenant utilisons

$$\frac{d}{dx} \ln(1-x^{-s}) = \frac{1}{1-x^{-s}} (s x^{-s-1}) = \frac{s}{x(x^s-1)}. \tag{225}$$

Intégrons des deux côtés pour obtenir

$$\ln(1-x^{-s}) = s \int \frac{1}{x(x^s-1)} dx + C \tag{226}$$

et utilisons cela dans (224), alors que convertir l'intégrale indéfinie en une intégrale sur $[n, n+1]$:

$$\begin{aligned} \ln \zeta(s) &= \sum_{n=2}^{\infty} \underbrace{\pi(n)}_{\text{const. sous l'intégrale}} \int_n^{n+1} \frac{s}{x(x^s-1)} dx \\ &= \sum_{n=2}^{\infty} \int_n^{n+1} \frac{s\pi(x)}{x(x^s-1)} dx \quad n : 2 \to 3, 3 \to 4, \ldots \\ \ln \zeta(s) &= \int_2^{\infty} \frac{s\pi(x)}{x(x^s-1)} dx \end{aligned}$$

ou

$$\frac{\ln\zeta(s)}{s} = \int_2^\infty \frac{\pi(x)}{x(x^s-1)}dx \quad .$$

Ceci conclut la démonstration.
Pour $s > 1$, il n'y a pas de zéros non triviaux de ζ. De tels zéros sont localisés dans la bande critique $0 < \mathfrak{Re}(s) = \sigma < 1$. L'hypothèse de Riemann énonce que $\sigma = \frac{1}{2}$ pour tous les zéros de la fonction ζ.

Donc la formule (222) n'est pas applicable et on doit faire un prolongement analytique dans le plan complexe complet s.

Références

[1] B. Riemann, Über die Anzahl der Primzahlen unter einer gegebenen Grösse. Monatsberichte der Berliner Akademie, November 1859, 671-680.

[2] M. Edwards, Riemann's Zeta Function, Dover Publications, New York 2001.

[3] D. Laugwitz, Bernhard Riemann 1826-1866, Birkhäuser Verlag, 1996.

[3a] R. Ayoub, Am. Mathem. Monthly **81**, No. 10, 1067 (1974).

[4] J. Havil, Gamma, Princeton University Press, 2003.

[5] J. Derbyshire, Prime Obsession, New York: Penguin, 2014.

[6] J. Stillwell, Mathematics and its history, Springer Verlag, 2002.

[7] G.W. Gibbons, Phys. Letters **60A**, 385 (1977).

[8] G.W. Hawking, Com. Math. Phys. **55**, 133 (1977).

[9] W. Dittrich, M. Reuter, Effective Lagrangians in QED, Lecture Notes in Physics, **220**, Springer Verlag 1985.

[10] W. Dittrich, M. Reuter, Effective QCD-Lagrangian with ζ-Function Regularization, Phys. Letters **128 B**, No. 5, 321 (1983).

[11] W. Dittrich, M. Reuter Regularization schemes for the Casimir Effect, Eur. J. Phys. **6**, 33 (1985).

[12] E.C. Tichmarsh and D.R. Heath-Brown, The Theory of the Riemann Zeta Function, 2nd ed., Oxford University Press, Oxford, England, 1986.

Revenir à l'algorithme de calcul du nombre de nombres premiers inférieurs à un nombre donné en utilisant les valuations p-adiques (Denise Vella-Chemla, août 2023)

On revient à l'algorithme de calcul du nombre de nombres premiers inférieurs à un nombre x donné qui utilise les valuations k-adiques de ce nombre avec comme bases les nombres k qui sont inférieurs à la moitié de x [1].

On utilise la formule :

$$\pi(x) = \sum_{2 \leq y \leq x} \frac{1}{\left|1 - (f(y))^{15}\right|} = \frac{1}{\left|1 - \left(\sum_{2 \leq k \leq \lfloor y/2 \rfloor} v_k(y)\right)^{15}\right|}$$

Le programme en python est très simple :

```
def v(k, y):
    if ((y%k) != 0):
       return 0
    else:
       return v(k, y/k)+1

xmax = 1000
pix = 0.0
for x in range(2,xmax+1):
    print('',x, ' :  ', end='')
    somme = 0
    for k in range(2, x//2+1):
       somme = somme+v(k,x)
    pix = pix + 1.0/abs(1.0-pow(float(somme),15))
    print(' sum val k-adiques jusqu a moitie du nb ', somme)
    print(' pix ', pix)
```

Dans le tableau ci-dessous sont fournies les valeurs des sommes des valuations k-adiques de x pour k allant de 2 à $\lfloor x/2 \rfloor$ [2], pour les nombres de 2 à 100.

[1] On avait proposé cet algorithme en septembre 2018. Voir http://denise.vella.chemla.free.fr/fracto.pdf.

[2] Le signe "//" est celui de la division entière en python.

	f(21) = 2	f(41) = 0	f(61) = 0	f(81) = 7
f(2) = 0	f(22) = 2	f(42) = 6	f(62) = 2	f(82) = 2
f(3) = 0	f(23) = 0	f(43) = 0	f(63) = 5	f(83) = 0
f(4) = 2	f(24) = 8	f(44) = 5	f(64) = 13	f(84) = 11
f(5) = 0	f(25) = 2	f(45) = 5	f(65) = 2	f(85) = 2
f(6) = 2	f(26) = 2	f(46) = 2	f(66) = 6	f(86) = 2
f(7) = 0	f(27) = 4	f(47) = 0	f(67) = 0	f(87) = 2
f(8) = 4	f(28) = 5	f(48) = 12	f(68) = 5	f(88) = 8
f(9) = 2	f(29) = 0	f(49) = 2	f(69) = 2	f(89) = 0
f(10) = 2	f(30) = 6	f(50) = 5	f(70) = 6	f(90) = 11
f(11) = 0	f(31) = 0	f(51) = 2	f(71) = 0	f(91) = 2
f(12) = 5	f(32) = 9	f(52) = 5	f(72) = 14	f(92) = 5
f(13) = 0	f(33) = 2	f(53) = 0	f(73) = 0	f(93) = 2
f(14) = 2	f(34) = 2	f(54) = 8	f(74) = 2	f(94) = 2
f(15) = 2	f(35) = 2	f(55) = 2	f(75) = 5	f(95) = 2
f(16) = 7	f(36) = 10	f(56) = 8	f(76) = 5	f(96) = 15
f(17) = 0	f(37) = 0	f(57) = 2	f(77) = 2	f(97) = 0
f(18) = 5	f(38) = 2	f(58) = 2	f(78) = 6	f(98) = 5
f(19) = 0	f(39) = 2	f(59) = 0	f(79) = 0	f(99) = 5
f(20) = 5	f(40) = 8	f(60) = 11	f(80) = 12	f(100) = 10

On constate par programme que $\pi(x)$ compte bien les nombres premiers.[3]

Le nombre de nombres premiers $\pi(x)$ "saute" de 1 à chaque nombre premier tandis qu'à chaque nombre composé, il est incrémenté de :

$$\Delta(x) = \frac{1.0}{\left| 1.0 - \left(\sum_{2 \leq k \leq \lfloor x/2 \rfloor} v_k(x) \right)^{15} \right|}$$

Il faudrait démontrer que l'ajout à $\pi(x)$, entre deux nombres premiers successifs, des nombres décimaux $\Delta(x)$ associés aux nombres composés, ne fait pas augmenter $\pi(x)$ de plus de 1, ce qui perturberait complètement le comptage.

On visualise dans le tableau ci-dessous la variation de $\pi(x)$ selon la formule qu'on a proposée.

[3] Se reporter par exemple à cette page de wikipedia https://en.wikipedia.org/wiki/Prime-counting_function.

		26	9.000305186124626	51	15.000549335267118	76	21.0007629650016
2	1.0	27	9.000305187055949	52	15.000549335299887	77	21.000793483511075
3	2.0	28	9.000305187088717	53	16.000549335299887	78	21.000793483513203
4	2.000030518509476	29	10.000305187088717	54	16.000549335299915	79	22.000793483513203
5	3.000030518509476	30	10.000305187090843	55	16.00057985380939	80	22.000793483513203
6	3.000061037018952	31	11.000305187090843	56	16.00057985380942	81	22.000793483513412
7	4.000061037018952	32	11.000305187090849	57	16.000610372318896	82	22.00082400202289
8	4.000061037950275	33	11.000335705600325	58	16.00064089082837	83	23.00082400202289
9	4.000091556459751	34	11.0003662241098	59	17.00064089082837	84	23.00082400202289
10	4.000122074969227	35	11.000396742619277	60	17.00064089082837	85	23.000854520532364
11	5.000122074969227	36	11.000396742619278	61	18.00064089082837	86	23.00088503904184
12	5.000122075001994	37	12.000396742619278	62	18.000671409337848	87	23.000915557551316
13	6.000122075001994	38	12.000427261128754	63	18.000671409370614	88	23.000915557551345
14	6.00015259351147	39	12.00045777963823	64	18.000671409370614	89	24.000915557551345
15	6.000183112020946	40	12.000457779638259	65	18.00070192788009	90	24.000915557551345
16	6.000183112021157	41	13.000457779638259	66	18.00070192788222	91	24.00094607606082
17	7.000183112021157	42	13.000457779640385	67	19.00070192788222	92	24.000946076093587
18	7.000183112053924	43	14.000457779640385	68	19.000701927914985	93	24.000976594603063
19	8.000183112053925	44	14.000457779673154	69	19.00073244642446	94	24.00100711311254
20	8.000183112086694	45	14.000457779705922	70	19.00073244642659	95	24.001037631622015
21	8.00021363059617	46	14.000488298215398	71	20.00073244642659	96	24.001037631622015
22	8.000244149105646	47	15.000488298215398	72	20.00073244642659	97	25.001037631622015
23	9.000244149105646	48	15.000488298215398	73	21.00073244642659	98	25.001037631654782
24	9.000244149105674	49	15.000518816724874	74	21.000762964936065	99	25.00103763168755
25	9.00027466761515	50	15.000518816757642	75	21.000762964968832	100	25.00103763168755

Ce qui est extraordinaire ici, c'est le fait que la quantité qui est ajoutée à $\pi(x)$ au fur et à mesure est la même pour des nombres très différents, mais de factorisations "semblables" : fournissons dans le tableau ci-dessous la différence (le delta $\Delta(x)$ vu plus haut) ajouté à $\pi(x)$ pour les entiers successifs, en regard de leur factorisation. On voit par exemple (on les a notés en bleu) qu'on ajoute la même quantité pour le nombre $95 = 5^1.19^1$ que pour un nombre (petit) comme $10 = 2^1.5^1$ ou pour un carré comme $25 = 5^2$. Pour tous ces nombres, notons-les n, la somme des valuations p-adiques $\sum_{2 \leq k \leq \lfloor n/2 \rfloor} v(k, n)$ est égale à 2.

Pour rappel, on a une vision syntaxique ("langagière") de la valuation k-adique[4] :

- pour trouver les valuations 2-adiques, "écris" 0-1-, puis recopie ce que tu viens d'écrire en changeant seulement le dernier nombre que tu as écrit en lui-même augmenté de 1 ; tu obtiens la séquence 0-1-0-2.

- recommence : recopie le tout, et augmente le dernier nombre écrit de 1 ; tu obtiens 0-1-0-2-0-1-0-3 : tu as, sans même diviser, obtenu les exposants de 2 dans les factorisations des nombres de 1 à 8 ;

[4]Elle serait par sa simplicité enseignable en école élémentaire. Pour un autre exemple d'un procédé syntaxique pur appliqué au dessin du fractal appelé "Minkowski sausage" par Mandelbrot, voir le programme http://denise.vella.chemla.free.fr/pgm-cx-grecque.png et son résultat http://denise.vella.chemla.free.fr/res-pgm-cx-grecque.png.

- recommence : 0-1-0-2-0-1-0-3-0-1-0-2-0-1-0-4, tu as les exposants de 2 dans les factorisations des nombres de 1 à 16.

- pour trouver les valuations 3-adiques, procède similairement mais en recopiant 3 fois la séquence de niveau n pour obtenir celle de niveau $n+1$. Pour obtenir les exposants de 3 dans les factorisations des nombres de 1 à 27, tu as obtenu successivement les chaînes 0-0-1, puis 0-0-1-0-0-1-0-0-2, puis 0-0-1-0-0-1-0-0-2-0-0-1-0-0-1-0-0-2-0-0-1-0-0-1-0-0-3.

- pour trouver les valuations k-adiques, procède similairement mais en recopiant k fois la séquence de niveau n pour obtenir celle de niveau $n+1$.

			26	$2^1.13^1$	3.051e-5	51	$3^1.17^1$	3.051e-5	76	$2^2.19^1$	3.276e-11
2	p	1	27	3^3	9.313e-10	52	$2^2.13^1$	3.276e-11	77	$7^1.11^1$	3.051e-5
3	p	1	28	$2^2.7^1$	3.276e-11	53	p	1	78	$2^1.3^1.13^1$	2.126e-12
4	2^2	3.051e-5	29	p	1	54	$2^1.3^3$	2.842e-14	79	p	1
5	p	1	30	$2^1.3^1.5^1$	2.126e-12	55	$5^1.11^1$	3.051e-5	80	$2^4.5^1$	6.490e-17
6	$2^1.3^1$	3.051e-5	31	p	1	56	$2^3.7^1$	2.842e-14	81	3^4	2.106e-13
7	p	1	32	2^5	4.856e-15	57	$3^1.19^1$	3.051e-5	82	$2^1.41^1$	3.051e-5
8	2^3	9.313e-10	33	$3^1.11^1$	3.051e-5	58	$2^1.29^1$	3.051e-5	83	p	1
9	3^2	3.051e-5	34	$2^1.17^1$		59	p	1	84	$2^2.3^1.7^1$	2.393e-16
10	$2^1.5^1$	3.051e-5	35	$5^1.7^1$	3.051e-5	60	$2^2.3^1.5^1$	2.393e-16	85	$5^1.17^1$	3.051e-5
11	p	1	36	$2^2.3^2$	1.000e-15	61	p	1	86	$2^1.43^1$	3.051e-5
12	$2^2.3^1$	3.276e-11	37	p	1	62	$2^1.31^1$		87	$3^1.29^1$	3.051e-5
13	p	1	38	$2^1.19^1$	3.051e-5	63	$3^2.7^1$	3.276e-11	88	$2^3.11^1$	2.842e-14
14	$2^1.7^1$	3.051e-5	39	$3^1.13^1$	3.051e-5	64	2^5	1.953e-17	89	p	1
15	$3^1.5^1$	3.051e-5	40	$2^1.5^1$	2.842e-14	65	$5^1.13^1$	3.051e-5	90	$2^1.3^2.5^1$	2.393e-16
16	2^4	2.106e-13	41	p	1	66	$2^1.3^1.11^1$	2.126e-12	91	$7^1.13^1$	3.051e-5
17	p	1	42	$2^1.3^1.7^1$	2.126e-12	67	p	1	92	$2^2.23^1$	3.276e-11
18	$2^1.3^2$	3.276e-11	43	p	1	68	$2^2.17^1$	3.276e-11	93	$3^1.31^1$	3.051e-5
19	p	1	44	$2^2.11^1$	3.276e-11	69	$3^1.13^1$	3.051e-5	94	$2^1.47^1$	3.051e-5
20	$2^2.5^1$	3.276e-11	45	$3^2.5^1$	3.276e-11	70	$2^1.5^1.7^1$	2.126e-12	95	$5^1.19^1$	3.051e-5
21	$3^1.7^1$	3.051e-5	46	$2^1.23^1$	3.051e-5	71	p	1	96	$2^5.3^1$	2.283e-18
22	$2^1.11^1$	3.051e-5	47	p	1	72	$2^3.3^2$	6.428e-18	97	p	1
23	p	1	48	$2^4.3^1$	6.490e-17	73	p	1	98	$2^1.7^2$	3.276e-11
24	$2^3.3^1$	2.842e-14	49	7^2	3.051e-5	74	$2^1.37^1$	3.051e-5	99	$3^2.11^1$	3.276e-11
25	5^2	3.051e-5	50	$2^1.5^2$	3.276e-11	75	$3^1.5^2$	3.276e-11	100	$2^2.5^2$	1.000e-15

Programmes ou idées de juillet 2023 (Denise Vella-Chemla, 25 juillet 2023)

Gamma en python

youpi-gamma-python.py - GNU Emacs at DESKTOP-4PROGGL

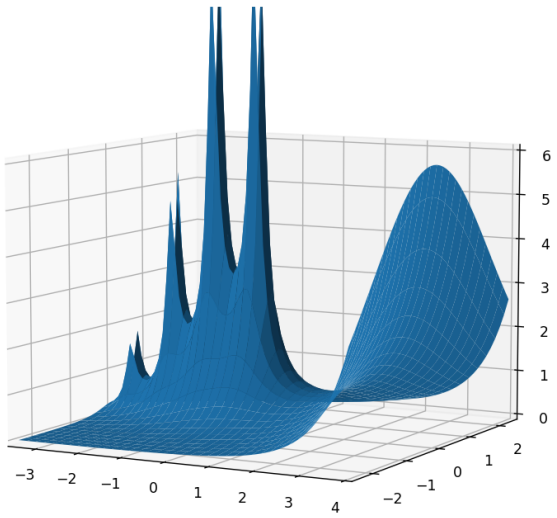
File Edit Options Buffers Tools Python Help

```
from mpl_toolkits.mplot3d import Axes3D
import matplotlib.pyplot as plt
from matplotlib import cm
import numpy as np

fig = plt.figure()
ax = Axes3D(fig)

N=70
theta = -np.pi + (2*np.pi/N) * (0.5 + np.arange(N))
c=-11
r=16
s=0.1
x = np.arange( -3.5, 4+s, s)
y = np.arange(-2.5, 2.5+s, s)
xx, yy = np.meshgrid(x, y)
zz = xx + 1j*yy
gaminv = 0*zz
for k in range(N):
    t = c + r*np.exp(1j*theta[k])
    gaminv += np.exp(t)*(t**(-zz))*(t-c)
gaminv = gaminv/N
gam = 1.0/gaminv
ax = fig.add_subplot(111, projection='3d')
ax.plot_surface(xx,yy, abs(gam))
ax.set_xlim(-3.5,4)
ax.set_ylim(-2.5,2.5)
ax.set_zlim(0,6)
plt.show()
```

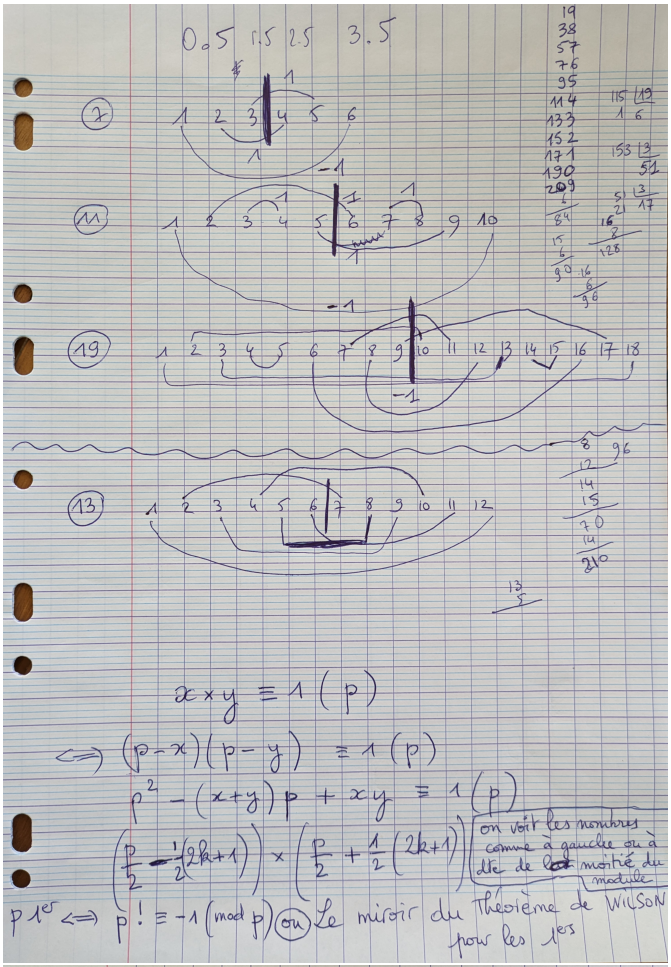
-\--- **youpi-gamma-python.py** All L1 (Python El

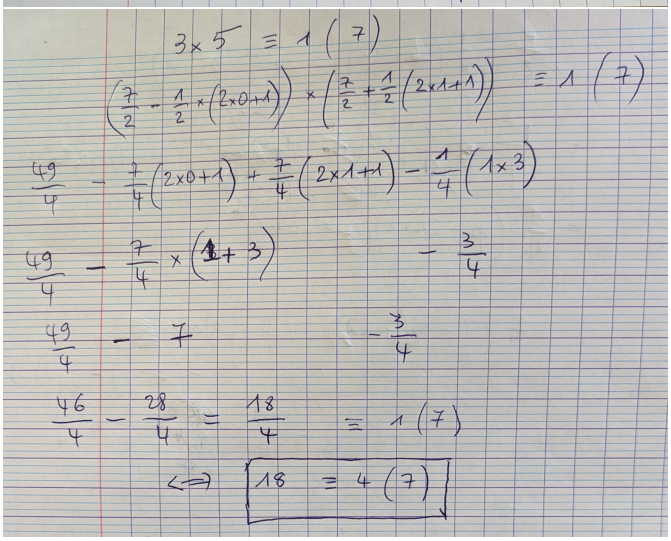
Wrote c:/Users/DENISE 2022/Desktop/youpi-gamma-python

Figure 1



Symétrie-miroir non vue jusque-là des nombres p q dont le produit vaut 1 (mod p), pour p premier, autour du milieu (les complémentaires de p et q que sont $n-p$ et $n-q$ ont aussi leur produit qui vaut 1 (mod p) et c'est chouette (même si c'est normal).



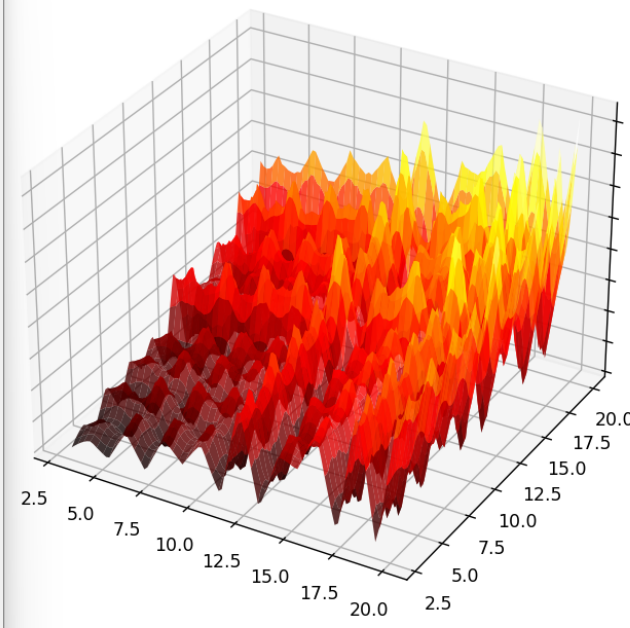


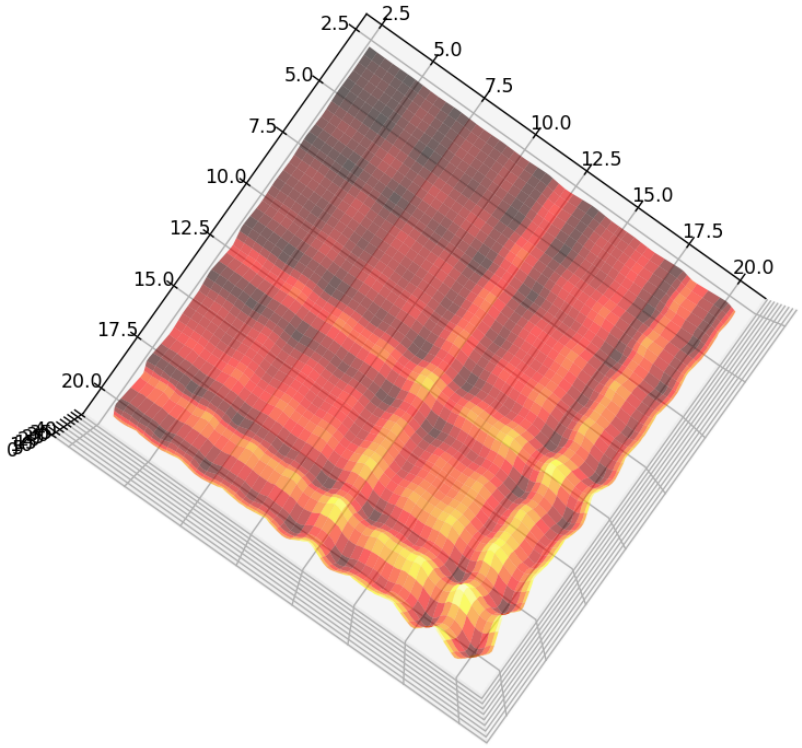
Enfin ma surface bosselée avec les décompositions de Goldbach qui “tombent au sol” ($z = 0$) en python, avec en deuxième graphique : Plaid Goldbach vu de dessus (on distingue en foncé 3+3, 3+5, 3+7), et en troisième graphique : les nombres premiers de 3 à 19 vus en coupe de profil de la surface bosselée.

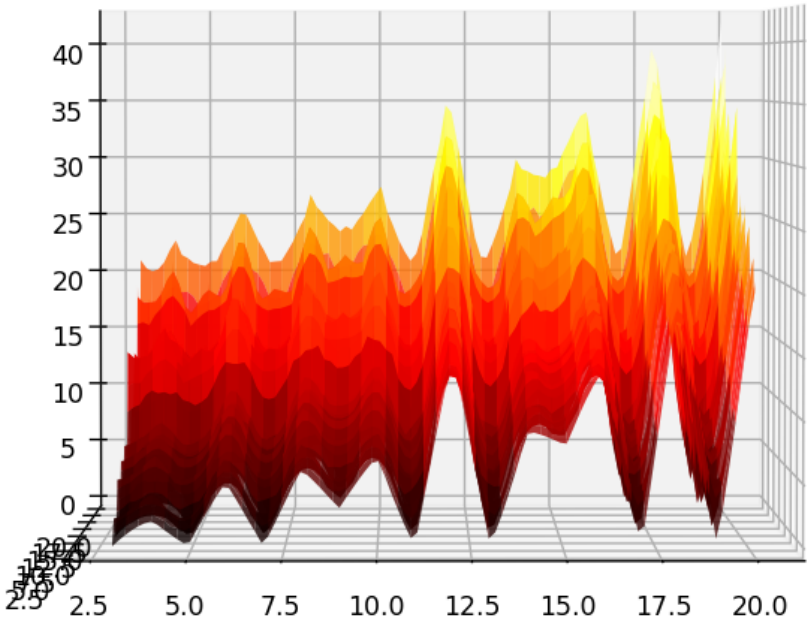
Jacques-interpole-ma-surface.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

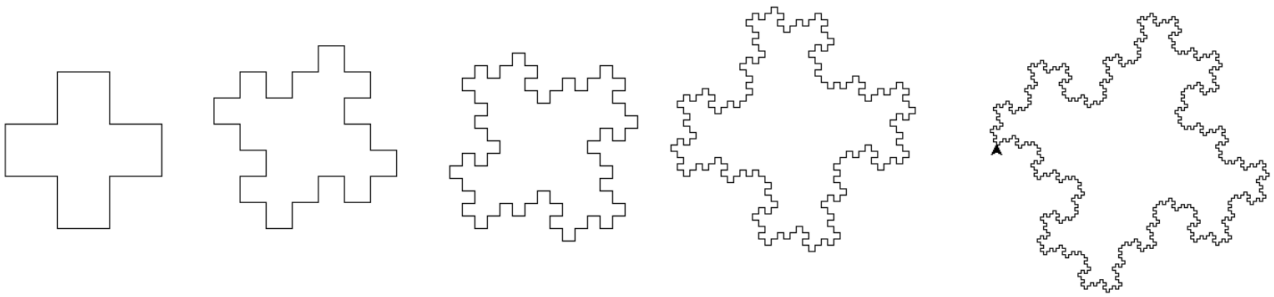
```
from mpl_toolkits.mplot3d import Axes3D
import matplotlib.pyplot as plt
import math
import numpy as np
from scipy.interpolate import RBFInterpolator

fig = plt.figure()
ax = Axes3D(fig)

def sd(n):
  return(np.sum([np.sum([np.cos(2*np.pi*n*l/k) for l in range(1,k+1)]) for k in range(1,n+1)]))
print(sd(100))

n = 20  # taille de la grille d'entiers
m = 5*n  # taille de sa discretisation

XY = np.array([[i, j] for j in range(3, n+1) for i in range(3, n+1)])
Z = np.array([sd(i) + sd(j)-i-j-2 for j in range(3, n+1) for i in range(3, n+1)])
print(Z)

Xd = Yd = np.linspace(3, n, num=m)
Xgrid, Ygrid = np.meshgrid(Xd, Yd)
XYd = np.array(list(zip(Xgrid.flat, Ygrid.flat)))
#print(f'\nXgrid =\n{Xgrid}\nYgrid =\n{Ygrid}\nXYd =\n{XYd}')

Zd = RBFInterpolator(XY, Z, kernel='linear', epsilon=7, neighbors=8)(XYd)
Zgrid = Zd.reshape(m, m)
#print(f'\nZd =\n{Zd}\nZgrid =\n{Zgrid}')

ax = fig.add_subplot(111, projection='3d')
ax.plot_surface(Xgrid, Ygrid, Zgrid, cmap=plt.cm.hot, linewidth=0,antialiased=True,alpha=0.8)
#ax.plot_wireframe(Xgrid, Ygrid, Zgrid, alpha=0.3)
#ax = fig.add_subplot(111)
#CS = ax.contour(Xgrid, Ygrid, Zgrid)
#ax.clabel(CS, inline=True, fontsize=10)
plt.show()
```



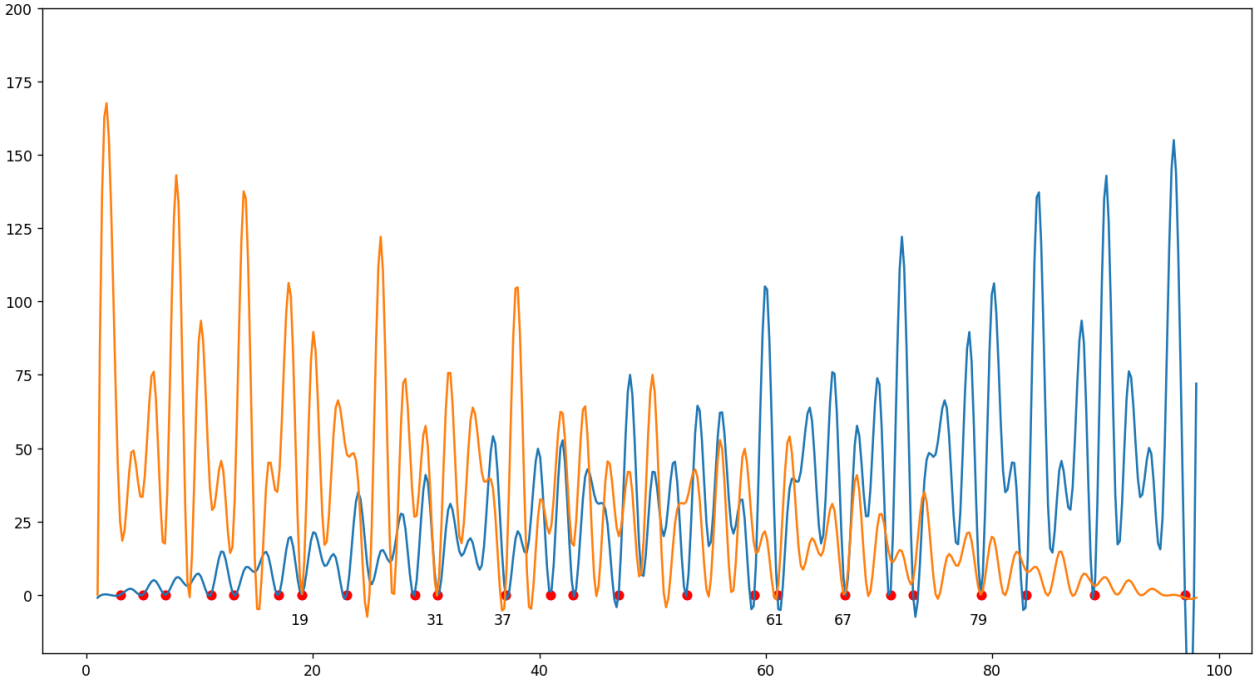

2.5
5.0
7.5
10.0
12.5
15.0
17.5
20.0


40
35
30
25
20
15
10
5
0
2.5
5.0
7.5
10.0
12.5
15.0
17.5
20.0

Vieux souvenirs : programme d'été d'une courbe presque aussi jolie que celle de Hilbert (Mandelbrot la dénomme Minkowski sausage, en l'honneur de son ami mort jeune). Je la programme d'abord "langagièrement" : A est pour Avance (en logo de Marvin Minsky ou en Scratch du MIT), G pour "Tourne à gauche", D pour "Tourne à droite" (les changements de direction s'effectuent en restant sur place). Pour passer d'un niveau n au niveau supplémentaire $n+1$, on itère 3 fois le programme de niveau n avec une toute petite modification : on change la dernière lettre de la deuxième itération de D en G, c'est tout, les appels récursifs font le reste (j'ai programmé rapidement, il faudrait améliorer le programme, ça c'est sûr).



Une idée qui a fait son temps : on interpole la somme de somme de cos (qui s'annule pour les premiers) par une (smoothie !) cubique, on prend sa symétrique par rapport au milieu et on voit les points nuls communs qui sont les décomposants de Goldbach.



miroir-interpol.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
from mpl_toolkits.mplot3d import Axes3D
import matplotlib.pyplot as plt
import math
import numpy as np
from scipy.interpolate import interp1d

fig, ax = plt.subplots(figsize=(15, 10))

def sd(n):
    # somme des diviseurs de n >= 1
    return sum([sum([math.cos(2*math.pi*n*l/k) for l in range(1, k+1)]) for k in range(1, n+1)])
#for n in 1, 2, 3, 4, 5, 6, 12, 100: print(f'sd({n:3}) = {sd(n):6.2f}')

n = 98  # taille de la grille d'entiers
m = 5*n  # taille de sa discretisation

X = np.array([i for i in range(1, n+1)])
Z = np.array([sd(i) - i - 1 for i in range(1, n+1)])
#print(f'\nX =\n{X}\nZ =\n{Z}')
Zp = np.array([sd(n-i) - n + i - 1 for i in range(1, n+1)])

Xd = np.linspace(1, n, num=m)
#print(f'\nXd =\n{Xd}')

Zd = interp1d(X, Z, kind='cubic')(Xd)
Zdp = interp1d(X, Zp, kind='cubic')(Xd)
#print(f'\nZd =\n{Zd}')

ax.plot(Xd, Zd)
ax.plot(Xd, Zdp)
ax.set_ylim(-20,200)
#ax.scatter(X, Z, c='r', marker='o')
ax.scatter([3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97], [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0], c='r', marker='o')
plt.text(18,-10,'19')
plt.text(30,-10,'31')
plt.text(36,-10,'37')
plt.text(78,-10,'79')
plt.text(66,-10,'67')
plt.text(60,-10,'61')
plt.show()
```

Spirale d'Archimède sur laquelle on positionne les nombres entiers successifs soit sur l'axe des abscisses s'ils sont multiples d'un nombre entier, soit sur les angles correspondant aux racines de l'unité suivant qu'ils sont congrus à $1, \ldots, k-1$ selon le nombre k choisi (on montre le résultat pour $k = 3$, ou $k = 5$.

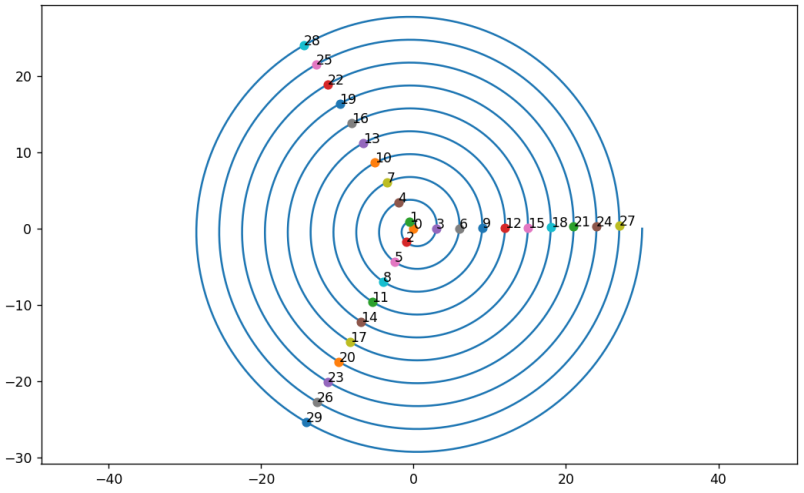
pc2.py - GNU Emacs at DESKTOP-4PROGGL

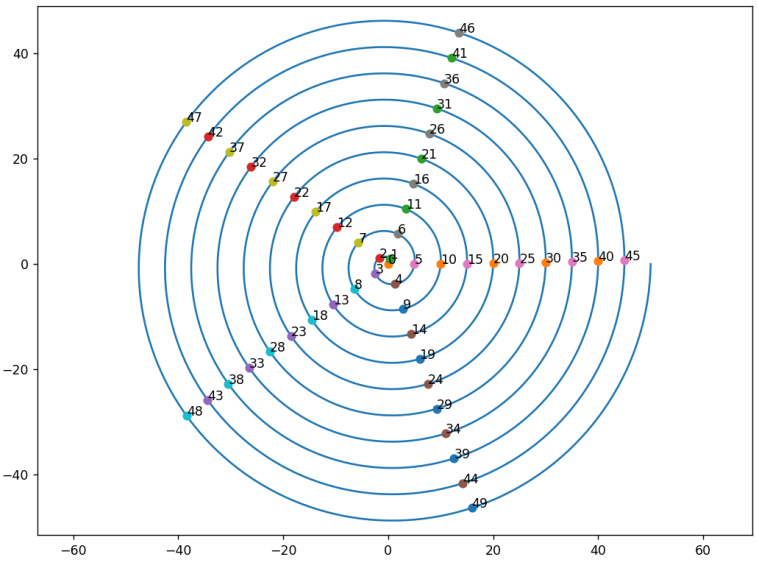
File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import pi, sin, cos

a = 3/(2*pi)
nbtours = 10
print(np.pi)
theta = np.linspace(0, nbtours*2*pi, nbtours*360)
rho = a*theta
x = rho*cos(theta)
y = rho*sin(theta)
plt.plot(x,y)
for nb in range(10):
    ici = nb*360
    icix = rho[ici]*cos(theta[ici])
    iciy = rho[ici]*sin(theta[ici])
    plt.plot([icix],[iciy], 'o')
    plt.annotate(3*nb,xy=(icix,iciy))
    ici = ici+120
    icix = rho[ici]*cos(theta[ici])
    iciy = rho[ici]*sin(theta[ici])
    plt.plot([icix],[iciy], 'o')
    plt.annotate(3*nb+1,xy=(icix,iciy))
    ici = ici+120
    icix = rho[ici]*cos(theta[ici])
    iciy = rho[ici]*sin(theta[ici])
    plt.plot([icix],[iciy], 'o')
    plt.annotate(3*nb+2,xy=(icix,iciy))
plt.axis('equal')
plt.show()
```

-\--- **pc2.py** All L1 (Python ElDoc)

Figure 1





Fractales d'anneaux de polynômes : il s'agissait de programmer les exemples de l'article de Connes-Consani de juillet 2023 "Sur la métaphysique de $\mathbb{F}_1$".

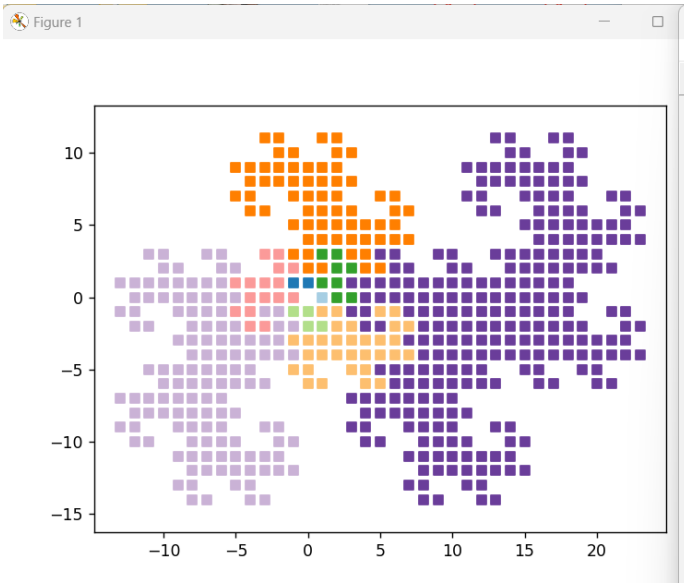


fig-entiers-de-Gauss.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos
cmap = plt.colormaps['Paired']

n = 2
X = -1+1j
lesmu = [1]
polynomes = [0]

degre = 9
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        facecolor=cmap(k/(degre+1)), marker='s')
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```

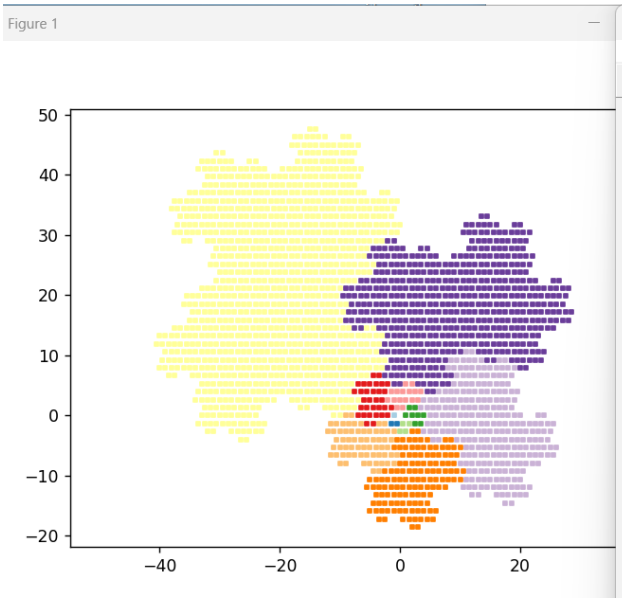


fig614.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos, sqrt
cmap = plt.colormaps['Paired']

X = 0.5*(1+1j*sqrt(7))
lesmu = [-1]
polynomes = [0]

degre = 11
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        facecolor=cmap(k/(degre+1)), marker='s', s=5)
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```

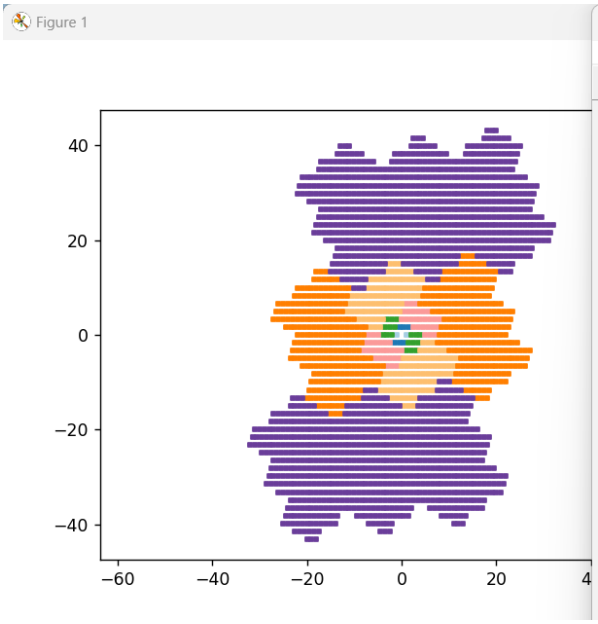


fig7.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos, sqrt
cmap = plt.colormaps['Paired']

n = 3
X = 0.5*(1+1j*sqrt(11))
lesmu = [-1,1]
polynomes = [0]

degre = 7
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        facecolor=cmap(k/(degre+1)), marker='s', s=5)
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```

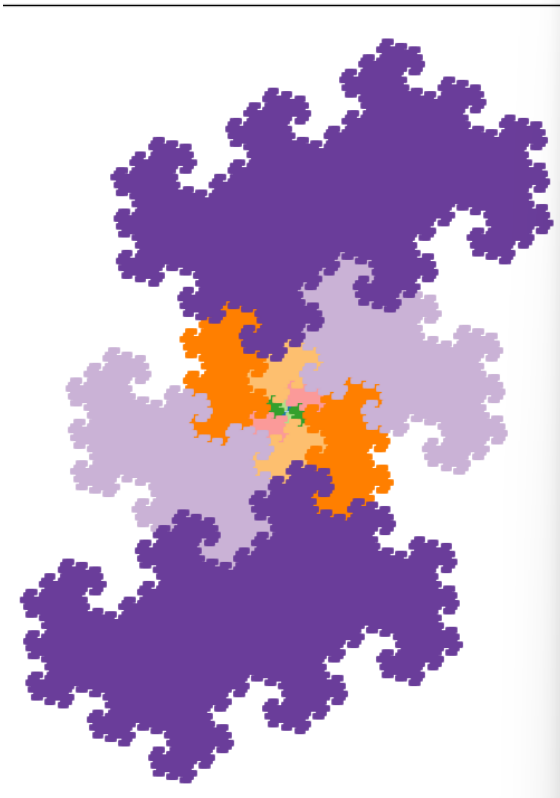


fig8.py - GNU Emacs at DESKTOP-4PROGGL

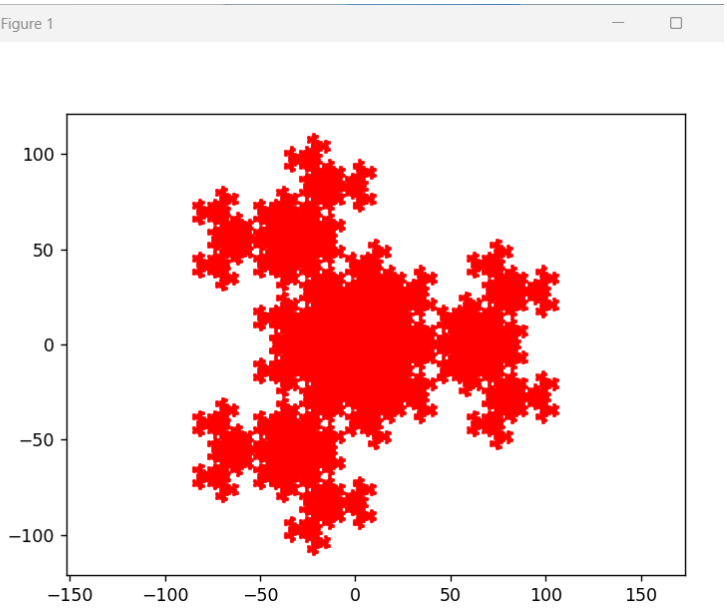
File Edit Options Buffers Tools Python Help

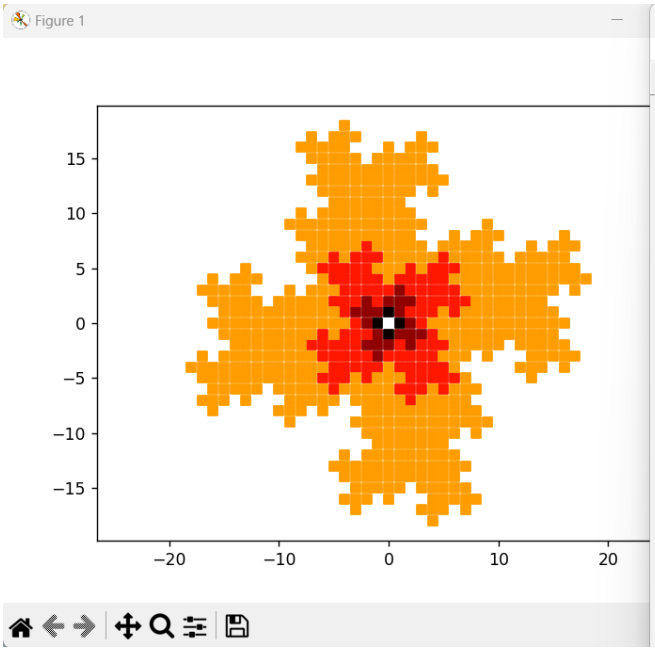
```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos, sqrt
cmap = plt.colormaps['Paired']

X = 1+1j*sqrt(2)
lesmu = [-1,1]
polynomes = [0]

degre = 9
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        facecolor=cmap(k/(degre+1)), marker='s', s=5
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```

triflake.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos
cmap = plt.colormaps['Paired']

n = 3
X = -2
lesmu = [exp(1j*2*pi*k/n) for k in range(n)]
polynomes = [0]

degre = 7
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        color='red', marker='s', s=2)
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```





unfractaldes.py - GNU Emacs at DESKTOP-4PROGGL

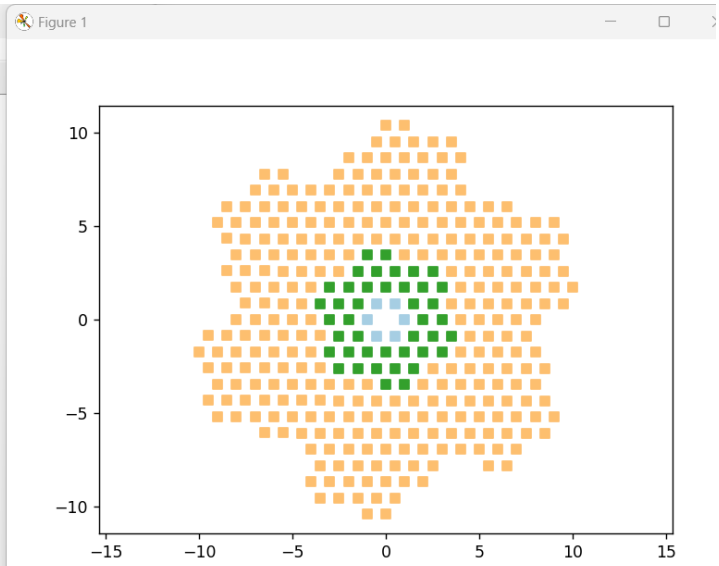
File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos
cmap = plt.colormaps['hot']

n = 4
X = 1+2j
lesmu = [exp(1j*2*pi*k/n) for k in range(n)]
polynomes = [0]

degre = 4
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        facecolor=cmap(k/(degre+1)), marker='s')
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```

hexabis.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos, sqrt
cmap = plt.colormaps['Paired']

n = 6
X = 0.5*(5-sqrt(3)*1j)
lesmu = [exp(1j*2*pi*k/n) for k in range(n)]
polynomes = [0]

degre = 3
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        facecolor=cmap(k/(degre+1)), marker='s')
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```

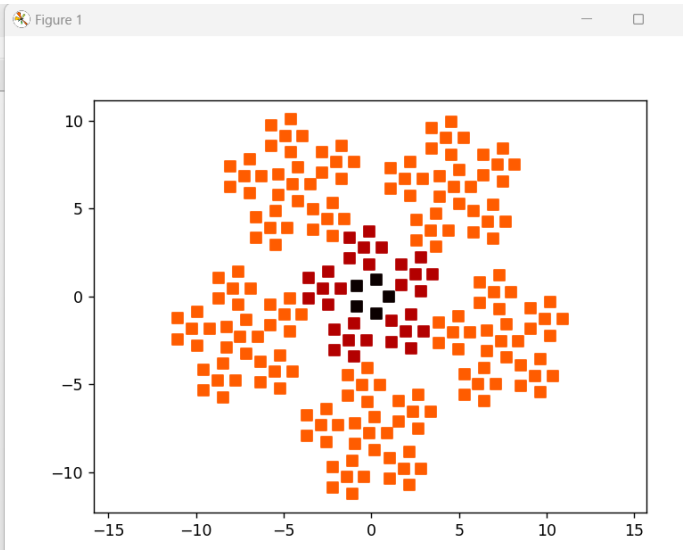


Mon pentaflake plein de trous, sans bijection donc, mais j'aime bien !

tente-pentaflake.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos, sqrt
cmap = plt.colormaps['hot']

n = 5
X = 2.5+0.25*1j
lesmu = [exp(1j*2*pi*k/n) for k in range(n)]
polynomes = [0]

degre = 3
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        facecolor=cmap(k/(degre+1)), marker='s', s=50)
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```



Pour mémoire : programmes python3 des programmes Matlab du livre de référence de Trefethen "Spectral methods in Matlab" (Denise Vella-Chemla, juillet 2023)

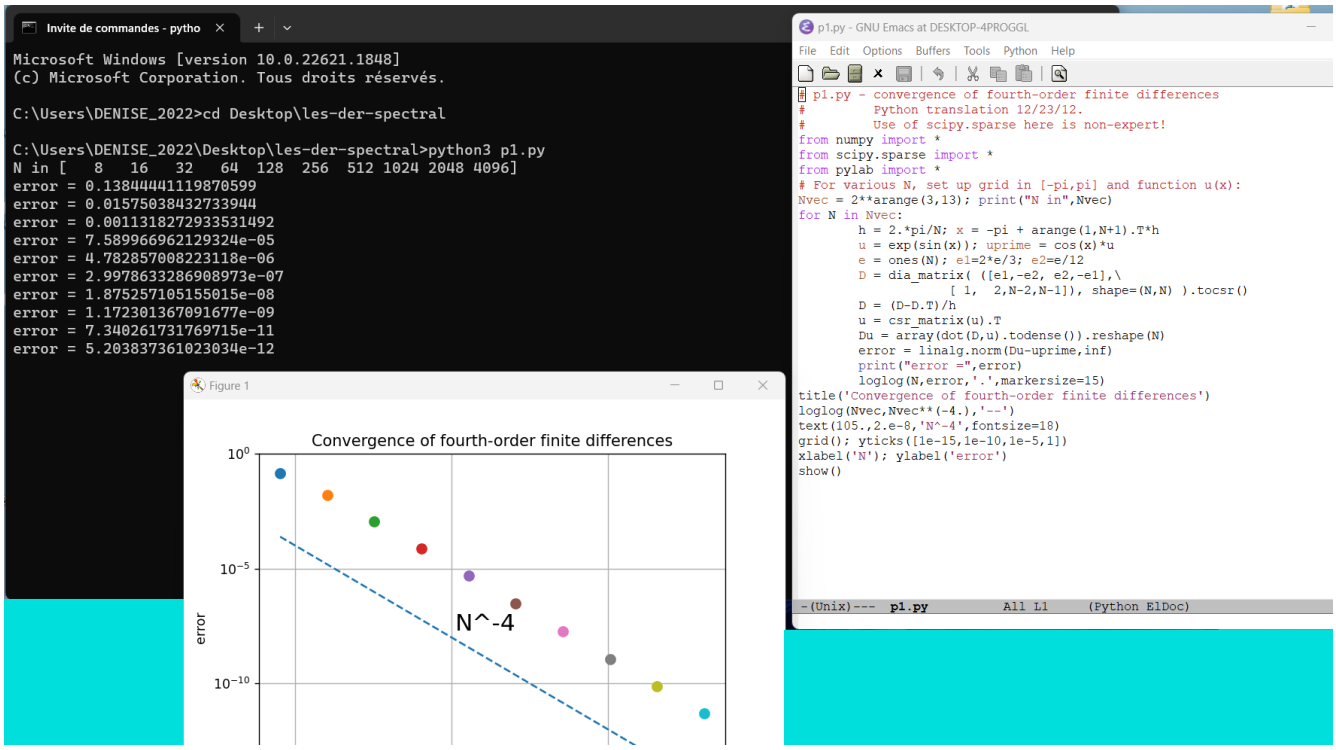
On essaie de se former tant bien que mal à l'analyse spectrale. Dans ce but, on a repris les programmes des deux pages ci-dessous pour qu'ils tournent de façon autonome en python3 et on les a accolés à leur résultat, pour mémoire.

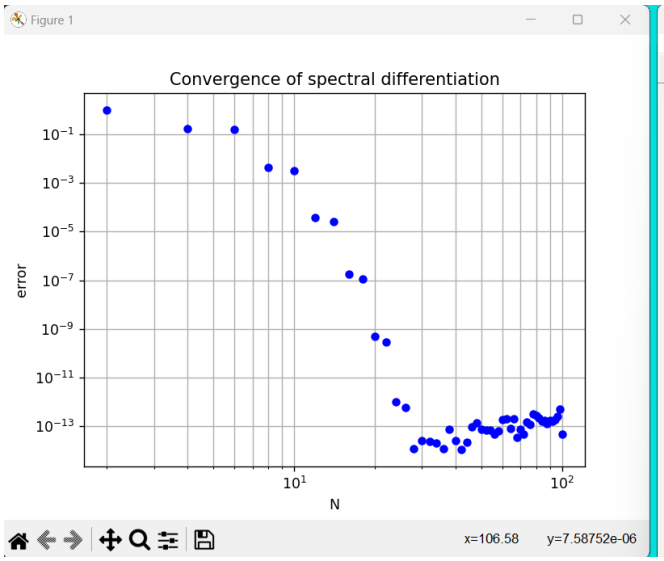
- les programmes (auteur inconnu : JR ?)

  https://blue.math.buffalo.edu/438/trefethen_spectral/all_py_files/ ;

- les programmes de Praveen Chandrashekar du Centre de Mathématiques appliquées de Bangalore en Inde

  http://cpraveen.github.io/teaching/chebpy.html ;

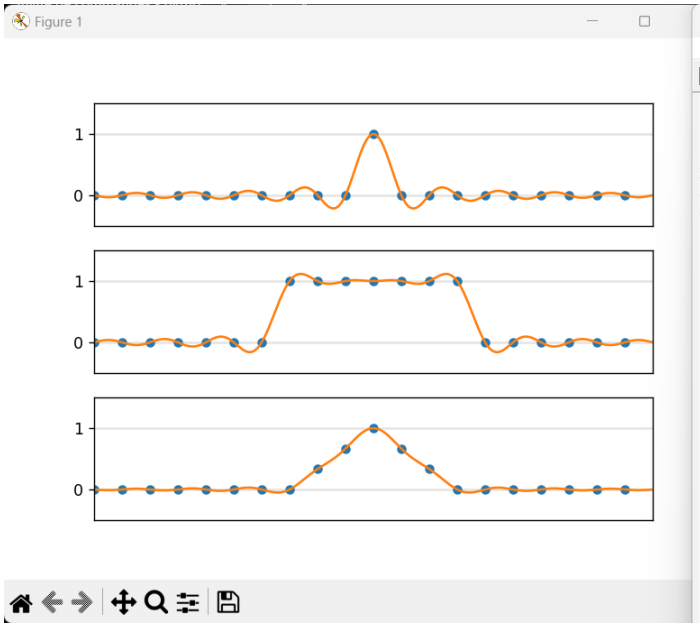




p2.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

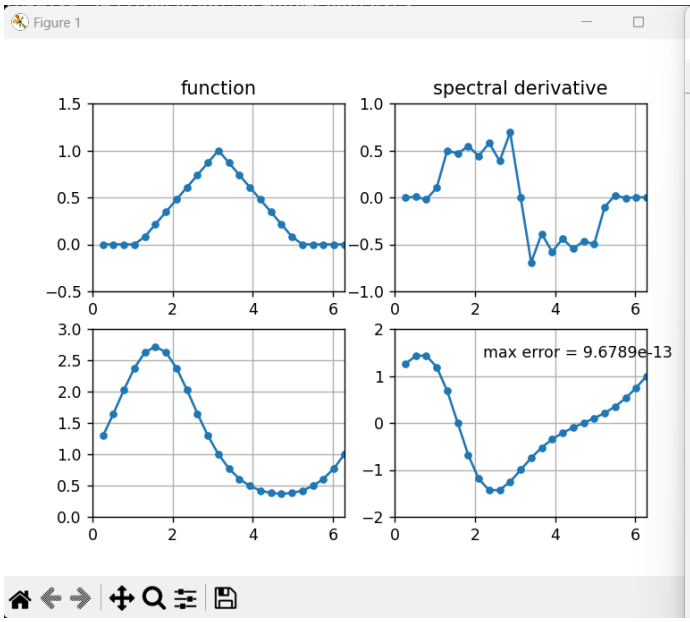
```
# p2.py - convergence of periodic spectral method (compare p1.m)
# JR translation 12/12/12

from numpy import *
from scipy.linalg import toeplitz
#from pylab import title, grid, loglog, xlabel, ylabel, show
from pylab import *

# For various N (even), set up grid as before:

for N in range(2,101,2):
        h = 2.*pi/N;
        x = -pi + arange(0,N).T*h # (including left endpoint instead of right)
        u = exp(sin(x)); uprime = cos(x)*u;
        # Construct spectral differentiation matrix:
        i = array( range(1,N) )
        column   = hstack(( [0.], .5*(-1)**i/tan(i*h/2.) ))
        row      = hstack(( [0.], column[N-1:0:-1]       ))
        D = toeplitz(column,row)
        error = linalg.norm(dot(D,u)-uprime,inf)
        loglog(N,error,'bo',markersize=5)

grid(True,which='both')
xlabel('N'); ylabel('error')
title('Convergence of spectral differentiation')
show()
```



p3.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

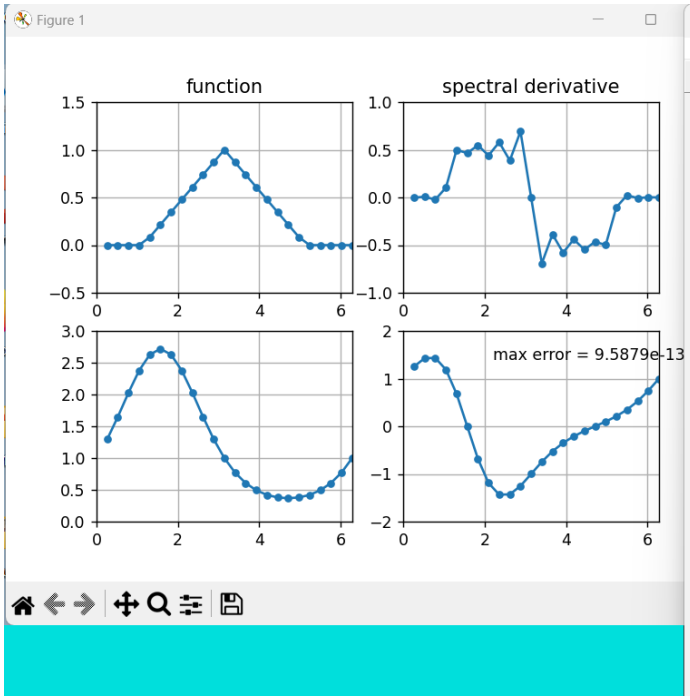
```
# p3.py - band-limited interpolation
# JR translation, 12/13/12
from numpy import *
from pylab import *
h = 1.; xmax = 10.
x = arange(-xmax,xmax,h)                # computational grid
xx = arange(-xmax-h/20,xmax+h/20,h/10)  # plotting grid
for pl in range(3):
        subplot(3,1,pl+1)
        if pl==0: v = x==0                      # delta function
        if pl==1: v = abs(x)<=3.                # square wave
        if pl==2: v = maximum(0.,1.-abs(x)/3.)  # hat function
        v = array(v,dtype=float) # convert boolean to float
        plot([-xmax,xmax],[0.,0.],'k',alpha=0.1)
        plot([-xmax,xmax],[1.,1.],'k',alpha=0.1)
        plot(x,v,'.',markersize=10)
        p = zeros_like(xx)
        for i,xi in enumerate(x):
                p += v[i]*sin(pi*(xx-xi)/h)/(pi*(xx-xi)/h)
        plot(xx,p)
        xlim(-xmax,xmax); ylim(-.5,1.5)
        xticks([]); yticks([0.,1.])
show()
```



p4.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

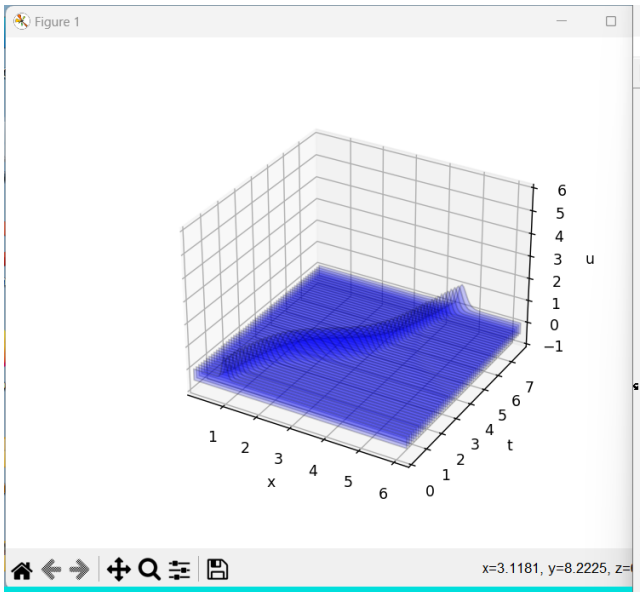
```
# p4.m - periodic spectral differentiation
# Translation 12/13/12
from numpy import *
from scipy.linalg import toeplitz
from pylab import *

# Set up grid and differentiation matrix:
N = 24; h = 2*pi/N; x = h*arange(1,N+1);
i = array( range(1,N) )
column   = hstack(( [0.], .5*(-1)**i/tan(i*h/2.) ))
row      = hstack(( [0.], column[N-1:0:-1]       ))
D = toeplitz(column,row)

# Differentiation of a hat function:
v = maximum(0.,1.-abs(x-pi)/2.)
subplot(2,2,1); plot(x,v,'.-',markersize=8)
xlim(0,2*pi); ylim(-0.5,1.5); grid(); title('function')
subplot(2,2,2); plot(x,dot(D,v),'.-',markersize=8)
xlim(0,2*pi); ylim(-1.,1.); grid(); title('spectral derivative')

# Differentiation of exp(sin(x)):
v = exp(sin(x)); vprime = cos(x)*v;
subplot(2,2,3); plot(x,v,'.-',markersize=8)
xlim(0,2*pi); ylim(0.,3.); grid()
subplot(2,2,4); plot(x,dot(D,v),'.-',markersize=8)
xlim(0,2*pi); ylim(-2.,2.); grid()
error = linalg.norm(dot(D,v)-vprime,inf);
text(2.2,1.4,'max error = '+str('%.4e' % error))
show()
```



p5.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

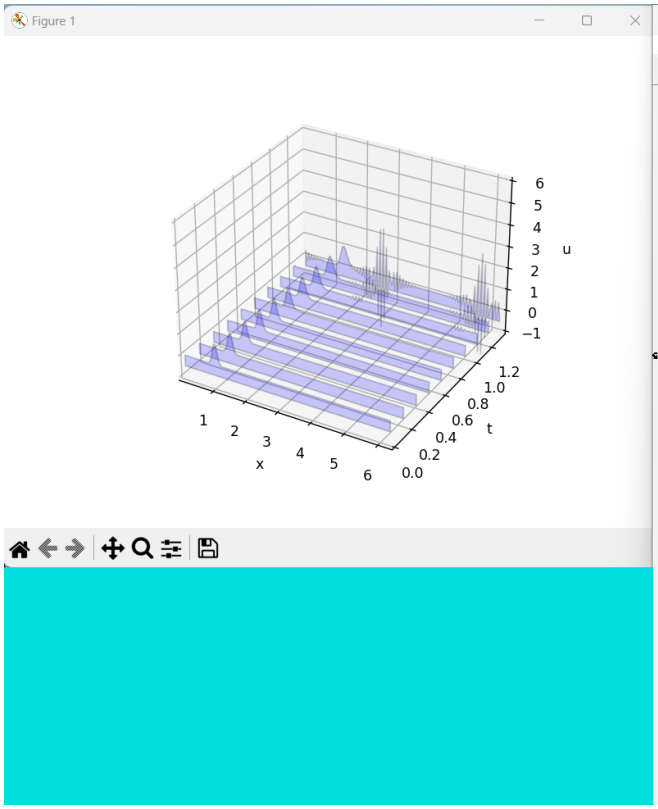
```
# p5.py - repetition of p4.py via FFT
#         For complex v, delete "real" commands.
#         Python/NumPy translation 12/14/12

from numpy import *
from numpy.fft import fft,ifft
from pylab import *

# Differentiation of a hat function:
N = 24; h = 2*pi/N; x = h*arange(1,N+1)
v = maximum(0.,1.-abs(x-pi)/2.); v_hat = fft(v)
w_hat = 1j*hstack(( range(N//2),[0.],range(-N//2+1,0) ))*v_hat
w = real(ifft(w_hat))
subplot(2,2,1), plot(x,v,'.-',markersize=8)
#axis([0 2*pi -.5 1.5]), grid on, title('function')
xlim(0,2*pi); ylim(-0.5,1.5); grid(); title('function')
subplot(2,2,2), plot(x,w,'.-',markersize=8)
xlim(0,2*pi); ylim(-1.,1.); grid(); title('spectral derivative')

# Differentiation of exp(sin(x)):
v = exp(sin(x)); vprime = cos(x)*v
v_hat = fft(v)
w_hat = 1j*hstack(( range(N//2),[0.],range(-N//2+1,0) ))*v_hat
w = real(ifft(w_hat))
subplot(2,2,3); plot(x,v,'.-',markersize=8)
xlim(0,2*pi); ylim(0.,3.); grid()
subplot(2,2,4); plot(x,w,'.-',markersize=8)
xlim(0,2*pi); ylim(-2.,2.); grid()
error = linalg.norm(w-vprime,inf)
text(2.2,1.4,'max error = '+str('%.4e' % error))

show()
```



p6.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

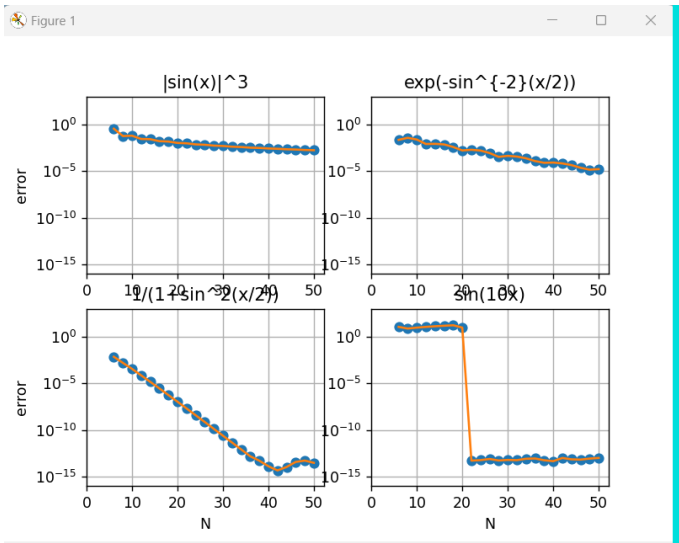
```
import numpy as np ; from numpy import * ; from numpy.fft import fft,ifft
import matplotlib.pyplot as plt ; from mpl_toolkits import mplot3d
import matplotlib ; from matplotlib.colors import to_rgba
from matplotlib.collections import PolyCollection

def waterfall(x,t,u,labels=['x','t','u'],slabthickness=0.5,zrange=[-1.,6.]):
        fig = plt.figure()
        ax = plt.axes(projection='3d')
        cc = lambda arg: matplotlib.colors.to_rgba(arg, alpha=1.0)
        xs = np.hstack(( x,x[-1],x[0] ))
        verts = []
        zs = t
        baseline  = 0.        -                          slabthickness
        for ti,z in enumerate(zs):
                ys = np.hstack(( u[ti,:],baseline,baseline ))
                verts.append(list(zip(xs, ys)))
        poly = PolyCollection(verts, edgecolors = 'black', facecolors = [cc('blue
e')], alpha=.6)
        poly.set_alpha(0.2)
        ax.add_collection3d(poly, zs=zs, zdir='y')
        ax.set_xlabel(labels[0]) ; ax.set_xlim3d(min(xs),max(xs))
        ax.set_ylabel(labels[1]) ; ax.set_ylim3d(min(zs),max(zs))
        ax.set_zlabel(labels[2])
        ax.set_zlim3d(zrange[0],zrange[1])

N=128; h = 2*pi/N; x = h*arange(1,N+1); t = 0.; dt = h/4
c = .2 + sin(x-1)**2
v    = exp(-100*(x      -1)**2)
vold = exp(-100*(x-.2*dt-1)**2)
tmax = 8.; tplot = .15
plotgap = int(round(tplot/dt)); dt = tplot/plotgap
nplots  = int(round(tmax/tplot))
data = vstack(( v, zeros((nplots,N)) )); tdata = [t]
for i in range(nplots):
        for n in range(plotgap):
                t += dt;
                v_hat = fft(v)
                w_hat = 1j*hstack(( range(N//2),[0.],range(-N//2+1,0) ))*v_hat
                w = real(ifft(w_hat))
                vnew = vold - 2*dt*c*w; vold = v.copy(); v = vnew
        data[i+1,:] = v; tdata.append(t)
waterfall(x,tdata,data)
plt.show()
```



p6u.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

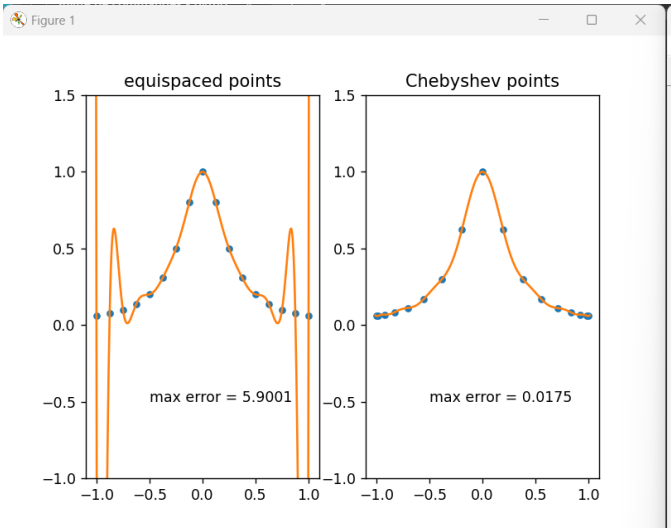
```
import numpy as np ; from numpy import *
from numpy.fft import fft,ifft
import matplotlib ; import matplotlib.pyplot as plt
from mpl_toolkits import mplot3d ; from matplotlib.colors import to_rgba
from matplotlib.collections import PolyCollection

def waterfall(x,t,u,labels=['x','t','u'],slabthickness=0.5,zrange=[-1.,6.]):
        fig = plt.figure()
        ax = plt.axes(projection='3d')
        cc = lambda arg: matplotlib.colors.to_rgba(arg, alpha=1.0)
        xs = np.hstack(( x,x[-1],x[0] ))
        verts = [] ; zs = t ; baseline  = 0.-slabthickness
        for ti,z in enumerate(zs):
                ys = np.hstack(( u[ti,:],baseline,baseline ))
                verts.append(list(zip(xs, ys)))
        poly = PolyCollection(verts, edgecolors = 'black', facecolors = [cc('blue
e')], alpha=.4)
        poly.set_alpha(0.2)
        ax.add_collection3d(poly, zs=zs, zdir='y')
        ax.set_xlabel(labels[0]) ; ax.set_xlim3d(min(xs),max(xs))
        ax.set_ylabel(labels[1]) ; ax.set_ylim3d(min(zs),max(zs))
        ax.set_zlabel(labels[2]) ; ax.set_zlim3d(zrange[0],zrange[1])

N=128; h = 2*pi/N; x = h*arange(1,N+1)
c = .2 + sin(x-1)**2
t = 0.; dt = 1.9/N
v    = exp(-100*(x      -1)**2)
vold = exp(-100*(x-.2*dt-1)**2)
tmax = 1.4; tplot = .15
plotgap = int(round(tplot/dt)); dt = tplot/plotgap
nplots  = int(round(tmax/tplot))
data = vstack(( v, zeros((nplots,N)) )); tdata = [t]
for i in range(nplots):
        for n in range(plotgap):
                t += dt;
                v_hat = fft(v)
                w_hat = 1j*hstack(( range(N//2),[0.],range(-N//2+1,0) ))*v_hat
                w = real(ifft(w_hat))
                vnew = vold - 2*dt*c*w;                 # leap frog formula
                vold = v.copy(); v = vnew
        data[i+1,:] = v; tdata.append(t)
ax = waterfall(x,tdata,data)
plt.show()
```




```
p7.py - GNU Emacs at DESKTOP-4PROGGL
File  Edit  Options  Buffers  Tools  Python  Help
from numpy import *
from scipy.linalg import toeplitz
from pylab import *
set_printoptions(linewidth=200,precision=5)
# Compute derivatives for various values of N:
Nmax = 50; E = zeros((4,Nmax//2-2))
Ns = range(6,Nmax+2,2)
for N in Ns:
        h = 2*pi/N; x = h*arange(1,N+1)
        i = array( range(1,N) )
        column   = hstack(( [0.], .5*(-1)**i/tan(i*h/2.) ))
        row      = hstack(( [0.], column[N-1:0:-1]       ))
        D = toeplitz(column,row)
        #print D
        v = abs(sin(x))**3
        # 3rd deriv in BV
        vprime = 3*sin(x)*cos(x)*abs(sin(x))
        E[0,N//2-3] = linalg.norm(dot(D,v)-vprime,inf)
        v = exp(-sin(x/2)**(-2))
# C-infinity
        vprime = .5*v*sin(x)/sin(x/2)**4
        E[1,N//2-3] = linalg.norm(dot(D,v)-vprime,inf)
        v = 1/(1+sin(x/2)**2)
# analytic in a strip
        vprime = -sin(x/2)*cos(x/2)*v**2
        E[2,N//2-3] = linalg.norm(dot(D,v)-vprime,inf)
        v = sin(10*x); vprime = 10*cos(10*x)            # band-limited
        E[3,N//2-3] = linalg.norm(dot(D,v)-vprime,inf)

# Plot results:
titles = ['|sin(x)|^3','exp(-sin^{-2}(x/2))',\
          '1/(1+sin^2(x/2))','sin(10x)'      ]
for iplot in [0,1,2,3]:
        subplot(2,2,iplot+1)
        semilogy(Ns,E[iplot,:],'.',markersize=12)
        plot(Ns,E[iplot,:])
        ylim(1e-16, 1e3)
        xticks(arange(0,Nmax+10,10));
        if iplot>1: xlabel('N')
        yticks(10.**(arange(-15,5,5)));
        if iplot%2==0: ylabel('error')
        grid()
        title(titles[iplot])
show()
```

```
C:\Users\DENISE_2022\Desktop\les-der-spectral>python3 p8.py
6 [ 0.46147291699547  7.49413462105052  7.72091605300656 28.8324837783401 ]
12 [0.97813728129861 3.17160532064719 4.4559352911668  8.92452905811993]
18 [0.9999700014993  3.00064406679582 4.99259532440077  7.03957189798149]
24 [0.99999999762905 3.00000009841086 4.99999796527329 7.00002499815655]
30 [0.99999999999998 3.00000000000073 4.9999999999756  7.0000000005086 ]
36 [1.               3.               4.99999999999999 7.              ]

C:\Users\DENISE_2022\Desktop\les-der-spectral>
```

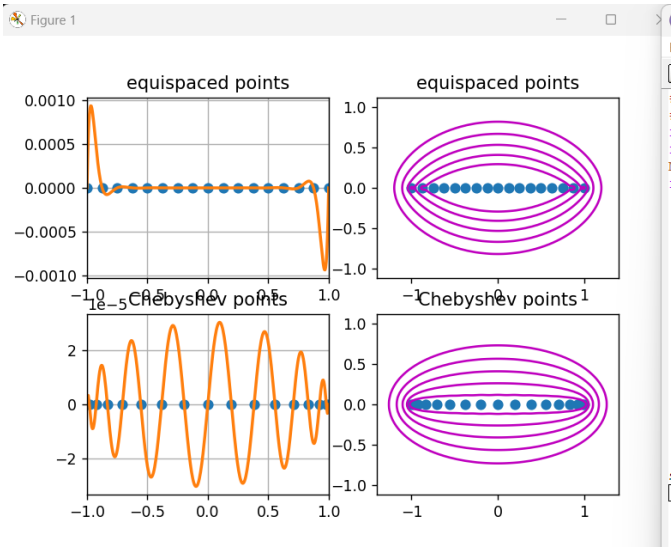
```
# p8.py - eigenvalues of harmonic oscillator -u"+x^2 u on R
#         Python translation 12/19/12
from numpy import *
from scipy.linalg import toeplitz
set_printoptions(linewidth=200,precision=14)

L = 8.                                  # domain is [-L L], periodic
for N in range(6,42,6):
        h = 2*pi/N; x = h*arange(1,N+1); x = L*(x-pi)/pi
        i = array( range(1,N) )
        column = hstack(( [-pi**2/(3*h**2)-1./6.] ,\
                          -.5*(-1)**i/sin(h*i/2.)**2 ))
        D2 = (pi/L)**2*toeplitz(column)  # 2nd-order differentiation
        eigenvalues = sort(linalg.eigvals(-D2 + diag(x**2)))
        print(N, eigenvalues[0:4])
```



p9.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

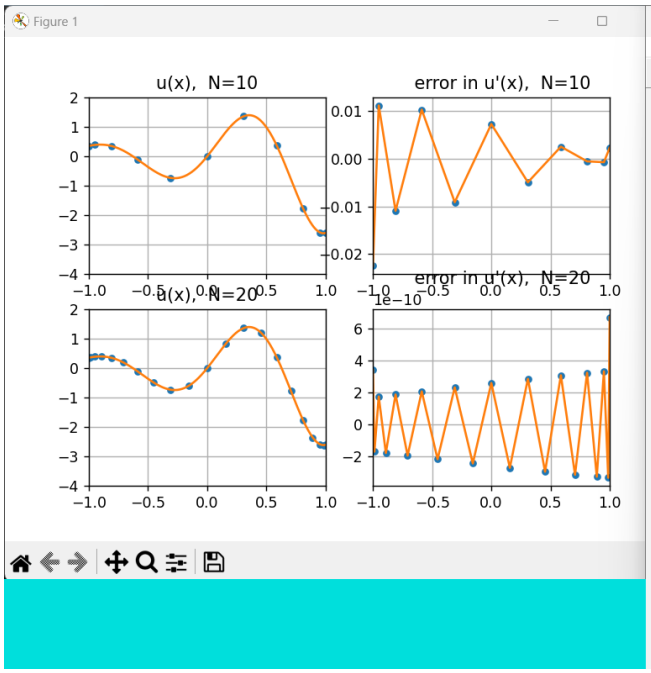
```
# p9.py - polynomial interpolation in equispaced and Chebyshev pts
# Python translation 12/17/12
from numpy import *
from pylab import *
N = 16
xx = arange(-1.01,1.015,.005) #-1.01:.005:1.01
for i in [1,2]:
        if i==1: s = 'equispaced points'; x = -1. + 2.*arange(0,N+1)/N
        if i==2: s =  'Chebyshev points'; x = cos(pi*arange(0,N+1)/N)
        subplot(1,2,i)
        u  = 1/(1+16*x**2 )
        uu = 1/(1+16*xx**2)
        p = polyfit(x,u,N)              # interpolation
        pp = polyval(p,xx)              # evaluation of interpolant
        plot(x,u,'.',markersize=8)
        plot(xx,pp)
        xlim(-1.1,1.1); ylim(-1,1.5); title(s)
        error = linalg.norm(uu-pp,inf)
        text(-.5,-.5,'max error = '+str('%.4f' % error) )
show()
```



p10.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

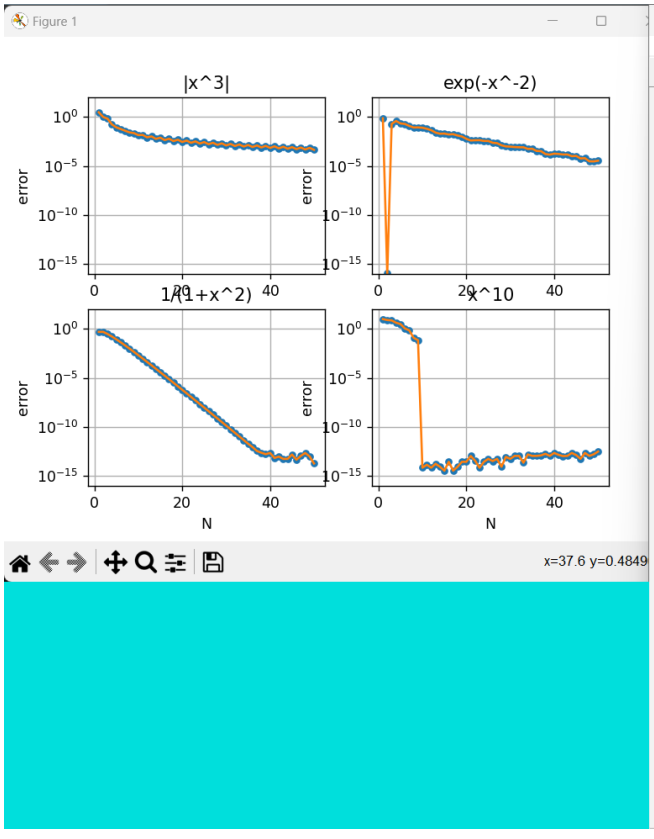
```
# p10.py - polynomials and corresponding equipotential curves
#          Translation started 12/20/12
from numpy import *
from pylab import *
N = 16
for i in [0,1]:
        if i==0: s = 'equispaced points'; x = linspace(-1.,1.,N+1)
        if i==1: s = 'Chebyshev points' ; x = cos(linspace(0,pi,N+1))
        p = poly(x)
        # Plot p(x) over [-1,1]:
        xx = arange(-1.,1.005,.005); pp = polyval(p,xx)
        subplot(2,2,int(2*i+1))
        plot(x,0*x,'.',markersize=12)
        plot(xx,pp,linewidth=2); grid(); xlim(-1.,1.)
        xticks([-1.,-.5,0,.5,1]); title(s)
        # Plot equipotential curves:
        subplot(2,2,int(2*i+2))
        plot(real(x),imag(x),'.',markersize=12)
        xgrid = arange(-1.4,1.42,.02); ygrid = arange(-1.12,1.14,.02)
        xx,yy = meshgrid(xgrid,ygrid); zz = xx+1j*yy
        pp = polyval(p,zz); levels = 10.**arange(-4,1)
        contour(xx,yy,abs(pp),levels,colors=['m']); title(s)
show()
```



p11.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

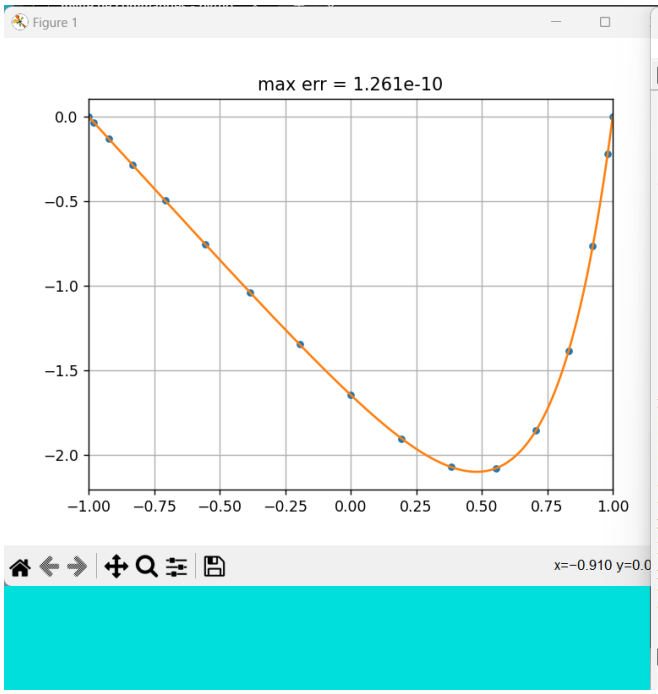
```
# p11.py - Chebyshev differentation of a smooth function
#          Python/NumPy translation by JR 12/22/12
from numpy import *
from pylab import *

def cheb(N):
        if N==0:
                D = 0.; x = 1.
        else:
                n = np.arange(0,N+1)
                x = cos(pi*n/N).reshape(N+1,1)
                c = (hstack(( [2.], ones(N-1), [2.]))*(-1)**n).reshape(N+1,1)
                X = tile(x,(1,N+1))
                dX = X - X.T
                D = dot(c,1./c.T)/(dX+eye(N+1))
                D -= diag(sum(D.T,axis=0))
        return D, x.reshape(N+1)

xx = arange(-1,1.01,.01); uu = exp(xx)*sin(5*xx)
for N in [10, 20]:
        D,x = cheb(N); u = exp(x)*sin(5*x)
        subplot(2,2,2*(N==20)+1)
        plot(x,u,'.',markersize=8); grid()
        plot(xx,uu)
        xlim(-1,1); ylim(-4,2); title('u(x),  N='+str(N))
        error = dot(D,u) - exp(x)*(sin(5*x)+5*cos(5*x))
        subplot(2,2,2*(N==20)+2)
        plot(x,error,'.',markersize=8); grid()
        plot(x,error)
        xlim(-1,1); title("    error in u'(x),  N="+str(N))
show()
```



p12.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

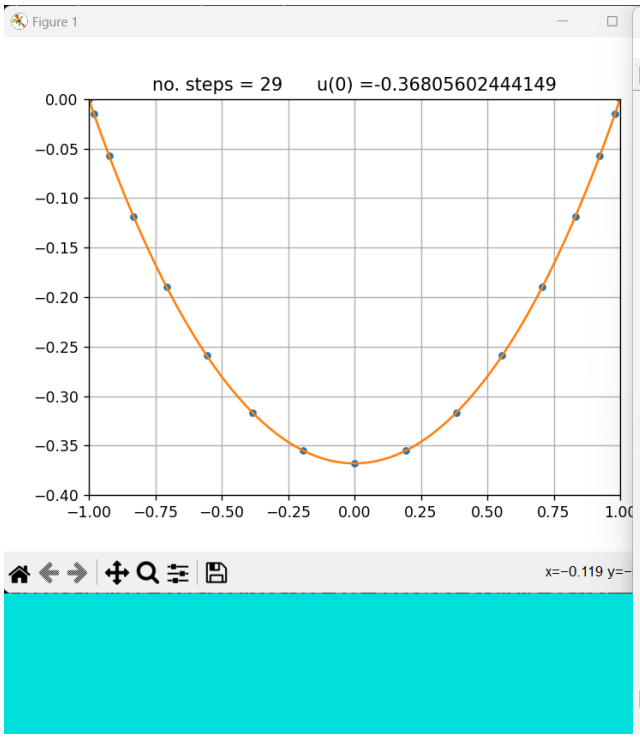
```
# p12.py - accuracy of Chebyshev spectral differentiation
#          (compare p7.py)
#          Python/NumPy translation 12/22/12
from numpy import *
from pylab import *

def cheb(N):
        if N==0:
                D = 0.; x = 1.
        else:
                n = np.arange(0,N+1)
                x = cos(pi*n/N).reshape(N+1,1)
                c = (hstack(( [2.], ones(N-1), [2.]))*(-1)**n).reshape(N+1,1)
                X = tile(x,(1,N+1))
                dX = X - X.T
                D = dot(c,1./c.T)/(dX+eye(N+1))
                D -= diag(sum(D.T,axis=0))
        return D, x.reshape(N+1)

# Compute derivatives for various values of N:
Nmax = 50; E = zeros((4,Nmax))
for N in range(1,Nmax+1):
        D,x = cheb(N)
        v = abs(x)**3;      vprime = 3*x*abs(x) # 3rd deriv in BV
        E[0,N-1] = linalg.norm(dot(D,v)-vprime,inf)
        v = exp(-x**(-2)); vprime = 2*v/x**3   # C-infinity
        E[1,N-1] = linalg.norm(dot(D,v)-vprime,inf)
        v = 1/(1+x**2);     vprime = -2*x*v**2  # analytic in [-1,1]
        E[2,N-1] = linalg.norm(dot(D,v)-vprime,inf)
        v = x**10;          vprime = 10*x**9    # polynomial
        E[3,N-1] = linalg.norm(dot(D,v)-vprime,inf)

# Plot results:
titles = ['|x^3|','exp(-x^-2)','1/(1+x^2)','x^10']
for iplot in range(4):
        subplot(2,2,iplot+1)
        semilogy(range(1,Nmax+1),E[iplot,:],'.',markersize=8)
        plot(range(1,Nmax+1),E[iplot,:])
        ylim(1e-16,100); grid()
        yticks(10.**arange(-15,5,5))
        if iplot>1: xlabel('N');
        ylabel('error'); title(titles[iplot])
show()
```



p13.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

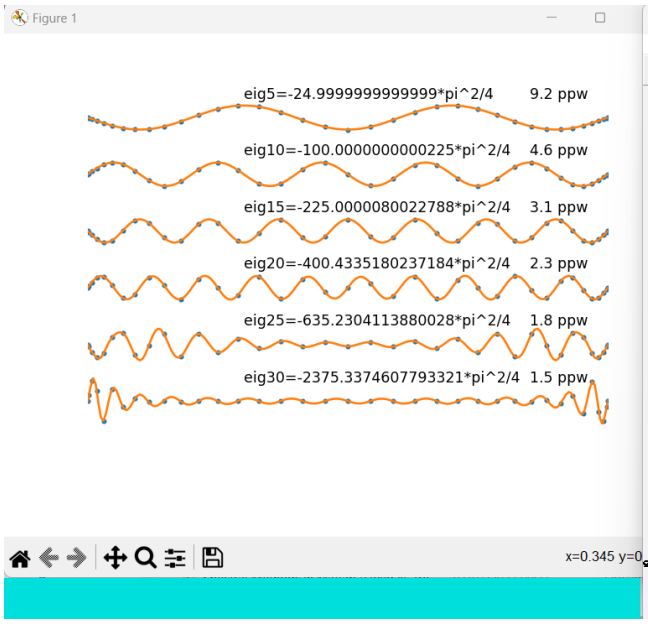
```
# p13.py - solve linear BVP u_xx = exp(4x), u(-1)=u(1)=0
#          Python/NumPy translation 12/23/12
from numpy import *
from pylab import *

def cheb(N):
        if N==0:
                D = 0.; x = 1.
        else:
                n = np.arange(0,N+1)
                x = cos(pi*n/N).reshape(N+1,1)
                c = (hstack(( [2.], ones(N-1), [2.]))*(-1)**n).reshape(N+1,1)
                X = tile(x,(1,N+1))
                dX = X - X.T
                D = dot(c,1./c.T)/(dX+eye(N+1))
                D -= diag(sum(D.T,axis=0))
        return D, x.reshape(N+1)

N = 16
D,x = cheb(N)
D2 = dot(D,D)
D2 = D2[1:-1,1:-1]                # boundary conditions
f = exp(4*x[1:-1])
u = linalg.solve(D2,f)            # Poisson eq. solved here
u = hstack(([0.],u,[0.]))
plot(x,u,'.',markersize=8)
xx = arange(-1,1.01,.01)
uu = polyval(polyfit(x,u,N),xx)   # interpolate grid data
plot(xx,uu)
grid(); xlim(-1,1)
exact = ( exp(4*xx) - sinh(4)*xx - cosh(4) )/16
title('max err = '+str('%.3e' % norm(uu-exact,inf)),fontsize=12)
show()
```

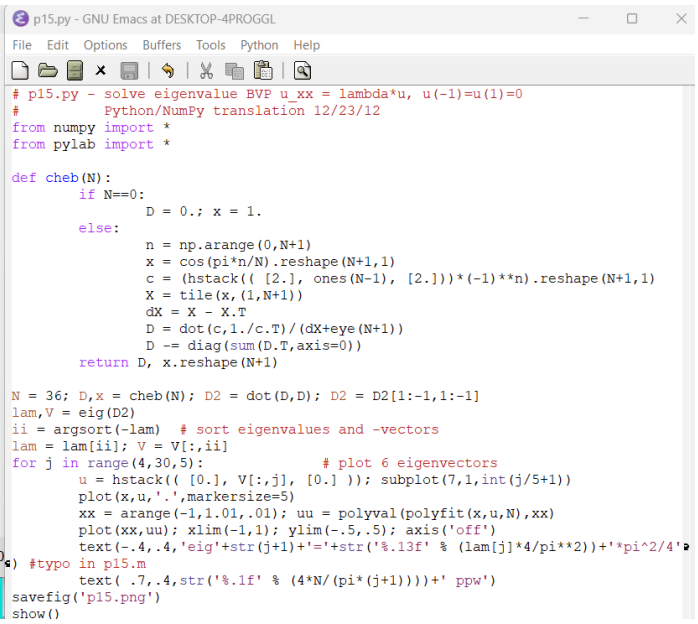


p14.py - GNU Emacs at DESKTOP-4PROGGL

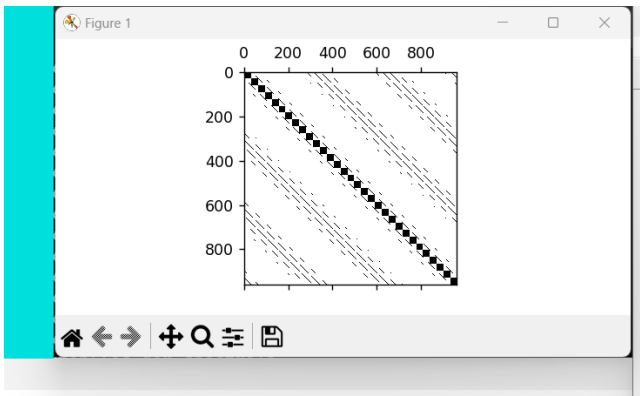
File Edit Options Buffers Tools Python Help

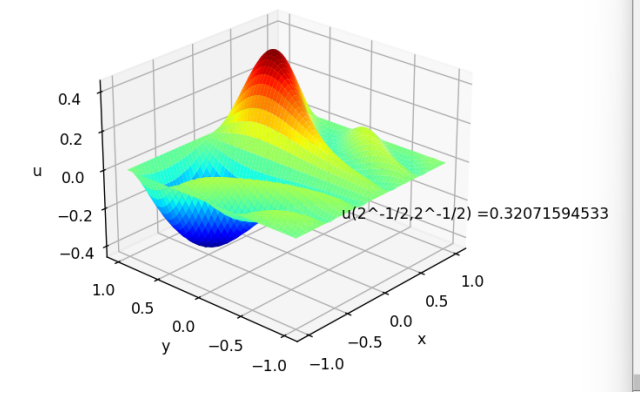
```
# p14.py - solve nonlinear BVP u_xx = exp(u), u(-1)=u(1)=0
#          (compare p13.py)
#          Python/NumPy translation 12/23/12
from numpy import *
from pylab import *

def cheb(N):
        if N==0:
                D = 0.; x = 1.
        else:
                n = np.arange(0,N+1)
                x = cos(pi*n/N).reshape(N+1,1)
                c = (hstack(( [2.], ones(N-1), [2.]))*(-1)**n).reshape(N+1,1)
                X = tile(x,(1,N+1))
                dX = X - X.T
                D = dot(c,1./c.T)/(dX+eye(N+1))
                D -= diag(sum(D.T,axis=0))
        return D, x.reshape(N+1)

N = 16
D,x = cheb(N); D2 = dot(D,D); D2 = D2[1:-1,1:-1]
u = zeros(N-1)
change = 1.; it = 0
while change > 1e-15:   # fixed-point iteration
        unew = linalg.solve(D2,exp(u))
        change = linalg.norm(unew-u,inf)
        u = unew; it += 1
u = hstack(([0.],u,[0.]))
plot(x,u,'.',markersize=8)
xx = arange(-1,1.01,.01)
uu = polyval(polyfit(x,u,N),xx)    # interpolate grid data
plot(xx,uu)
grid(); xlim(-1,1); ylim(-0.4,0)
title('no. steps = '+str(it)+'      u(0) ='+str('%.14f' % u[N//2]) )
show()
```

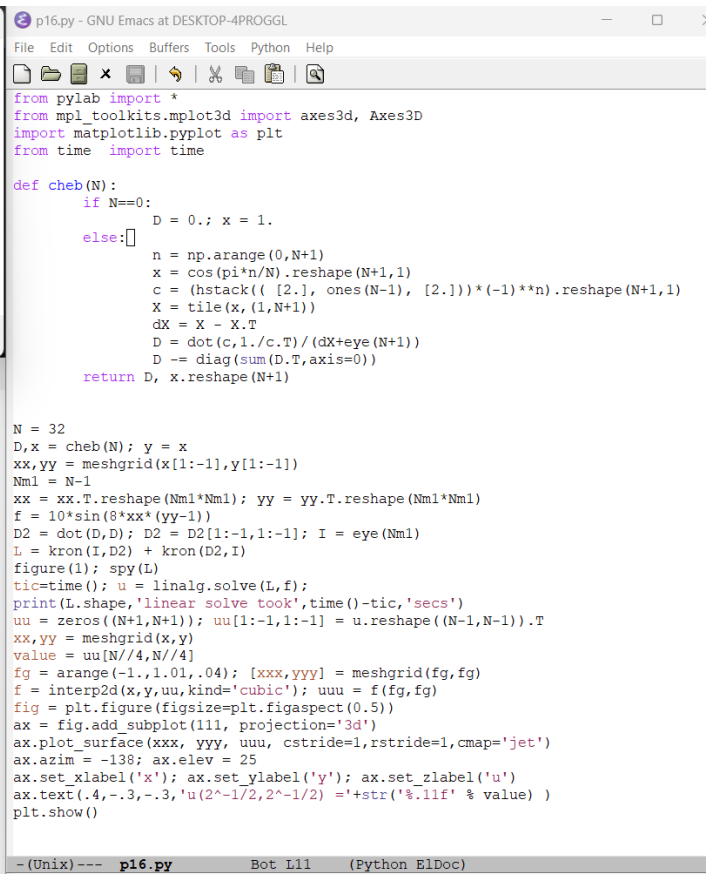




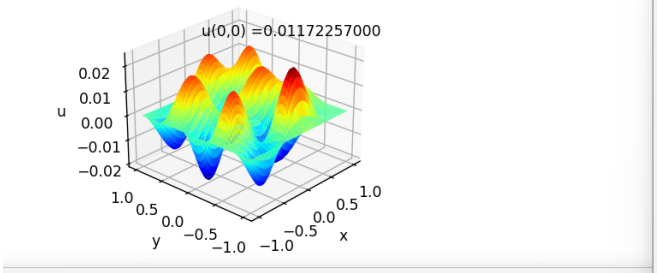

```
# p15.py - solve eigenvalue BVP u_xx = lambda*u, u(-1)=u(1)=0
#          Python/NumPy translation 12/23/12
from numpy import *
from pylab import *

def cheb(N):
        if N==0:
                D = 0.; x = 1.
        else:
                n = np.arange(0,N+1)
                x = cos(pi*n/N).reshape(N+1,1)
                c = (hstack(( [2.], ones(N-1), [2.]))*(-1)**n).reshape(N+1,1)
                X = tile(x,(1,N+1))
                dX = X - X.T
                D = dot(c,1./c.T)/(dX+eye(N+1))
                D -= diag(sum(D.T,axis=0))
        return D, x.reshape(N+1)

N = 36; D,x = cheb(N); D2 = dot(D,D); D2 = D2[1:-1,1:-1]
lam,V = eig(D2)
ii = argsort(-lam)  # sort eigenvalues and -vectors
lam = lam[ii]; V = V[:,ii]
for j in range(4,30,5):              # plot 6 eigenvectors
        u = hstack(( [0.], V[:,j], [0.] )); subplot(7,1,int(j/5+1))
        plot(x,u,'.',markersize=5)
        xx = arange(-1,1.01,.01); uu = polyval(polyfit(x,u,N),xx)
        plot(xx,uu); xlim(-1,1); ylim(-.5,.5); axis('off')
        text(-.4,.4,'eig'+str(j+1)+'='+str('%.13f' % (lam[j]*4/pi**2))+'*pi^2/4'
) #typo in p15.m
        text( .7,.4,str('%.1f' % (4*N/(pi*(j+1))))+' ppw')
savefig('p15.png')
show()
```

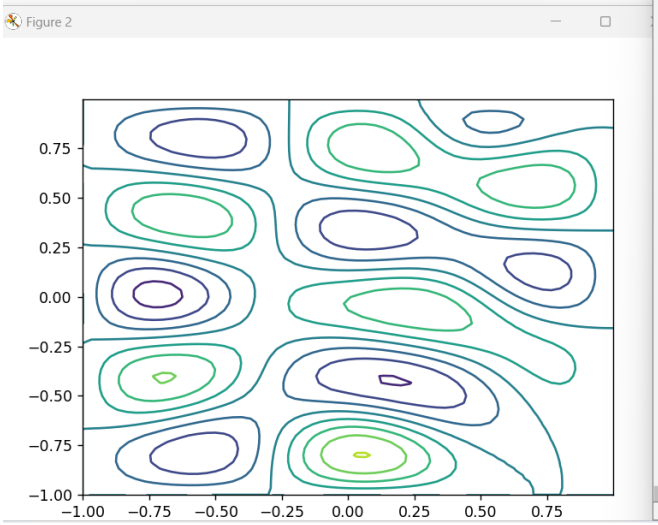







```
from pylab import *
from mpl_toolkits.mplot3d import axes3d, Axes3D
import matplotlib.pyplot as plt
from time  import time

def cheb(N):
        if N==0:
                D = 0.; x = 1.
        else:
                n = np.arange(0,N+1)
                x = cos(pi*n/N).reshape(N+1,1)
                c = (hstack(( [2.], ones(N-1), [2.]))*(-1)**n).reshape(N+1,1)
                X = tile(x,(1,N+1))
                dX = X - X.T
                D = dot(c,1./c.T)/(dX+eye(N+1))
                D -= diag(sum(D.T,axis=0))
        return D, x.reshape(N+1)


N = 32
D,x = cheb(N); y = x
xx,yy = meshgrid(x[1:-1],y[1:-1])
Nm1 = N-1
xx = xx.T.reshape(Nm1*Nm1); yy = yy.T.reshape(Nm1*Nm1)
f = 10*sin(8*xx*(yy-1))
D2 = dot(D,D); D2 = D2[1:-1,1:-1]; I = eye(Nm1)
L = kron(I,D2) + kron(D2,I)
figure(1); spy(L)
tic=time(); u = linalg.solve(L,f);
print(L.shape,'linear solve took',time()-tic,'secs')
uu = zeros((N+1,N+1)); uu[1:-1,1:-1] = u.reshape((N-1,N-1)).T
xx,yy = meshgrid(x,y)
value = uu[N//4,N//4]
fg = arange(-1.,1.01,.04); [xxx,yyy] = meshgrid(fg,fg)
f = interp2d(x,y,uu,kind='cubic'); uuu = f(fg,fg)
fig = plt.figure(figsize=plt.figaspect(0.5))
ax = fig.add_subplot(111, projection='3d')
ax.plot_surface(xxx, yyy, uuu, cstride=1,rstride=1,cmap='jet')
ax.azim = -138; ax.elev = 25
ax.set_xlabel('x'); ax.set_ylabel('y'); ax.set_zlabel('u')
ax.text(.4,-.3,-.3,'u(2^-1/2,2^-1/2) ='+str('%.11f' % value) )
plt.show()
```





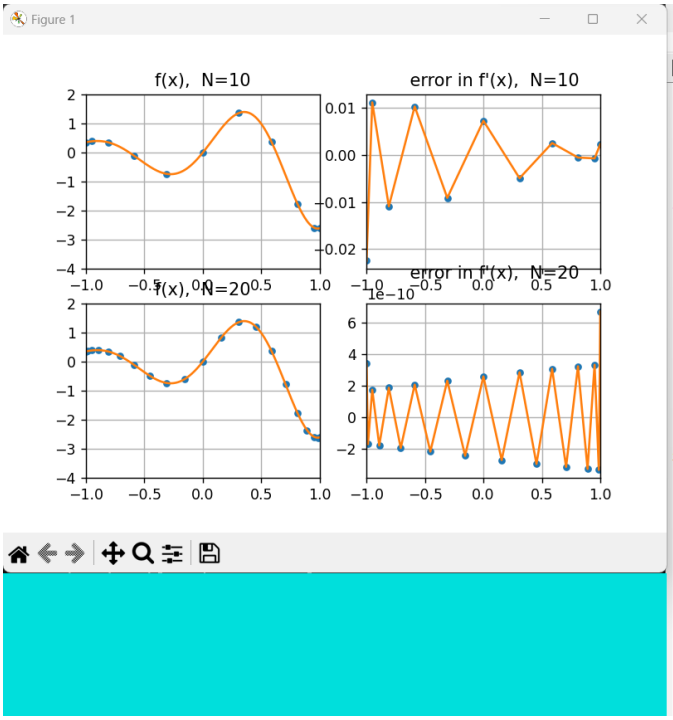
p17.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
# p17.py - Helmholtz eq. u_xx + u_yy + (k^2)u = f
#          on [-1,1]x[-1,1]    (compare p16.py)
#          Python translation 12/25/12
from numpy import *
from scipy.interpolate import interp2d
from pylab import *

def cheb(N):
        if N==0:
                D = 0.; x = 1.
        else:
                n = np.arange(0,N+1)
                x = cos(pi*n/N).reshape(N+1,1)
                c = (hstack(( [2.], ones(N-1), [2.]))*(-1)**n).reshape(N+1,1)
                X = tile(x,(1,N+1))
                dX = X - X.T
                D = dot(c,1./c.T)/(dX+eye(N+1))
                D -= diag(sum(D.T,axis=0))
        return D, x.reshape(N+1)

from mpl_toolkits.mplot3d import axes3d, Axes3D
import matplotlib.pyplot as plt

# Set up spectral grid and tensor product Helmholtz operator:
N = 24; D,x = cheb(N); y = x
xx,yy = meshgrid(x[1:-1],y[1:-1])
Nm1 = N-1; xx = xx.T.reshape(Nm1*Nm1); yy = yy.T.reshape(Nm1*Nm1)
f = exp(-10*((yy-1)**2+(xx-.5)**2));
D2 = dot(D,D); D2 = D2[1:-1,1:-1]; I = eye(Nm1)
k = 9.
L = kron(I,D2) + kron(D2,I) + k**2*eye(Nm1*Nm1)
# Solve for u, reshape to 2D grid, and plot:
u = linalg.solve(L,f)
uu = zeros((N+1,N+1)); uu[1:-1,1:-1] = u.reshape((N-1,N-1)).T
xx,yy = meshgrid(x,y)
fg = arange(-1.,1.001,.0333); [xxx,yyy] = meshgrid(fg,fg)
f = interp2d(x,y,uu,kind='cubic'); uuu = f(fg,fg)
fig = plt.figure(figsize=plt.figaspect(0.5))
ax = fig.add_subplot(111, projection='3d')
ax.plot_surface(xxx, yyy, uuu, cstride=1,rstride=1,cmap='jet')
ax.azim = -138; ax.elev = 25
ax.set_xlabel('x'); ax.set_ylabel('y'); ax.set_zlabel('u')
ax.text(.2,1,.022,'u(0,0) ='+str('%.11f' % uu[N//2,N//2]) )
figure(2);
```

-(Unix)--- **p17.py** Top L20 (Python ElDoc)

Wrote c:/Users/DENISE_2022/Desktop/les-der-spectral/p17.py

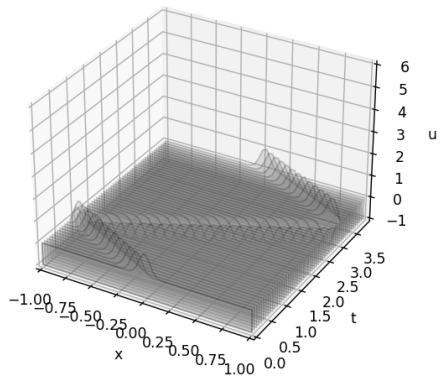


p18.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
# p18.py - Chebyshev differentiation via FFT (compare p11.py)
#          Python/NumPy translation 12/26/12
from numpy import *
from numpy.fft import fft,ifft
from pylab import *


def chebfft(v):
        N = len(v)-1;
        if N==0: return 0
        x = cos(arange(0,N+1)*pi/N)
        ii = arange(0,N); iir = arange(1-N,0); iii = array(ii,dtype=int)
        #v = v[:]
        V = hstack((v,v[N-1:0:-1])) # transform x -> theta
        U = real(fft(V))
        W = real(ifft(1j*hstack((ii,[0.],iir))*U))
        w = zeros(N+1)
        w[1:N] = -W[1:N]/sqrt(1-x[1:N]**2)     # transform theta -> x
        w[0] = sum(iii**2*U[iii])/N + .5*N*U[N]
        w[N] = sum((-1)**(iii+1)*ii**2*U[iii])/N + .5*(-1)**(N+1)*N*U[N]
        return w

xx = arange(-1,1.01,.01); ff = exp(xx)*sin(5*xx)
for N in [10, 20]:
        x = cos(pi*arange(0,N+1)/N); f = exp(x)*sin(5*x)
        subplot(2,2,2*(N==20)+1)
        plot(x,f,'.',markersize=8); grid()
        plot(xx,ff)
        xlim(-1,1); ylim(-4,2); title('f(x),  N='+str(N))
        error = chebfft(f) - exp(x)*(sin(5*x)+5*cos(5*x))
        subplot(2,2,2*(N==20)+2)
        plot(x,error,'.',markersize=8); grid()
        plot(x,error)
        xlim(-1,1); title("    error in f'(x),  N="+str(N))
show()
```

Figure 1

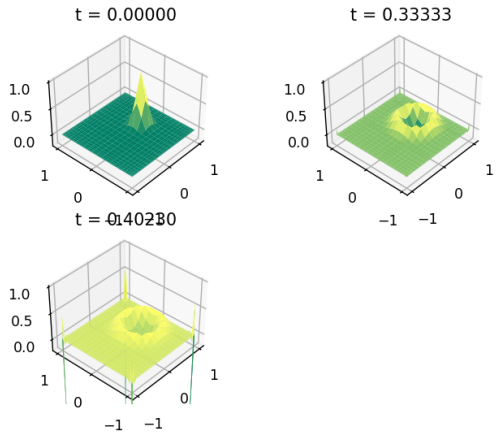


p19.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
from mpl_toolkits import mplot3d
from matplotlib.collections import PolyCollection

def chebfft(v):
        N = len(v)-1 ; if N==0: return 0
        x = cos(arange(0,N+1)*pi/N)
        ii = arange(0,N); iir = arange(1-N,0); iii = array(ii,dtype=int)
        V = hstack((v,v[N-1:0:-1])) # transform x -> theta
        U = real(fft(V)) ; W = real(ifft(1j*hstack((ii,[0.],iir))*U))
        w = zeros(N+1)
        w[1:N] = -W[1:N]/sqrt(1-x[1:N]**2)     # transform theta -> x
        w[0] = sum(iii**2*U[iii])/N + .5*N*U[N]
        w[N] = sum((-1)**(iii+1)*ii**2*U[iii])/N + .5*(-1)**(N+1)*N*U[N]
        return w

def waterfall(x,t,u,labels=['x','t','u'],slabthickness=0.5,zrange=[-1.,6.]):
        fig = plt.figure()
        ax = plt.axes(projection='3d')
        cc = lambda arg: matplotlib.colors.to_rgba(arg, alpha=0.7)
        xs = np.hstack(( x,x[-1],x[0] )) ; verts = [] ; zs = t
        baseline  = 0.-slabthickness
        for ti,z in enumerate(zs):
                ys = np.hstack(( u[ti,:],baseline,baseline ))
                verts.append(list(zip(xs, ys)))
        poly = PolyCollection(verts, edgecolors = 'black', facecolors = [cc('gra
'y')], alpha=.6) ; poly.set_alpha(0.2)
        ax.add_collection3d(poly, zs=zs, zdir='y')
        ax.set_xlabel(labels[0]) ; ax.set_xlim3d(min(xs),max(xs))
        ax.set_ylabel(labels[1]) ; ax.set_ylim3d(min(zs),max(zs))
        ax.set_zlabel(labels[2]) ; ax.set_zlim3d(zrange[0],zrange[1])

N = 80; x = cos(pi*arange(0,N+1)/N); dt = 8./N**2
v = exp(-200*x**2); vold = exp(-200*(x-dt)**2)
tmax = 4.; tplot = .075;
plotgap = int(round(tplot/dt)); dt = tplot/plotgap
nplots  = int(round(tmax/tplot))
plotdata = vstack(( v, zeros((nplots,N+1)) )); tdata = [0.]
for i in range(nplots):
        for n in range(plotgap):
                w = chebfft(chebfft(v)); w[0] = 0; w[N] = 0
                vnew = 2*v - vold + dt**2*w; vold = v.copy(); v = vnew
        plotdata[i+1,:] = v; tdata.append(dt*i*plotgap)
waterfall(x,tdata,plotdata,slabthickness=1.)
plt.show()
```

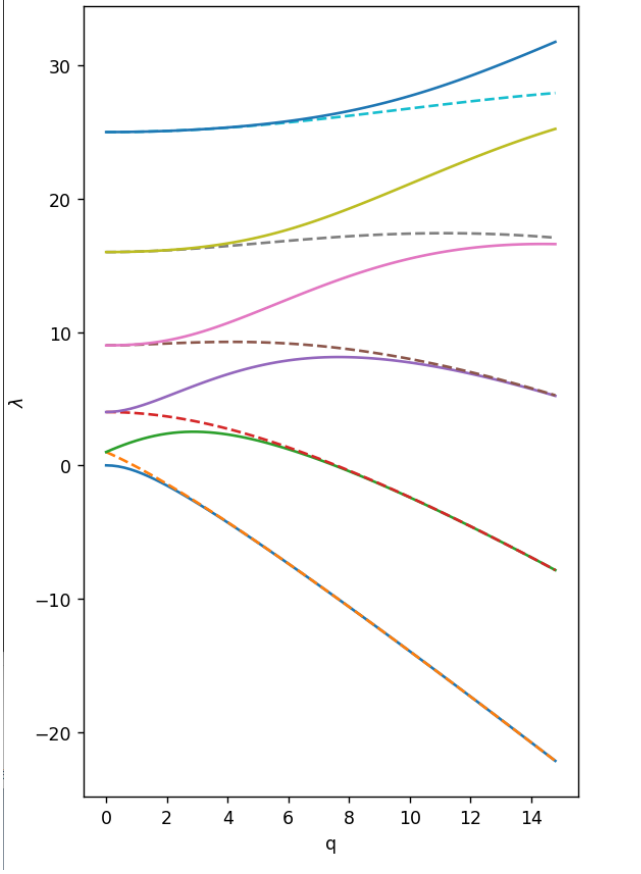
Figure 1



p20u.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
set_printoptions(precision=4,linewidth=200)
N = 24; x = cos(pi*arange(0,N+1)/N); y = x; dt = 6.6/N**2
[xx,yy] = meshgrid(x,y)
plotgap = int(round(1./3./dt)); dt = 1./3./plotgap
vv = exp(-40*((xx-.4)**2 + yy**2))
vvold = vv.copy(); vvnew=0*vv
[ay,ax] = meshgrid([.56, .06],[.1, .55])
for n in array(range(3*plotgap+1)):
        t = n*dt
        if (n+.5)%plotgap < 1:      # plots at multiples of t=1/3
                iplot = n/plotgap
                ax = subplot(2,2,int(iplot+1),projection='3d')
                xxxrange = arange(-1,1.01,.05)
                [xxx,yyy] = meshgrid(xxxrange,xxxrange)
                f = interp2d(x,y,vv,kind='cubic');
                vvv = f(xxxrange,xxxrange)
                ax.plot_surface(xx, yy, vv, cstride=1,rstride=1,cmap='summer')
                title('t = '+str('%.5f' % t)); ax.azim = -138; ax.elev = 38; ax.s
'set_zlim3d(-0.2,1)
        uxx = zeros((N+1,N+1)); uyy = zeros_like(uxx)
        ii = range(1,N); iip = range(0,N); iim = range(1-N,0)
        for i in range(1,N):
                v = vv[i,:]; V = hstack(( v, v[N-1:0:-1] ))
                U = real(fft(V))
                W1 = real(ifft(1j*hstack((iip,[0.],iim))*U)) # diff wrt theta
                W2 = real(ifft(-hstack(( range(0,N+1), iim ))**2.*U))
                uxx[i,ii] = W2[ii]/(1-x[ii]**2) - x[ii]* \
                                W1[ii]/(1-x[ii]**2)**(3./2.)
        for j in range(1,N):
                v = vv[:,j]; V = hstack(( v, v[N-1:0:-1] ))
                U = real(fft(V))
                W1 = real(ifft(1j*hstack((iip,[0.],iim))*U)) # diff wrt theta
                W2 = real(ifft(-hstack(( range(0,N+1), iim ))**2.*U))    # diff^
'2 wrt theta
                uyy[ii,j] = W2[ii]/(1-y[ii]**2) - y[ii]* \
                                W1[ii]/(1-y[ii]**2)**(3./2.)
        vvnew = 2*vv - vvold + dt**2*(uxx+uyy)
        vvold = vv.copy(); vv = vvnew
        if max(abs(vv.ravel()  ))>2: break   # ravel is just a new view
ax = subplot(2,2,int(iplot+2),projection='3d')
ax.plot_surface(xx, yy, vv, cstride=1,rstride=1,cmap='summer')
title('t = '+str('%.5f' % t)); ax.azim = -138; ax.elev = 38; ax.set_zlim3d(-0.2,
'1)
show()
```

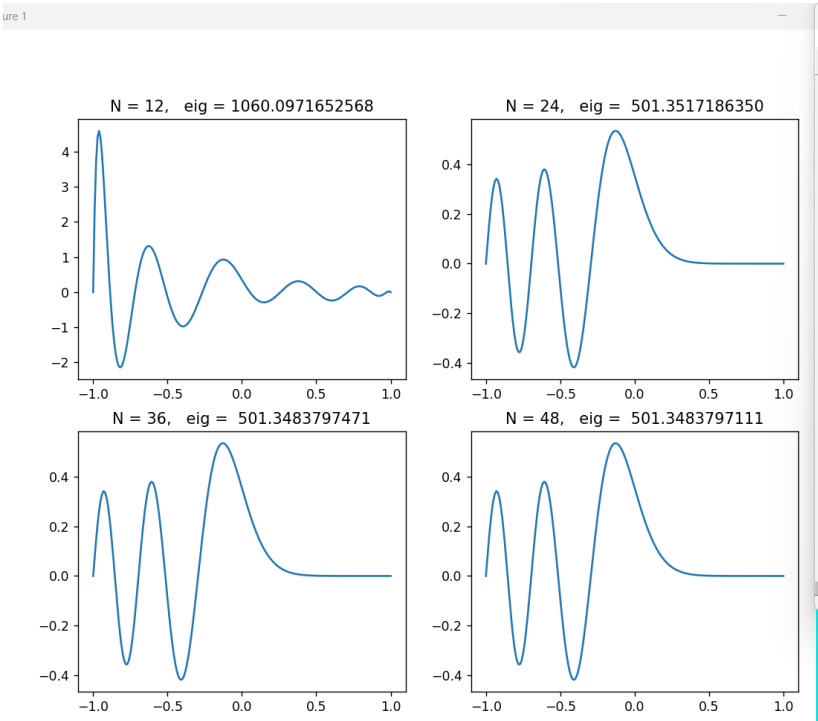


p21.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
from numpy import pi,arange,sin,cos,zeros,diag,sort,real
from scipy.linalg import toeplitz
from numpy.linalg import eig
from itertools import cycle
from matplotlib.pyplot import figure,plot,xlabel,ylabel

N = 42; h = 2.0*pi/N; x = h*arange(1,N+1)
col = zeros(N)
col[0] = -pi**2/(3.0*h**2) - 1.0/6.0
col[1:] = -0.5*(-1.0)**arange(1,N)/sin(0.5*h*arange(1,N))**2
D2 = toeplitz(col)

ne = 11 # number of eigenvalues to plot
qq = arange(0.0, 15.0, 0.2)
data= zeros((len(qq),ne))
i = 0
for q in qq:
    evals,evecs = eig(-D2 + 2.0*q*diag(cos(2.0*x)))
    e = real(sort(evals))
    data[i,:] = e[0:ne]
    i = i + 1

figure(figsize=(5,10))
lines=cycle(["-","--"])
for i in range(ne):
    plot(qq,data[:,i],next(lines))
xlabel("q")
ylabel("$\lambda$");
plt.show()
```

-\--- **p21.py** All L17 (Python ElDoc)

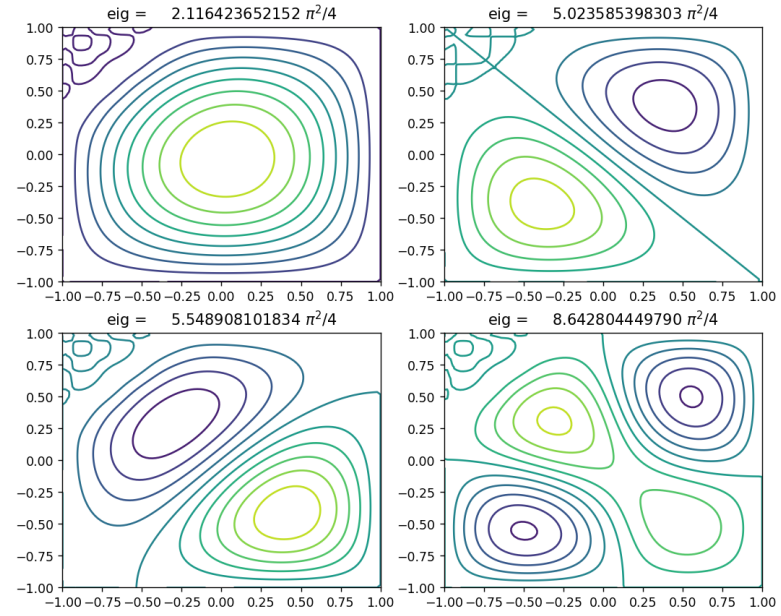


p22.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import *
from scipy.linalg import eig
from scipy.special import airy
from matplotlib.pyplot import figure,subplot,plot,title

def cheb(N):
        if N==0:
                D = 0.; x = 1.
        else:
                n = np.arange(0,N+1)
                x = cos(pi*n/N).reshape(N+1,1)
                c = (hstack(( [2.], ones(N-1),
                              [2.]))*(-1)**n).reshape(N+1,1)
                X = tile(x,(1,N+1))
                dX = X - X.T
                D = dot(c,1./c.T)/(dX+eye(N+1))
                D -= diag(sum(D.T,axis=0))
        return D, x.reshape(N+1)

figure(figsize=(10,8))
for N in range(12,60,12):
    D,x = cheb(N); D2 = dot(D,D); D2 = D2[1:N,1:N]
    Lam,V = eig(D2,diag(x[1:N]))
    Lam = real(Lam); ii = where(Lam>0)[0]
    V = real(V[:,ii]); Lam = Lam[ii]
    ii = argsort(Lam); ii=ii[4]; Lam=Lam[ii]
    v = zeros(N+1); v[1:N] = V[:,ii]; v = v/v[N//2]*airy(0.0)[0]
    xx = linspace(-1.0,1.0,200); vv = polyval(polyfit(x,v,N),xx);
    subplot(2,2,N//12); plot(xx,vv)
    title("N = %d,   eig = %15.10f"%(N,Lam));
plt.show()
```

-**- **p22.py** All L15 (Python ElDoc)

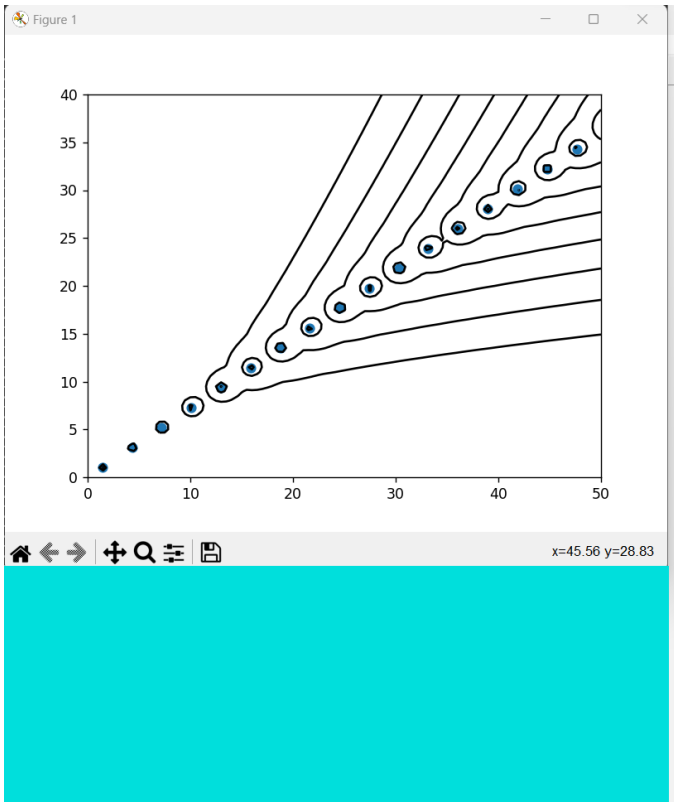


p23.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import *
from matplotlib.pyplot import figure,subplot,plot,title,contour
from scipy.linalg import eig,norm
from scipy.interpolate import interp2d

def cheb(N):
        if N==0:
                D = 0.; x = 1.
        else:
                n = np.arange(0,N+1)
                x = cos(pi*n/N).reshape(N+1,1)
                c = (hstack(( [2.], ones(N-1),
                              [2.]))*(-1)**n).reshape(N+1,1)
                X = tile(x,(1,N+1))
                dX = X - X.T
                D = dot(c,1./c.T)/(dX+eye(N+1))
                D -= diag(sum(D.T,axis=0))
        return D, x.reshape(N+1)

# Set up tensor product Laplacian and compute 4 eigenmodes
N = 16; D,x = cheb(N); y = x;
xx,yy = meshgrid(x[1:N],y[1:N])
xx = reshape(xx,(N-1)**2)
yy = reshape(yy,(N-1)**2)
D2 = dot(D,D); D2 = D2[1:N,1:N]; I = eye(N-1)
L = -kron(I,D2) - kron(D2,I)
L = L + diag(exp(20*(yy-xx-1)))
D,V = eig(L); D = real(D); V = real(V)
ii = argsort(D); ii = ii[0:4]; D = D[ii]; V = V[:,ii]
# Reshape them to 2D grid, interpolate to finer grid, and plot
fine = linspace(-1.0,1.0,100,True);
uu = zeros((N+1,N+1));
figure(figsize=(10,10))
for i in range(4):
    uu[1:N,1:N] = reshape(V[:,i],(N-1,N-1))
    uu = uu/norm(uu,inf)
    f = interp2d(x,y,uu,kind='cubic')
    uuu = f(fine,fine)
    subplot(2,2,i+1)
    contour(fine,fine,uuu,10)
    title("eig = %18.12f $\pi^2/4$"%(D[i]/(pi**2/4)))
plt.show()
```

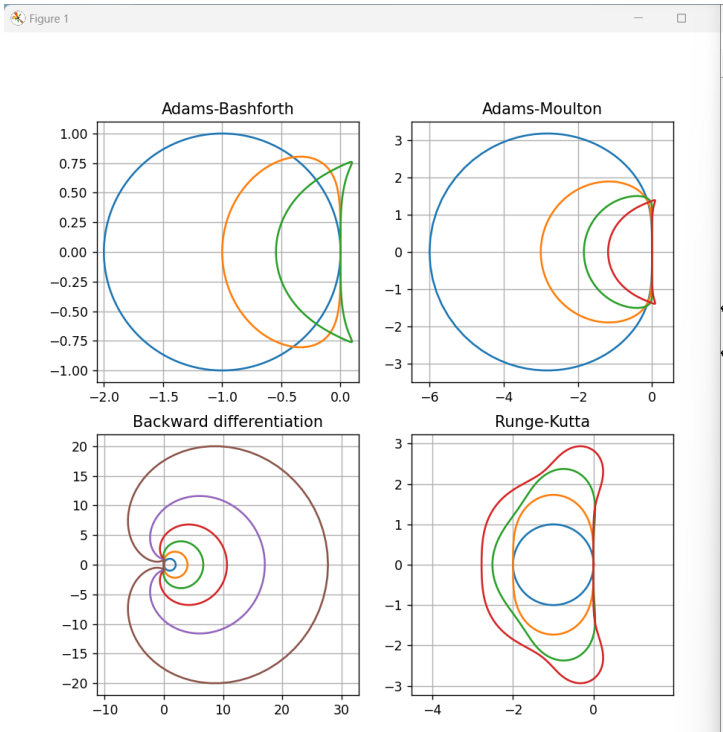
-**- **p23.py** Top L15 (Python ElDoc)



p24.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import *
from scipy.linalg import solve,eig,svd,svdvals
from matplotlib.pyplot import figure,plot,title,axis,contour

def cheb(N):
        if N==0:
                D = 0.; x = 1.
        else:
                n = np.arange(0,N+1)
                x = cos(pi*n/N).reshape(N+1,1)
                c = (hstack(( [2.], ones(N-1), [2.]))*(-1)**n).reshape(N+1,1)
                X = tile(x,(1,N+1))
                dX = X - X.T
                D = dot(c,1./c.T)/(dX+eye(N+1))
                D -= diag(sum(D.T,axis=0))
        return D, x.reshape(N+1)

N = 70; D, x = cheb(N); x = x[1:N];
L = 6.0; x = L*x; D = D/L;
A = -dot(D,D);
A = A[1:N,1:N] + (1+3j)*diag(x**2);
lam, v = eig(A)
fig = figure()
plot(real(lam),imag(lam),"o")
axis([0, 50, 0, 40])

h = 0.5 #Smaller the value, finer the plot
x = arange(0,50+h,h); y = arange(0,40+h,h); xx,yy = meshgrid(x,y);
zz = xx + 1j*yy;
I = eye(N-1); sigmin = zeros((len(y),len(x)))
for j in range(0,len(x)):
    for i in range(0,len(y)):
        sigmin[i,j] = min(svdvals(zz[i,j]*I - A));

levels = 10.0**arange(-4.5,0.0,0.5);
contour(x,y,sigmin,levels,colors = 'k');
plt.show()
```



p25.py - GNU Emacs at DESKTOP-4PROGGL

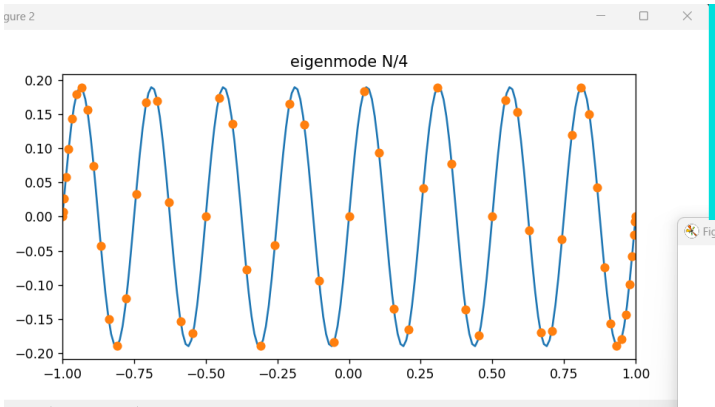
File Edit Options Buffers Tools Python Help

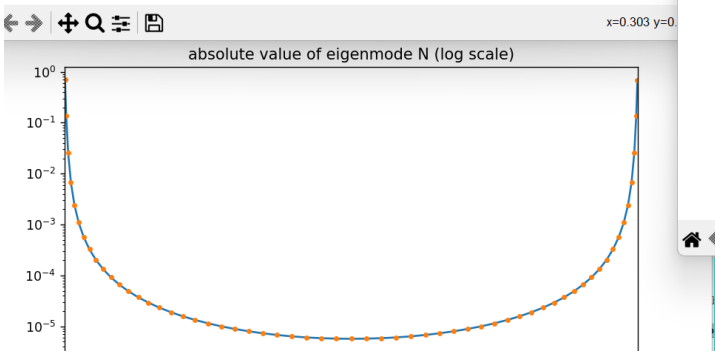
```
import matplotlib.pyplot as plt ; from matplotlib.pyplot import *
from numpy import pi,real,imag,zeros,exp,arange
figure(figsize=(8,8))

subplot(2,2,1)
z = exp(1j*pi*arange(0,201)/100); r = z - 1
s = 1; rr = r/s; plot(real(rr),imag(rr))
s = (3 - 1/z)/2; rr = r/s; plot(real(rr),imag(rr))
s = (23 - 16/z + 5/z**2)/12; rr = r/s; plot(real(rr),imag(rr))
axis('equal'); grid('on') ; title('Adams-Bashforth')

subplot(2,2,2)
s = (5*z + 8 - 1/z)/12; rr = r/s; plot(real(rr),imag(rr))
s = (9*z + 19 - 5/z + 1/z**2)/24; rr = r/s; plot(real(rr),imag(rr))
s = (251*z + 646 - 264/z + 106/z**2 - 19/z**3)/720; rr = r/s; plot(real(rr),imag(rr))
d = 1 - 1/z
s = 1 - d/2 - d**2/12 - d**3/24 - 19*d**4/720 - 3*d**5/160; dd = d/s; plot(real(dd),imag(dd))
axis('equal'); grid('on') ; title('Adams-Moulton')

subplot(2,2,3)
r = 0
for i in range(1,7):
    r = r + d**i/i; plot(real(r),imag(r))
axis('equal'); grid('on') ; title('Backward differentiation')

subplot(2,2,4)
w = 0; W = 1j*zeros(len(z)); W[0] = w;
for i in range(1,len(z)): w = w - (1+w-z[i]); W[i] = w
plot(real(W),imag(W))
w = 0; W = 1j*zeros(len(z)); W[0] = w;
for i in range(1,len(z)): w = w - (1+w+0.5*w**2-z[i]**2)/(1+w); W[i] = w
plot(real(W),imag(W))
w = 0; W = 1j*zeros(len(z)); W[0] = w;
for i in range(1,len(z)):
    w = w - (1+w+0.5*w**2+w**3/6-z[i]**3)/(1+w+0.5*w**2); W[i] = w
plot(real(W),imag(W))
w = 0; W = 1j*zeros(len(z)); W[0] = w;
for i in range(1,len(z)):
    w = w - (1+w+0.5*w**2+w**3/6+w**4/24-z[i]**4)/(1+w+w**2/2+w**3/6); W[i] = w
plot(real(W),imag(W))
axis('equal'); grid('on') ; title('Runge-Kutta');
plt.show()
```

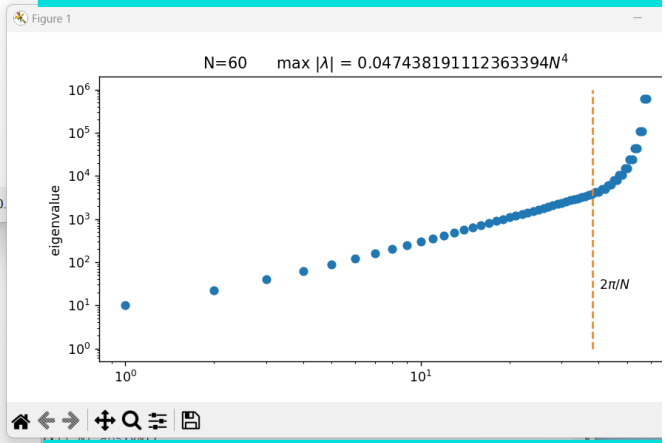
p26.py - GNU Emacs at DESKTOP-4PROGGL

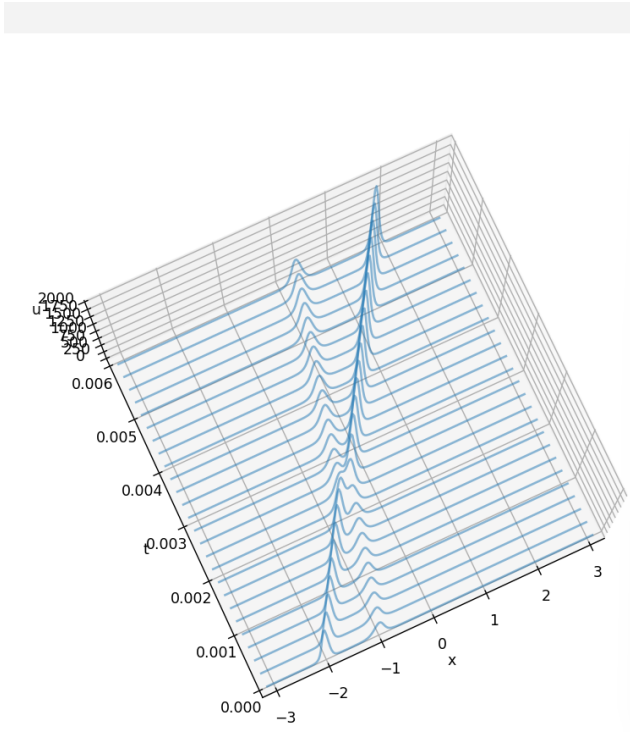
File Edit Options Buffers Tools Python Help

```
def cheb(N):
        if N==0:
                D = 0.; x = 1.
        else:
                n = np.arange(0,N+1)
                x = cos(pi*n/N).reshape(N+1,1)
                c = (hstack(( [2.], ones(N-1), [2.]))*(-1)**n).reshape(N+1,1)
                X = tile(x,(1,N+1))
                dX = X - X.T
                D = dot(c,1./c.T)/(dX+eye(N+1))
                D -= diag(sum(D.T,axis=0))
        return D, x.reshape(N+1)

N = 60; D, x = cheb(N); D2 = dot(D,D); D2 = D2[1:N,1:N]
Lam, V = eig(D2)
ii = argsort(-Lam); e = Lam[ii]; V = V[:,ii]

# Plot eigenvalues
figure(figsize=(8,4))
loglog(-e,'o')
semilogy(2*N/pi*array([1,1]),array([1,1e6]),'--')
ylabel('eigenvalue')
title('N='+str(N)+'      max |$\lambda$| = '+str(max(-e)/N**4)+'$N^4$')
text(2.1*N/pi,24,'$2\pi/N$')

# Plot eigenmode N/4 (physical)
figure(figsize=(8,4))
vN4 = zeros(N+1)
vN4[1:N] = V[:,N//4];
xx = arange(-1.0,1.01,0.01)
vv = polyval(polyfit(x,vN4,N),xx)
plot(xx,vv,'-')
plot(x,vN4,'o')
xlim((-1.0,1.0))
title('eigenmode N/4')

# Plot eigenmode N (nonphysical)
figure(figsize=(8,4))
vN = V[:,N-2]
semilogy(x[1:N],abs(vN))
plot(x[1:N],abs(vN),'.')
xlim((-1.0,1.0))
title('absolute value of eigenmode N (log scale)');
plt.show()
```







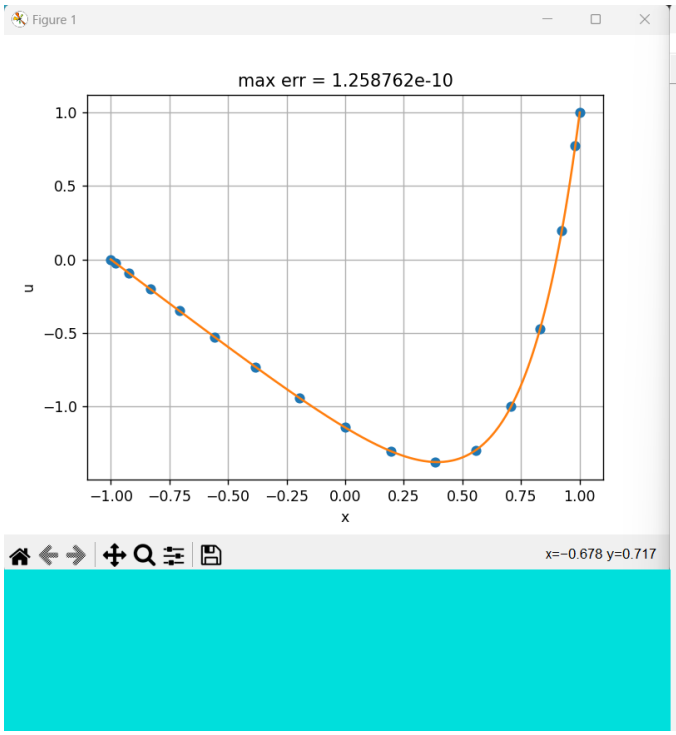


p27.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
from mpl_toolkits.mplot3d import Axes3D
from matplotlib.collections import LineCollection
from numpy import pi,cosh,exp,round,zeros,arange,real
from numpy.fft import fft,ifft
from matplotlib.pyplot import figure

# Set up grid and differentiation matrix:
N = 256; dt = 0.4/N**2; x = (2*pi/N)*arange(-N/2,N/2);
A, B = 25.0, 16.0
u = 3*A**2/cosh(0.5*A*(x+2))**2 + 3*B**2/cosh(0.5*B*(x+1))**2
v = fft(u);
k = zeros(N); k[0:N//2] = arange(0,N/2); k[N//2+1:] = arange(-N/2+1,0,1)
ik3 = 1j*k**3

# Time-stepping by Runge-Kutta
tmax = 0.006; nplt = int(round((tmax/25)/dt))
nmax = int(round(tmax/dt))
udata = []; udata.append(list(zip(x, u)))
tdata = [0.0]
for n in range(1,nmax+1):
    t = n*dt; g = -0.5j*dt*k
    E = exp(dt*ik3/2); E2 = E**2
    a = g * fft(real(ifft( v          ))**2)
    b = g * fft(real(ifft( E*(v+a/2) ))**2)
    c = g * fft(real(ifft( E*v+b/2   ))**2)
    d = g * fft(real(ifft( E2*v+E*c  ))**2)
    v = E2*v + (E2*a + 2*E*(b+c) + d)/6
    if n%nplt == 0:
        u = real(ifft(v))
        udata.append(list(zip(x, u)))
        tdata.append(t);

fig = figure(figsize=(12,10))
```

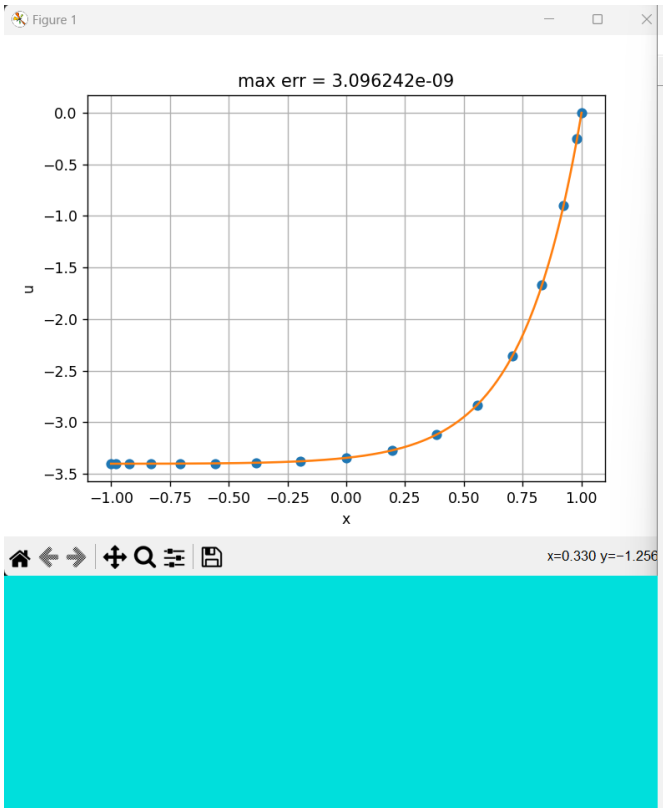
-\--- **p27.py** Top L1 (Python ElDoc)



p32.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import numpy as np
from numpy import *
from numpy.linalg import norm, solve
import matplotlib.pyplot as plt
from matplotlib.pyplot import title,plot,xlabel,ylabel,grid

def cheb(N):
        if N==0:
                D = 0.; x = 1.
        else:
                n = np.arange(0,N+1)
                x = cos(pi*n/N).reshape(N+1,1)
                c = (hstack(( [2.], ones(N-1), [2.]))*(-1)**n).reshape(N+1,1)
                X = tile(x,(1,N+1))
                dX = X - X.T
                D = dot(c,1./c.T)/(dX+eye(N+1))
                D -= diag(sum(D.T,axis=0))
        return D, x.reshape(N+1)

N = 16
D,x = cheb(N)
D2 = dot(D,D)
D2 = D2[1:N,1:N]
f = exp(4.0*x[1:N])
u = solve(D2,f)
s = zeros(N+1)
s[1:N] = u
s = s + (x + 1.0)/2.0 # Correction for bc

xx = linspace(-1.0,1.0,200)
uu = polyval(polyfit(x,s,N),xx)     # interpolate grid data
exact = (exp(4.0*xx) - sinh(4.0)*xx - cosh(4.0))/16.0 + (xx + 1.0)/2.0
maxerr = norm(uu-exact,inf)

title('max err = %e' % maxerr)
plot(x,s,'o',xx,exact)
xlabel('x'); ylabel('u'); grid(True);
plt.show()
```



p33.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import numpy as np
from numpy import *
from numpy.linalg import norm
from scipy.linalg import solve
import matplotlib.pyplot as plt
from matplotlib.pyplot import *

def cheb(N):
        if N==0:
                D = 0.; x = 1.
        else:
                n = np.arange(0,N+1)
                x = cos(pi*n/N).reshape(N+1,1)
                c = (hstack(( [2.], ones(N-1), [2.]))*(-1)**n).reshape(N+1,1)
                X = tile(x,(1,N+1))
                dX = X - X.T
                D = dot(c,1./c.T)/(dX+eye(N+1))
                D -= diag(sum(D.T,axis=0))
        return D, x.reshape(N+1)

N = 16
# Build matrix
D,x = cheb(N)
D2 = dot(D,D)
D2[N,:] = D[N,:] # Last eqn has neumann bc
D2 = D2[1:N+1,1:N+1]
# RHS
f = zeros(N)
f[0:-1] = exp(4.0*x[1:N])
# Solve
u = solve(D2,f)
s = zeros(N+1)
s[1:N+1] = u
# Compute error
xx = linspace(-1.0,1.0,200)
uu = polyval(polyfit(x,s,N),xx)     # interpolate grid data
exact = (exp(4.0*xx) - 4.0*exp(-4.0)*(xx-1.0) - exp(4.0))/16.0
maxerr = norm(uu-exact,inf)
title('max err = %e' % maxerr)
plot(x,s,'o',xx,exact)
xlabel('x'); ylabel('u'); grid(True);
plt.show()
```

Indices concordants et état des lieux (Denise Vella-Chemla, juin 2023)

Pour mémoire, il nous faut poster ici les indices concordants qui fixent la ligne à suivre pour la suite du travail.

D'abord, longtemps, on avait aimé une fonction qui trouvait les nombres premiers par des annulations de sommes de sommes de cosinus. On avait essayé de voir cette fonction comme une onde, de calculer par programme sa transformée de Fourier, et ça avait donné ce genre de programmes et copies d'écrans de résultats ci-dessous (voir Fig. 1 et 2).

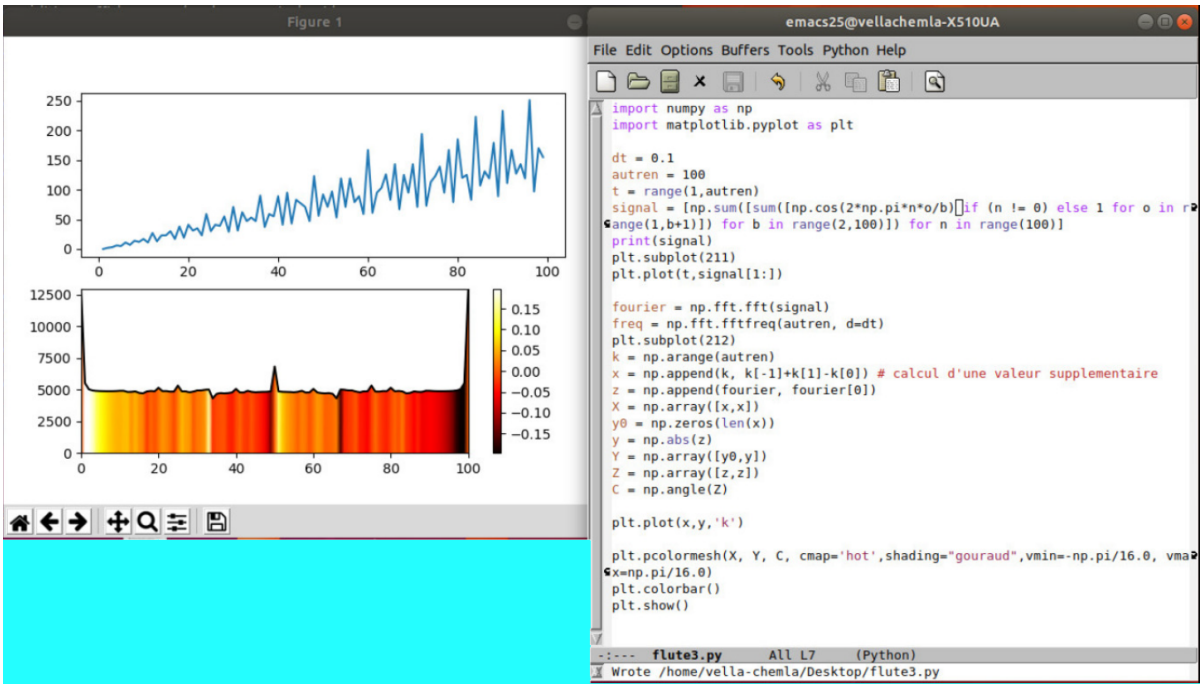


FIG. 1 : fonction qui voit les nombres premiers comme annulant une somme de somme de cosinus et transformée de Fourier de cette fonction si on la considère comme une sorte de signal.

Récemment, on a programmé des histogrammes (voir Fig. 3) qui comptent les décompositions de Goldbach des nombres en les ramenant toutes dans l'intervalle $[0, 1]$, et en associant à la décomposition de Goldbach $19 + 79$ de 98 les deux rationnels $\frac{19}{98}$ et $\frac{79}{98}$. L'histogramme correspondant a la même forme, il montre que les décompositions de Goldbach "éloignées du centre" (i.e. faisant intervenir un tout petit premier et un nombre premier proche de n pour décomposer n en une somme de deux nombres premiers), sont plus nombreuses que les autres. Il y a cependant une petite pointe au centre de l'histogramme qui compte les décompositions de Goldbach triviales des doubles de nombres premiers.

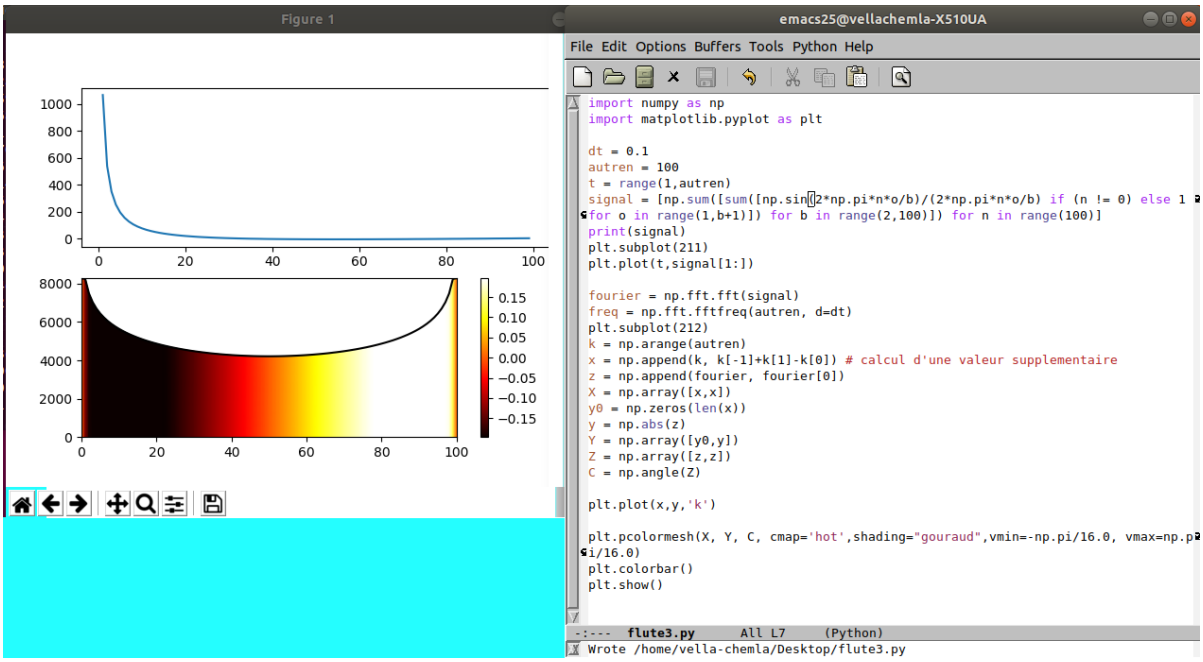


FIG. 2 : similaire à la FIG. 1 mais avec une somme de somme de sinus.

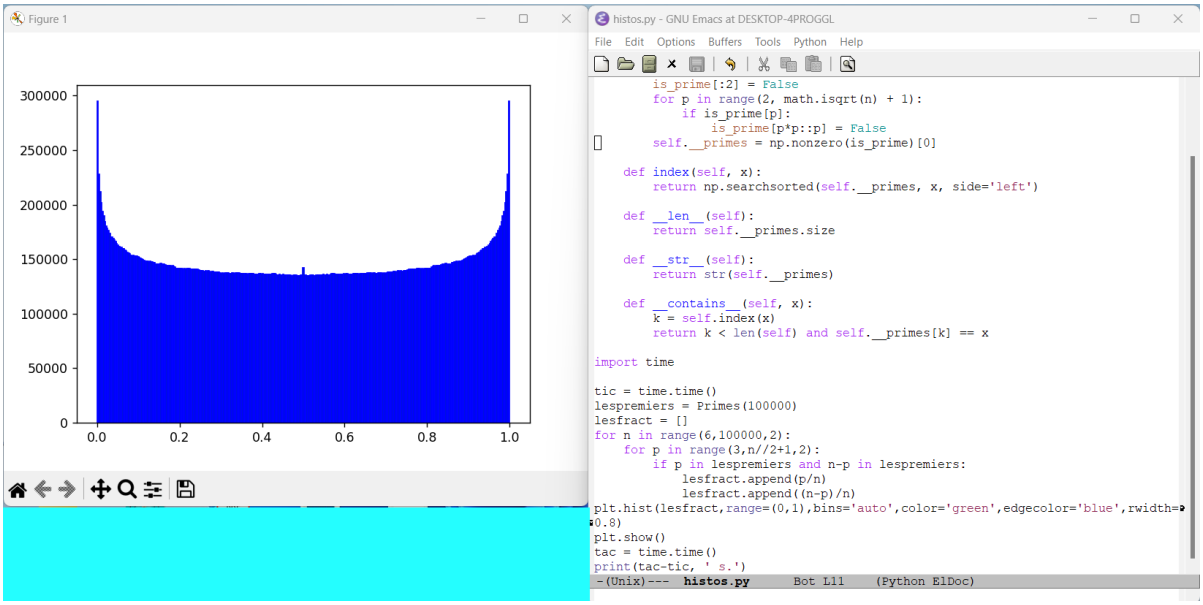


FIG. 3 : Histogrammes des décomposants de Goldbach,
tous “quotientés rationnellement” sur l'intervalle $[0, 1]$.

Or il s'avère qu'en revenant aux fonctions sphéroïdales prolates, notamment en parcourant à nouveau le livre de Osipov, Rokhlin et Xiao[1], on retrouve à la page 221 une figure qui ressemble à nos figures 2 et 3.

[1] *Prolate spheroidal wave functions of order zero, Mathematical tools for bandlimited approximation*, A. Osipov, V. Rokhlin, H. Xiao, Springer, Applied mathematical Sciences, AMS, vol. 187, 2013.

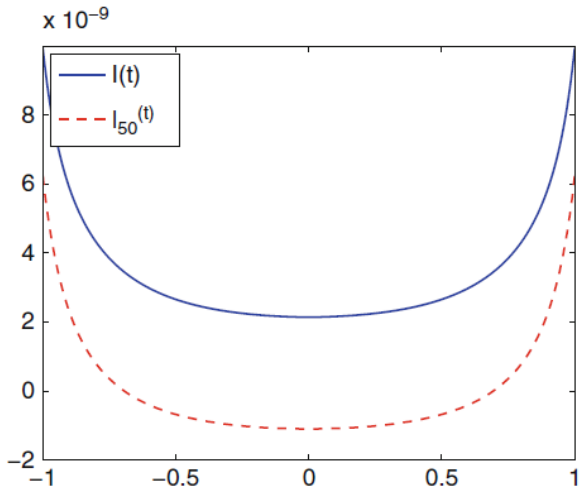


Figure 6.5: Illustration of Theorem 6.31 with $c = 100$, $n = 80$. $|\lambda_n| =$ 0.58925E-07

FIG. 4 : page 221 du livre sur les fonctions d'onde sphéroïdales prolates d'Osipov, Rokhlin et Xiao, pour illustrer un théorème de leur ouvrage.

Même si les manières dont ont été obtenus ces graphiques n'ont strictement rien à voir, cela conforte l'idée que les nombres premiers et les valeurs propres de fonctions sphéroïdales prolates ont des comportements similaires.

D'autre part, lors de tentatives totalement hasardeuses, on avait posté ce "Jeu avec la fonction zeta" sur notre premier blog[2].

On avait noté : "C'est marrant ce que l'on obtient lorsqu'on prend les carrés des parties réelles des zéros de zêta[3], et qu'on divise ces différences par $e^{2\pi}$.

Voici le résultat du programme :

[2]un blog anciennement Google+, mais Google avait brutalement fermé tous les blogs Google+, et ce blog se trouve maintenant à l'adresse https://milliardsdautres.blogspot.com. On avait posté le jeu avec les zéros de zeta le 21.2.2018 ; l'article en question se trouve à cette adresse : https://milliardsdautres.blogspot.com/2019/10/jeu-avec-la-fonction-zeta.html.

[3]Là, en calculant à nouveau, je réalise que pour obtenir les résultats fournis, il ne fallait pas soustraire le carré du premier zéro, contrairement à ce qui est indiqué.

$\zeta_1 = 14.1347$ `de carré` 199.79 `et qu'on divise par` $e^{2\pi} \to 0.373097.$
$\zeta_2 = 21.022 \to 441.926 \to 0.825272$
$\zeta_3 = 25.0109 \to 625.543 \to 1.16817$
$\zeta_4 = 30.4249 \to 925.673 \to 1.72864$
$\zeta_5 = 32.9351 \to 1084.72 \to 2.02565$
$\zeta_6 = 37.5862 \to 1412.72 \to 2.63818$
$\zeta_7 = 40.9187 \to 1674.34 \to 3.12674$
$\zeta_8 = 43.3271 \to 1877.24 \to 3.50563$
$\zeta_9 = 48.0052 \to 2304.49 \to 4.30351$
$\zeta_{10} = 49.7738 \to 2477.43 \to 4.62647$
$\zeta_{11} = 52.9703 \to 2805.85 \to 5.23977$
$\zeta_{12} = 56.4462 \to 3186.18 \to 5.95001$
$\zeta_{13} = 59.347 \to 3522.07 \to 6.57727$
$\zeta_{14} = 60.8318 \to 3700.51 \to 6.91048$
$\zeta_{15} = 65.1125 \to 4239.64 \to 7.91729$
$\zeta_{16} = 67.0798 \to 4499.7 \to 8.40293$
$\zeta_{17} = 69.5464 \to 4836.7 \to 9.03226$
$\zeta_{18} = 72.0672 \to 5193.68 \to 9.69889$
$\zeta_{19} = 75.7047 \to 5731.2 \to 10.7027$
$\zeta_{20} = 77.1448 \to 5951.33 \to 11.1138$
$\zeta_{21} = 79.3374 \to 6294.42 \to 11.7545$
$\zeta_{22} = 82.9104 \to 6874.13 \to 12.837$
$\zeta_{23} = 84.7355 \to 7180.1 \to 13.4084$
$\zeta_{24} = 87.4253 \to 7643.18 \to 14.2732$
$\zeta_{25} = 88.8091 \to 7887.06 \to 14.7286.''$

Et ça continue comme ça, un peu un nombre de plus tous les 2 nombres environ, et ça, très loin[4]).

Un autre jeu pour lequel on obtient, un peu de la même façon, cette augmentation de 1 environ un coup sur deux, au niveau de la partie imaginaire :

Il s'agit là de mener cette nouvelle expérience marrante ainsi : on prend les parties imaginaires des zéros de zêta et on les divise par $\frac{\pi^2}{4}$.

[4]Enfin assez loin, face à l'infini... enfin, cacahuètes, quoi !

$1 \to 5.72859$	$21 \to 32.1542$	$41 \to 50.3594$	$61 \to 67.0896$	$81 \to 82.0676$	$101 \to 96.3645$
$2 \to 8.51991$	$22 \to 33.6023$	$42 \to 51.6806$	$62 \to 67.7573$	$82 \to 82.755$	$102 \to 97.0882$
$3 \to 10.1365$	$23 \to 34.342$	$43 \to 52.5163$	$63 \to 68.5314$	$83 \to 83.2433$	$103 \to 97.6935$
$4 \to 12.3307$	$24 \to 35.4321$	$44 \to 53.1278$	$64 \to 68.8627$	$84 \to 84.2612$	$104 \to 98.4126$
$5 \to 13.3481$	$25 \to 35.993$	$45 \to 54.1046$	$65 \to 70.281$	$85 \to 84.9382$	$105 \to 98.9182$
$6 \to 15.2331$	$26 \to 37.4856$	$46 \to 54.6148$	$66 \to 70.8252$	$86 \to 85.7951$	$106 \to 100.161$
$7 \to 16.5837$	$27 \to 38.3607$	$47 \to 55.9763$	$67 \to 71.509$	$87 \to 86.4667$	$107 \to 100.552$
$8 \to 17.5598$	$28 \to 38.8549$	$48 \to 56.633$	$68 \to 72.2936$	$88 \to 86.9526$	$108 \to 101.148$
$9 \to 19.4558$	$29 \to 40.0548$	$49 \to 57.1953$	$69 \to 72.9174$	$89 \to 87.6102$	$109 \to 101.733$
$10 \to 20.1726$	$30 \to 41.0626$	$50 \to 58.001$	$70 \to 73.8457$	$90 \to 88.7848$	$110 \to 102.565$
$11 \to 21.4681$	$31 \to 42.0384$	$51 \to 59.172$	$71 \to 74.9268$	$91 \to 89.4524$	$111 \to 103.472$
$12 \to 22.8768$	$32 \to 42.7359$	$52 \to 59.7482$	$72 \to 75.2204$	$92 \to 89.7425$	$112 \to 103.907$
$13 \to 24.0525$	$33 \to 43.4338$	$53 \to 60.8144$	$73 \to 75.881$	$93 \to 90.7866$	
$14 \to 24.6542$	$34 \to 44.9986$	$54 \to 61.1677$	$74 \to 76.7675$	$94 \to 91.1823$	
$15 \to 26.3891$	$35 \to 45.3411$	$55 \to 62.0186$	$75 \to 77.8255$	$95 \to 92.1704$	
$16 \to 27.1864$	$36 \to 46.3322$	$56 \to 63.2702$	$76 \to 78.2523$	$96 \to 92.947$	
$17 \to 28.1861$	$37 \to 47.1049$	$57 \to 63.8719$	$77 \to 79.1381$	$97 \to 93.7222$	
$18 \to 29.2077$	$38 \to 48.1441$	$58 \to 64.3795$	$78 \to 79.791$	$98 \to 94.0209$	
$19 \to 30.682$	$39 \to 49.1895$	$59 \to 65.3274$	$79 \to 80.2526$	$99 \to 94.7124$	
$20 \to 31.2656$	$40 \to 49.8285$	$60 \to 66.0739$	$80 \to 81.5695$	$100 \to 95.8597$	

Et ces deux expériences qui ont pour résultats des nombres qui “sautent à peu près” de 1 en 1 sont à mettre en regard des fonctions sphéroïdales prolates : on voit sur les figures 2 et 3 de l’article d’Estelle Sonnenblick et David Slepian que de tels écarts d’à peu près 1 ont lieu sur l’axe des abscisses par exemple entre les courbes successives.

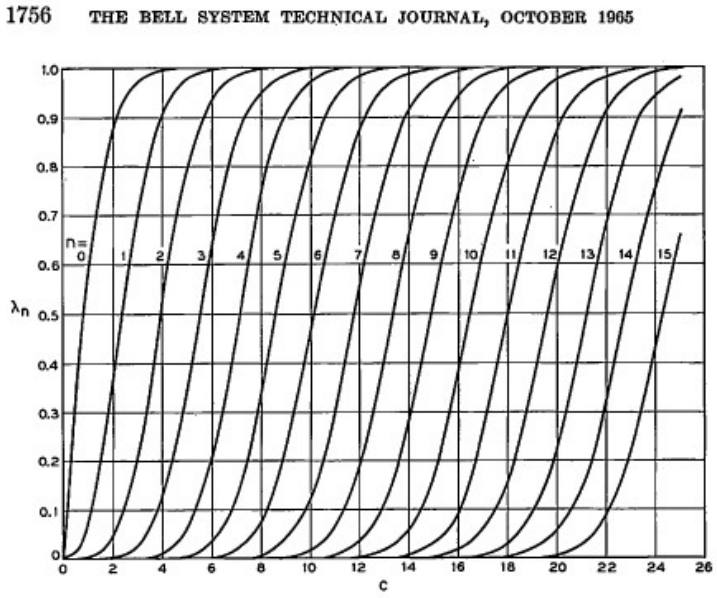


Fig. 4 : Fig. 2 de l’article de Estelle Sonnenblick et David Slepian

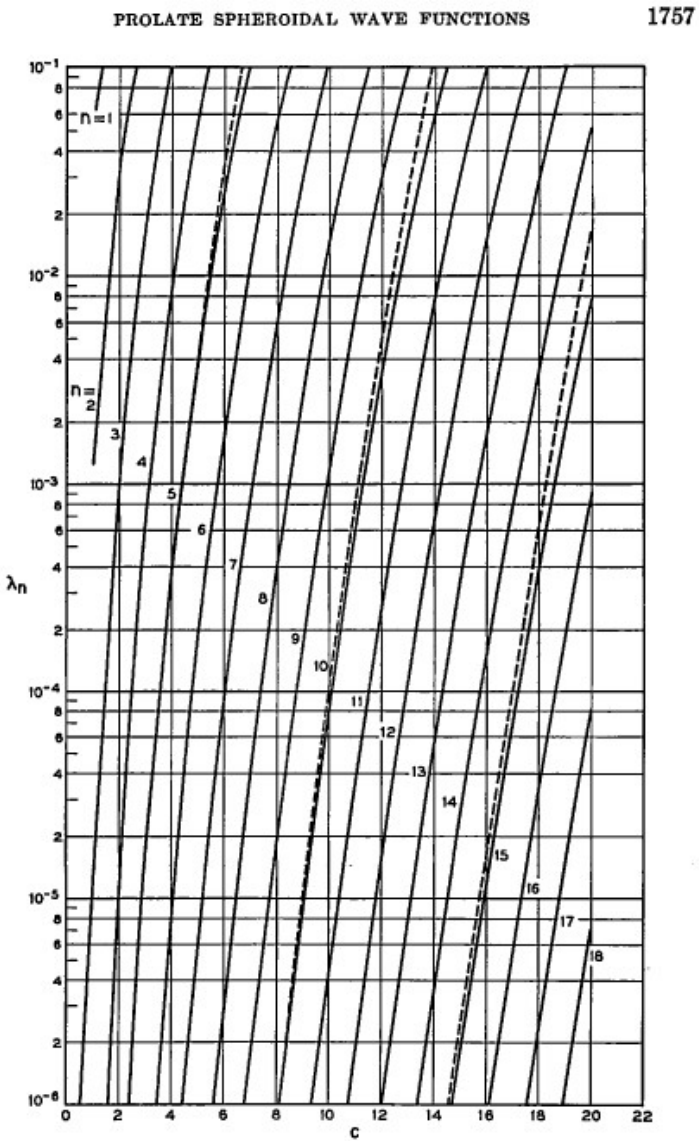


FIG. 5 : Fig. 3 de l'article de Estelle Sonnenblick et David Slepian

On note ici pour mémoire, qu'il nous faudrait comprendre, les 3 extraits suivants d'articles d'Alain Connes, en lien avec les fonctions sphéroïdales prolates, ou bien à propos du spectre de l'ensemble des nombres premiers :

- un extrait d'un article fournissant l'opérateur qui aurait $\mathcal{P}$, les nombres premiers, comme valeurs propres lien 1 ;
- deux extraits de deux articles traitant de fonctions sphéroïdales prolates : lien 2 et lien 3.

On colle ici pour mémoire un graphique des fonctions de projections sur l'ellipsoïde

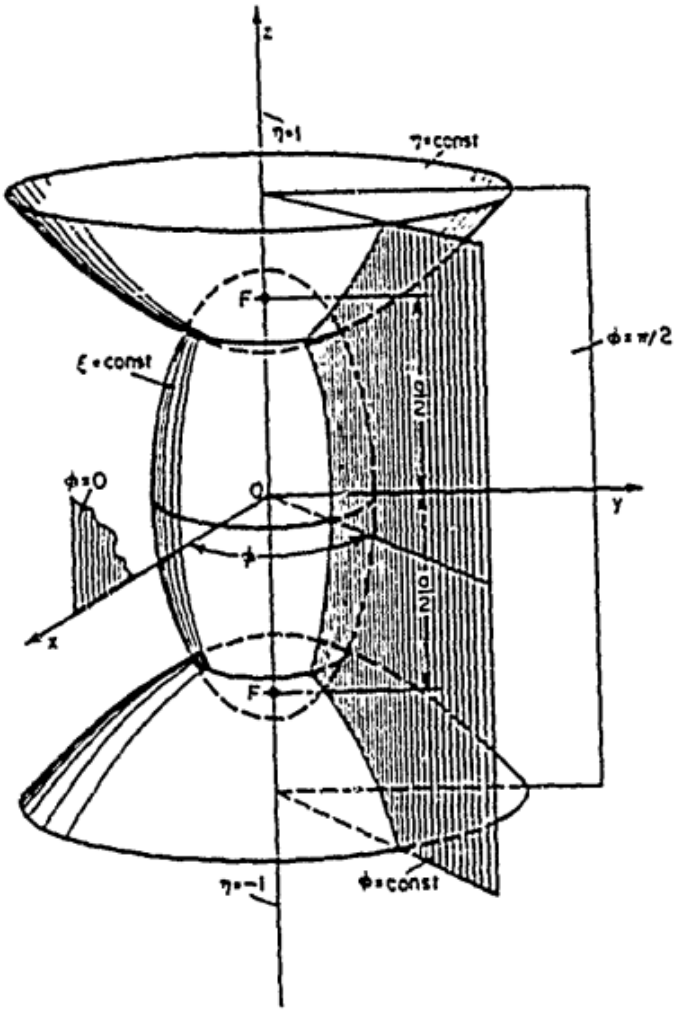
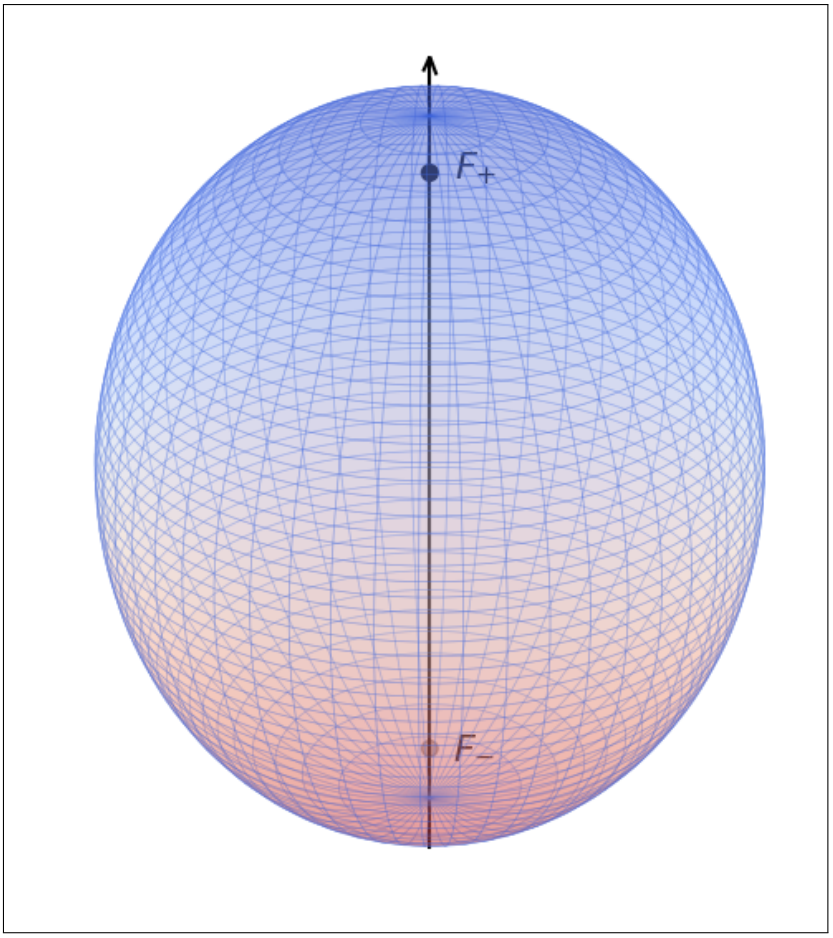


Fig. 1 - The prolate spheroidal coordinate system

ainsi que le programme python de dessin de l'ellipsoïde.

```
import matplotlib.pyplot as plt, numpy as np

fig = plt.figure(figsize=(8, 8)
ax = fig.add_subplot(projection='3d')
mu = 0.6
a = np.cosh(mu)
b, c = np.meshgrid(np.linspace(-1, 1, 100), np.linspace(0, 2*np.pi, 100))
x = np.sqrt((a**2-1)*(1-b**2))*np.cos(c)
y = np.sqrt((a**2-1)*(1-b**2))*np.sin(c)
z = a*b
ax.plot_surface(x, y, z, cmap=plt.cm.coolwarm_r, alpha=0.3, edgecolor='royalblue', lw=0.5)
ax.set(xlim=(-1, 1), ylim=(-1, 1), zlim=(-a, a))
ax.dist = 6
ax.set_axis_off()
```

```
Z = a*1.16
ax.quiver([0],[0],[0],[0],[0],[2*Z],pivot='middle',color='k', arrow_length_ratio=0.02)
fc, fl = np.array([[0, 0, -1], [0, 0, 1]]), ['$F_-$', '$F_+$']
ax.scatter(fc[:, 0], fc[:, 1], fc[:, 2], s=7**2, c='k')
for k in range(len(fl)):
        ax.text(fc[k, 0] + 0.05, fc[k, 1], fc[k, 2], fl[k], size=16)
plt.show()
```



Traduction d'un article de David Slepian et Estelle Sonnenblick (Denise Vella-Chemla, juin 2023)

Dans le quatrième article de Slepian[1] dédié aux fonctions d'ondes sphéroïdales prolates, on trouve cette phrase de David Slepian, en fin d'article avant l'annexe, de remerciement à l'informaticienne Estelle Sonnenblick qui a procédé aux calculs. Voici la traduction en français de leur article.

I am indebted to Mrs. E. Sonnenblick for programming and carrying out the computations reported here.

Valeurs propres associées aux fonctions d'onde sphéroïdales prolates d'ordre zéro

David Slepian, Estelle Sonnenblick

(Manuscrit reçu le 10 juin 1965)

Résumé. *Sont présentées ici les tables des valeurs de χ_n et λ_n, des quantités définies par les problèmes de valeurs propres*

$$(1-x^2)\psi_n'' - 2x\psi_n' + (\chi_n - c^2x^2)\psi_n = 0$$

et

$$\lambda_n\psi_n(x) = \int_{-1}^{1} \frac{\sin\ c(x-y)}{\pi(x-y)}\psi_n(y)dy.$$

De plus, quelques approximations de ces quantités sont données et évaluées.

Les fonctions sphéroïdales prolates d'ordre zéro, $\psi_n(x)$, $n = 0, 1, \ldots$, sont les solutions continues bornées des deux équations l'une différentielle

$$(1-x^2)\frac{d^2\psi_n}{dx^2} - 2x\frac{d\psi_n}{dx} + (\chi_n - c^2x^2)\psi_n = 0$$

et l'autre intégrale

$$\lambda_n\psi_n(x) = \int_{-1}^{1} \frac{\sin\ c(x-y)}{\pi(x-y)}\psi_n(y)dy.$$

L'importance de ces fonctions et des valeurs propres correspondantes χ_n et λ_n pour une grande variété de problèmes, traitant de sujets si divers que les lasers, la théorie de la communication, l'optique, la théorie du bruit, etc., peuvent être trouvées dans les articles [1] et [2] en bibliographie. Notre but ici, en réponse à de nombreuses requêtes, est de présenter quelques valeurs numériques de ces valeurs propres.

[1] Voir D. Slepian et H. Pollak, *Prolate spheroidal wave functions, Fourier analysis and uncertainty I*, Bell Syst. Tech. J. 40, no. 1, pp. 43-63 (1961) lien, H.J. Landau et H. Pollak, *Prolate spheroidal wave functions, Fourier analysis and uncertainty II*, Bell Syst. Tech. J. 40, no. 1, pp. 65-84 (1961) lien, H.J. Landau, H. Pollak, *Prolate spheroidal wave functions, Fourier analysis and uncertainty III, The Dimension of the Space of Essentially Time- and Band-Limited*, Bell Syst. Tech. J. 41, no. 4, pp. 1295-1336 (1962) lien, D. Slepian, *Prolate spheroidal wave functions, Fourier analysis and uncertainty IV : Extensions to many dimensions ; generalized prolate spheroidal functions*, Bell Syst. Tech. J. 43, no. 6, pp. 3009-3057 (1964) lien et *Prolate spheroidal wave functions, fourier analysis, and uncertainty - V : the discrete case*, Bell Syst. Tech. J. vol. 57, no. 5, pp. 1371-1430 (1978) lien.

Les Tables I et II listent les valeurs de χ_n et λ_n pour $n = 0(1)20(5)40$ et $c = 0(1)20(5)40$. Les valeurs données sont, selon nous, précises pour les huit figures listées[2]. Les résultats des calculs sont montrés graphiquement sur les figures Fig. 1-4.

Les valeurs de χ_n ont été obtenues en utilisant la méthode de Bouwkamp comme cela est expliqué par exemple dans le livre de Flammer [1]. Le calcul fournit également les coefficients d'expansion $d_r^{0n}(c)$ dans la notation de Flammer, dont la quantité $R_{0n}^{(1)}(c,1)$ peut être calculée. Les λ ont été trouvés par la formule

$$\lambda_n = \frac{2c}{\pi}[R_{0n}^{(1)}(c,1)]^2.$$

Les tables présentées ont nécessité 0.027 heures de calcul sur un IBM 7090.

Les formules suivantes pour λ_n et χ_n sont données dans la référence [2]. Pour de petites valeurs de n et c :

$$\lambda_n = \frac{2}{\pi}\left[\frac{2^{2n}(n!)^3}{(2n)!(2n+1)!}\right]^2 c^{2n+1}\cdot\left[1 - \frac{(2n+1)c^2}{(2n-1)^2(2n+3)^2} + O(c^4)\right]. \tag{1}$$

Pour n fixé et c grand

$$1 - \lambda_n = \frac{2^{3n+2}\sqrt{\pi}c^{n+\frac{1}{2}}e^{-2c}}{n!}\left[1 - \frac{6n^2 - 2n + 3}{32c} + O\left(\frac{1}{c^2}\right)\right]. \tag{2}$$

Certaines valeurs calculées à partir des termes explicitement fournis en (1) et (2) sont représentées par les lignes en pointillés sur les figures Fig. 3 et Fig. 4.

Pour n et c grands tous les deux, on a le résultat suivant. Soit b fixé et posons

$$n = \left[\frac{2}{\pi}(c + b\ln 2\sqrt{c})\right] \tag{3}$$

où les crochets dénotent la "partie entière de". Alors

$$\lim_{c\to\infty} \lambda_n = (1 + e^{\pi b})^{-1}. \tag{4}$$

[2]La notation $E \pm XY$ après une entrée dans les tables indique que l'entrée doit être multipliée par 10 où XY est un entier en notation décimale, par exemple $E + 03$ dénote un facteur de 10^3.

TABLE I—χ_n

n \ c =	1.	2.	3.	4.	5.	6.
0	3.1900006E − 01	1.1277341E + 00	2.1367322E + 00	3.1720674E + 00	4.1951289E + 00	5.2082692E + 00
1	2.5930846E + 00	4.2871285E + 00	6.8208883E + 00	9.8059438E + 00	1.2911703E + 01	1.6000443E + 01
2	6.5334718E + 00	8.2257130E + 00	1.1192939E + 01	1.5306300E + 01	2.0176915E + 01	2.5356479E + 01
3	1.2514462E + 01	1.4100204E + 01	1.6889030E + 01	2.1048961E + 01	2.6587360E + 01	3.3204199E + 01
4	2.0508274E + 01	2.2054830E + 01	2.4708535E + 01	2.8596855E + 01	3.3897096E + 01	4.0720194E + 01
5	3.0505405E + 01	3.2035263E + 01	3.4631281E + 01	3.8367138E + 01	4.3358996E + 01	4.9773712E + 01
6	4.2503818E + 01	4.4024748E + 01	4.6591428E + 01	5.0252698E + 01	5.5080962E + 01	6.1180757E + 01
7	5.6502845E + 01	5.8018371E + 01	6.0567636E + 01	6.4186116E + 01	6.8924773E + 01	7.4852867E + 01
8	7.2502203E + 01	7.4014194E + 01	7.6552160E + 01	8.0143235E + 01	8.4825931E + 01	9.0651159E + 01
9	9.0501757E + 01	9.2011304E + 01	9.4541490E + 01	9.8113806E + 01	1.0275858E + 02	1.0851545E + 02
10	1.1050143E + 02	1.1200922E + 02	1.1453381E + 02	1.1809267E + 02	1.2271039E + 02	1.2841888E + 02
11	1.3250119E + 02	1.3400766E + 02	1.3652809E + 02	1.4007696E + 02	1.4467463E + 02	1.5034744E + 02
12	1.5650101E + 02	1.5800647E + 02	1.6052372E + 02	1.6406496E + 02	1.6864733E + 02	1.7429300E + 02
13	1.8250086E + 02	1.8400554E + 02	1.8652029E + 02	1.9005557E + 02	1.9462601E + 02	2.0025051E + 02
14	2.1050075E + 02	2.1200480E + 02	2.1451756E + 02	2.1804808E + 02	2.2260902E + 02	2.2821669E + 02
15	2.4050065E + 02	2.4200419E + 02	2.4451535E + 02	2.4804202E + 02	2.5259526E + 02	2.5818931E + 02
16	2.7250058E + 02	2.7400370E + 02	2.7651353E + 02	2.8003704E + 02	2.8458396E + 02	2.9016684E + 02
17	3.0650051E + 02	3.0800328E + 02	3.1051202E + 02	3.1403289E + 02	3.1857456E + 02	3.2414815E + 02
18	3.4250046E + 02	3.4400294E + 02	3.4651075E + 02	3.5002941E + 02	3.5456666E + 02	3.6013245E + 02
19	3.8050041E + 02	3.8200264E + 02	3.8450967E + 02	3.8802645E + 02	3.9255996E + 02	3.9811912E + 02
20	4.2050037E + 02	4.2200239E + 02	4.2450874E + 02	4.2802392E + 02	4.3255422E + 02	4.3810771E + 02
25	6.5050024E + 02	6.5200154E + 02	6.5450564E + 02	6.5801543E + 02	6.6253497E + 02	6.6806946E + 02
30	9.3050017E + 02	9.3200108E + 02	9.3450394E + 02	9.3801078E + 02	9.4252442E + 02	9.4804850E + 02
35	1.2605001E + 03	1.2620008E + 03	1.2645029E + 03	1.2680079E + 03	1.2725180E + 03	1.2780358E + 03
40	1.6405001E + 03	1.6420006E + 03	1.6445022E + 03	1.6480061E + 03	1.6525138E + 03	1.6580275E + 03

TABLE I—

n \ c =	7.	8.	9.	10.	11.	12.
0	6.2162529E + 00	7.2215789E + 00	8.2254064E + 00	9.2283043E + 00	1.0230581E + 01	1.1232421E + 01
1	1.9056678E + 01	2.2092154E + 01	2.5116120E + 01	2.8133464E + 01	3.1146682E + 01	3.4157135E + 01
2	3.0560201E + 01	3.5706417E + 01	4.0802950E + 01	4.5868953E + 01	5.0916879E + 01	5.5953514E + 01
3	4.0405727E + 01	4.7757099E + 01	5.5051178E + 01	6.2257700E + 01	6.9401323E + 01	7.6505824E + 01
4	4.8910585E + 01	5.8016770E + 01	6.7500818E + 01	7.6993289E + 01	8.6369707E + 01	9.5638659E + 01
5	5.7777751E + 01	6.7364750E + 01	7.8205025E + 01	8.9739267E + 01	1.0144734E + 02	1.1305411E + 02
6	6.8701439E + 01	7.7825223E + 01	8.8658000E + 01	1.0103543E + 02	1.1446976E + 02	1.2835139E + 02
7	8.2064637E + 01	9.0691430E + 01	1.0090790E + 02	1.1288107E + 02	1.2660565E + 02	1.4174147E + 02
8	9.7684571E + 01	1.0601169E + 02	1.1574796E + 02	1.2705083E + 02	1.4010628E + 02	1.5502454E + 02
9	1.1543428E + 02	1.2357716E + 02	1.3302232E + 02	1.4387201E + 02	1.5626473E + 02	1.7038033E + 02
10	1.3525788E + 02	1.4327579E + 02	1.5253134E + 02	1.6309665E + 02	1.7506323E + 02	1.8855245E + 02
11	1.5712799E + 02	1.6505554E + 02	1.7417688E + 02	1.8454762E + 02	1.9623470E + 02	2.0932095E + 02
12	1.8102925E + 02	1.8888879E + 02	1.9791014E + 02	2.0813839E + 02	2.1962634E + 02	2.3243647E + 02
13	2.0695232E + 02	2.1475915E + 02	2.2370349E + 02	2.3382295E + 02	2.4516097E + 02	2.5776775E + 02
14	2.3489114E + 02	2.4265622E + 02	2.5153975E + 02	2.6157378E + 02	2.7279496E + 02	2.8524510E + 02
15	2.6484166E + 02	2.7257305E + 02	2.8140764E + 02	2.9137313E + 02	3.0250101E + 02	3.1482692E + 02
16	2.9680105E + 02	3.0450484E + 02	3.1329940E + 02	3.2320895E + 02	3.3426093E + 02	3.4648622E + 02
17	3.3076730E + 02	3.3844819E + 02	3.4720956E + 02	3.5707281E + 02	3.6806210E + 02	3.8020452E + 02
18	3.6673895E + 02	3.7440061E + 02	3.8313413E + 02	3.9295859E + 02	4.0389544E + 02	4.1596869E + 02
19	4.0471489E + 02	4.1236024E + 02	4.2107018E + 02	4.3086179E + 02	4.4175430E + 02	4.5376914E + 02
20	4.4469430E + 02	4.5232571E + 02	4.6101548E + 02	4.7077902E + 02	4.8163367E + 02	4.9359870E + 02
25	6.7462529E + 02	6.8220999E + 02	6.9083226E + 02	7.0050200E + 02	7.1123026E + 02	7.2302932E + 02
30	9.5458747E + 02	9.6214660E + 02	9.7073194E + 02	9.8035039E + 02	9.9100965E + 02	1.0027182E + 03
35	1.2845645E + 03	1.2921081E + 03	1.3006711E + 03	1.3102584E + 03	1.3208759E + 03	1.3325297E + 03
40	1.6645496E + 03	1.6720830E + 03	1.6806314E + 03	1.6901985E + 03	1.7007886E + 03	1.7124067E + 03

TABLE I—

n \ c =	13.	14.	15.	16.	17.	18.
0	1.2233939E + 01	1.3235214E + 01	1.4236300E + 01	1.5237237E + 01	1.6238054E + 01	1.7238772E + 01
1	3.7165631E + 01	4.0172681E + 01	4.3178630E + 01	4.6183721E + 01	4.9188129E + 01	5.2191983E + 01
2	6.0982596E + 01	6.6006328E + 01	7.1026104E + 01	7.6042858E + 01	8.1057244E + 01	8.6069739E + 01
3	8.3585719E + 01	9.0649230E + 01	9.7701181E + 01	1.0474459E + 02	1.1178148E + 02	1.1881324E + 02
4	1.0483494E + 02	1.1398465E + 02	1.2310348E + 02	1.3220071E + 02	1.4128205E + 02	1.5035127E + 02
5	1.2450713E + 02	1.3584050E + 02	1.4709398E + 02	1.5829441E + 02	1.6945806E + 02	1.8059490E + 02
6	1.4223009E + 02	1.5593166E + 02	1.6945804E + 02	1.8285785E + 02	1.9617229E + 02	2.0942797E + 02
7	1.5768187E + 02	1.7382917E + 02	1.8983663E + 02	2.0562050E + 02	2.2121898E + 02	2.3668721E + 02
8	1.7164637E + 02	1.8946449E + 02	2.0780930E + 02	2.2615098E + 02	2.4425790E + 02	2.6211708E + 02
9	1.8639078E + 02	2.0430123E + 02	2.2377440E + 02	2.4417004E + 02	2.6481922E + 02	2.8529987E + 02
10	2.0372711E + 02	2.2077813E + 02	2.3982549E + 02	2.6072449E + 02	2.8296138E + 02	3.0581686E + 02
11	2.2391335E + 02	2.4015533E + 02	2.5823139E + 02	2.7832097E + 02	3.0044546E + 02	3.2428066E + 02
12	2.4664450E + 02	2.6234574E + 02	2.7966575E + 02	2.9877161E + 02	3.1985976E + 02	3.4306306E + 02
13	2.7170195E + 02	2.8703335E + 02	3.0384785E + 02	3.2225590E + 02	3.4240470E + 02	3.6448308E + 02
14	2.9897207E + 02	3.1403113E + 02	3.3048712E + 02	3.4841822E + 02	3.6792260E + 02	3.8912905E + 02
15	3.2839115E + 02	3.4323943E + 02	3.5942402E + 02	3.7700550E + 02	3.9605573E + 02	4.1666293E + 02
16	3.5991943E + 02	3.7459944E + 02	3.9056997E + 02	4.0788062E + 02	4.2658830E + 02	4.4675957E + 02
17	3.9353027E + 02	4.0807299E + 02	4.2387018E + 02	4.4096376E + 02	4.5940093E + 02	4.7923537E + 02
18	4.2920498E + 02	4.4363385E + 02	4.5928798E + 02	4.7620357E + 02	4.9442089E + 02	5.1398496E + 02
19	4.6693004E + 02	4.8126322E + 02	4.9679753E + 02	5.1356471E + 02	5.3159977E + 02	5.5094143E + 02
20	5.0669542E + 02	5.2094728E + 02	5.3638001E + 02	5.5302178E + 02	5.7090346E + 02	5.9005891E + 02
25	7.3591267E + 02	7.4989504E + 02	7.6499245E + 02	7.8122221E + 02	7.9860305E + 02	8.1715510E + 02
30	1.0154855E + 03	1.0293217E + 03	1.0442378E + 03	1.0602457E + 03	1.0773582E + 03	1.0955890E + 03
35	1.3452267E + 03	1.3589745E + 03	1.3737811E + 03	1.3896552E + 03	1.4066063E + 03	1.4246442E + 03
40	1.7250580E + 03	1.7387482E + 03	1.7534835E + 03	1.7692707E + 03	1.7861168E + 03	1.8040295E + 03

TABLE I—

n \ c =	19.	20.	25.	30.	35.	40.
0	1.8239408E + 01	1.9239976E + 01	2.4242094E + 01	2.9243472E + 01	3.4244440E + 01	3.9245159E + 01
1	5.5195383E + 01	5.8198404E + 01	7.3209570E + 01	8.8216755E + 01	1.0322177E + 02	1.1822547E + 02
2	9.1080697E + 01	9.6090388E + 01	1.2112584E + 02	1.4614836E + 02	1.7116395E + 02	1.9617538E + 02
3	1.2584090E + 02	1.3286522E + 02	1.6795309E + 02	2.0300813E + 02	2.3804589E + 02	2.7307342E + 02
4	1.5941100E + 02	1.6846310E + 02	2.1364862E + 02	2.5876280E + 02	3.0384036E + 02	3.4889654E + 02
5	1.9171143E + 02	2.0281205E + 02	2.5816358E + 02	3.1337546E + 02	3.6851770E + 02	4.2361994E + 02
6	2.2264133E + 02	2.3582286E + 02	3.0144041E + 02	3.6680477E + 02	4.3204536E + 02	4.9721681E + 02
7	2.5206574E + 02	2.6738042E + 02	3.4341554E + 02	4.1900403E + 02	4.9438749E + 02	5.6965810E + 02
8	2.7978768E + 02	2.9732623E + 02	3.8400598E + 02	4.6991994E + 02	5.5550429E + 02	6.4091212E + 02
9	3.0548786E + 02	3.2541914E + 02	4.2311389E + 02	5.1949088E + 02	6.1535127E + 02	7.1094418E + 02
10	3.2868309E + 02	3.5126388E + 02	4.6061231E + 02	5.6764441E + 02	6.7387820E + 02	7.7971605E + 02
11	3.4916478E + 02	3.7436419E + 02	4.9632769E + 02	6.1429371E + 02	7.3102784E + 02	8.4718535E + 02
12	3.6825795E + 02	3.9493519E + 02	5.2999995E + 02	6.5933191E + 02	7.8673407E + 02	9.1330472E + 02
13	3.8867917E + 02	4.1503422E + 02	5.6120901E + 02	7.0262235E + 02	8.4091938E + 02	9.7802077E + 02
14	4.1220822E + 02	4.3736223E + 02	5.8939527E + 02	7.4397983E + 02	8.9349109E + 02	1.0412727E + 03
15	4.3894029E + 02	4.6303801E + 02	6.1457579E + 02	7.8313074E + 02	9.4433551E + 02	1.1029905E + 03
16	4.6847456E + 02	4.9183371E + 02	6.3866220E + 02	8.1963882E + 02	9.9330804E + 02	1.1630922E + 03
17	5.0052914E + 02	5.2335572E + 02	6.6469676E + 02	8.5289508E + 02	1.0402144E + 03	1.2214800E + 03
18	5.3494661E + 02	5.5736402E + 02	6.9431366E + 02	8.8272216E + 02	1.0847715E + 03	1.2780344E + 03
19	5.7163273E + 02	5.9372195E + 02	7.2743245E + 02	9.1079959E + 02	1.1265337E + 03	1.3326043E + 03
20	6.1052541E + 02	6.3234422E + 02	7.6357631E + 02	9.4039863E + 02	1.1648560E + 03	1.3849884E + 03
25	8.3690003E + 02	8.5786114E + 02	9.8185790E + 02	1.1410460E + 03	1.3423987E + 03	1.6007929E + 03
30	1.1149527E + 03	1.1354649E + 03	1.2558699E + 03	1.4079656E + 03	1.5952330E + 03	1.8229611E + 03
35	1.4437796E + 03	1.4640237E + 03	1.5823180E + 03	1.7304322E + 03	1.9106676E + 03	2.1260735E + 03
40	1.8230168E + 03	1.8430874E + 03	1.9600239E + 03	2.1056213E + 03	2.2815621E + 03	2.4899642E + 03

TABLE II — λ_n

n \ c =	1.	2.	3.	4.	5.	6.
0	5.7258178E − 01	8.8055992E − 01	9.7582863E − 01	9.9588549E − 01	9.9935241E − 01	9.9990188E − 01
1	6.2791274E − 02	3.5564063E − 01	7.0996324E − 01	9.1210742E − 01	9.7986456E − 01	9.9606164E − 01
2	1.2374793E − 03	3.5867688E − 02	2.0513868E − 01	5.1905484E − 01	7.9992193E − 01	9.4017339E − 01
3	9.2009770E − 06	1.1522328E − 03	1.8203800E − 02	1.1021099E − 01	3.4356219E − 01	6.4679195E − 01
4	3.7179286E − 08	1.8881549E − 05	7.0814710E − 04	8.8278764E − 03	5.6015851E − 02	2.0734922E − 01
5	9.4914367E − 11	1.9358522E − 07	1.6551244E − 05	3.8129172E − 04	4.1820948E − 03	2.7387166E − 02
6	1.6715716E − 13	1.3660608E − 09	2.6410165E − 07	1.0950871E − 05	1.9330846E − 04	1.9550007E − 03
7	2.1544491E − 16	7.0488855E − 12	3.0737365E − 09	2.2786389E − 07	6.3591502E − 06	9.4848766E − 05
8	2.1207239E − 19	2.7767898E − 14	2.7281307E − 11	3.6065493E − 09	1.5822998E − 07	3.4367833E − 06
9	1.6466214E − 22	8.6266788E − 17	1.9085689E − 13	4.4938297E − 11	3.0917257E − 09	9.7321160E − 08
10	1.0343492E − 25	2.1680119E − 19	1.0797906E − 15	4.5252285E − 13	4.8757393E − 11	2.2189805E − 09
11	5.3650197E − 29	4.4986573E − 22	5.0431156E − 18	3.7603029E − 15	6.3402794E − 13	4.1662263E − 11
12	2.3367231E − 32	7.8382450E − 25	1.9775436E − 20	2.6228187E − 17	6.9173022E − 15	6.5574786E − 13
13	8.6674831E − 36	1.1630367E − 27	6.6033063E − 23	1.5575942E − 19	6.4235507E − 17	8.7803771E − 15
14	2.7709612E − 39	1.4873466E − 30	1.9002929E − 25	7.9711081E − 22	5.1393068E − 19	1.0125783E − 16
15	0.	1.6563614E − 33	4.7620029E − 28	3.5519080E − 24	3.5797463E − 21	1.0163838E − 18
16	0.	1.6207613E − 36	1.0485031E − 30	1.3905716E − 26	2.1905130E − 23	8.9610464E − 21
17	0.	0.	2.0444867E − 33	4.8210691E − 29	1.1869344E − 25	6.9950907E − 23
18	0.	0.	3.5551880E − 36	1.4905449E − 31	5.7350388E − 28	4.8687451E − 25
19	0.	0.	5.5475853E − 39	4.1352414E − 34	2.4864675E − 30	3.0405184E − 27
20	0.	0.	0.	1.0352225E − 36	9.7273155E − 33	1.7132439E − 29
25	0.	0.	0.	0.	0.	0.
30	0.	0.	0.	0.	0.	0.
35	0.	0.	0.	0.	0.	0.
40	0.	0.	0.	0.	0.	0.

TABLE II —

n \ c =	7.	8.	9.	10.	11.	12.
0	9.9998546E − 01	9.9999787E − 01	9.9999969E − 01	9.9999996E − 01	9.9999999E − 01	1.0000000E + 00
1	9.9929217E − 01	9.9987898E − 01	9.9997999E − 01	9.9999677E − 01	9.9999949E − 01	9.9999992E − 01
2	9.8570806E − 01	9.9700462E − 01	9.9941873E − 01	9.9989273E − 01	9.9998091E − 01	9.9999670E − 01
3	8.6456615E − 01	9.6054568E − 01	9.9039622E − 01	9.9790124E − 01	9.9957158E − 01	9.9991663E − 01
4	4.7705272E − 01	7.4790284E − 01	9.1013316E − 01	9.7445778E − 01	9.9371700E − 01	9.9858732E − 01
5	1.1572386E − 01	3.2027663E − 01	5.9909617E − 01	8.2514635E − 01	9.4136927E − 01	9.8366430E − 01
6	1.3055972E − 02	6.0784427E − 02	1.9693935E − 01	4.4015011E − 01	7.0394130E − 01	8.8175663E − 01
7	9.0657300E − 04	6.1262894E − 03	3.0565075E − 02	1.1232482E − 01	2.9607849E − 01	5.5736081E − 01
8	4.5623948E − 05	4.1825206E − 04	2.8466070E − 03	1.4920175E − 02	6.0370339E − 02	1.8342927E − 01
9	1.7774751E − 06	2.1663088E − 05	1.9230822E − 04	1.3145890E − 03	7.1417030E − 03	3.1054179E − 02
10	5.5526131E − 08	8.9304272E − 07	1.0194316E − 05	8.8213430E − 05	6.0469421E − 04	3.3745471E − 03
11	1.4251398E − 09	3.0137350E − 08	4.3973999E − 07	4.7664454E − 06	4.0395675E − 05	2.7741888E − 04
12	3.0622379E − 11	8.4965846E − 10	1.5795600E − 08	2.1339628E − 07	2.2179166E − 06	1.8475085E − 05
13	5.5928434E − 13	2.0334083E − 11	4.8068821E − 10	8.0707164E − 09	1.0243298E − 07	1.0282524E − 06
14	8.7926605E − 15	4.1852675E − 13	1.2564804E − 11	2.6170188E − 10	4.0455355E − 09	4.8758791E − 08
15	1.2026890E − 16	7.4905020E − 15	2.8533973E − 13	7.3634903E − 12	1.3840557E − 10	1.9981456E − 09
16	1.4445726E − 18	1.1767148E − 16	5.6843266E − 15	1.8159383E − 13	4.1453619E − 12	7.1571886E − 11
17	1.5359357E − 20	1.6358709E − 18	1.0016699E − 16	3.9589753E − 15	1.0966649E − 13	2.2619074E − 12
18	1.4559023E − 22	2.0270123E − 20	1.5727550E − 18	7.6870812E − 17	2.5823710E − 15	6.3575326E − 14
19	1.2380854E − 24	2.2529462E − 22	2.2145250E − 20	1.3380681E − 18	5.4488496E − 17	1.6002320E − 15
20	9.4989023E − 27	2.2588880E − 24	2.8123556E − 22	2.1001719E − 20	1.0363386E − 18	3.6290304E − 17
25	6.3410693E − 38	5.7412040E − 35	2.3265268E − 32	4.9987005E − 30	6.4253487E − 28	5.4015219E − 26
30	0.	0.	0.	0.	5.4863023E − 38	1.1037482E − 35
35	0.	0.	0.	0.	0.	0.
40	0.	0.	0.	0.	0.	0.

TABLE II—

n \ c =	13.	14.	15.	16.	17.	18.
0	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00
1	9.9999999E − 01	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00
2	9.9999944E − 01	9.9999991E − 01	9.9999998E − 01	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00
3	9.9998436E − 01	9.9999715E − 01	9.9999949E − 01	9.9999991E − 01	9.9999998E − 01	1.0000000E + 00
4	9.9970100E − 01	9.9993948E − 01	9.9998818E − 01	9.9999776E − 01	9.9999958E − 01	9.9999992E − 01
5	9.9595266E − 01	9.9907074E − 01	9.9979787E − 01	9.9995783E − 01	9.9999149E − 01	9.9999833E − 01
6	9.6225505E − 01	9.8963945E − 01	9.9741834E − 01	9.9939756E − 01	9.9986611E − 01	9.9997138E − 01
7	7.8874478E − 01	9.2170099E − 01	9.7594492E − 01	9.9346756E − 01	9.9836416E − 01	9.9961326E − 01
8	4.0633176E − 01	6.6365081E − 01	8.5371077E − 01	9.4900699E − 01	9.8478345E − 01	9.9589845E − 01
9	1.0588399E − 01	2.7254759E − 01	5.1899118E − 01	7.5367260E − 01	9.0120813E − 01	9.6721066E − 01
10	1.5487268E − 02	5.7772021E − 02	1.6922485E − 01	3.7484512E − 01	6.2548476E − 01	8.2543081E − 01
11	1.5807741E − 03	7.5604029E − 03	3.0214721E − 02	9.8343344E − 02	2.5013211E − 01	4.8298471E − 01
12	1.2703997E − 04	7.3609236E − 04	3.6365712E − 03	1.5325905E − 02	5.4203716E − 02	1.5521339E − 01
13	8.4414630E − 06	5.8099164E − 05	3.4130591E − 04	1.7310585E − 03	7.6061834E − 03	2.8698205E − 02
14	4.7534082E − 07	3.8540665E − 06	2.6544166E − 05	1.5775571E − 04	8.1779798E − 04	3.7164510E − 03
15	2.3057257E − 08	2.1923715E − 07	1.7585578E − 06	1.2118149E − 05	7.2740820E − 05	3.8416435E − 04
16	9.7549162E − 10	1.0846150E − 08	1.0092888E − 07	8.0200884E − 07	5.5289258E − 06	3.3476998E − 05
17	3.6359074E − 11	4.7180556E − 10	5.0802489E − 09	4.6393027E − 08	3.6561510E − 07	2.5213492E − 06
18	1.2039857E − 12	1.8208273E − 11	2.2646216E − 10	2.3711707E − 09	2.1297926E − 08	1.6661751E − 07
19	3.5675475E − 14	6.2816688E − 13	9.0124935E − 12	1.0801803E − 10	1.1034773E − 09	9.7669046E − 09
20	9.5186419E − 16	1.9498859E − 14	3.2240722E − 13	4.4178809E − 12	5.1252279E − 11	5.1225654E − 10
25	3.1773164E − 24	1.3781710E − 22	4.5947254E − 21	1.2173462E − 19	2.6337453E − 18	4.7585812E − 17
30	1.4501905E − 33	1.3251429E − 31	8.8515118E − 30	4.4989186E − 28	1.7978779E − 26	5.8040997E − 25
35	0.	0.	0.	3.1590168E − 37	2.3233738E − 35	1.3343537E − 33
40	0.	0.	0.	0.	0.	0.

TABLE II—

n \ c =	19.	20.	25.	30.	35.	40.
0	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00
1	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00
2	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00
3	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00
4	9.9999999E − 01	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00
5	9.9999968E − 01	9.9999994E − 01	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00
6	9.9999408E − 01	9.9999881E − 01	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00
7	9.9991254E − 01	9.9998093E − 01	9.9999999E − 01	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00
8	9.9896831E − 01	9.9975345E − 01	9.9999988E − 01	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00
9	9.9042654E − 01	9.9743251E − 01	9.9999821E − 01	1.0000000E + 00	1.0000000E + 00	1.0000000E + 00
10	9.3461880E − 01	9.7911569E − 01	9.9997682E − 01	9.9999999E − 01	1.0000000E + 00	1.0000000E + 00
11	7.1923718E − 01	8.7971361E − 01	9.9974565E − 01	9.9999983E − 01	1.0000000E + 00	1.0000000E + 00
12	3.4534703E − 01	5.8879338E − 01	9.9766185E − 01	9.9999783E − 01	1.0000000E + 00	1.0000000E + 00
13	9.0528307E − 02	2.2898871E − 01	9.8251216E − 01	9.9997547E − 01	9.9999998E − 01	1.0000000E + 00
14	1.4751648E − 02	5.0245996E − 02	9.0214476E − 01	9.9975907E − 01	9.9999980E − 01	1.0000000E + 00
15	1.7952937E − 03	7.4212338E − 03	6.5129574E − 01	9.9796698E − 01	9.9999766E − 01	1.0000000E + 00
16	1.7967267E − 04	8.5983868E − 04	2.9167771E − 01	9.8564508E − 01	9.9997604E − 01	9.9999998E − 01
17	1.5383334E − 05	8.3739541E − 05	7.5468799E − 02	9.2101083E − 01	9.9978298E − 01	9.9999978E − 01
18	1.1493460E − 06	7.0600702E − 06	1.3031043E − 02	7.0692287E − 01	9.9828070E − 01	9.9999766E − 01
19	7.5908731E − 08	5.2374892E − 07	1.7588754E − 03	3.5647890E − 01	9.8836235E − 01	9.9997777E − 01
20	4.4748828E − 09	3.4574493E − 08	2.0082884E − 04	1.0627740E − 01	9.3662832E − 01	9.9981076E − 01
25	7.3154280E − 16	9.7203030E − 15	6.7594641E − 10	4.7379571E − 06	5.3273087E − 03	4.8731168E − 01
30	1.5483211E − 23	3.4788064E − 22	2.4882077E − 16	1.3177338E − 11	1.0489720E − 07	1.7876070E − 04
35	6.1447670E − 32	2.3202540E − 30	1.6231560E − 23	5.8407336E − 18	2.5646331E − 13	2.2391506E − 09
40	0.	0.	2.4836333E − 31	5.8205690E − 25	1.3022033E − 19	4.9862021E − 15

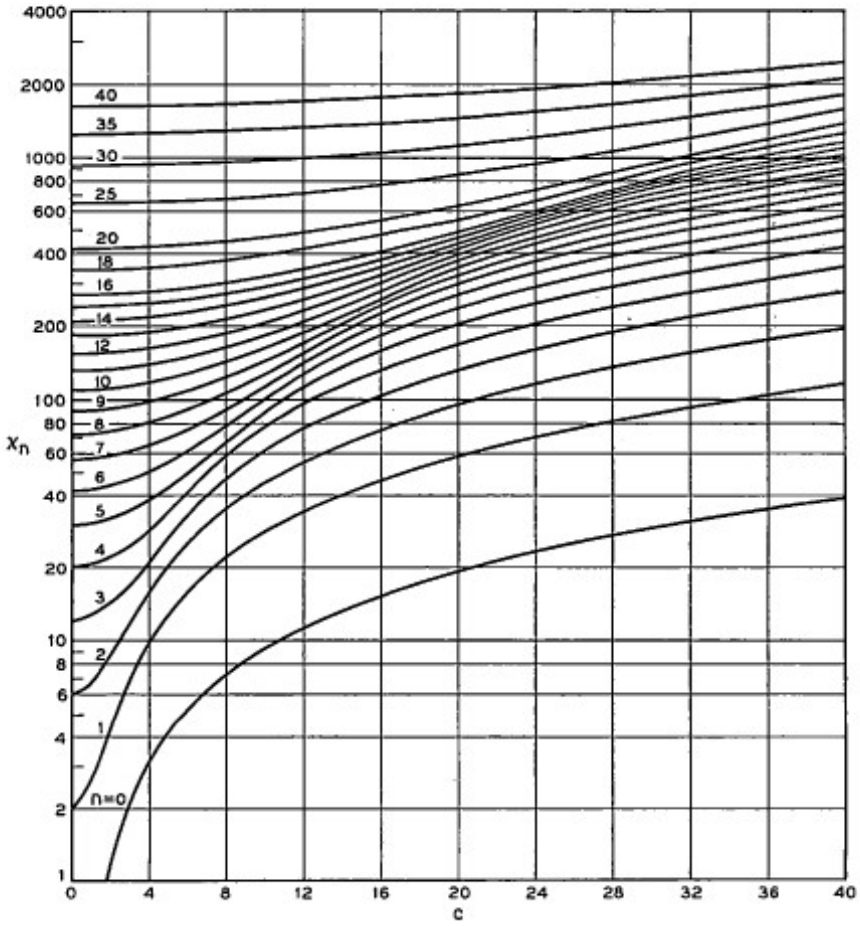


FIG. 1 : valeurs propres, χ_n, de $(1-x^2)\psi'' - 2x\psi' + (\chi - c^2x^2)\psi = 0$.

Les déductions de (3) et (4) fournies dans [2] suggèrent la formule d'approximation suivante

$$\lambda_n \approx \widehat{\lambda}_n = (1 + e^{\pi \widehat{b}})^{-1} \tag{5}$$

$$\widehat{b} = \frac{n\frac{\pi}{2} - c + \frac{\pi}{4}}{(\gamma/2) + 2\ln 2 + \frac{1}{2}\ln c} \tag{6}$$

pour les portions proches de la verticale des courbes de λ_n montrées sur la figure Fig. 2. Ici $\gamma = 0.5772156649$ est la constante d'Euler-Mascheroni. La précision remarquable de cette approximation est montrée sur la Fig. 5. Ici, pour des valeurs fixées de n et b, on a déterminé les valeurs de c à partir de (6) et pour ces valeurs de n et c, on a visualisé $|(\widehat{\lambda}/\lambda) - 1|$ par rapport à n. On voit que pour $0.2 \leq \widehat{\lambda}_n \leq 0.9$, (5) et (6) fournissent une excellente approximation même pour de petites valeurs de n.

Les formules correspondantes pour les χ_n sont les suivantes. Pour n fixé et c petit :

$$\chi_n = n(n+1) + \frac{1}{2}\left[1 + \frac{1}{(2n-1)(2n+3)}\right] c^2 + O(c^4)$$

et pour n fixé et c grand :

$$\chi_n = (2n+1)c - \frac{2n^2+2n+3}{4} - \frac{(2n+1)(n^2+n+3)}{16c} + O\left(\frac{1}{c^2}\right).$$

Si n et c deviennent grands selon (3) avec b fixé,

$$\chi_n = c^2 + 2bc + \frac{b^2-1}{2} - \frac{b^2-b}{8c} + O\left(\frac{1}{c^2}\right)$$

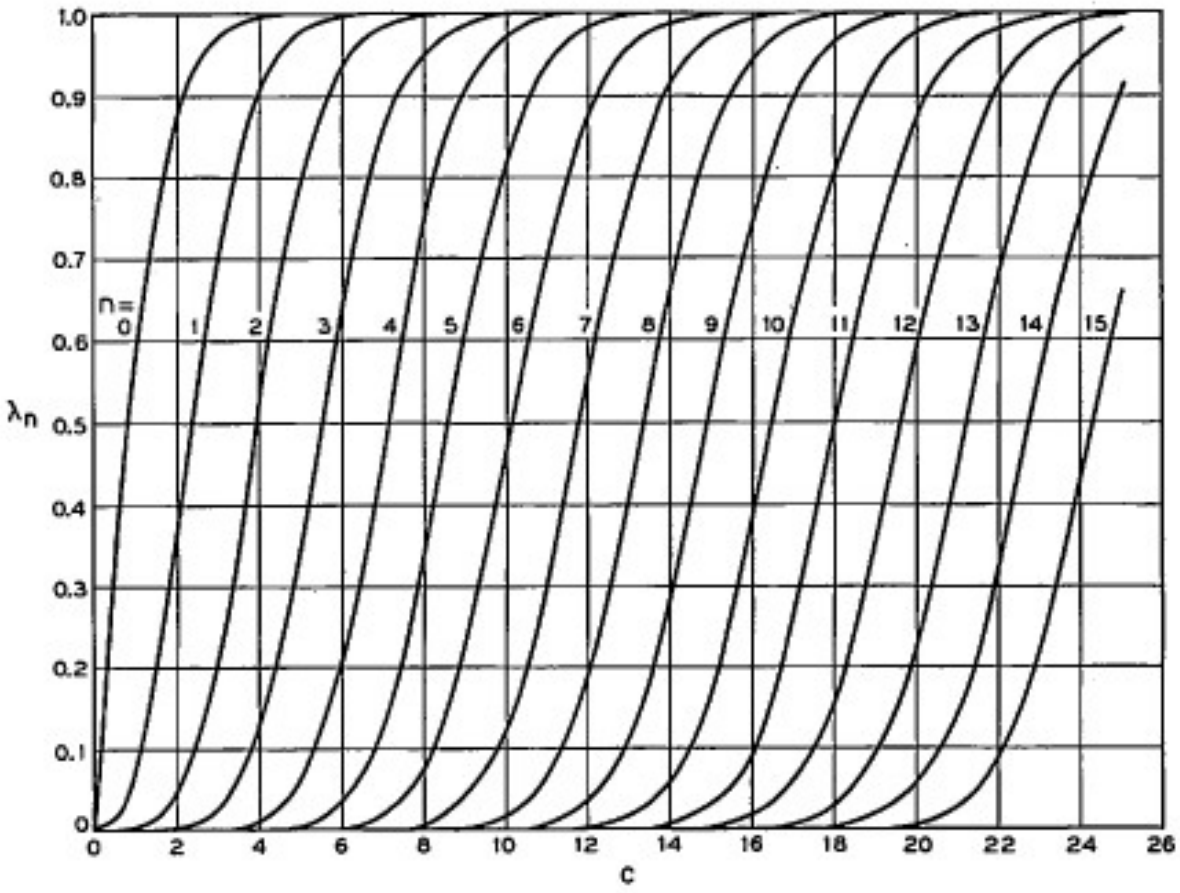


FIG. 2 : valeurs propres, λ_n, de l'équation intégrale. Échelle linéaire.

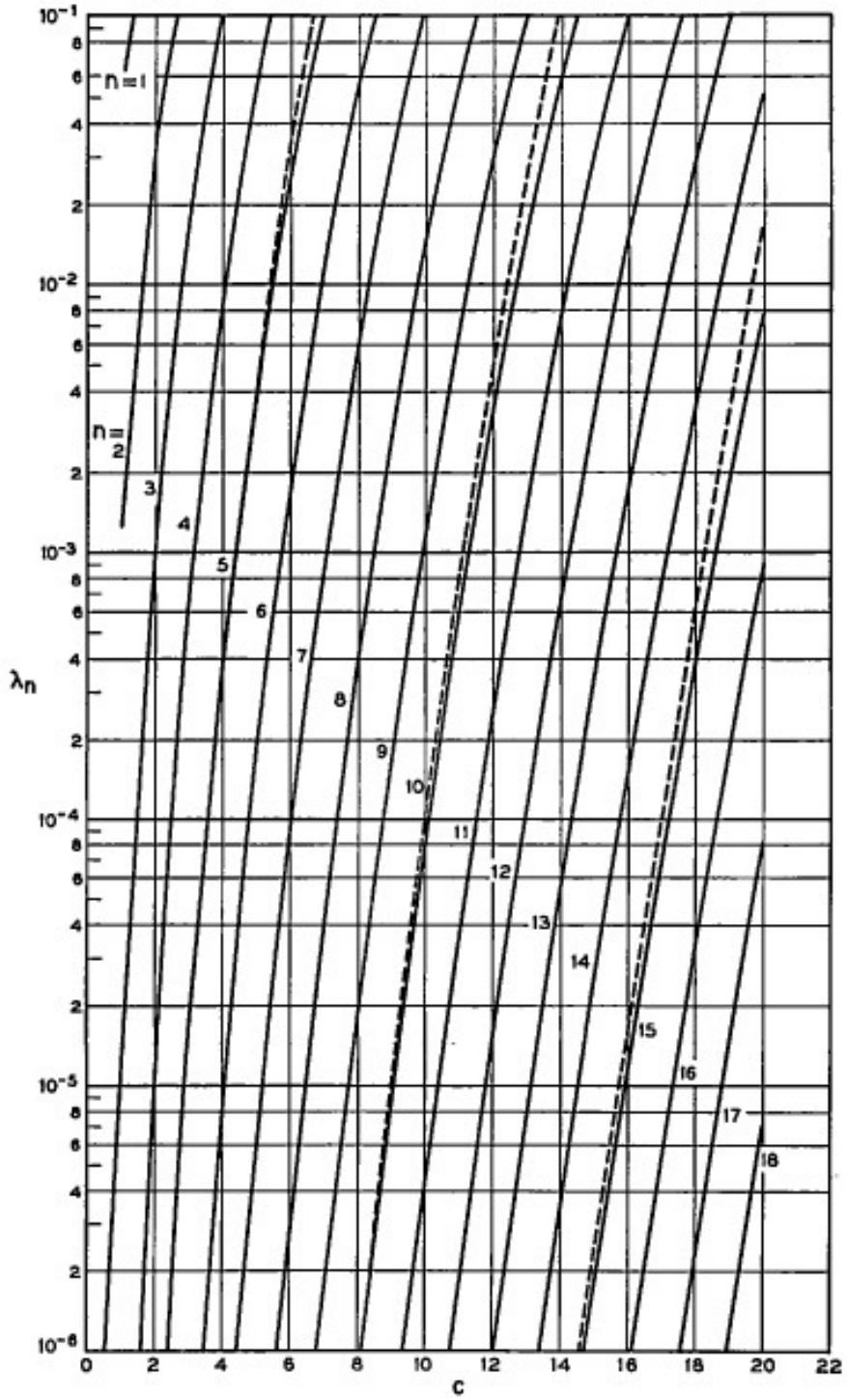


FIG. 3 : valeurs propres, λ_n, de l'équation intégrale pour $c < n\pi/2$. Les lignes pointillées sont l'approximation (1).

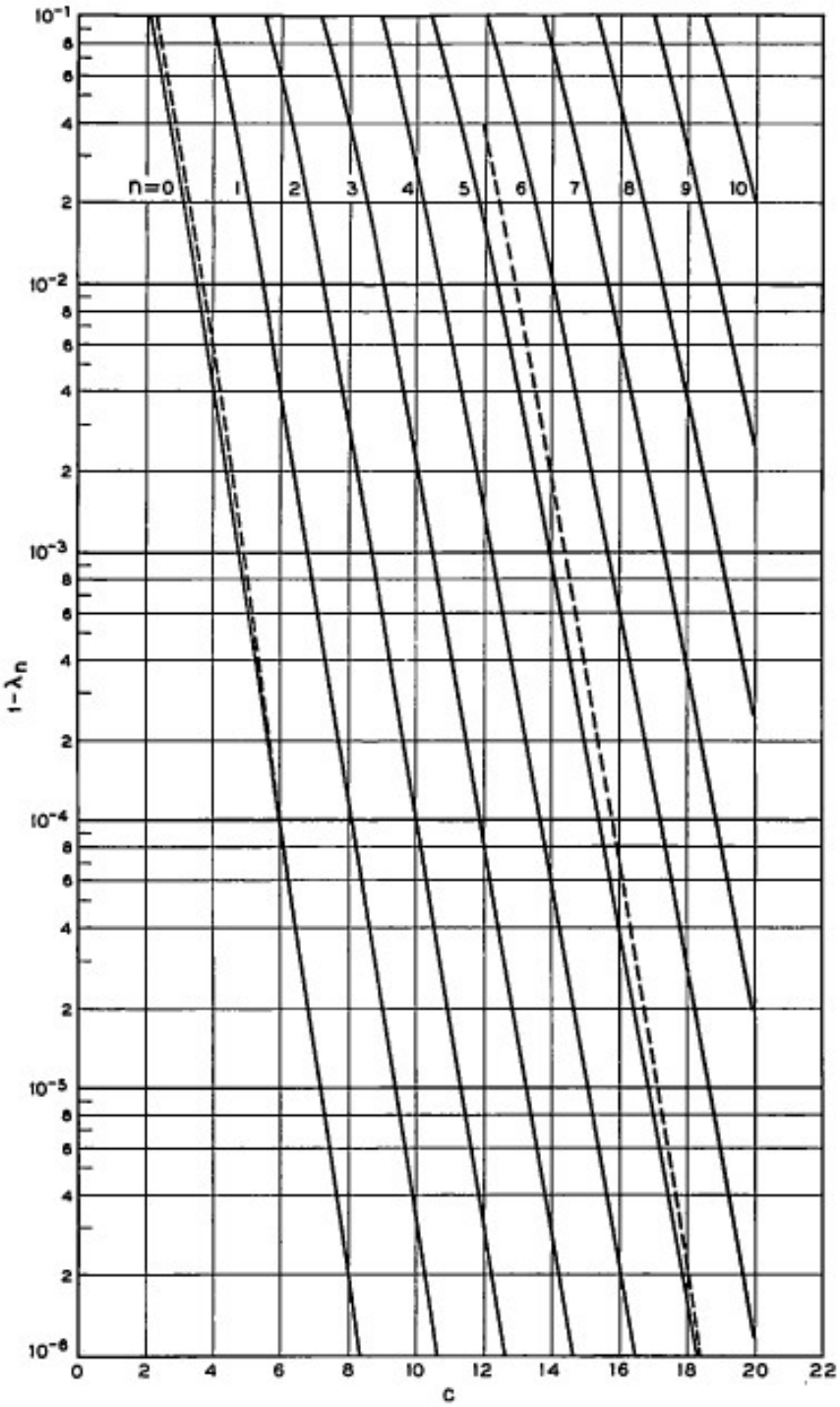


FIG. 4 : valeurs propres, λ_n, de l'équation intégrale pour $c > n\pi/2$. Les lignes pointillées sont l'approximation (2).

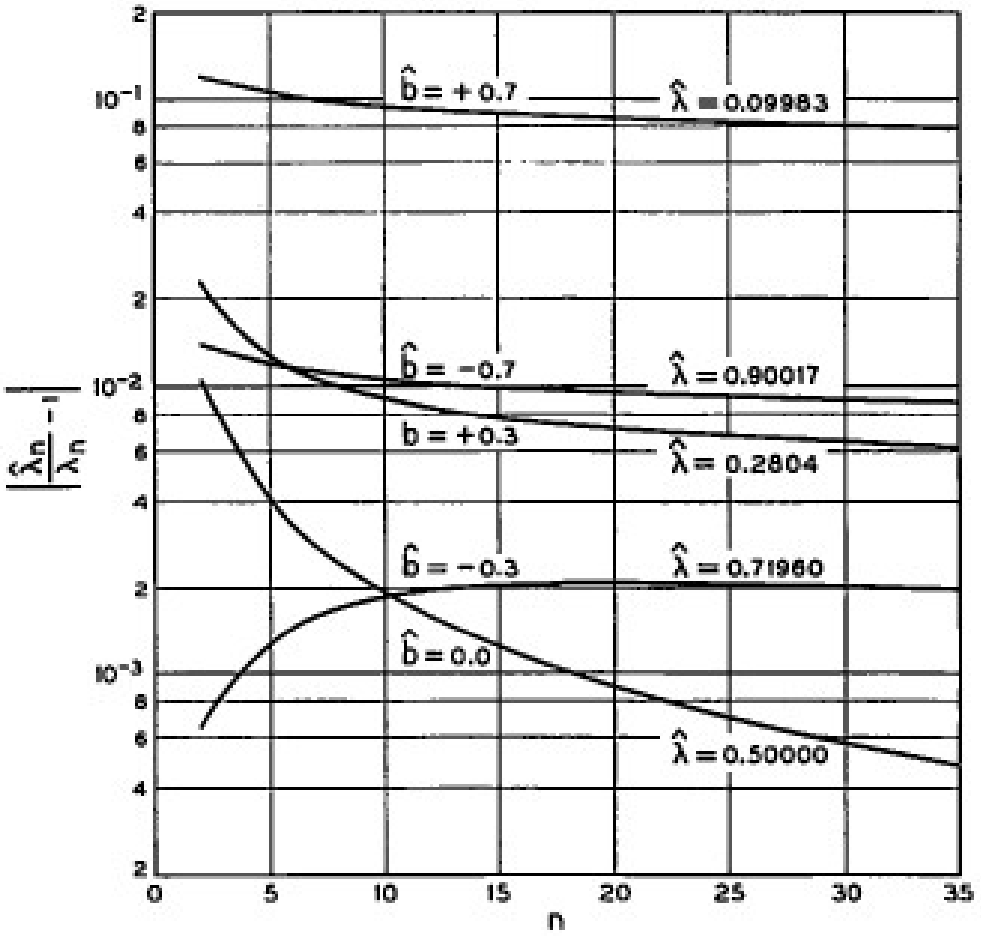


FIG. 5 : précision de l'approximation (5) - (6) pour les valeurs propres λ_n.

Références

[1] Flammer, C., *Spheroidal Wave Functions*, Stanford Univ. Press, Stanford, 1957.

[2] Slepian, D., *Some Asymptotic Expansions for Prolate Spheroidal Wave Functions*, J. Math. and Phys., 44, n° 2, June, 1965, pp. 99-140.

Les χ_n

1.	2.	3.	4.	5.	6.
3.1900006 e − 01	1.1277341 e + 00	2.1367322 e + 00	3.1720674 e + 00	4.1951289 e + 00	5.2082692 e + 00
2.5930846 e + 00	4.2871285 e + 00	6.8208883 e + 00	9.8059438 e + 00	1.2911703 e + 01	1.6000443 e + 01
6.5334718 e + 00	8.2257130 e + 00	1.1192939 e + 01	1.5306300 e + 01	2.0176915 e + 01	2.5356479 e + 01
1.2514462 e + 01	1.4100204 e + 01	1.6889030 e + 01	2.1048961 e + 01	2.6587360 e + 01	3.3204199 e + 01
2.0508274 e + 01	2.2054830 e + 01	2.4708535 e + 01	2.8596855 e + 01	3.3897096 e + 01	4.0720194 e + 01
3.0505405 e + 01	3.2035263 e + 01	3.4631281 e + 01	3.8367138 e + 01	4.3358996 e + 01	4.9773712 e + 01
4.2503818 e + 01	4.4024748 e + 01	4.6591428 e + 01	5.0252698 e + 01	5.5080962 e + 01	6.1180757 e + 01
5.6502845 e + 01	5.8018371 e + 01	6.0567636 e + 01	6.4186116 e + 01	6.8924773 e + 01	7.4852867 e + 01
7.2502203 e + 01	7.4014194 e + 01	7.6552160 e + 01	8.0143235 e + 01	8.4825931 e + 01	9.0651159 e + 01
9.0501757 e + 01	9.2011304 e + 01	9.4541490 e + 01	9.8113806 e + 01	1.0275858 e + 02	1.0851545 e + 02
1.1050143 e + 02	1.1200922 e + 02	1.1453381 e + 02	1.1809267 e + 02	1.2271039 e + 02	1.2841888 e + 02
1.3250119 e + 02	1.3400766 e + 02	1.3652809 e + 02	1.4007696 e + 02	1.4467463 e + 02	1.5034744 e + 02
1.5650101 e + 02	1.5800647 e + 02	1.6052372 e + 02	1.6406496 e + 02	1.6864733 e + 02	1.7429300 e + 02
1.8250086 e + 02	1.8400554 e + 02	1.8652029 e + 02	1.9005557 e + 02	1.9462601 e + 02	2.0025051 e + 02
2.1050075 e + 02	2.1200480 e + 02	2.1451756 e + 02	2.1804808 e + 02	2.2260902 e + 02	2.2821669 e + 02
2.4050065 e + 02	2.4200419 e + 02	2.4451535 e + 02	2.4804202 e + 02	2.5259526 e + 02	2.5818931 e + 02
2.7250058 e + 02	2.7400370 e + 02	2.7651353 e + 02	2.8003704 e + 02	2.8458396 e + 02	2.9016684 e + 02
3.0650051 e + 02	3.0800328 e + 02	3.1051202 e + 02	3.1403289 e + 02	3.1857456 e + 02	3.2414815 e + 02
3.4250046 e + 02	3.4400294 e + 02	3.4651075 e + 02	3.5002941 e + 02	3.5456666 e + 02	3.6013245 e + 02
3.8050041 e + 02	3.8200264 e + 02	3.8450967 e + 02	3.8802645 e + 02	3.9255996 e + 02	3.9811912 e + 02
4.2050037 e + 02	4.2200239 e + 02	4.2450874 e + 02	4.2802392 e + 02	4.3255422 e + 02	4.3810771 e + 02
6.5050024 e + 02	6.5200154 e + 02	6.5450564 e + 02	6.5801543 e + 02	6.6253497 e + 02	6.6806946 e + 02
9.3050017 e + 02	9.3200108 e + 02	9.3450394 e + 02	9.3801078 e + 02	9.4252442 e + 02	9.4804850 e + 02
1.2605001 e + 03	1.2620008 e + 03	1.2645029 e + 03	1.2680079 e + 03	1.2725180 e + 03	1.2780358 e + 03
1.6405001 e + 03	1.6420006 e + 03	1.6445022 e + 03	1.6480061 e + 03	1.6525138 e + 03	1.6580275 e + 03

7.	8.	9.	10.	11.	12.
6.2162529 e + 00	7.2215789 e + 00	8.2254064 e + 00	9.2283043 e + 00	1.0230581 e + 01	1.1232421 e + 01
1.9056678 e + 01	2.2092154 e + 01	2.5116120 e + 01	2.8133464 e + 01	3.1146682 e + 01	3.4157135 e + 01
3.0560201 e + 01	3.5706417 e + 01	4.0802950 e + 01	4.5868953 e + 01	5.0916879 e + 01	5.5953514 e + 01
4.0405727 e + 01	4.7757099 e + 01	5.5051178 e + 01	6.2257700 e + 01	6.9401323 e + 01	7.6505824 e + 01
4.8910585 e + 01	5.8016770 e + 01	6.7500818 e + 01	7.6993289 e + 01	8.6369707 e + 01	9.5638659 e + 01
5.7777751 e + 01	6.7364750 e + 01	7.8205025 e + 01	8.9739267 e + 01	1.0144734 e + 02	1.1305411 e + 02
6.8701439 e + 01	7.7825223 e + 01	8.8658000 e + 01	1.0103543 e + 02	1.1446976 e + 02	1.2835139 e + 02
8.2064637 e + 01	9.0691430 e + 01	1.0090790 e + 02	1.1288107 e + 02	1.2660565 e + 02	1.4174147 e + 02
9.7684571 e + 01	1.0601169 e + 02	1.1574796 e + 02	1.2705083 e + 02	1.4010628 e + 02	1.5502454 e + 02
1.1543428 e + 02	1.2357716 e + 02	1.3302232 e + 02	1.4387201 e + 02	1.5626473 e + 02	1.7038033 e + 02
1.3525788 e + 02	1.4327579 e + 02	1.5253134 e + 02	1.6309665 e + 02	1.7506323 e + 02	1.8855245 e + 02
1.5712799 e + 02	1.6505554 e + 02	1.7417688 e + 02	1.8454762 e + 02	1.9623470 e + 02	2.0932095 e + 02
1.8102925 e + 02	1.8888879 e + 02	1.9791014 e + 02	2.0813839 e + 02	2.1962634 e + 02	2.3243647 e + 02
2.0695232 e + 02	2.1475915 e + 02	2.2370349 e + 02	2.3382295 e + 02	2.4516097 e + 02	2.5776775 e + 02
2.3489114 e + 02	2.4265622 e + 02	2.5153975 e + 02	2.6157378 e + 02	2.7279496 e + 02	2.8524510 e + 02
2.6484166 e + 02	2.7257305 e + 02	2.8140764 e + 02	2.9137313 e + 02	3.0250101 e + 02	3.1482692 e + 02
2.9680105 e + 02	3.0450484 e + 02	3.1329940 e + 02	3.2320895 e + 02	3.3426093 e + 02	3.4648622 e + 02
3.3076730 e + 02	3.3844819 e + 02	3.4720956 e + 02	3.5707281 e + 02	3.6806210 e + 02	3.8020452 e + 02
3.6673895 e + 02	3.7440061 e + 02	3.8313413 e + 02	3.9295859 e + 02	4.0389544 e + 02	4.1596869 e + 02
4.0471489 e + 02	4.1236024 e + 02	4.2107018 e + 02	4.3086179 e + 02	4.4175430 e + 02	4.5376914 e + 02
4.4469430 e + 02	4.5232571 e + 02	4.6101548 e + 02	4.7077902 e + 02	4.8163367 e + 02	4.9359870 e + 02
6.7462529 e + 02	6.8220999 e + 02	6.9083226 e + 02	7.0050200 e + 02	7.1123026 e + 02	7.2302932 e + 02
9.5458747 e + 02	9.6214660 e + 02	9.7073194 e + 02	9.8035039 e + 02	9.9100965 e + 02	1.0027182 e + 03
1.2845645 e + 03	1.2921081 e + 03	1.3006711 e + 03	1.3102584 e + 03	1.3208759 e + 03	1.3325297 e + 03
1.6645496 e + 03	1.6720830 e + 03	1.6806314 e + 03	1.6901985 e + 03	1.7007886 e + 03	1.7124067 e + 03

13.	14.	15.	16.	17.	18.
1.2233939 e + 01	1.3235214 e + 01	1.4236300 e + 01	1.5237237 e + 01	1.6238054 e + 01	1.7238772 e + 01
3.7165631 e + 01	4.0172681 e + 01	4.3178630 e + 01	4.6183721 e + 01	4.9188129 e + 01	5.2191983 e + 01
6.0982596 e + 01	6.6006328 e + 01	7.1026104 e + 01	7.6042858 e + 01	8.1057244 e + 01	8.6069739 e + 01
8.3585719 e + 01	9.0649230 e + 01	9.7701181 e + 01	1.0474459 e + 02	1.1178148 e + 02	1.1881324 e + 02
1.0483494 e + 02	1.1398465 e + 02	1.2310348 e + 02	1.3220071 e + 02	1.4128205 e + 02	1.5035127 e + 02
1.2450713 e + 02	1.3584050 e + 02	1.4709398 e + 02	1.5829441 e + 02	1.6945806 e + 02	1.8059490 e + 02
1.4223009 e + 02	1.5593166 e + 02	1.6945804 e + 02	1.8285785 e + 02	1.9617229 e + 02	2.0942797 e + 02
1.5768187 e + 02	1.7382917 e + 02	1.8983663 e + 02	2.0562050 e + 02	2.2121898 e + 02	2.3668721 e + 02
1.7164637 e + 02	1.8946449 e + 02	2.0780930 e + 02	2.2615098 e + 02	2.4425790 e + 02	2.6211708 e + 02
1.8639078 e + 02	2.0430123 e + 02	2.2377440 e + 02	2.4417004 e + 02	2.6481922 e + 02	2.8529987 e + 02
2.0372711 e + 02	2.2077813 e + 02	2.3982549 e + 02	2.6072449 e + 02	2.8296138 e + 02	3.0581686 e + 02
2.2391335 e + 02	2.4015533 e + 02	2.5823139 e + 02	2.7832097 e + 02	3.0044546 e + 02	3.2428066 e + 02
2.4664450 e + 02	2.6234574 e + 02	2.7966575 e + 02	2.9877161 e + 02	3.1985976 e + 02	3.4306306 e + 02
2.7170195 e + 02	2.8703335 e + 02	3.0384785 e + 02	3.2225590 e + 02	3.4240470 e + 02	3.6448308 e + 02
2.9897207 e + 02	3.1403113 e + 02	3.3048712 e + 02	3.4841822 e + 02	3.6792260 e + 02	3.8912905 e + 02
3.2839115 e + 02	3.4323943 e + 02	3.5942402 e + 02	3.7700550 e + 02	3.9605573 e + 02	4.1666293 e + 02
3.5991943 e + 02	3.7459944 e + 02	3.9056997 e + 02	4.0788062 e + 02	4.2658830 e + 02	4.4675957 e + 02
3.9353027 e + 02	4.0807299 e + 02	4.2387018 e + 02	4.4096376 e + 02	4.5940093 e + 02	4.7923537 e + 02
4.2920498 e + 02	4.4363385 e + 02	4.5928798 e + 02	4.7620357 e + 02	4.9442089 e + 02	5.1398496 e + 02
4.6693004 e + 02	4.8126322 e + 02	4.9679753 e + 02	5.1356471 e + 02	5.3159977 e + 02	5.5094143 e + 02
5.0669542 e + 02	5.2094728 e + 02	5.3638001 e + 02	5.5302178 e + 02	5.7090346 e + 02	5.9005891 e + 02
7.3591267 e + 02	7.4989504 e + 02	7.6499245 e + 02	7.8122221 e + 02	7.9860305 e + 02	8.1715510 e + 02
1.0154855 e + 03	1.0293217 e + 03	1.0442378 e + 03	1.0602457 e + 03	1.0773582 e + 03	1.0955890 e + 03
1.3452267 e + 03	1.3589745 e + 03	1.3737811 e + 03	1.3896552 e + 03	1.4066063 e + 03	1.4246442 e + 03
1.7250580 e + 03	1.7387482 e + 03	1.7534835 e + 03	1.7692707 e + 03	1.7861168 e + 03	1.8040295 e + 03

19.	20.	25.	30.	35.	40.
1.8239408 e + 01	1.9239976 e + 01	2.4242094 e + 01	2.9243472 e + 01	3.4244440 e + 01	3.9245159 e + 01
5.5195383 e + 01	5.8198404 e + 01	7.3209570 e + 01	8.8216755 e + 01	1.0322177 e + 02	1.1822547 e + 02
9.1080697 e + 01	9.6090388 e + 01	1.2112584 e + 02	1.4614836 e + 02	1.7116395 e + 02	1.9617538 e + 02
1.2584090 e + 02	1.3286522 e + 02	1.6795309 e + 02	2.0300813 e + 02	2.3804589 e + 02	2.7307342 e + 02
1.5941100 e + 02	1.6846310 e + 02	2.1364862 e + 02	2.5876280 e + 02	3.0384036 e + 02	3.4889654 e + 02
1.9171143 e + 02	2.0281205 e + 02	2.5816358 e + 02	3.1337546 e + 02	3.6851770 e + 02	4.2361994 e + 02
2.2264133 e + 02	2.3582286 e + 02	3.0144041 e + 02	3.6680477 e + 02	4.3204536 e + 02	4.9721681 e + 02
2.5206574 e + 02	2.6738042 e + 02	3.4341554 e + 02	4.1900403 e + 02	4.9438749 e + 02	5.6965810 e + 02
2.7978768 e + 02	2.9732623 e + 02	3.8400598 e + 02	4.6991994 e + 02	5.5550429 e + 02	6.4091212 e + 02
3.0548786 e + 02	3.2541914 e + 02	4.2311389 e + 02	5.1949088 e + 02	6.1535127 e + 02	7.1094418 e + 02
3.2868309 e + 02	3.5126388 e + 02	4.6061231 e + 02	5.6764441 e + 02	6.7387820 e + 02	7.7971605 e + 02
3.4916478 e + 02	3.7436419 e + 02	4.9632769 e + 02	6.1429371 e + 02	7.3102784 e + 02	8.4718535 e + 02
3.6825795 e + 02	3.9493519 e + 02	5.2999995 e + 02	6.5933191 e + 02	7.8673407 e + 02	9.1330472 e + 02
3.8867917 e + 02	4.1503422 e + 02	5.6120901 e + 02	7.0262235 e + 02	8.4091938 e + 02	9.7802077 e + 02
4.1220822 e + 02	4.3736223 e + 02	5.8939527 e + 02	7.4397983 e + 02	8.9349109 e + 02	1.0412727 e + 03
4.3894029 e + 02	4.6303801 e + 02	6.1457579 e + 02	7.8313074 e + 02	9.4433551 e + 02	1.1029905 e + 03
4.6847456 e + 02	4.9183371 e + 02	6.3866220 e + 02	8.1963882 e + 02	9.9330804 e + 02	1.1630922 e + 03
5.0052914 e + 02	5.2335572 e + 02	6.6469676 e + 02	8.5289508 e + 02	1.0402144 e + 03	1.2214800 e + 03
5.3494661 e + 02	5.5736402 e + 02	6.9431366 e + 02	8.8272216 e + 02	1.0847715 e + 03	1.2780344 e + 03
5.7163273 e + 02	5.9372195 e + 02	7.2743245 e + 02	9.1079959 e + 02	1.1265337 e + 03	1.3326043 e + 03
6.1052541 e + 02	6.3234422 e + 02	7.6357631 e + 02	9.4039863 e + 02	1.1648560 e + 03	1.3849884 e + 03
8.3690003 e + 02	8.5786114 e + 02	9.8185790 e + 02	1.1410460 e + 03	1.3423987 e + 03	1.6007929 e + 03
1.1149527 e + 03	1.1354649 e + 03	1.2558699 e + 03	1.4079656 e + 03	1.5952330 e + 03	1.8229611 e + 03
1.4437796 e + 03	1.4640237 e + 03	1.5823180 e + 03	1.7304322 e + 03	1.9106676 e + 03	2.1260735 e + 03
1.8230168 e + 03	1.8430874 e + 03	1.9600239 e + 03	2.1056213 e + 03	2.2815621 e + 03	x2.4899642 e + 03

Les λ_n

1.	2.	3.	4.	5.	6.
5.7258178 e − 01	8.8055992 e − 01	9.7582863 e − 01	9.9588549 e − 01	9.9935241 e − 01	9.9990188 e − 01
6.2791274 e − 02	3.5564063 e − 01	7.0996324 e − 01	9.1210742 e − 01	9.7986456 e − 01	9.9606164 e − 01
1.2374793 e − 03	3.5867688 e − 02	2.0513868 e − 01	5.1905484 e − 01	7.9992193 e − 01	9.4017339 e − 01
9.2009770 e − 06	1.1522328 e − 03	1.8203800 e − 02	1.1021099 e − 01	3.4356219 e − 01	6.4679195 e − 01
3.7179286 e − 08	1.8881549 e − 05	7.0814710 e − 04	8.8278764 e − 03	5.6015851 e − 02	2.0734922 e − 01
9.4914367 e − 11	1.9358522 e − 07	1.6551244 e − 05	3.8129172 e − 04	4.1820948 e − 03	2.7387166 e − 02
1.6715716 e − 13	1.3660608 e − 09	2.6410165 e − 07	1.0950871 e − 05	1.9330846 e − 04	1.9550007 e − 03
2.1544491 e − 16	7.0488855 e − 12	3.0737365 e − 09	2.2786389 e − 07	6.3591502 e − 06	9.4848766 e − 05
2.1207239 e − 19	2.7767898 e − 14	2.7281307 e − 11	3.6065493 e − 09	1.5822998 e − 07	3.4367833 e − 06
1.6466214 e − 22	8.6266788 e − 17	1.9085689 e − 13	4.4938297 e − 11	3.0917257 e − 09	9.7321160 e − 08
1.0343492 e − 25	2.1680119 e − 19	1.0797906 e − 15	4.5252285 e − 13	4.8757393 e − 11	2.2189805 e − 09
5.3650197 e − 29	4.4986573 e − 22	5.0431156 e − 18	3.7603029 e − 15	6.3402794 e − 13	4.1662263 e − 11
2.3367231 e − 32	7.8382450 e − 25	1.9775436 e − 20	2.6228187 e − 17	6.9173022 e − 15	6.5574786 e − 13
8.6674831 e − 36	1.1630367 e − 27	6.6033063 e − 23	1.5575942 e − 19	6.4235507 e − 17	8.7803771 e − 15
2.7709612 e − 39	1.4873466 e − 30	1.9002929 e − 25	7.9711081 e − 22	5.1393068 e − 19	1.0125783 e − 16
0.	1.6563614 e − 33	4.7620029 e − 28	3.5519080 e − 24	3.5797463 e − 21	1.0163838 e − 18
0.	1.6207613 e − 36	1.0485031 e − 30	1.3905716 e − 26	2.1905130 e − 23	8.9610464 e − 21
0.	0.	2.0444867 e − 33	4.8210691 e − 29	1.1869344 e − 25	6.9950907 e − 23
0.	0.	3.5551880 e − 36	1.4905449 e − 31	5.7350388 e − 28	4.8687451 e − 25
0.	0.	5.5475853 e − 39	4.1352414 e − 34	2.4864675 e − 30	3.0405184 e − 27
0.	0.	0.	1.0352225 e − 36	9.7273155 e − 33	1.7132439 e − 29
0.	0.	0.	0.	0.	0.
0.	0.	0.	0.	0.	0.
0.	0.	0.	0.	0.	0.
0.	0.	0.	0.	0.	0.

7.	8.	9.	10.	11.	12.
9.9998546 e − 01	9.9999787 e − 01	9.9999969 e − 01	9.9999996 e − 01	9.9999999 e − 01	1.0000000 e + 00
9.9929217 e − 01	9.9987898 e − 01	9.9997999 e − 01	9.9999677 e − 01	9.9999949 e − 01	9.9999992 e − 01
9.8570806 e − 01	9.9700462 e − 01	9.9941873 e − 01	9.9989273 e − 01	9.9998091 e − 01	9.9999670 e − 01
8.6456615 e − 01	9.6054568 e − 01	9.9039622 e − 01	9.9790124 e − 01	9.9957158 e − 01	9.9991663 e − 01
4.7705272 e − 01	7.4790284 e − 01	9.1013316 e − 01	9.7445778 e − 01	9.9371700 e − 01	9.9858732 e − 01
1.1572386 e − 01	3.2027663 e − 01	5.9909617 e − 01	8.2514635 e − 01	9.4136927 e − 01	9.8366430 e − 01
1.3055972 e − 02	6.0784427 e − 02	1.9693935 e − 01	4.4015011 e − 01	7.0394130 e − 01	8.8175663 e − 01
9.0657300 e − 04	6.1262894 e − 03	3.0565075 e − 02	1.1232482 e − 01	2.9607849 e − 01	5.5736081 e − 01
4.5623948 e − 05	4.1825206 e − 04	2.8466070 e − 03	1.4920175 e − 02	6.0370339 e − 02	1.8342927 e − 01
1.7774751 e − 06	2.1663088 e − 05	1.9230822 e − 04	1.3145890 e − 03	7.1417030 e − 03	3.1054179 e − 02
5.5526131 e − 08	8.9304272 e − 07	1.0194316 e − 05	8.8213430 e − 05	6.0469421 e − 04	3.3745471 e − 03
1.4251398 e − 09	3.0137350 e − 08	4.3973999 e − 07	4.7664454 e − 06	4.0395675 e − 05	2.7741888 e − 04
3.0622379 e − 11	8.4965846 e − 10	1.5795600 e − 08	2.1339628 e − 07	2.2179166 e − 06	1.8475085 e − 05
5.5928434 e − 13	2.0334083 e − 11	4.8068821 e − 10	8.0707164 e − 09	1.0243298 e − 07	1.0282524 e − 06
8.7926605 e − 15	4.1852675 e − 13	1.2564804 e − 11	2.6170188 e − 10	4.0455355 e − 09	4.8758791 e − 08
1.2026890 e − 16	7.4905020 e − 15	2.8533973 e − 13	7.3634903 e − 12	1.3840557 e − 10	1.9981456 e − 09
1.4445726 e − 18	1.1767148 e − 16	5.6843266 e − 15	1.8159383 e − 13	4.1453619 e − 12	7.1571886 e − 11
1.5359357 e − 20	1.6358709 e − 18	1.0016699 e − 16	3.9589753 e − 15	1.0966649 e − 13	2.2619074 e − 12
1.4559023 e − 22	2.0270123 e − 20	1.5727550 e − 18	7.6870812 e − 17	2.5823710 e − 15	6.3575326 e − 14
1.2380854 e − 24	2.2529462 e − 22	2.2145250 e − 20	1.3380681 e − 18	5.4488496 e − 17	1.6002320 e − 15
9.4989023 e − 27	2.2588880 e − 24	2.8123556 e − 22	2.1001719 e − 20	1.0363386 e − 18	3.6290304 e − 17
6.3410693 e − 38	5.7412040 e − 35	2.3265268 e − 32	4.9987005 e − 30	6.4253487 e − 28	5.4015219 e − 26
0.	0.	0.	0.	5.4863023 e − 38	1.1037482 e − 35
0.	0.	0.	0.	0.	0.
0.	0.	0.	0.	0.	0.

13.	14.	15.	16.	17.	18.
1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00
9.9999999 e − 01	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00
9.9999944 e − 01	9.9999991 e − 01	9.9999998 e − 01	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00
9.9998436 e − 01	9.9999715 e − 01	9.9999949 e − 01	9.9999991 e − 01	9.9999998 e − 01	1.0000000 e + 00
9.9970100 e − 01	9.9993948 e − 01	9.9998818 e − 01	9.9999776 e − 01	9.9999958 e − 01	9.9999992 e − 01
9.9595266 e − 01	9.9907074 e − 01	9.9979787 e − 01	9.9995783 e − 01	9.9999149 e − 01	9.9999833 e − 01
9.6225505 e − 01	9.8963945 e − 01	9.9741834 e − 01	9.9939756 e − 01	9.9986611 e − 01	9.9997138 e − 01
7.8874478 e − 01	9.2170099 e − 01	9.7594492 e − 01	9.9346756 e − 01	9.9836416 e − 01	9.9961326 e − 01
4.0633176 e − 01	6.6365081 e − 01	8.5371077 e − 01	9.4900699 e − 01	9.8478345 e − 01	9.9589845 e − 01
1.0588399 e − 01	2.7254759 e − 01	5.1899118 e − 01	7.5367260 e − 01	9.0120813 e − 01	9.6721066 e − 01
1.5487268 e − 02	5.7772021 e − 02	1.6922485 e − 01	3.7484512 e − 01	6.2548476 e − 01	8.2543081 e − 01
1.5807741 e − 03	7.5604029 e − 03	3.0214721 e − 02	9.8343344 e − 02	2.5013211 e − 01	4.8298471 e − 01
1.2703997 e − 04	7.3609236 e − 04	3.6365712 e − 03	1.5325905 e − 02	5.4203716 e − 02	1.5521339 e − 01
8.4414630 e − 06	5.8099164 e − 05	3.4130591 e − 04	1.7310585 e − 03	7.6061834 e − 03	2.8698205 e − 02
4.7534082 e − 07	3.8540665 e − 06	2.6544166 e − 05	1.5775571 e − 04	8.1779798 e − 04	3.7164510 e − 03
2.3057257 e − 08	2.1923715 e − 07	1.7585578 e − 06	1.2118149 e − 05	7.2740820 e − 05	3.8416435 e − 04
9.7549162 e − 10	1.0846150 e − 08	1.0092888 e − 07	8.0200884 e − 07	5.5289258 e − 06	3.3476998 e − 05
3.6359074 e − 11	4.7180556 e − 10	5.0802489 e − 09	4.6393027 e − 08	3.6561510 e − 07	2.5213492 e − 06
1.2039857 e − 12	1.8208273 e − 11	2.2646216 e − 10	2.3711707 e − 09	2.1297926 e − 08	1.6661751 e − 07
3.5675475 e − 14	6.2816688 e − 13	9.0124935 e − 12	1.0801803 e − 10	1.1034773 e − 09	9.7669046 e − 09
9.5186419 e − 16	1.9498859 e − 14	3.2240722 e − 13	4.4178809 e − 12	5.1252279 e − 11	5.1225654 e − 10
3.1773164 e − 24	1.3781710 e − 22	4.5947254 e − 21	1.2173462 e − 19	2.6337453 e − 18	4.7585812 e − 17
1.4501905 e − 33	1.3251429 e − 31	8.8515118 e − 30	4.4989186 e − 28	1.7978779 e − 26	5.8040997 e − 25
0.	0.	0.	3.1590168 e − 37	2.3233738 e − 35	1.3343537 e − 33
0.	0.	0.	0.	0.	0.

19.	20.	25.	30.	35.	40.
1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00
1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00
1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00
1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00
9.9999999 e − 01	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00
9.9999968 e − 01	9.9999994 e − 01	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00
9.9999408 e − 01	9.9999881 e − 01	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00
9.9991254 e − 01	9.9998093 e − 01	9.9999999 e − 01	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00
9.9896831 e − 01	9.9975345 e − 01	9.9999988 e − 01	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00
9.9042654 e − 01	9.9743251 e − 01	9.9999821 e − 01	1.0000000 e + 00	1.0000000 e + 00	1.0000000 e + 00
9.3461880 e − 01	9.7911569 e − 01	9.9997682 e − 01	9.9999999 e − 01	1.0000000 e + 00	1.0000000 e + 00
7.1923718 e − 01	8.7971361 e − 01	9.9974565 e − 01	9.9999983 e − 01	1.0000000 e + 00	1.0000000 e + 00
3.4534703 e − 01	5.8879338 e − 01	9.9766185 e − 01	9.9999783 e − 01	1.0000000 e + 00	1.0000000 e + 00
9.0528307 e − 02	2.2898871 e − 01	9.8251216 e − 01	9.9997547 e − 01	9.9999998 e − 01	1.0000000 e + 00
1.4751648 e − 02	5.0245996 e − 02	9.0214476 e − 01	9.9975907 e − 01	9.9999980 e − 01	1.0000000 e + 00
1.7952937 e − 03	7.4212338 e − 03	6.5129574 e − 01	9.9796698 e − 01	9.9999766 e − 01	1.0000000 e + 00
1.7967267 e − 04	8.5983868 e − 04	2.9167771 e − 01	9.8564508 e − 01	9.9997604 e − 01	9.9999998 e − 01
1.5383334 e − 05	8.3739541 e − 05	7.5468799 e − 02	9.2101083 e − 01	9.9978298 e − 01	9.9999978 e − 01
1.1493460 e − 06	7.0600702 e − 06	1.3031043 e − 02	7.0692287 e − 01	9.9828070 e − 01	9.9999766 e − 01
7.5908731 e − 08	5.2374892 e − 07	1.7588754 e − 03	3.5647890 e − 01	9.8836235 e − 01	9.9997777 e − 01
4.4748828 e − 09	3.4574493 e − 08	2.0082884 e − 04	1.0627740 e − 01	9.3662832 e − 01	9.9981076 e − 01
7.3154280 e − 16	9.7203030 e − 15	6.7594641 e − 10	4.7379571 e − 06	5.3273087 e − 03	4.8731168 e − 01
1.5483211 e − 23	3.4788064 e − 22	2.4882077 e − 16	1.3177338 e − 11	1.0489720 e − 07	1.7876070 e − 04
6.1447670 e − 32	2.3202540 e − 30	1.6231560 e − 23	5.8407336 e − 18	2.5646331 e − 13	2.2391506 e − 09
0.	0.	2.4836333 e − 31	5.8205690 e − 25	1.3022033 e − 19	2.2391506 e − 09

Programme qui trouverait les zéros de la fonction zeta comme valeurs propres d'un spectre (Denise Vella-Chemla, juin 2023)

On cherche à toucher du doigt ce "miracle"[1] qui consisterait à retrouver, comme indiqué dans les derniers articles d'Alain Connes et Henri Moscovici d'une part, et d'Alain Connes et Caterina Consani d'autre part, les zéros de la fonction zeta comme valeurs propres d'un opérateur en lien avec l'opérateur des fonctions prolates sphéroïdales. Ce que l'on a retenu de l'opérateur sphéroïdal prolate, c'est qu'il semblerait qu'il permette de contraindre le nombre de zéros d'une fonction sur un intervalle à être égal à une certaine valeur, cet opérateur procède à des sortes de confinements des nombres de zéros dans des intervalles emboîtés de plus en plus grands[2].

On ne comprend pas du tout la théorie développée dans les articles [1] et [2], il s'agit plutôt ici de tests de programmation. On souhaite d'abord réussir à obtenir par programme les mêmes valeurs numériques que celles fournies dans ces deux articles ou bien dans les diapositives des conférences de présentation de ces travaux, puis essayer de voir si on pourrait approcher davantage de zéros de la fonction zeta, en exécutant le programme pour des paramètres plus grands.

Cette démarche teste l'idée de Knuth, qui dit dans une interview des histoires contées de l'Université de Standford[3] :

> "*J'ai toujours pensé que la meilleure manière de comprendre quelque-chose était d'essayer de l'expliquer à un ordinateur. Vous ne réalisez à quel point vous en connaissez très peu sur un sujet que lorsque vous essayez de l'expliquer à quelqu'un qui ne connaît pas ce sujet et spécialement, lorsque vous essayez de l'expliquer à un ordinateur. Les ordinateurs ne font pas que hocher la tête et dire qu'ils ont compris. Les ordinateurs doivent comprendre...*"

On utilise le programme suivant pour les fonctions sphéroïdales prolates, écrit par J. Chemla, en janvier 2021[4] :

---

[1] Cf *Serendipity strikes again*, de F. Alberto Grünbaum, https://www.pnas.org/doi/10.1073/pnas.2207652119.

[2] Mais peut-être qu'on a mal compris.

[3] Voir la traduction de cette interview de Donald E. Knuth, *Histoire orale*, Université de Stanford, interview menée par Susan W. Schofield le 8 mai 2018 https://purl.stanford.edu/jq248bz8097 et traduction ici : http://denise.vella.chemla.free.fr/transc-Knuth-2018.pdf, cf. p. 42.

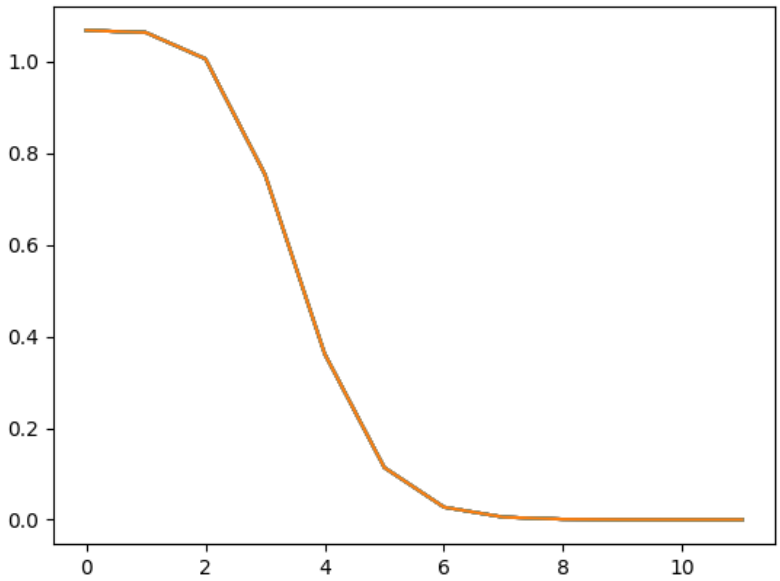
[4] Voir http://denise.vella.chemla.free.fr/pdf-Jacques.pdf. Les formules pour le calcul des fonctions d'onde sphéroïdales prolate sont à trouver à la page 111 dans la référence bibliographique *A review of prolate spheroidal wave functions from the perspective of spectral methods* de Li-Lian Wang, J. Math. Study, vol. 50, n° 2, p. 101-143, `doi:10.4208/jms.v50n2.17.01`. On obtient d'ailleurs des résultats similaires avec les formules similaires des articles tels que *Algorithm 840 : Computation of Grid Points, Quadrature Weights and Derivatives for spectral Element Methods Using Prolate Spheroidal Wave Functions—Prolate Elements*, J. P. Boyd, à la page 152 de ACM Transactions on Mathematical Software, Vol. 31, No. 1, March 2005, Pages 149–165 ou encore *A numerical study of the Legendre-Galerkin method for the evaluation of the prolate spheroidal wave functions*, S. Schmutzhard, T. Hrycak, H. G. Feichtinger, `https://doi.org/10.1007/s11075-014-9867-3`.

```
import math
from math import pi, sqrt
import matplotlib.pyplot as plt
import numpy as np

def solve_Sturm_Liouville(c, n):
    N = int (1.1*c + n + 100)
    A = np.zeros((N, N))
    for k in range(N):
        A[k,k] = k*(k+1)+(2*k*(k+1)-1)/((2*k+3)*(2*k-1))*c**2
        if k+2 in range(N):
            A[k,k+2] = A[k+2,k] = (k+1)*(k+2)/((2*k+3)*np.sqrt((2*k+1)*(2*k+5)))*c**2
    chi, beta = np.linalg.eigh(A)
    return chi, beta, A

def prolate(c, n):
    _, beta, _ = solve_Sturm_Liouville(c, n)
    coef = np.diag([np.sqrt(k + 1/2) for k in range(len(beta))]) @ beta
    psi = [np.polynomial.Legendre(coef[:, k]) for k in range(n+1)]
    lmb = [(-1)**(k//2) * np.sqrt(2) * (
        beta[0, k] / psi[k](0) if k % 2 == 0 else
        beta[1, k] / psi[k].deriv()(0) * c / np.sqrt(3)
    ) for k in range(n+1)]
    return lmb, psi

def test_Sturm_Liouville(c, n):
    chi, beta, A = solve_Sturm_Liouville(c, n)
    print(" Sturm-Liouville (c=:.2f,n=:d):N=:d".format(c,n,len(chi)).center(80,'-'))
    for k in range(n+1):
        mu, v = chi[k], beta[:, k]
        err = np.linalg.norm(A@v - mu*v)
        nrm = np.linalg.norm(v)
        print(k, ' --> ', chi[k], ' ---> ', 2*sqrt(chi[k]))

def test_Legendre(n):
    x = np.linspace(-1, 1, 500)
    for k in range(n):
        P = np.polynomial.Legendre.basis(k) * np.sqrt(k + 1/2)
        Q = P.convert(kind=np.polynomial.Polynomial)

c = 5.5
n = 11
test_Sturm_Liouville(2*pi*c, n)
test_Legendre(n)

lmb, psi = prolate(c, n)
print(" prolate (c = :.2f, n = :d) ".format(c, n).center(80, '-'))
for k, l in enumerate(lmb):
    plt.plot(lmb)
    print('lambda(:2d) = :.15f'.format(k, l))

plt.show()
```

Voici les résultats de ce programme pour certaines valeurs de μ ; ils ne sont pas identiques à ceux qu'on trouve dans l'article [2] et ils sont sûrement problématiques car les valeurs propres initiales dépassent 1. On ne sait pas comment modifier le programme pour qu'il y ait parfaite concordance.

Pour $\mu = 5.5$ et $n = 11$, on obtient :

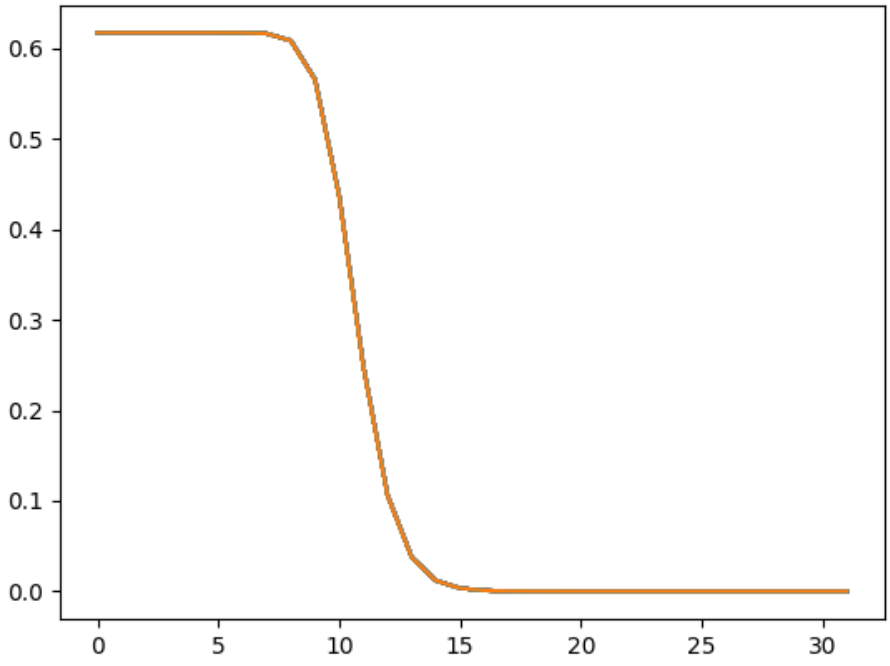
```
Invite de commandes

C:\Users\DENISE_2022\Desktop\donnes-numeriques>python3 schisme.py
---------------- Sturm-Liouville (c = 34.56, n = 11) : N = 149 -----------------
0  -->  33.80188564634639  --->  11.627877819507116
1  -->  101.89394432055506  --->  20.188506068607957
2  -->  168.95035825545474  --->  25.996181123807762
3  -->  234.94566225863076  --->  30.655874625176217
4  -->  299.8521878027104  --->  34.6324811587452
5  -->  363.63972821333545  --->  38.13868000932048
6  -->  426.27512824461667  --->  41.29286273653677
7  -->  487.72177453282455  --->  44.16884759795413
8  -->  547.9389537643357  --->  46.81619180430359
9  -->  606.8810306208757  --->  49.26991092424973
10  -->  664.4963742088509  --->  51.555654363371275
11  -->  720.7259232769846  --->  53.69267820762845
-------------------------- prolate (c = 5.50, n = 11) --------------------------
lambda( 0) = 1.068694704193759
lambda( 1) = 1.063992988597412
lambda( 2) = 1.006447812586847
lambda( 3) = 0.753643303365548
lambda( 4) = 0.362179480409258
lambda( 5) = 0.113779929316238
lambda( 6) = 0.027284099109160
lambda( 7) = 0.005470259037268
lambda( 8) = 0.000951448074434
lambda( 9) = 0.000146499345205
lambda(10) = 0.000020254774082
lambda(11) = 0.000002542181772
```



Si l'on met en regard les valeurs trouvées et les parties imaginaires des zéros non triviaux de la fonction zeta, comme le font Connes et Consani dans [2], on obtient :

λ_n	ζ_n
11.627877819507116	14.1347
20.188506068607957	21.022
25.996181123807762	25.0109
30.655874625176217	30.4249
34.6324811587452	32.9351
38.13868000932048	37.5862
41.29286273653677	37.5862
44.16884759795413	40.9187
46.81619180430359	43.3271
49.26991092424973	48.0052
51.555654363371275	49.7738
53.69267820762845	52.9703

Pour $\mu = 16.5$ et $n = 31$ (on souhaite aller jusqu'au zéro de la fonction zeta ζ_{31} égal à 0.5+103.7255), on obtient le graphique suivant :



et les valeurs suivantes pour les valeurs propres, que l'on met comme le font Connes et Consani dans [2] en regard des parties imaginaires des zéros non triviaux de ζ (on reporte le résultat du programme dans le tableau ci-dessous) :

---------- Sturm-Liouville (c = 103.67, n = 31) : N = 245 ----------

χ_n	$2\sqrt{\chi_n}$	ζ_n
102.92072677653609	20.289970603875805	14.1347
309.2584733282111	35.171492622759764	21.022
514.5850515688494	45.36893437447476	25.0109
718.8928581575877	53.62435484581937	30.4249
922.1740962957962	60.734639088276346	32.9351
1124.4207674701395	67.06476772404835	37.5862
1325.6246626978739	72.81825767478576	40.9187
1525.7773532354743	78.12240019957078	43.3271
1724.8701807078735	83.06311288912482	48.0052
1922.8942466111068	87.70163616743092	49.7738
2119.8404011368652	92.08344913472486	52.9703
2315.69923126167	96.24342536010799	56.4462
2510.461048037919	100.20900255042795	59.347
2704.1158730168577	104.00222830337546	60.8318
2896.653423726532	107.64113384253311	65.1125
3088.063098118746	111.140687385291	67.0798
3278.3339578897003	114.51347445413924	69.5464
3467.454710567861	117.770195050664	72.0672
3655.41369025025	120.92003457244378	75.7047
3842.198836854009	123.9709455776475	77.1448
4027.797673733609	126.92986526004995	79.3374
4212.197283495892	129.80288569205067	82.9104
4395.384281822778	132.5953887859269	84.7355
4577.3447890874295	135.31215450339158	87.4253
4758.064399520176	137.95744850525725	88.8091
4937.528147647454	140.53509380432283	92.4919
5115.720471687653	143.0485298307907	94.6513
5292.625173542325	145.50086148944033	95.8706
5468.225374967145	147.89490018208397	98.8312
5642.503469443964	150.233198321063	101.3179
5815.441069199909	152.51807852448061	103.7255

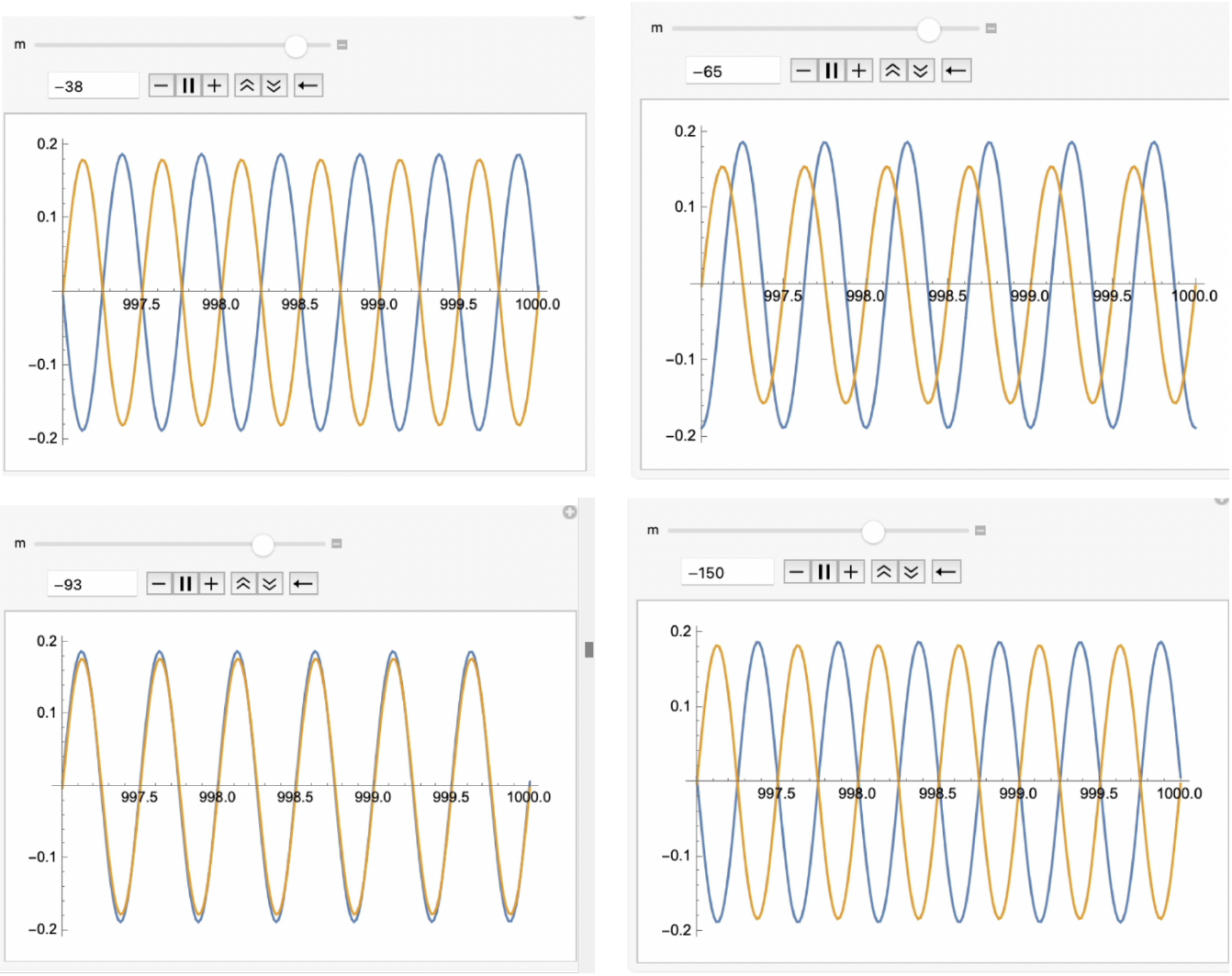
---------- prolate (c = 16.50, n = 31) ----------

λ_n	valeur	λ_n	valeur	λ_n	valeur	λ_n	valeur
λ_0	0.617089223310524	λ_1	0.617089223305512	λ_2	0.617089223009061	λ_3	0.617089211995113
λ_4	0.617088924550819	λ_5	0.617083356561762	λ_6	0.617001116618567	λ_7	0.616071330346991
λ_8	0.608297170629556	λ_9	0.565443877741659	λ_{10}	0.436665671887785	λ_{11}	0.248499294161039
λ_{12}	0.106015042181635	λ_{13}	0.037510655381883	λ_{14}	0.011792705842498	λ_{15}	0.003390334495125
λ_{16}	0.000903079023335	λ_{17}	0.000224653060628	λ_{18}	0.000052494332871	λ_{19}	0.000011574715711
λ_{20}	0.000002417378221	λ_{21}	0.000000479740690	λ_{22}	0.000000090719657	λ_{23}	0.000000016386606
λ_{24}	0.000000002833430	λ_{25}	0.000000000469915	λ_{26}	0.000000000074882	λ_{27}	0.000000000011484
λ_{28}	0.000000000001697	λ_{29}	0.000000000000242	λ_{30}	0.000000000000034	λ_{31}	0.000000000000005

Les espoirs suscités par l'approximation des valeurs des parties imaginaires des zéros non triviaux de zeta pour le cas $\mu = 5.5$ sont brutalement refroidis par le cas $\mu = 16.5$ pour pouvoir approximer davantage de zéros.

Dans 4 diapositives d'une présentation par Alain Connes des résultats que lui et ses collaborateurs ont obtenus récemment et qui sont reproduites ci-dessous, il semblerait que les valeurs propres

obtenues correspondent au fait que deux ondes soit coïncident, soit sont en opposition totale de phase. Ci-dessous, la valeur -65 n'apparaît pas dans la liste des valeurs propres parce qu'elle ne met pas les ondes en opposition ou coïncidence de phase.



Les valeurs propres obtenues par Alain Connes sont fournies dans les transparents d'une conférence que j'avais pu télécharger au moment de cette conférence mais dont je ne trouve plus trace (!) sur la toile et que j'ai déposés ici http://denise.vella.chemla.free.fr/transparents-AC-prolate.pdf, à la page 53/125 :

The first approximate negative eigenvalues of W are

$-39, -94, -152, -211, -279, -342, -416, -489, -561, -639, -718, -800, -887, -971,$

$-1058, -1148, -1242, -1337, -1433, -1528, -1627, -1728, -1834, -1940, -2044, -2155,$
$-2262, -2375, -2491, -2606, -2723, -2842, -2964, -3084, -3205, -3330, -3461, -3586,$
$-3716, -3845, -3977, -4112, -4245, -4381, -4523, -4662, -4803, -4943, -5088, -5232,$
$-5382, -5527, -5677, -5823, -5977, -6129, -6287, -6440, -6600, -6753, -6915, -7075,$
$-7240, -7402, -7562, -7730, -7902, -8064, -8237, -8408, -8581, -8748, -8924, -9100,$
$-9278, -9456, -9638, -9816, -10000, -10179, -10363, -10549, -10734, -10923, -11114,$
$-11299, -11491, -11681, -11876, -12066, -12267, -12459, -12660, -12860, -13059,$
$-13254, -13464, -13660, -13865, -14069, -14279, -14484, -14694, -14900, -15113,$
$-15326, -15543, -15753, -15967$

The comparison of $2\sqrt{-z}$ with the zeros of zeta then gives

L'obtention des approximations des zéros de la fonction ζ à partir des valeurs propres λ_n consiste à calculer $2\sqrt{\lambda_n}$ pour les λ_n négatives ; on a par exemple :

$$2\sqrt{-39} = 12.49i$$
$$2\sqrt{-94} = 19.39i$$

Si on raisonne inversement[5], il faudrait que l'opérateur soit capable de trouver les valeurs propres suivantes, pour mieux approcher les parties imaginaires des zéros non triviaux de la fonction ζ (on a calculé $f(x) = (\mathfrak{Re}(\zeta_x)/2)^2$ pour les 103 premiers zéros). Ce tableau doit être lu ligne par ligne.

49.94761370809672	110.48153764352064	156.38574922358276	231.41827181847404	271.1795704470434
353.180197146746	418.5853913987703	469.3088197724447	576.1236277809061	619.3585998788465
701.4637393631045	796.5447197695586	880.517907961705	925.1263196167948	1059.9108481033418
1124.9252451682091	1209.175497742996	1298.418803819659	1432.800048460991	1487.8315873130678
1573.6047687759221	1718.5328133423989	1795.0259426628136	1910.7946602950894	1971.7645583724961
2138.6878576687845	2239.719232169215	2297.7946268315004	2441.9012376485803	2566.326733104896
2689.74681044668	2779.747578284837	2871.277805791653	3081.8894407329944	3128.9848414920657
3267.278227539478	3377.160304601704	3527.8125234778768	3682.6768107758035	3778.98070833449
3859.939239311902	4065.1261669122364	4197.660145534928	4295.995521095704	4455.411459580152
4539.829230227787	4769.010268202413	4881.552023077732	4978.975197863942	5120.250102616045
5329.071721775203	5433.367935311849	5629.014747667726	5694.608346330363	5854.1392290027925
6092.810112077736	6209.250236676248	6308.329685515108	6495.4705399378045	6644.753075276554
6850.630318829933	6987.659242703959	7148.23878590651	7217.519937785038	7517.890249521409
7634.756863746298	7782.894934258316	7954.624901230262	8092.485305552848	8299.85486245202
8544.642215556116	8611.727125661113	8763.667362944732	8969.620290000345	9218.559188268915
9319.94520635395	9532.143785103477	9690.087275518297	9802.515716545486	10126.875093740156
10250.913954814292	10423.355517764887	10546.745409692086	10806.253121180875	10980.578356274887
11203.255326592458	11379.333673779616	11507.60860633237	11682.317344718927	11997.652942534442
12178.768849561242	12257.889340612324	12544.784040766575	12654.374094844668	12930.128329563819
13148.91228541734	13369.162443504118	13454.519330103598	13653.15178918165	13985.927804751942
14133.62188288285	14346.70670884627	14526.17411856633		

[5]Il y a notamment des articles bibliographiques de référence pour le problème dit "problème inverse des valeurs propres" de Françoise Chatelin née Laborde, Paul Morel, Ole H. Hald ou Shmuel Friedland.

Les résultats numériques de l'article [2] sont les suivants (on rappelle qu'on regarde les valeurs propres inférieures à $2\pi\mu$, i.e. inférieures à 34.44 pour $\mu = 5.5$ par exemple, puis etc).[6] :

$\mu =$	5.5	$\mu =$	6.5	$\mu =$	7.5
5	0.99999999999647719857	7	0.99999999998668315975	9	0.99999999996397226733
6	0.99999998894391115741	8	0.99999999731589077585	10	0.99999999453062631606
7	0.99999980631702676769	9	0.99999963978717981581	11	0.99999941709770526957
8	0.99997809227622865324	10	0.99996808936687677767	12	0.99995709581648305854
9	0.99852183576050441685	11	0.99821407841789989100	13	0.99792322303841470726
10	0.95065832620623051607	12	0.94788066237037484836	14	0.94552083061302325507
11	0.57197061534624863399	13	0.57534099083086049406	15	0.57809629788957190907
12	0.139174533954574303539	14	0.14710511279564130503	16	0.15383636015962926720

Les valeurs propres pour les différentes valeurs de μ sont :

pour $\mu = 5.5$, λ_j	pour $\mu = 6.5$, λ_j	pour $\mu = 7.5$, λ_j	ζ_j
14.781	13.936	15.06	14.1347
21.701	20.58	21.683	21.022
25.547	24.69	24.948	25.0109
29.345	30.194	30.979	30.4249
33.168	33.454	33.243	32.9351
	36.826	37.406	37.5862
	40.259	40.514	40.9187
		43.643	43.3271
		46.658	48.0052

Pour des valeurs plus grandes du paramètre μ, à la recherche de toujours plus d'approximations de zéros de la fonction ζ.

$\mu =$	8.5	$\mu =$	9.5	$\mu =$	10.5
11	0.99999999992101000288	13	0.99999999984990646525	15	0.99999999974270022369
12	0.99999999034148375362	14	0.99999998455736228573	16	0.99999997703659571104
13	0.99999913999089362040	15	0.99999881131048713492	17	0.99999843436641476606
14	0.99994536408530411219	16	0.99993308190344158164	18	0.99992039045021729410
15	0.99764801726717553636	17	0.99738707752987412262	19	0.99713907784499135361
16	0.94347292951033144975	18	0.94166650390462098514	20	0.94005235637340584775
17	0.58041289343441020661	19	0.58240244869697875785	21	0.58413979804862029634
18	0.15967051202562674536	20	0.16480962032526478957	22	0.16935919615152177689

Les valeurs propres pour ces nouvelles valeurs de μ sont :

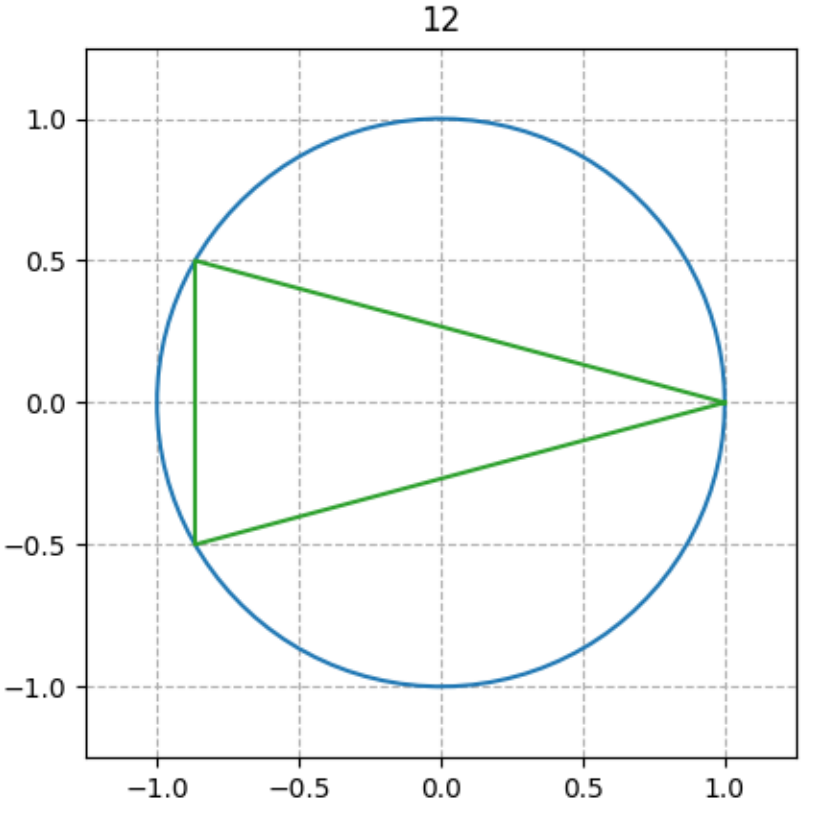
[6] Voir si on calcule bien Prolate$(2\pi\mu, \frac{x}{\sqrt{\mu}})$.

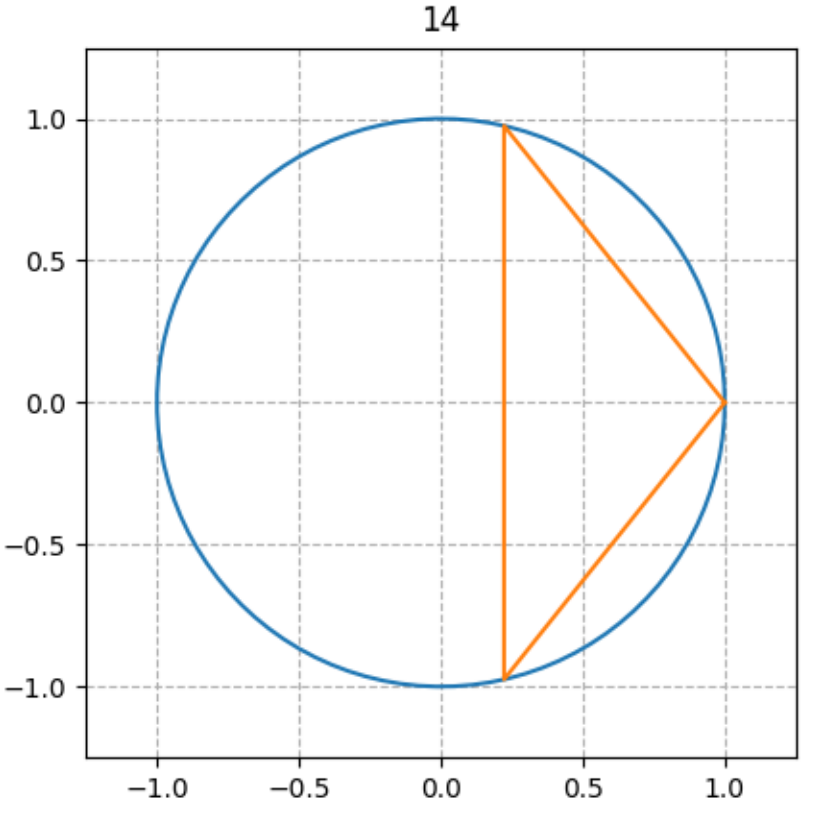
pour $\mu = 8.5$, λ_j	pour $\mu = 9.5$, λ_j	pour $\mu = 10.5$, λ_j	ζ_j
14.887	13.998	14.45	14.1347
20.778	21.501	21.455	21.022
25.535	25.121	25.356	25.0109
29.928	30.689	30.345	30.4249
32.473	33.583	32.6	32.9351
37.965	37.813	37.41	37.5862
41.088	41.272	40.387	40.9187
43.741	43.05	42.895	43.3271
46.685	47.319	48.095	48.0052
49.91	50.19	50.346	49.7738
52.845	53.026	53.272	52.9703
	55.731	56.05	56.4462
	58.581	58.737	59.347
		61.386	60.8318
		63.849	65.1125

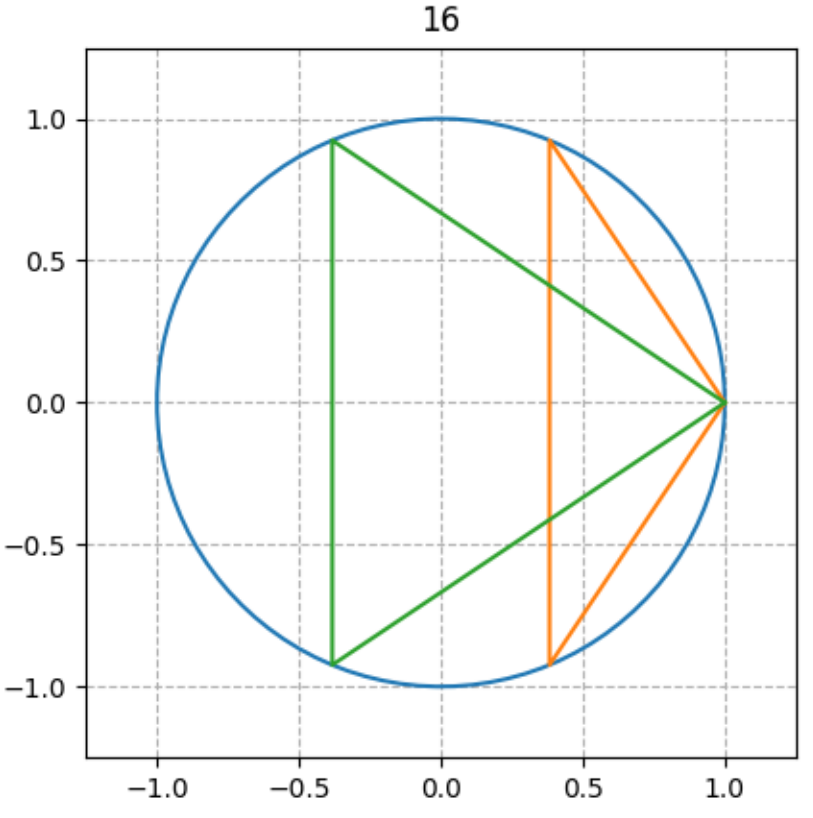
Bibliographie

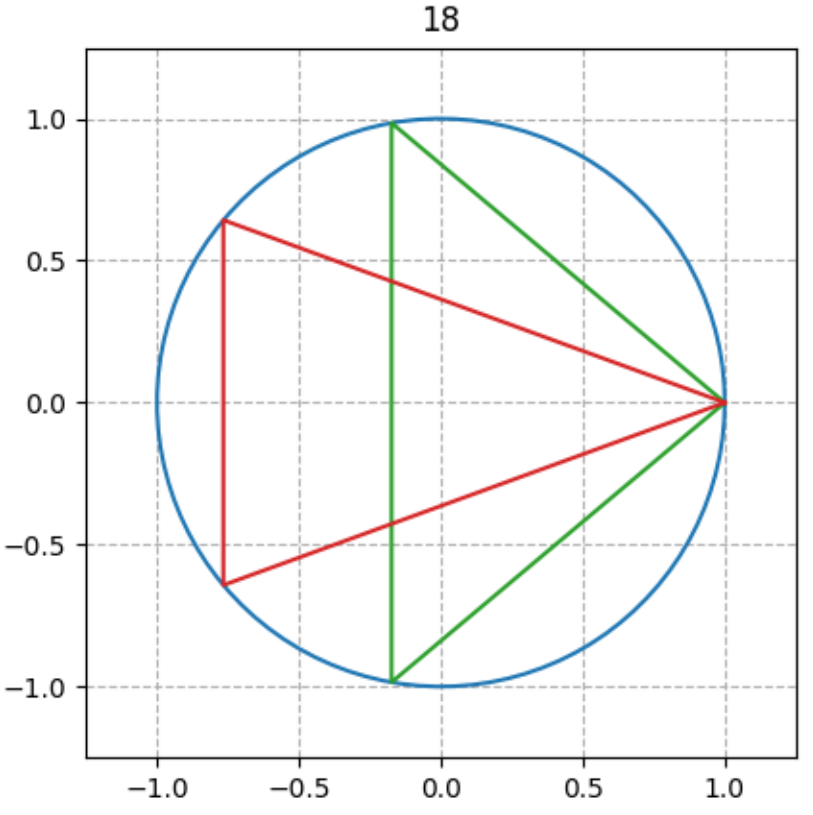
[1] Alain Connes, Henri Moscovici, The UV prolate spectrum matches the zeros of zeta, PNAS, vol. 119, n° 22, éd. Robion Kirby, Université de Californie, Berkeley, CA, États-Unis, https://www.pnas.org/doi/abs/10.1073/pnas.2123174119.

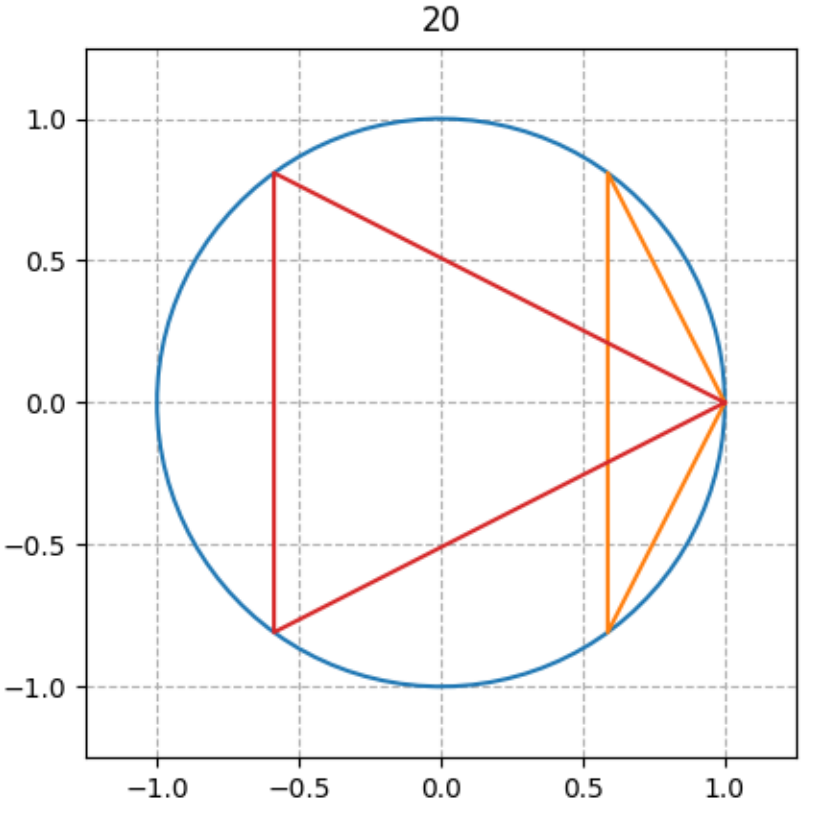
[2] Alain Connes, Caterina Consani, Spectral triples and zeta cycles, Fondation L'enseignement mathématique, Vol. 69, n°1/2, $EMS Press, pp.93–148, 2023 https://ems.press/journals/lem/articles/11033001, https://doi.org/10.4171/LEM/1049$.

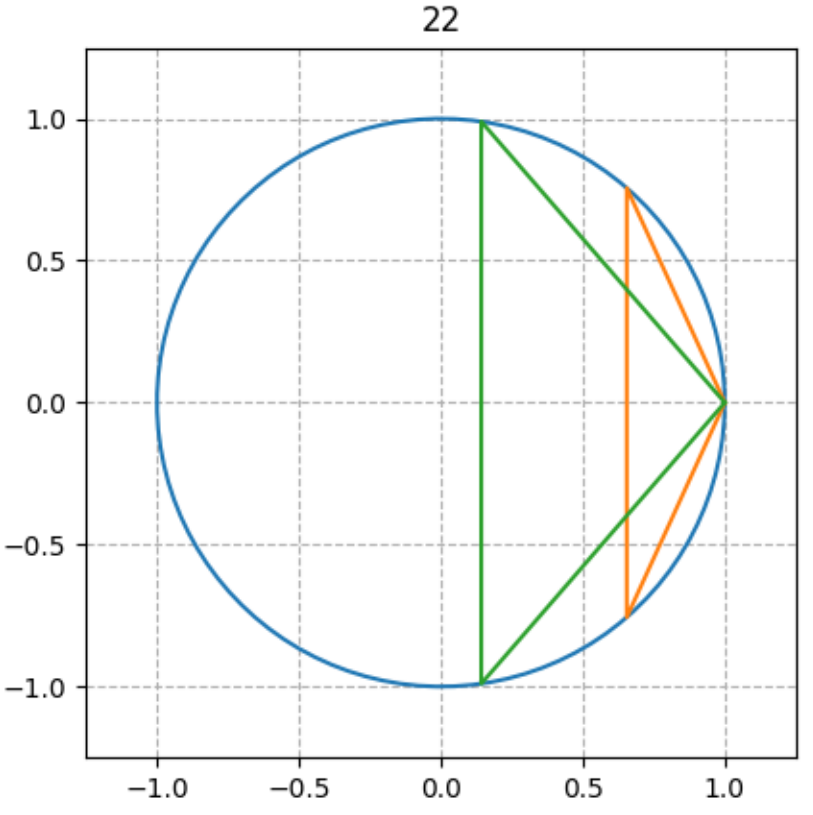

12
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

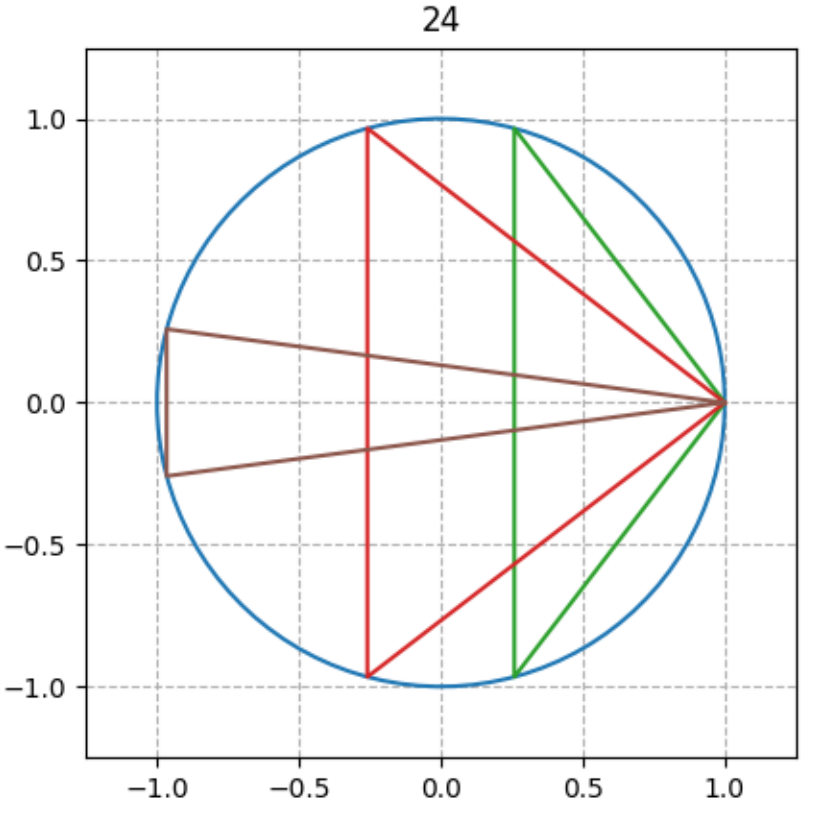

14
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

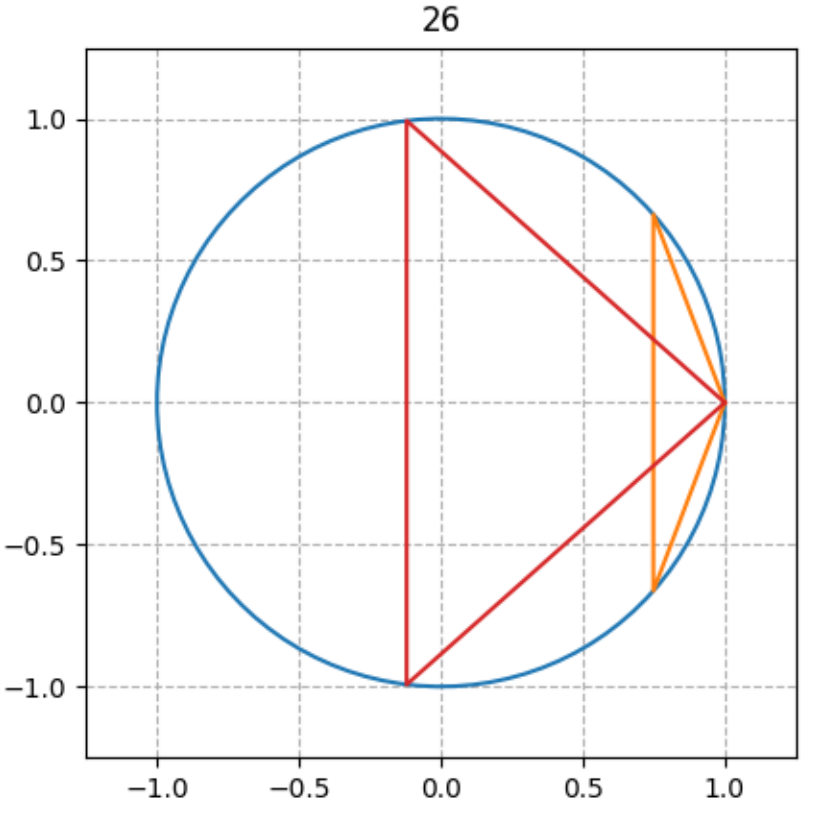

16
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

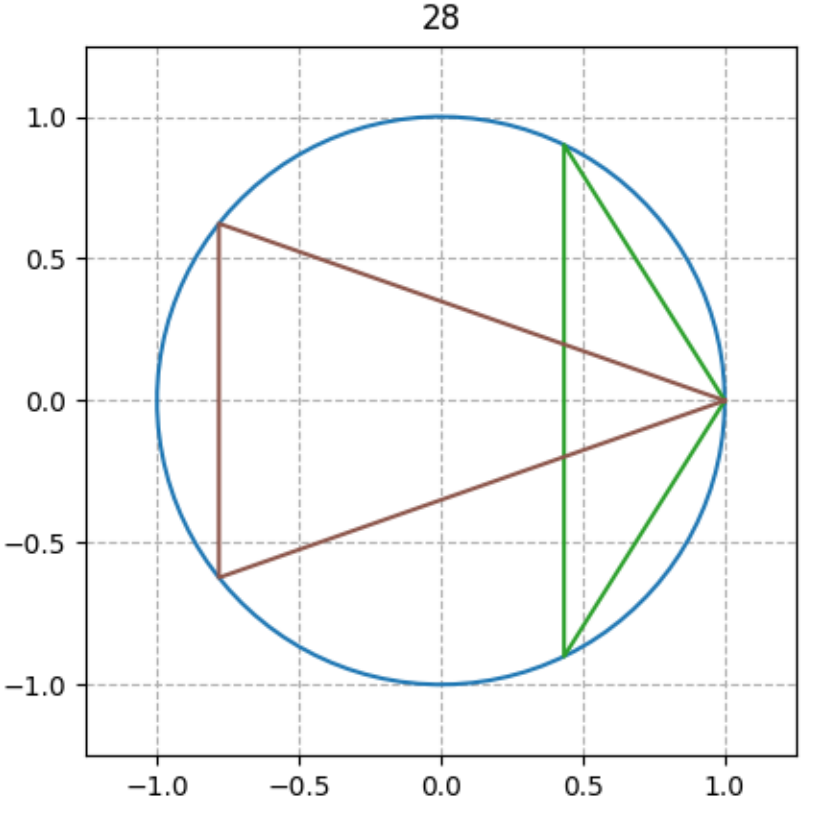

18
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

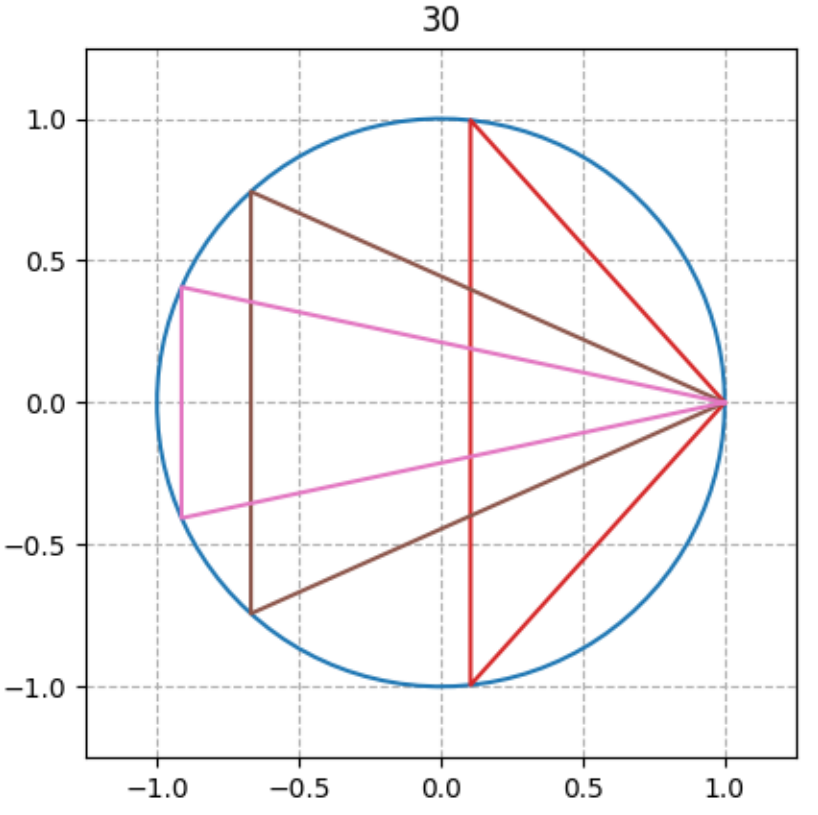

20
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

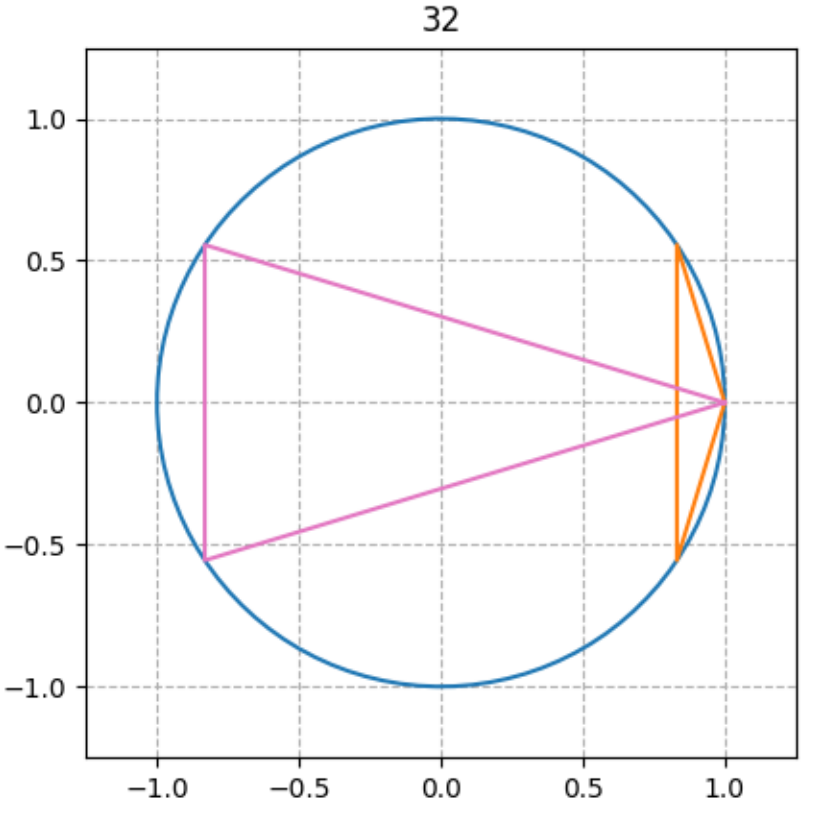

22
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

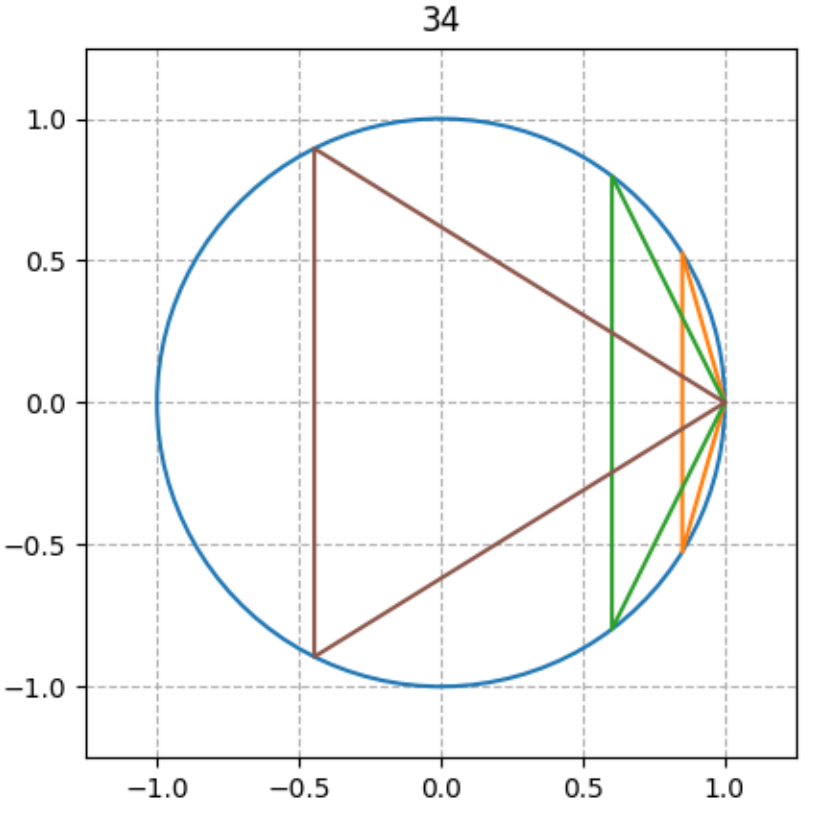

24
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

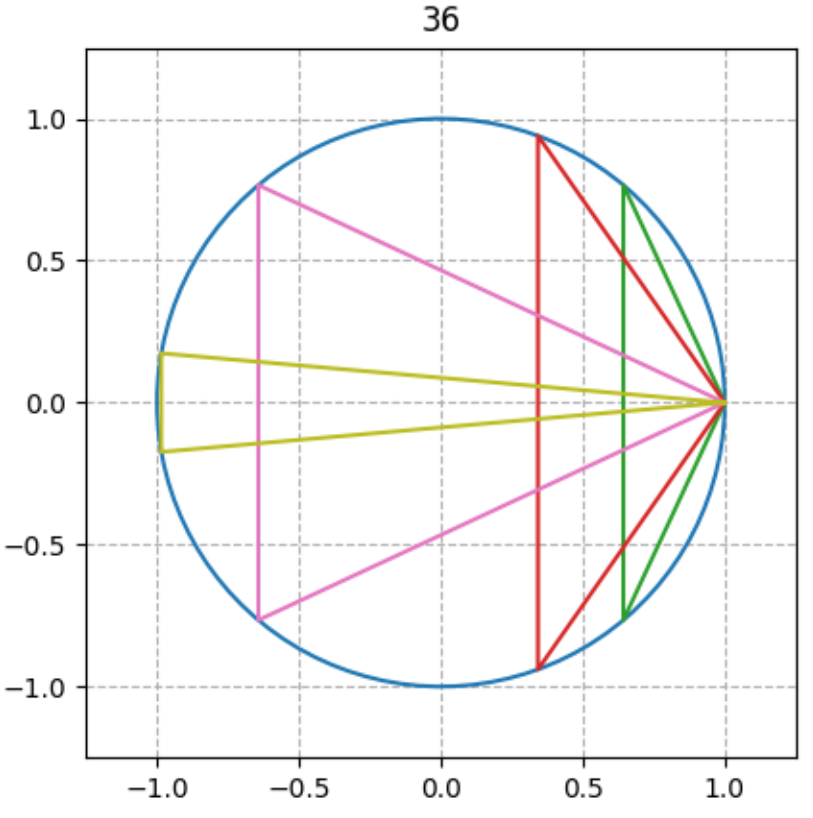

26
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

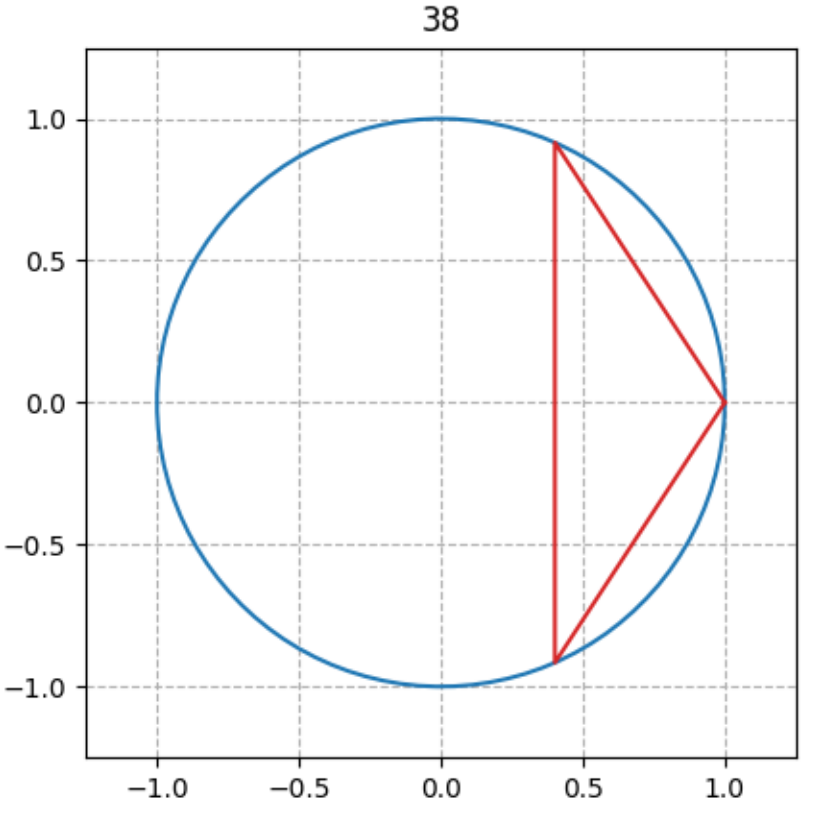

28
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

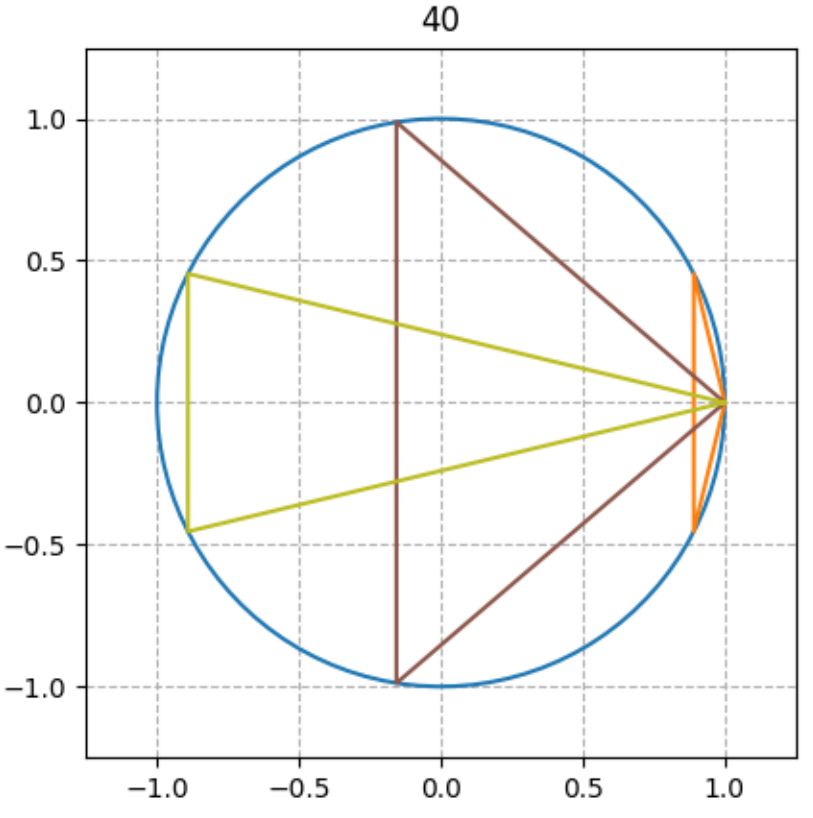

30
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

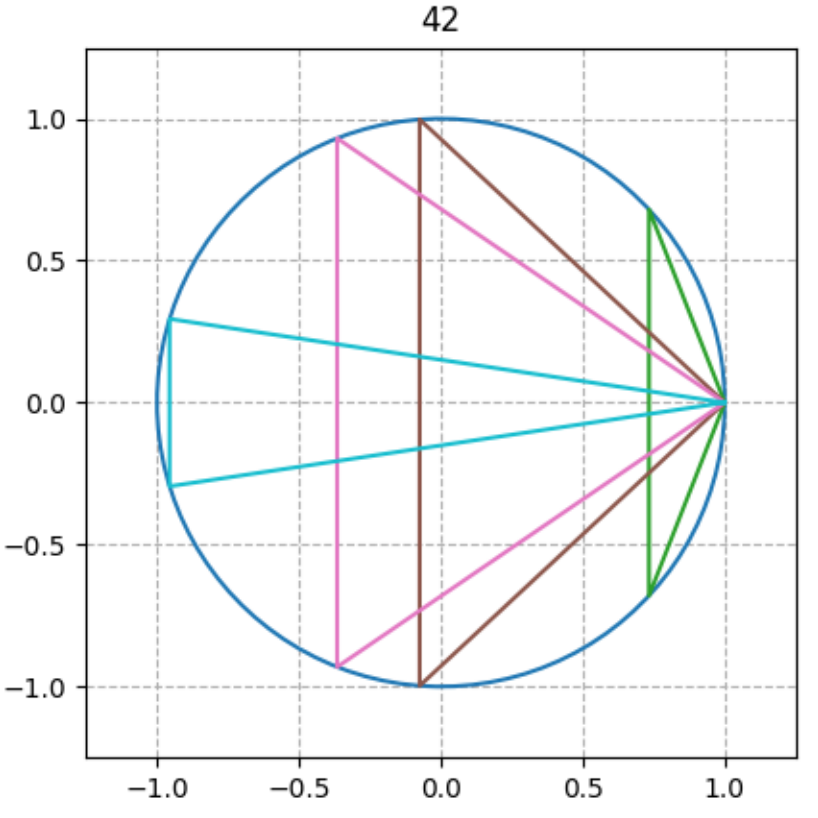

32
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

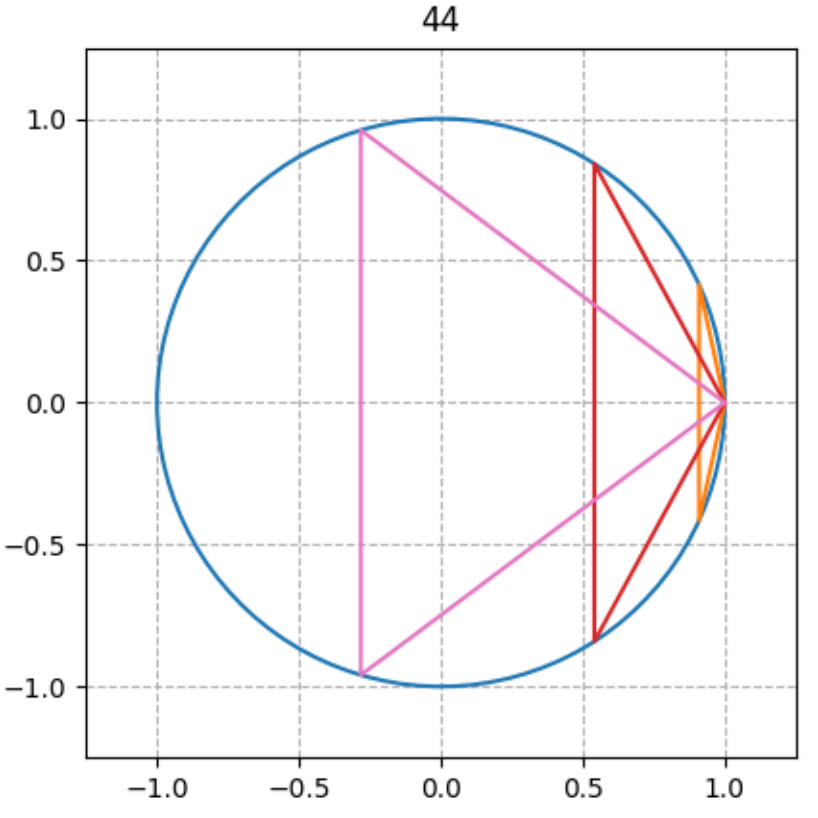

34
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

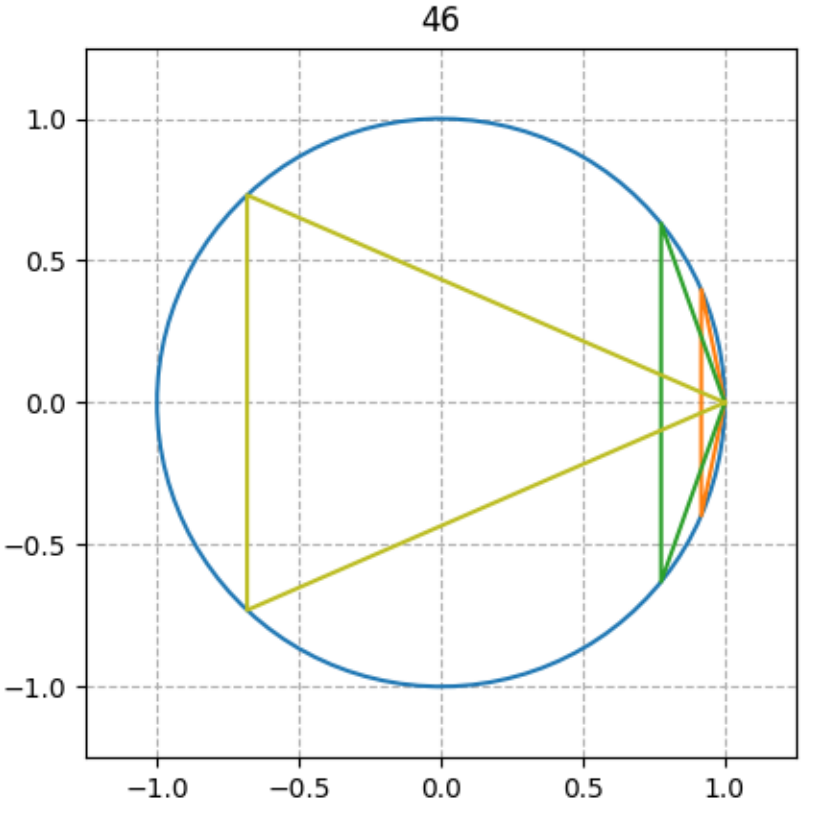

36
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

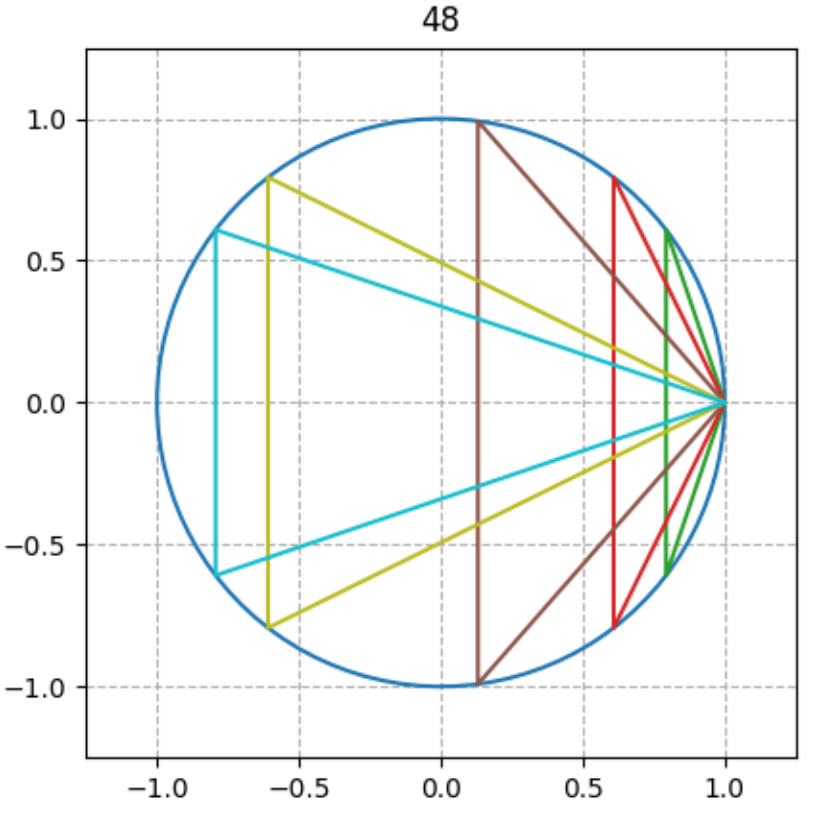

38
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

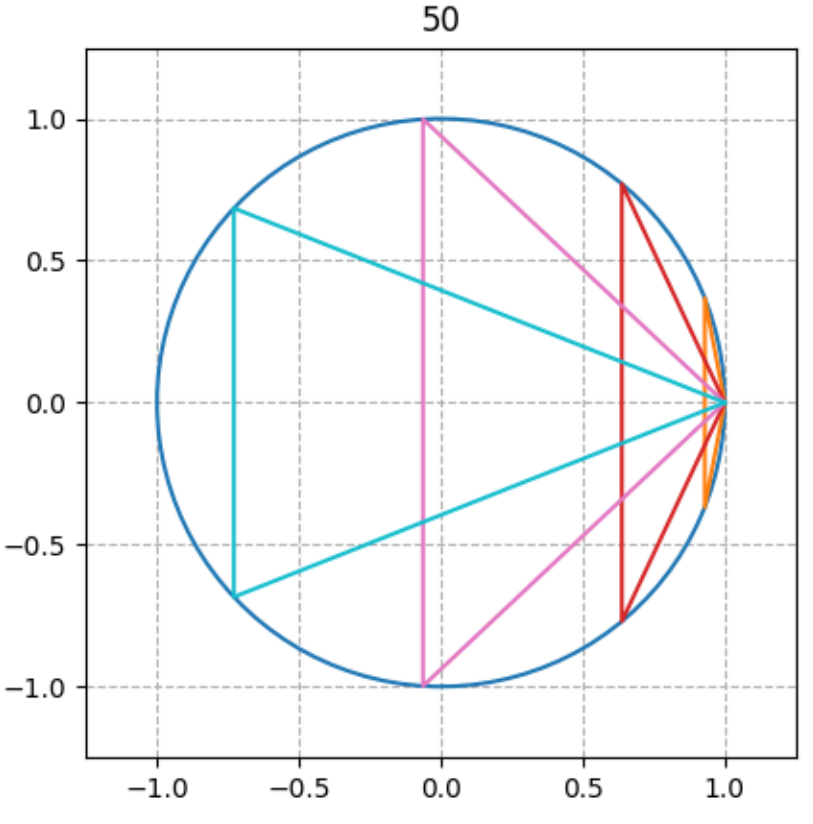

40
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

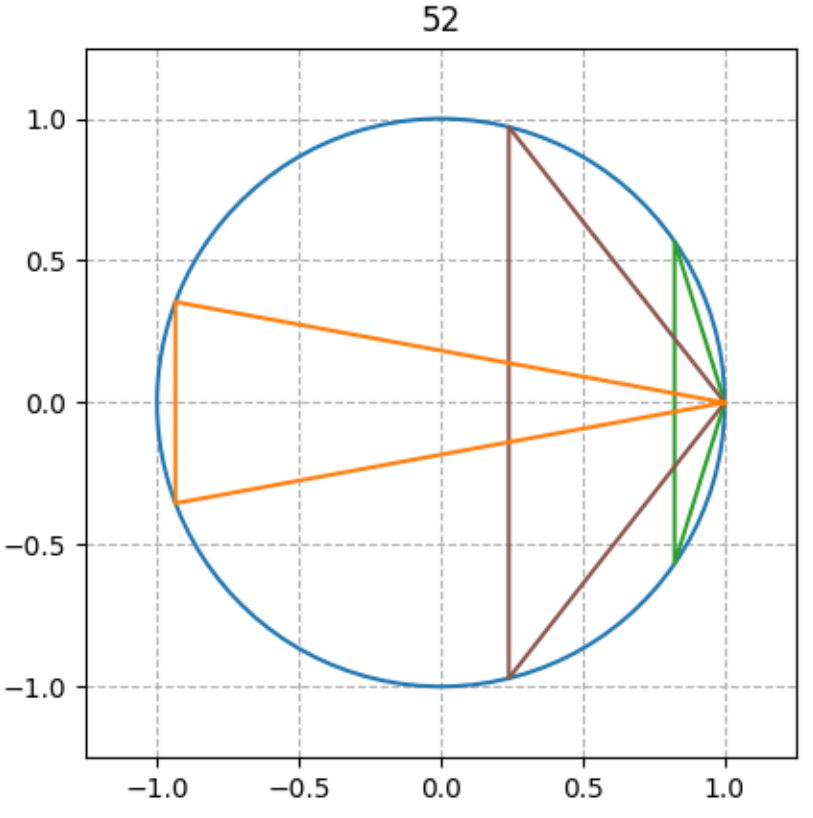

42
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

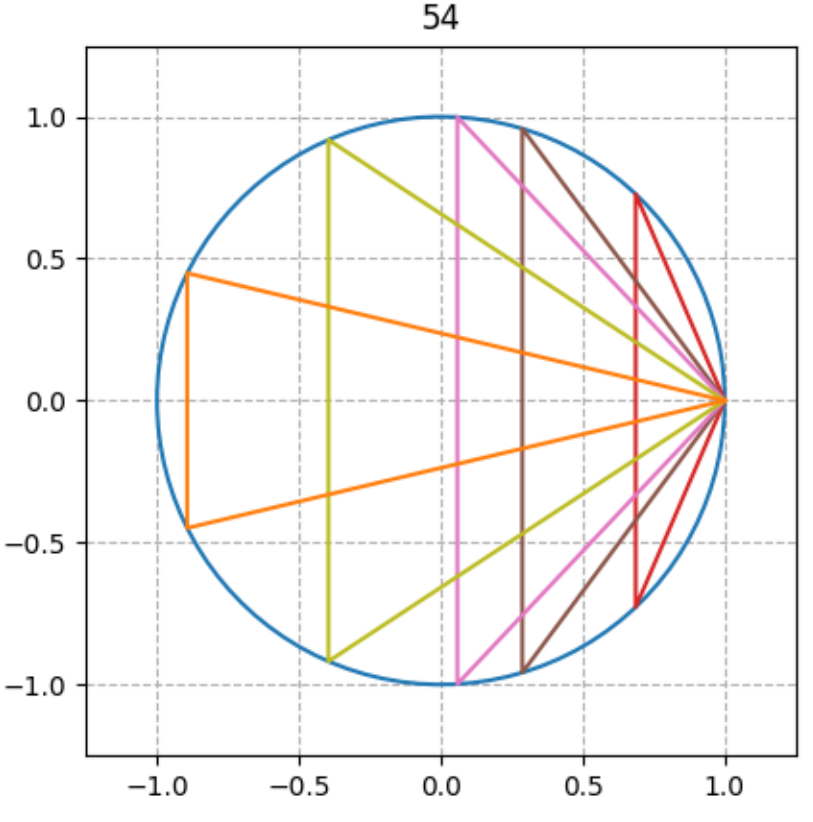

44
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

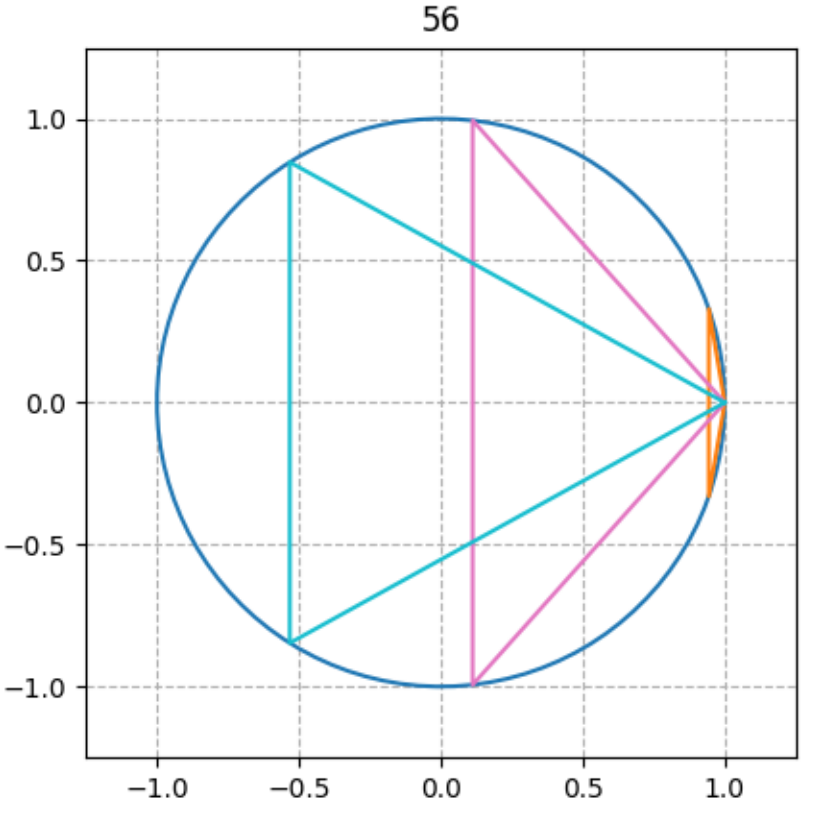

46
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

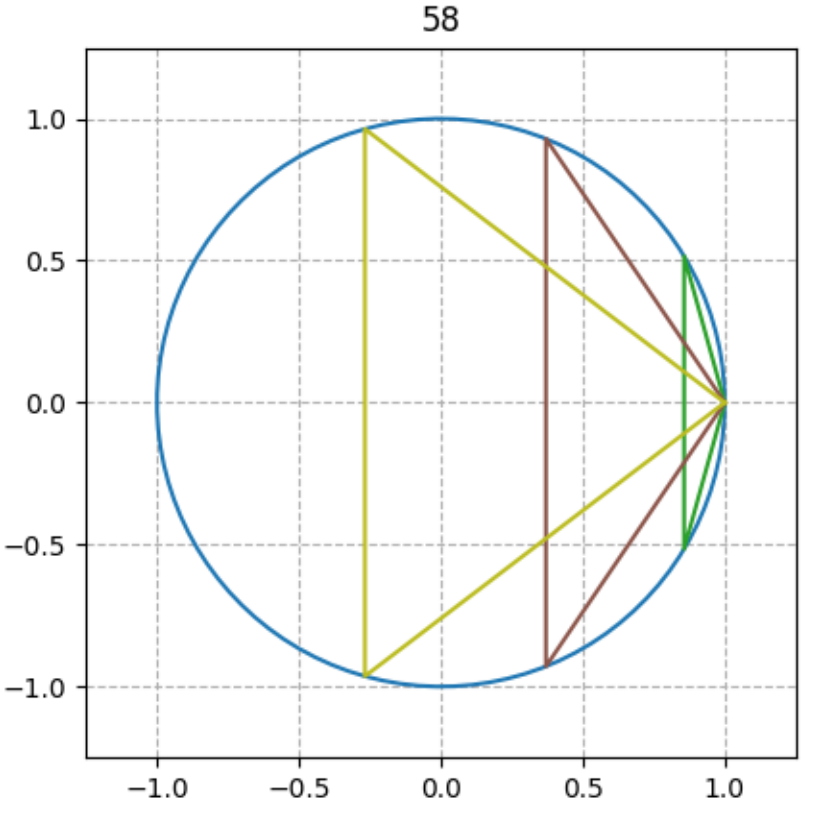

48
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

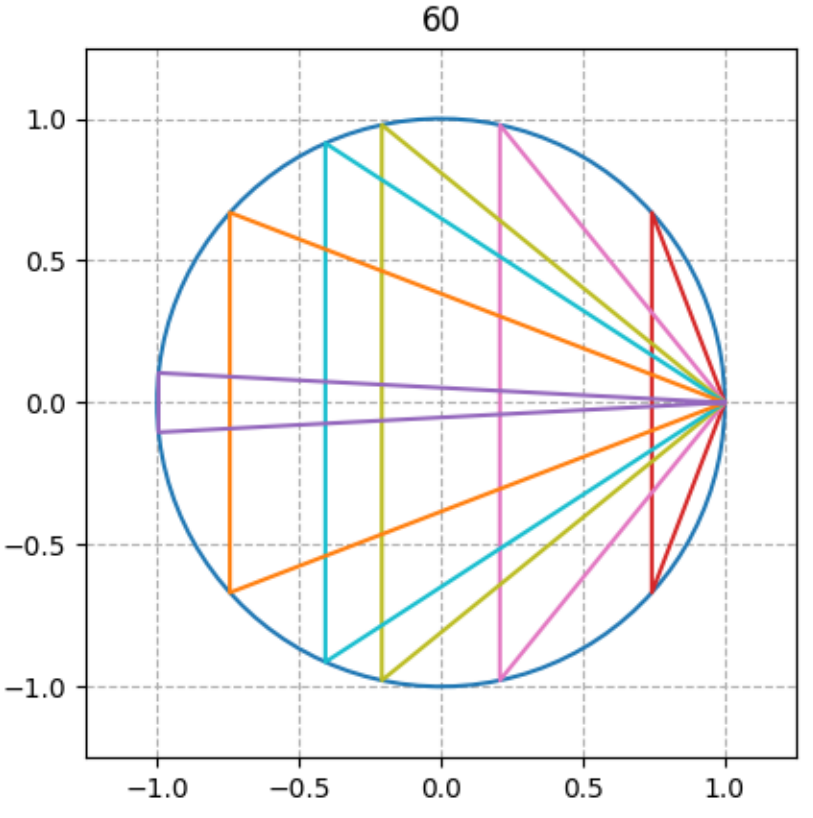

50
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

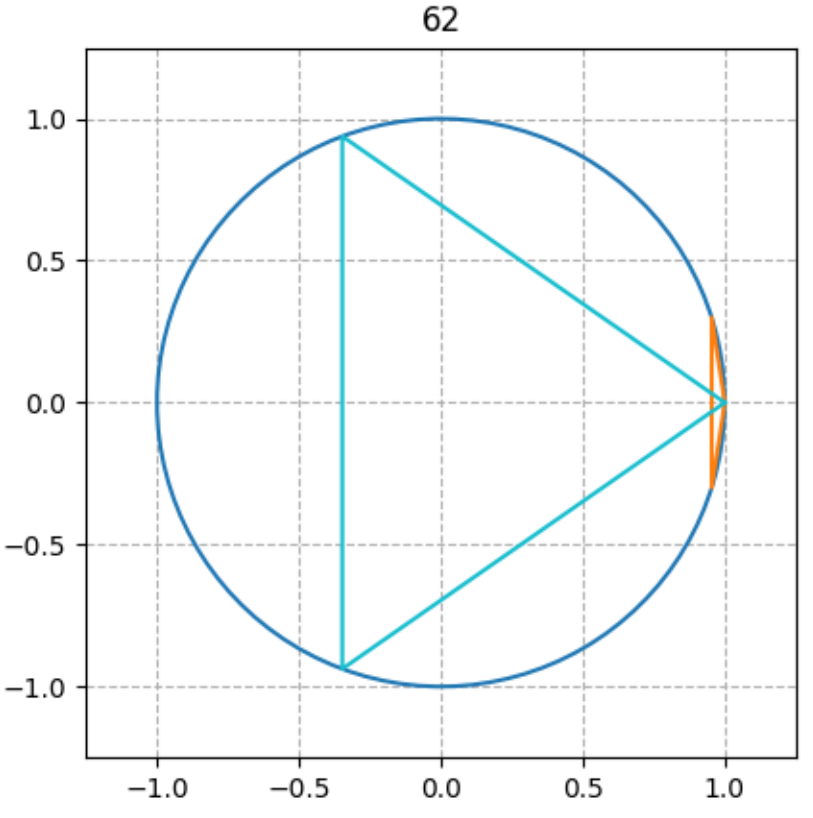

52
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

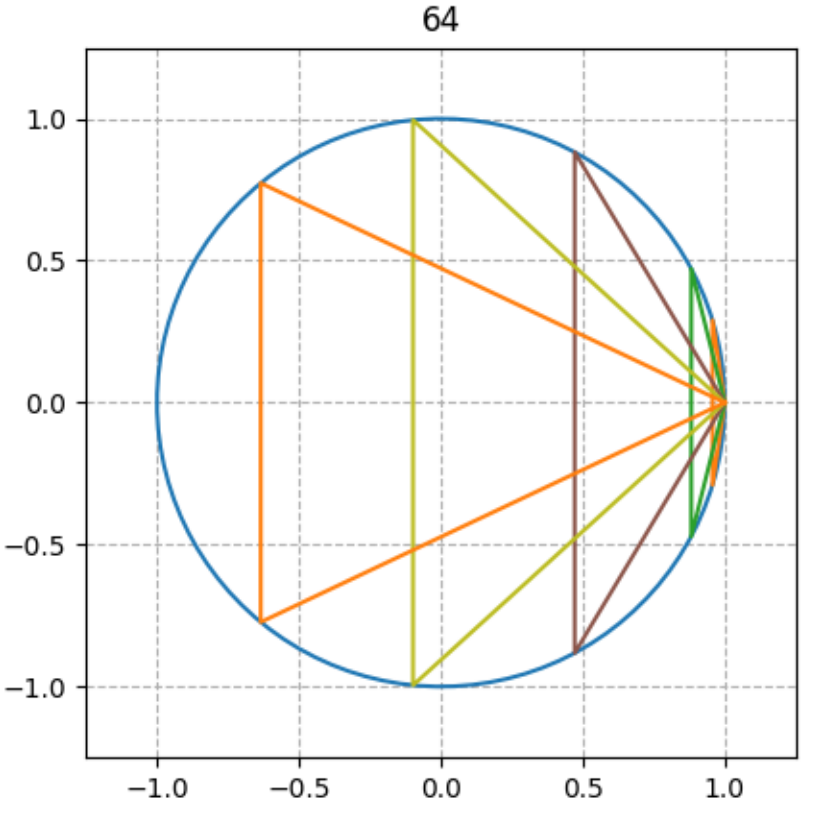

54
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

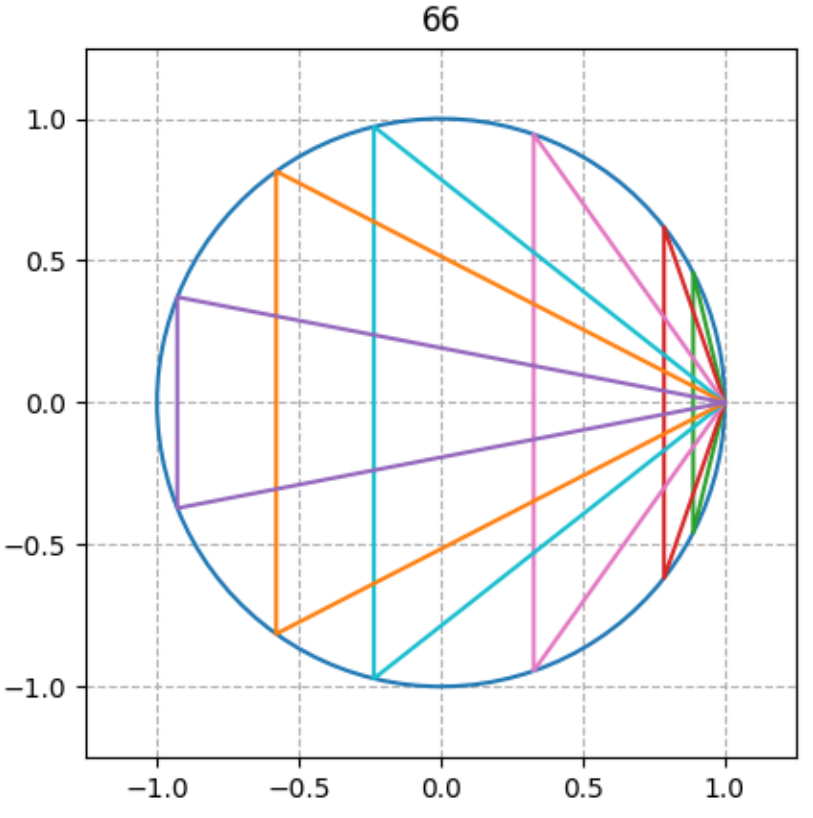

56
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

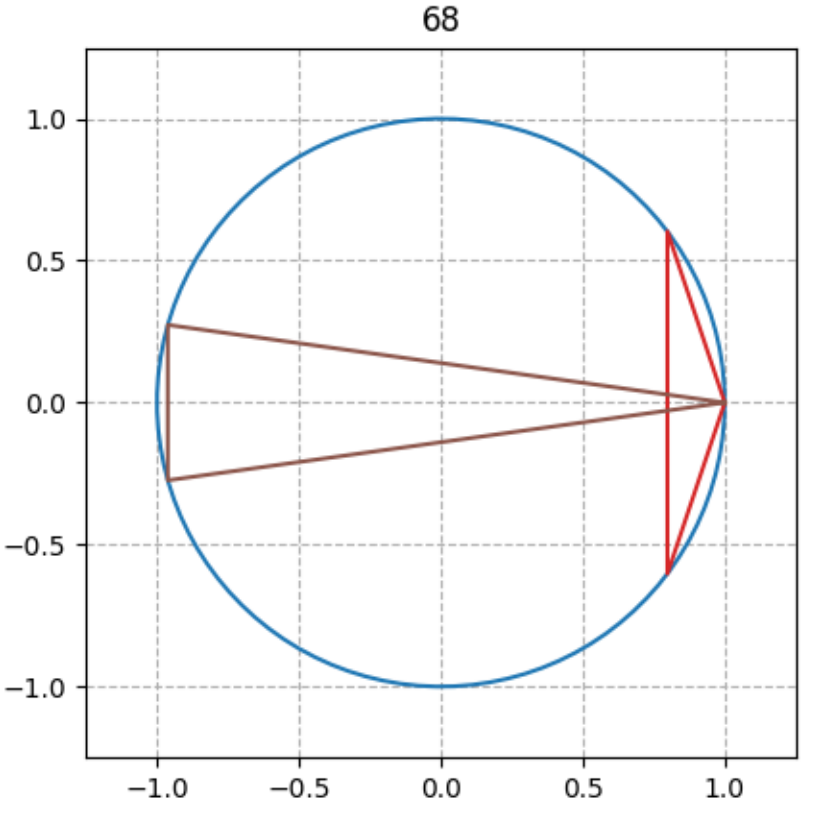

58
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

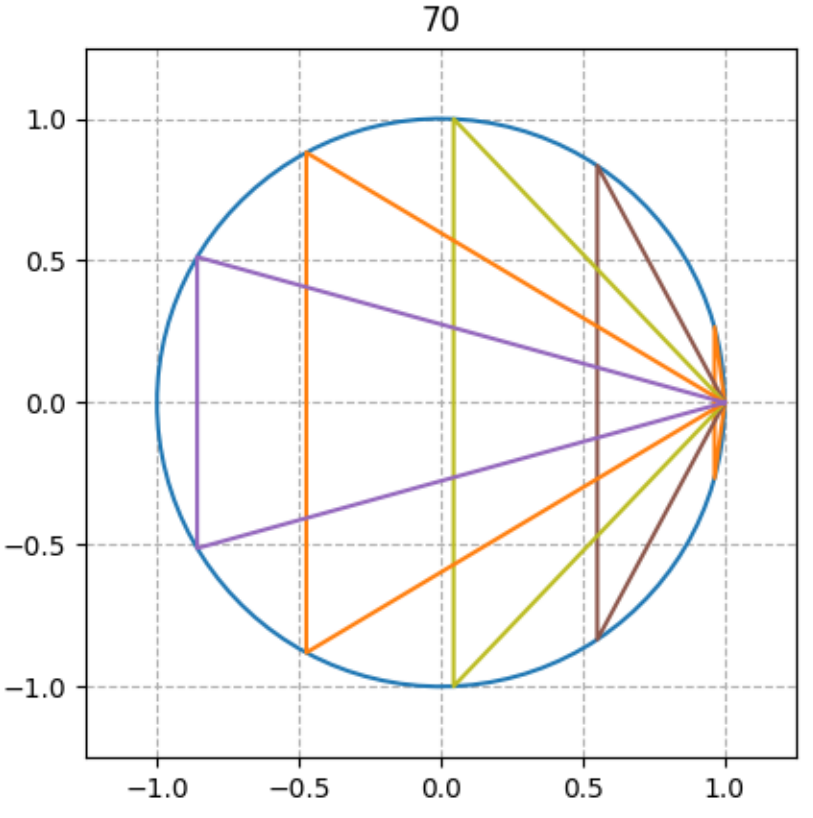

60
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

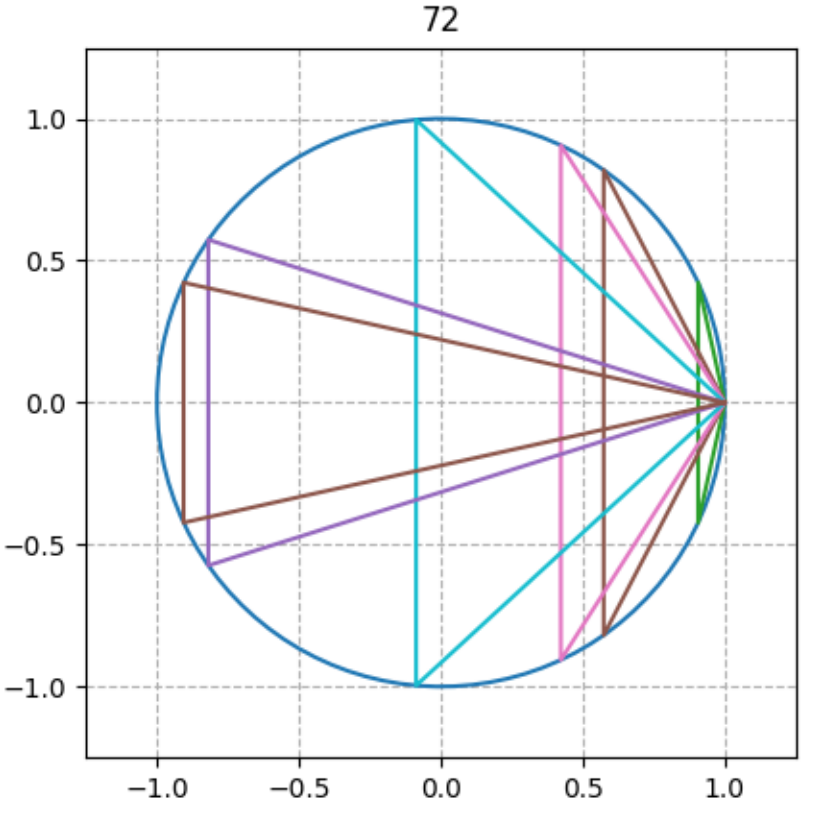

62
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

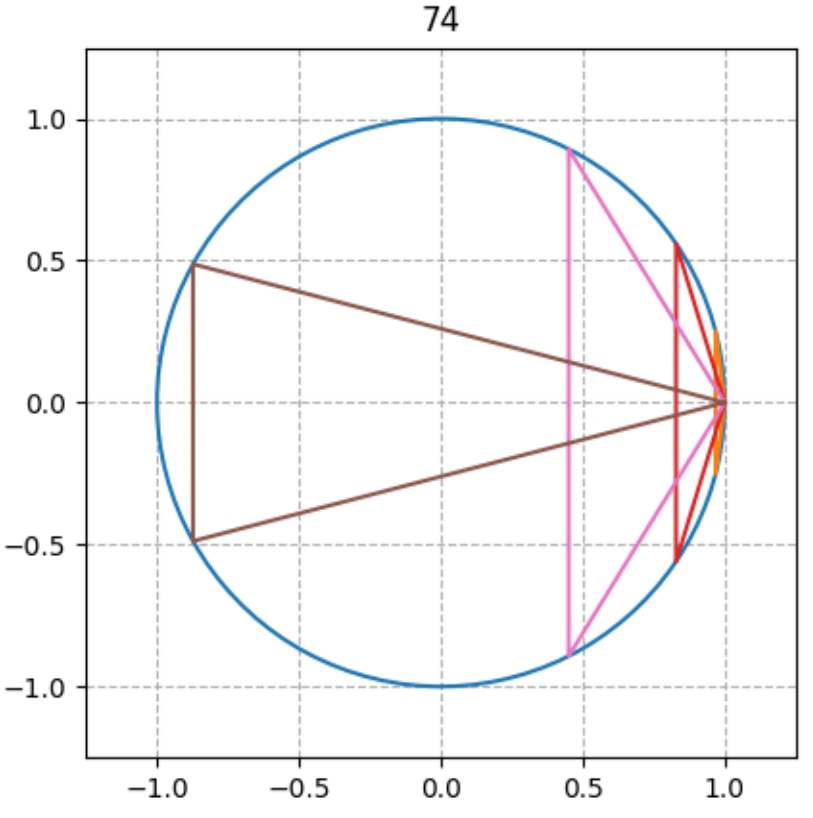

64
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

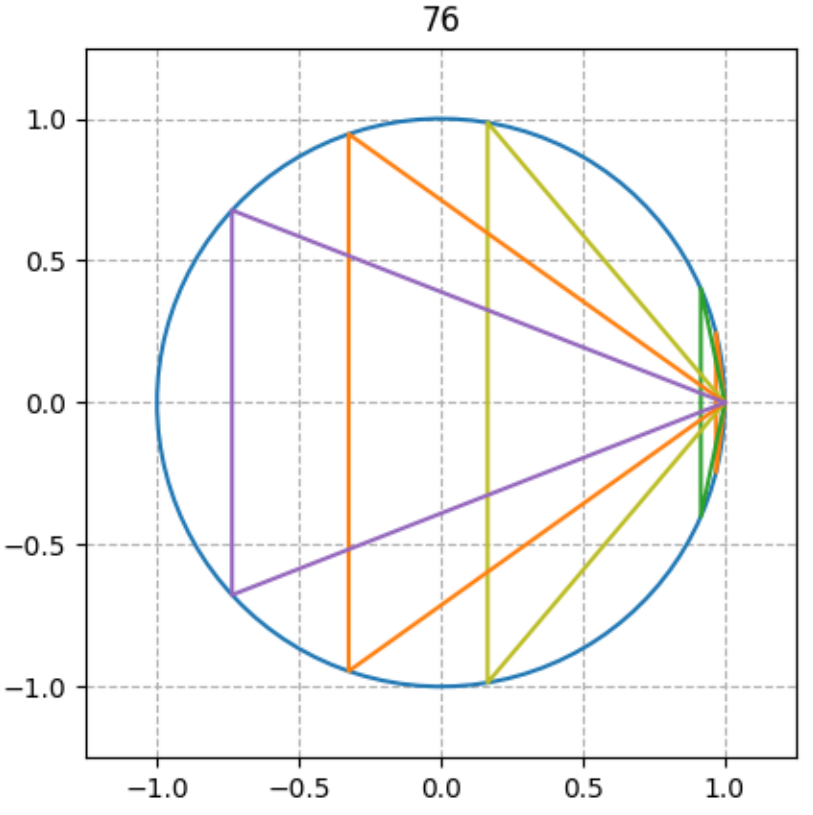

66
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

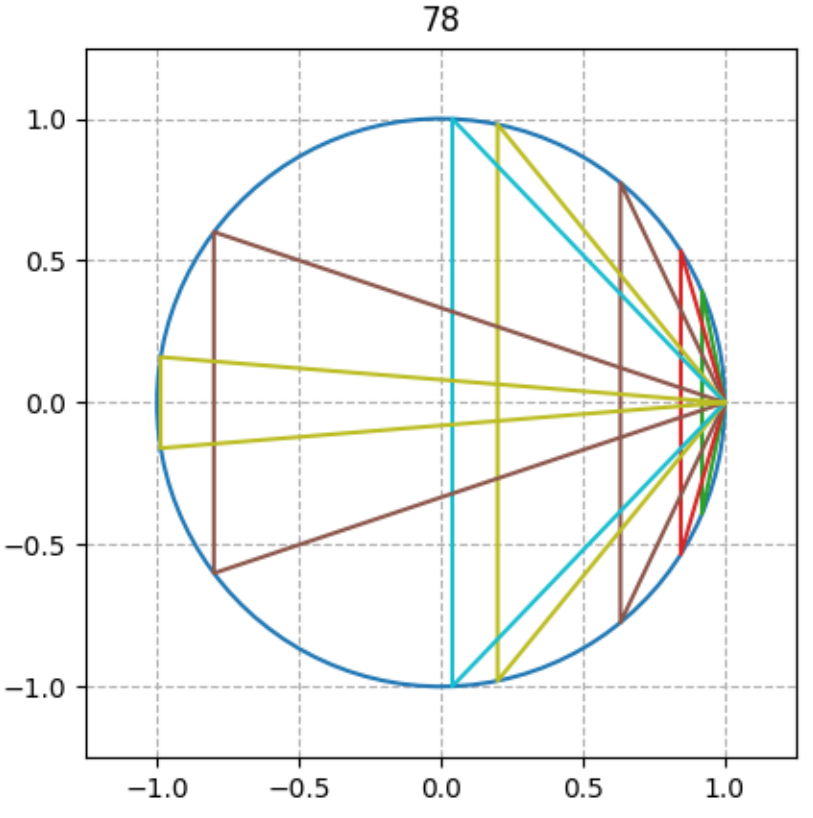

68
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

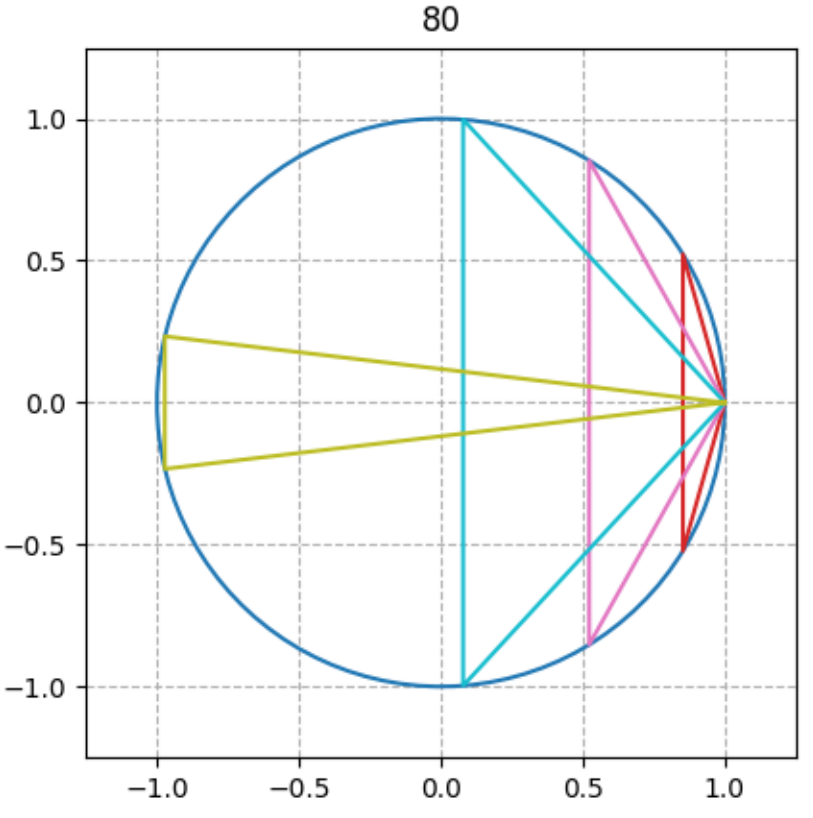

70
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

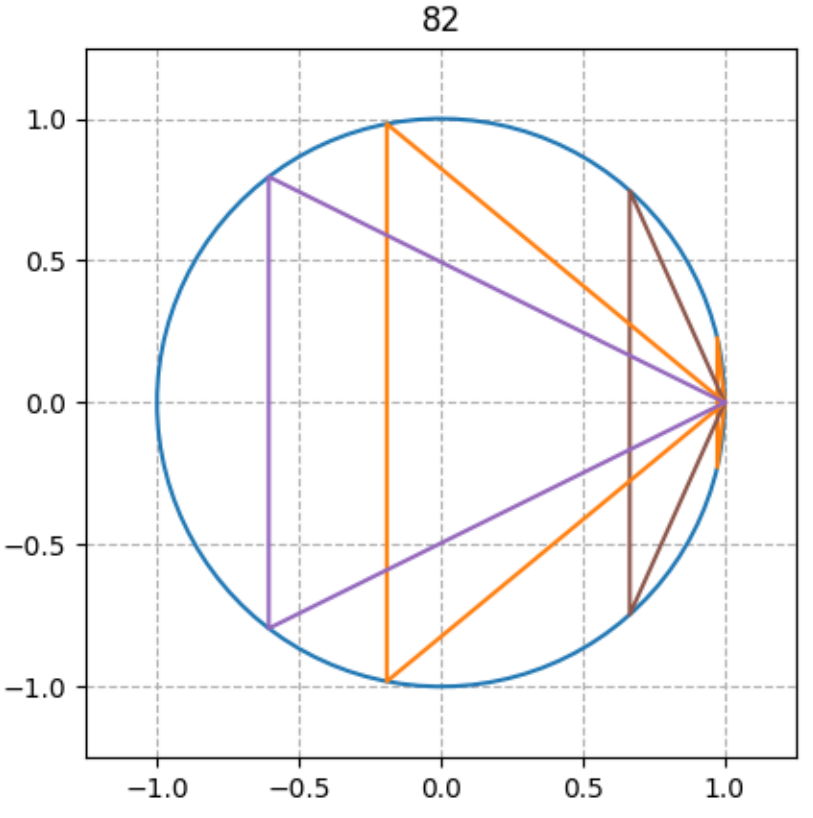

72
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

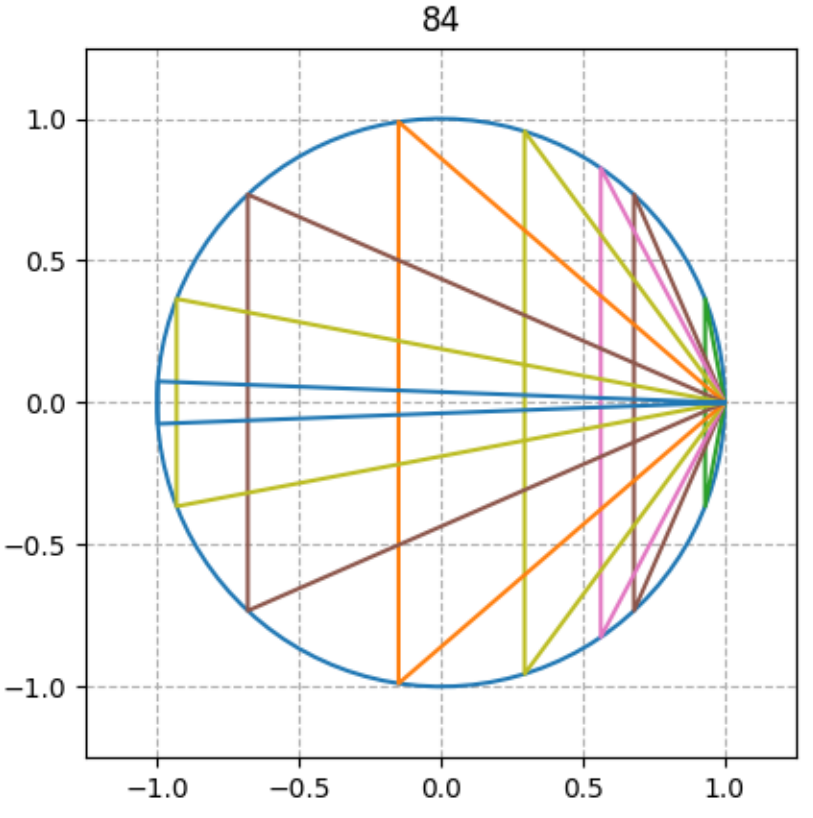

74
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

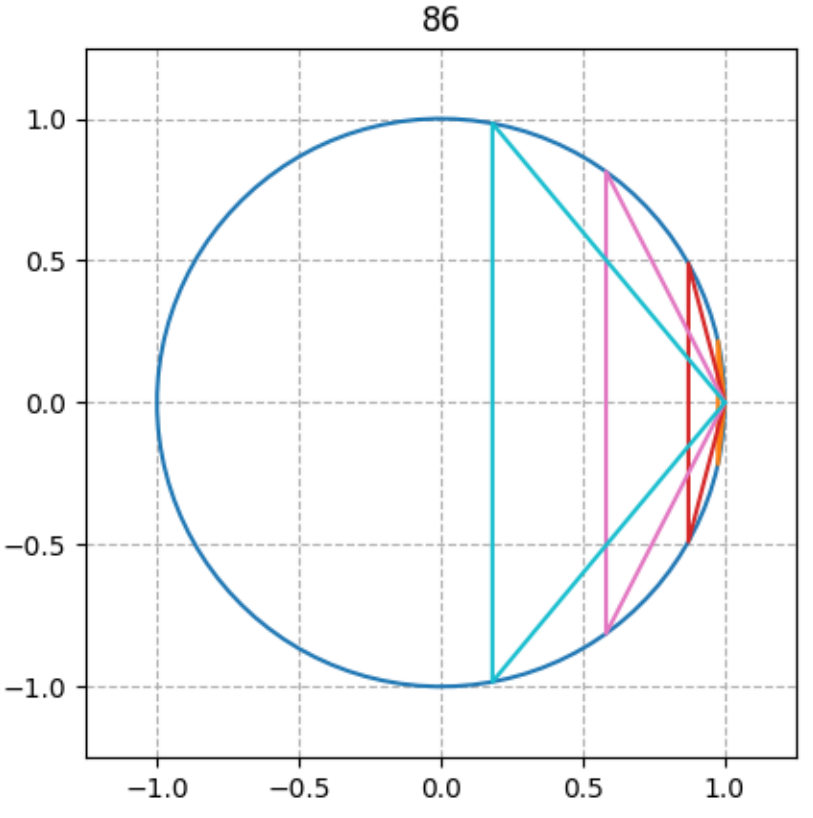

76
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

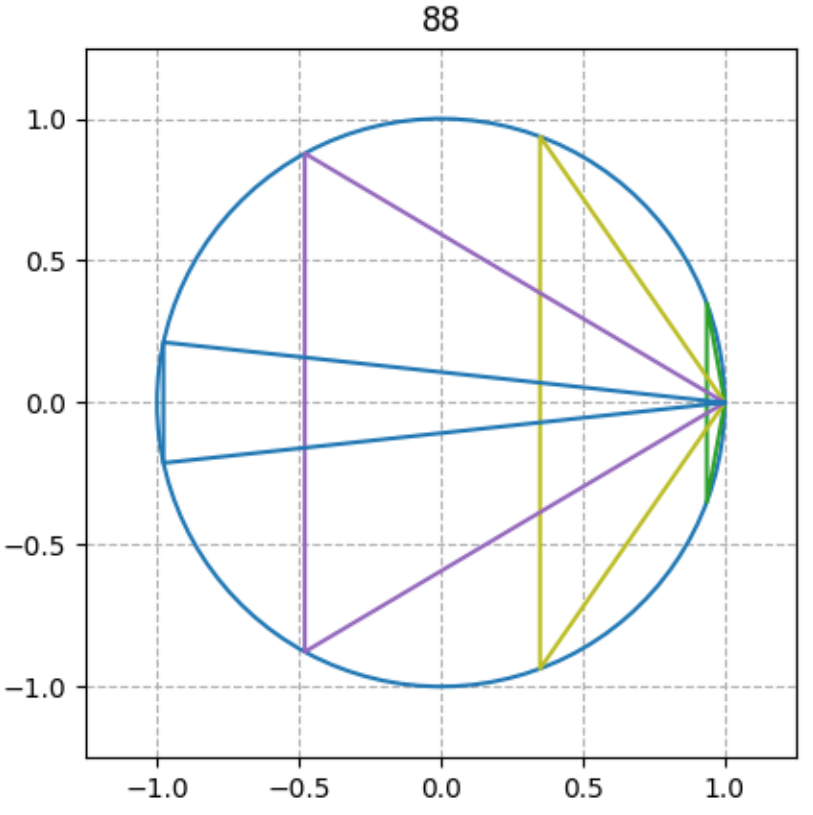

78
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

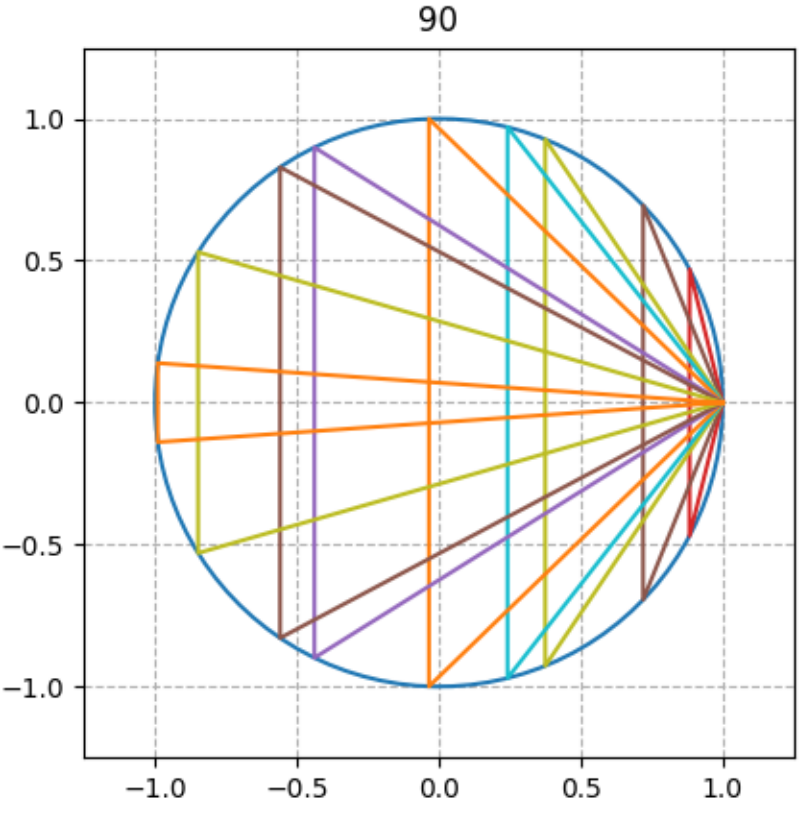

80
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

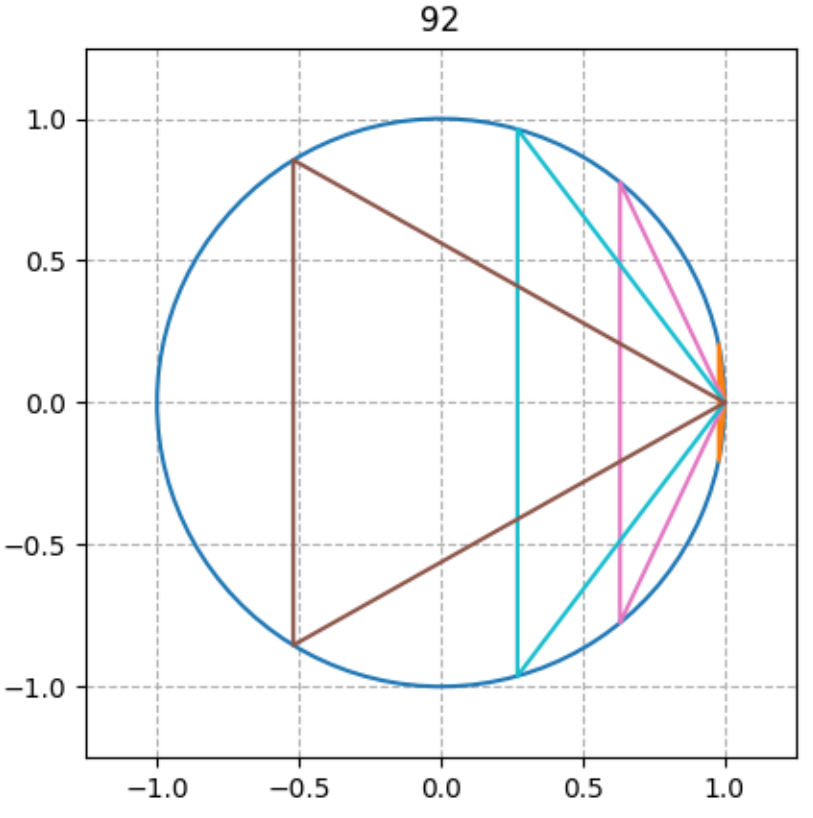

82
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

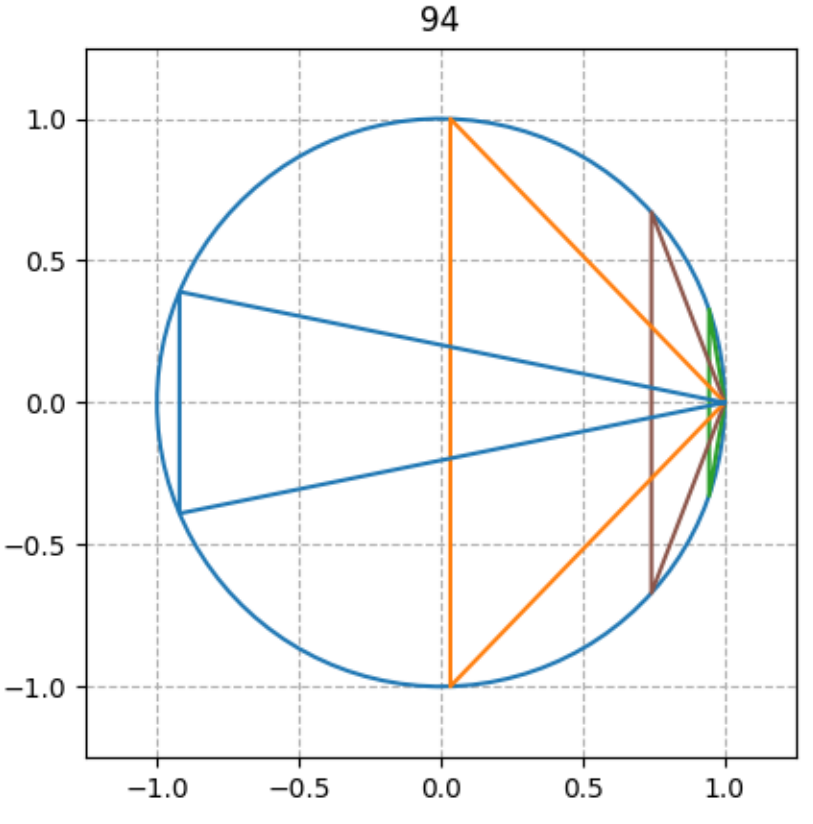

84
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

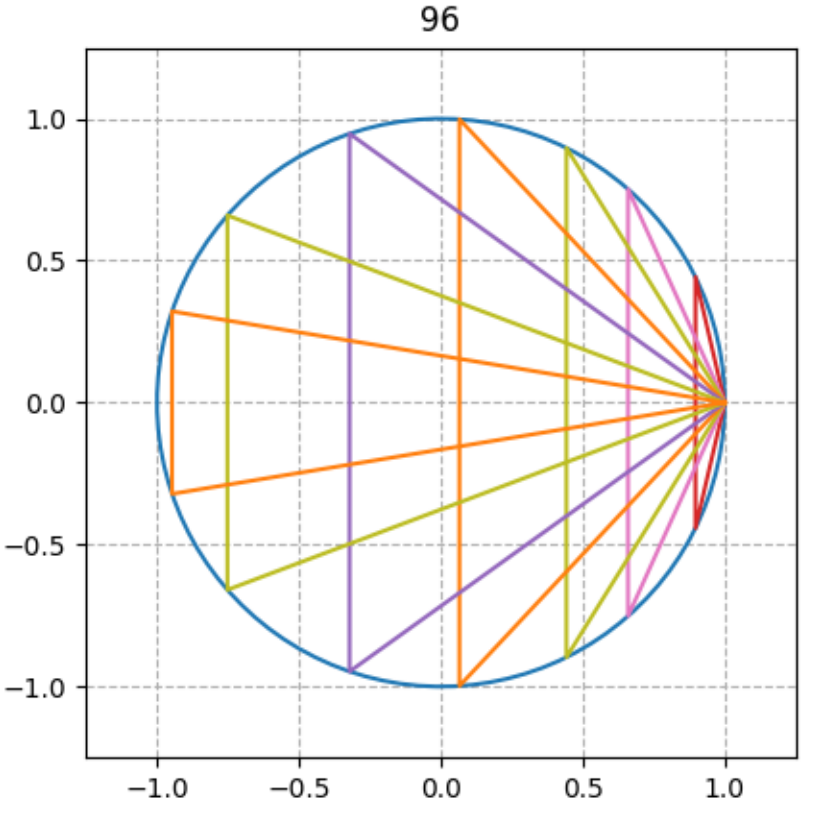

86
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

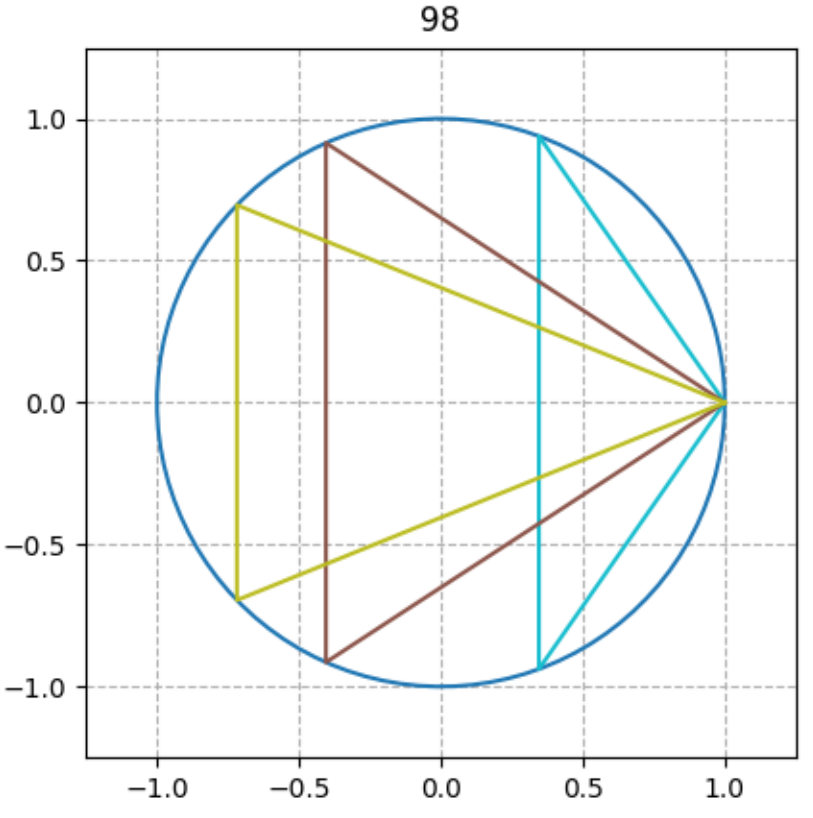

88
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

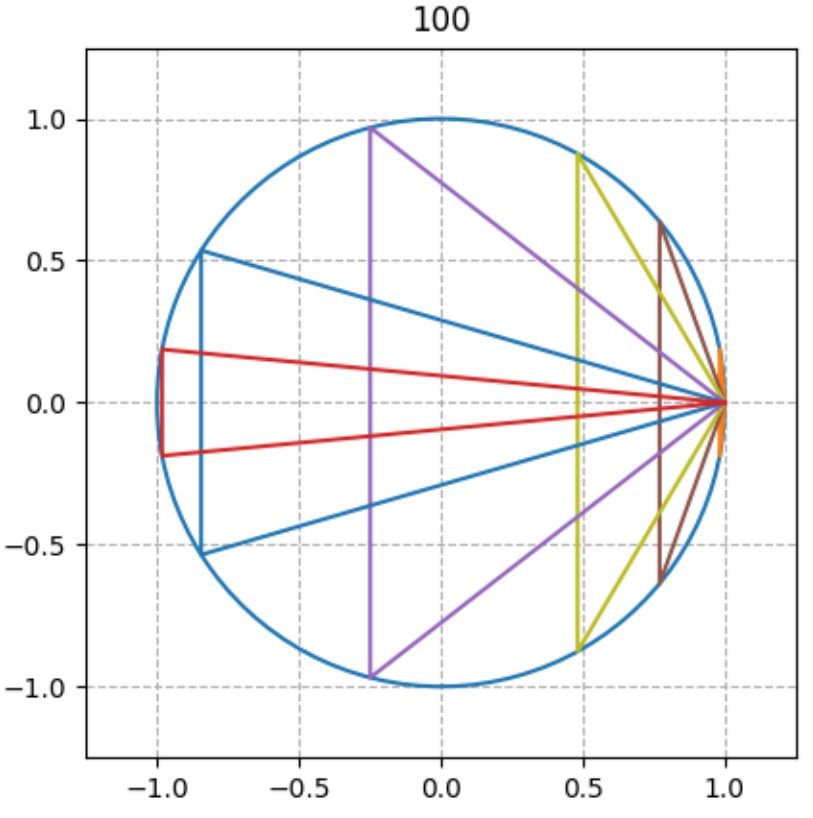

90
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

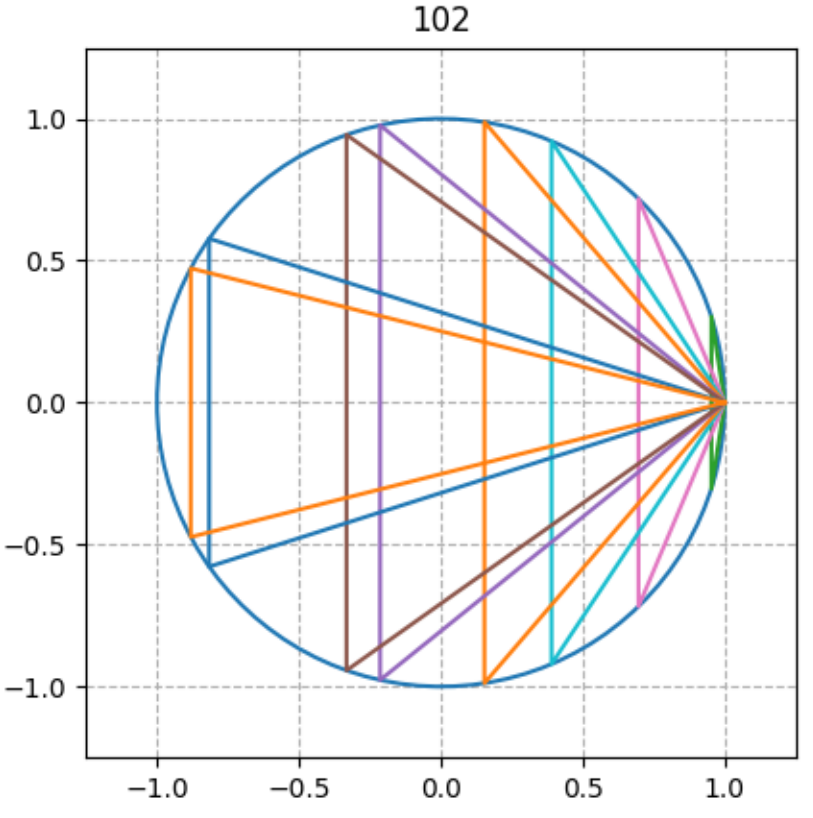

92
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0


94
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0


96
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0


98
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0


100
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0


102
1.0
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0

Traduction d'un extrait de A classical introduction to modern number theory de K. Ireland et M. Rosen, Springer, 1990, p. 69 et suivantes (Denise Vella-Chemla, juin 2023)[1]

2. Caractère quadratique de 2

Soit $\zeta = e^{2\pi i/8}$. Alors ζ est une racine primitive huitième de l'unité. Donc $0 = \zeta^8 - 1 = (\zeta^4 - 1)(\zeta^4 + 1)$. Puisque $\zeta^4 \neq 1$, on a $\zeta^4 = -1$. En multipliant par ζ^{-2} et en ajoutant alors ζ^{-2} au deux côtés de l'égalité, cela amène $\zeta^2 + \zeta^{-2} = 0$. Cette équation est également facilement dérivable de l'observation que $\zeta^2 = e^{i(\pi/2)} = i$.

Le caractère quadratique de 2 va maintenant être déduit de la relation

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2.$$

Appelons $\tau = \zeta + \zeta^{-1}$ et notons que et ζ et τ sont des nombres algébriques. On peut par conséquent travailler avec les congruences dans l'anneau des entiers algébriques.

Soit p un nombre premier impair dans $\mathbb{Z}$ et remarquons que

$$\tau^{p-1} = (\tau^2)^{(p-1)/2} = 2^{(p-1)/2} \equiv (2/p) \pmod{p}.$$

Il en découle que $\tau^p = (2/p)\tau \pmod{p}$. Par la proposition 6.1.6, $\tau^p = (\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \pmod{p}$.

En se rappelant que $\zeta^8 = 1$, on a $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$ pour $p = \pm 1 \pmod 8$ et $\zeta^p + \zeta^{-p} = \zeta^3 + \zeta^{-3}$ pour $p = \pm 3 \pmod 8$. Le résultat dans le dernier cas peut être simplifié en observant que $\zeta^4 = -1$ implique que $\zeta^3 = -\zeta^{-1}$. Ainsi $\zeta^p + \zeta^{-p} = -(\zeta + \zeta^{-1})$ si $p = \pm 3 \pmod 8$. Résumons

$$\zeta^p + \zeta^{-p} = \begin{cases} \tau, & \text{si } p \equiv \pm 1 \pmod 8, \\ -\tau, & \text{si } p \equiv \pm 3 \pmod 8, \end{cases}$$

Substituer ce résultat dans la relation $\tau^p \equiv (2/p)\tau \pmod{p}$ amène

$$(-1)^\varepsilon \tau \equiv \left(\frac{2}{p}\right) \tau \pmod{p}, \qquad \text{où } \varepsilon \equiv \frac{p^2 - 1}{8} \pmod 2.$$

Multiplions les deux côtés de la congruence par τ. Alors

$$(-1)^\varepsilon 2 \equiv \left(\frac{2}{p}\right) 2 \pmod{p},$$

ce qui implique que

$$-1^\varepsilon \equiv \left(\frac{2}{p}\right) \pmod{p}$$

Cette dernière congruence implique que $\left(\frac{2}{p}\right) = (-1)^\varepsilon$, qui est le résultat souhaité.

[1] On a utilisé la convention d'écrire le petit mot (mod ...) devant le module.

Euler (1707-1783), dans un article précédent a démontré que 2 est un résidu quadratique modulo les nombres premiers p avec $p \equiv 1 \pmod 8$. Sa méthode contient l'idée-clé de la preuve ci-dessous.

Euler suppose que $U(\mathbb{Z}/p\mathbb{Z})$ est un groupe cyclique. Gauss a été le premier à fournir une preuve rigoureuse de ce fait (voir le théorème 1 du chapitre 4). Soit λ un générateur de $U(\mathbb{Z}/p\mathbb{Z})$ et appelons $\gamma = \lambda^{(p-1)/8}$. Alors γ est d'ordre 8, de telle façon que $\gamma^4 = -1$ et $\gamma^2 + \gamma^{-2} = \overline{0}$. Donc, $(\gamma + \gamma^{-1})^2 = \gamma^2 + \overline{2} + \gamma^{-2} = \overline{2}$. Cela montre que $\overline{2}$ est un carré dans $U(\mathbb{Z}/p\mathbb{Z})$, ce qui est équivalent à dire que 2 est un résidu quadratique modulo p.

Si $p \not\equiv 1 \pmod 8$, cette preuve ne peut pas démarrer. Pourtant, la théorie des corps finis nous permet de mener à bien une preuve complète de la loi de réciprocité quadratique en utilisant l'idée d'Euler. Nous développerons la théorie des corps finis au chapitre 7.

3. Sommes quadratiques de Gauss

Étant donnée la relation $(\zeta + \zeta^{-1})^2 = 2$ de la section 2, on peut se demander s'il y a une relation similaire quand 2 est remplacé par un nombre premier impair p. La réponse est oui, et, de plus, la loi complète de la réciprocité quadratique découle de cette nouvelle relation en utilisant la méthode de la section 2.

Tout au long de cette section, ζ dénotera $e^{2\pi i/p}$, une racine primitive $p^{\text{ième}}$ de l'unité.

Lemme 1. $\sum_{t=0}^{p-1} \zeta^{at}$ est égal à p si $a \equiv 0 \pmod p$. Sinon, cette somme est nulle.

Preuve. Si $a = 0 \pmod p$, alors $\zeta^a = 1$, et donc $\sum_{t=0}^{p-1} \zeta^{at} = p$. Si $a \neq 0 \pmod p$, alors $\zeta^a \neq 1$ et $\sum_{t=0}^{p-1} \zeta^{at} = (\zeta^{ap} - 1)/(\zeta^a - 1) = 0$. □

Corollaire. $p^{-1} \sum_{t=0}^{p-1} \zeta^{t(x-y)} = \delta(x, y)$, où $\delta(x, y) = 1$ si $x = y \pmod p$ et $\delta(x, y) = 0$ if $x \not\equiv y \pmod p$.

Preuve. La preuve est immédiate à partir du lemme 1. □

Toutes les sommes du reste de cette section seront sur le domaine de zéro à $p - 1$. On simplifiera la notation en évitant de réécrire ce fait à chaque fois.

Lemme 2. $\sum_t (t/p) = 0$, *où* (t/p) *est le symbole de Legendre.*

Preuve. Par définition $(0/p) = 0$. Concernant les $p - 1$ termes restant dans la somme, la moitié sont des +1 et l'autre moitié sont des -1, puisque par le corollaire 1 de la proposition 5.1.2, il y a autant de résidus quadratiques que de non résidus quadratique mod p. □

Nous sommes maintenant en mesure d'introduire la notion de somme de Gauss.

Définition. $g_a = \sum_t (t/p)\zeta^{at}$ est appelée une *somme quadratique de Gauss.*

Proposition 6.3.1. $g_a = (a/p)g_1$.

PREUVE. Si $a \equiv 0 \pmod{p}$, alors $\zeta^{at} = 1$ pour tout t, et $g_a = \sum(t/p) = 0$ par le lemme 2. Cela donne le résultat dans le cas où $a \equiv 0 \pmod{p}$.

Maintenant supposons que $a \not\equiv 0 \pmod{p}$. Alors

$$\left(\frac{a}{p}\right) g_a = \sum_t \left(\frac{at}{p}\right) \zeta^{at} = \sum_x \left(\frac{x}{p}\right) \zeta^x = g_1.$$

On a utilisé le fait que at couvre un système complet de résidus mod p quand t le fait et que (x/p) et ζ^x dépendent seulement de la classe résiduelle de x modulo p.

Puisque $(a/p)^2 = 1$ quand $a \not\equiv 0 \pmod{p}$, notre résultat s'en déduit en multipliant l'équation $(a/p)g_a = g_1$ des deux côtés par (a/p). □

À partir de maintenant, on va changer g_1 en g. Il découle de la proposition 6.3.1 que $g_a^2 = g^2$ si $a \not\equiv 0 \pmod{p}$. On va maintenant déduire cette valeur commune.

Proposition 6.3.2. $g^2 = (-1)^{(p-1)/2}p$.

PREUVE. L'idée de la preuve consiste à évaluer la somme $\sum_a g_a g_{-a}$ de deux manières.

Si $a \not\equiv 0 \pmod{p}$, alors $g_a g_{-a} = (a/p)(-a/p)g^2 = (-1/p)g^2$. Il en découle que

$$\sum_a g_a g_{-a} = \left(\frac{-1}{p}\right)(p-1)g^2.$$

Maintenant, notons que

$$g_a g_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^{a(x-y)}.$$

En sommant les deux côtés sur a et en utilisant le corollaire du lemme 1, on obtient

$$\sum_a g_a g_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\delta(x,y)p = (p-1)p.$$

En mettant ces résultats ensemble, on obtient $(-1/p)(p-1)g^2 = (p-1)p$. Donc, $g^2 = (-1/p)p$. □

Soit $p^* = (-1)^{(p-1)/2}p$. L'équation $g^2 = p^*$ est l'analogue souhaité de l'équation $\tau^2 = 2$. Soit $q \neq p$ un autre nombre premier impair. On procède de la façon suivante, pour démontrer la loi de réciprocité quadratique en travaillant avec des congruences mod q dans l'anneau des entiers algébriques :

$$g^{q-1} = (g^2)^{(q-1)/2} = p^{*(q-1)/2} \equiv \left(\frac{p^*}{q}\right) \pmod{q}.$$

Par conséquent

$$g^q = \left(\frac{p^*}{q}\right) g \pmod{q}.$$

En utilisant la proposition 6.1.6, on voit que

$$g^q = \left(\sum \left(\frac{t}{p}\right)\zeta^t\right)^q \equiv \sum \left(\frac{t}{p}\right)^q \zeta^{qt} \equiv g_q \pmod q.$$

Il s'ensuit de cela que $g^q \equiv g_q \equiv (q/p)g \pmod q$ et donc que

$$\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g \pmod q.$$

En multipliant les deux côtés par g, et en utilisant $g^2 = p^*$:

$$\left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^* \pmod q,$$

ce qui implique que

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod q$$

et finalement

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right).$$

Pour voir que ce résultat est ce que nous souhaitions, notons simplement que

$$\left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2} \left(\frac{p}{q}\right) = (-1)^{((q-1)/2)((p-1)/2)} \left(\frac{p}{q}\right).$$

La notion de somme quadratique de Gauss que nous avons utilisée peut être considérablement généralisée. On présentera quelques-unes de ces généralisations après avoir développé la théorie des corps finis. Les sommes cubiques de Gauss seront utilisées pour démontrer la loi de réciprocité cubique, et les sommes de Gauss quartiques seront utilisées pour démontrer la loi de réciprocité biquadratique.

4. Le signe de la somme quadratique de Gauss[2]

Selon la proposition 6.3.2, la somme quadratique de Gauss a pour valeur $\pm\sqrt{p}$ si $p \equiv 1 \pmod 4$ et $\pm i\sqrt{p}$ si $p \equiv 3 \pmod 4$. Ainsi la valeur de $g(\chi)$ est déterminée au signe près. La détermination du signe est un problème beaucoup plus difficile. La conjecture que le signe plus est vérifiée dans chaque cas a été faite par Gauss et enregistrée dans son journal en mai 1801. Ce n'est que quatre ans plus tard qu'il a trouvé la démonstration. Le 30 août 1805, Gauss a noté dans son journal qu'il avait finalement terminé une preuve du "très élégant théorème mentionné en 1801". Il écrivit à son ami W. Olbers le 3 septembre 1805 qu'il s'était rarement passé une semaine depuis quatre ans sans qu'il ait essayé en vain de prouver sa conjecture. Finalement, selon Gauss, "Wie der Blitz einschlägt, hat sich das Räthsel gelöst..." (alors que la foudre tombait, le puzzle a été résolu).

Des preuves ultérieures ont été trouvées par Dirichlet, Cauchy, Kronecker, Mertens, Schur, et d'autres. Dans cette section, on présente l'une des démonstrations de Kronecker.

[2]Dans cette section, la somme de Gauss g sera dénotée par $g(\chi)$ avec $\chi(t) = (t/p)$ par définition.

Comme dans la section précédente, $\zeta = e^{2\pi i/p}$. Alors $1, \zeta, \ldots, \zeta^{p-1}$ sont les racines de $x^p - 1$.

Proposition 6.4.1. *Le polynôme* $1 + x + \ldots + x^{p-1}$ *est irréductible dans* $\mathbb{Q}[x]$.

PREUVE. Par l'exercice 4 à la fin du chapitre "lemme de Gauss"), il suffit de montrer que $1 + x + \ldots + x^{p-1}$ n'a pas de factorisation triviale dans $\mathbb{Z}[x]$. Supposons, au contraire, que $1 + x + x^2 + \ldots + x^{p-1} = f(x)g(x)$ où $f(x), g(x) \in \mathbb{Z}[x]$ et où chacun a un degré plus grand que un. En posant $x = 1$, on obtient $p = f(1)g(1)$. On peut donc supposer que $g(1) = 1$. En utilisant un trait au-dessus des nombres pour désigner les classes de congruences modulo p, on conclut que $\overline{g}(\overline{1}) \neq \overline{0}$. D'un autre côté, puisque $p| \binom{p}{j}, j = 1, \ldots, p-1$, on a $x^p - 1 = (x-1)^p \pmod p$ et la division des deux côtés à la fois par $x - 1$ nous montre que $1 + x + +x^{p-1} \equiv (x-1)^{p-1} \pmod p$. Par le théorème 2, le chapitre 1 et la proposition 3.3.2 il s'ensuit que $g(x) \equiv (x-1)^s \pmod p$ pour quelques entiers positifs s. Pourtant, cela contredit le fait que $g(\overline{1}) \neq (\overline{0})$, et la preuve est complète.□

En combinant la proposition ci-dessus avec la proposition 6.1.7, on voit que si $g(\zeta) = 0$ pour $g(x) \in \mathbb{Q}[x]$ alors $1 + x + \ldots + x^{p-1} | g(x)$. Cette observation sera utile plus tard.

Proposition 6.4.2. $\prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)})^2 = (-1)^{(p-1)/2} p$.

PREUVE. On a $x^p - 1 = (x-1)\prod_{j=1}^{p-1}(x - \zeta^j)$. Divisons par $x - 1$ et posons $x = 1$ pour obtenir $p = \prod_r (1 - \zeta^r)$, où le produit est calculé sur tout ensemble complet de représentants des classes suivant un sous-groupe non nulles modulo p. On voit facilement que les entiers $\pm(4k-2)$, $k = 1, 2, \ldots, (p-1)/2$ forment un tel système de restes. Donc

$$\begin{aligned} p &= \prod (1 - \zeta^{4k-2}) \prod (1 - \zeta^{-(4k-2)}) \\ &= \prod (\zeta^{-(2k-1)} - \zeta^{2k-1}) \prod (\zeta^{2k-1} - \zeta^{-(2k-1)}) \\ &= (-1)^{(p-1)/2} \prod (\zeta^{2k-1} - \zeta^{-(2k-1)})^2, \end{aligned}$$

tous les produits étant sur $k = 1, 2, \ldots, (p-1)/2$. □

Proposition 6.4.3.

$$\prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)}) = \begin{cases} \sqrt{p}, & \text{si } p \equiv 1 \pmod 4, \\ i\sqrt{p}, & \text{si } p \equiv 3 \pmod 4 \end{cases}$$

PREUVE. Par la Proposition 6.4.2, on a seulement à calculer le signe du produit. Le produit est

$$i^{(p-1)/2} \prod_{k=1}^{(p-1)/2} 2 \sin \frac{(4k-2)\pi}{p}.$$

Mais $\sin((4k-2)/p)\pi < 0$ if $(p+2)/4 < k \leq (p-1)/2$. Il en découle que le produit a $(p-1)/2 - [(p+2)/4]$ termes négatifs et on voit que ce nombre est égal à $(p-1)/4$ ou $(p-3)/4$ selon que $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$, respectivement. Le résultat recherché en découle

immédiatement. □

Par la proposition 6.3.2 et la proposition 6.4.2, on sait que

$$g(\chi) = \varepsilon \prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)}), \tag{1}$$

où $\varepsilon = \pm 1$. L'évaluation de la somme de Gauss est complété par la proposition 6.4.3 si on peut montrer que $\varepsilon = +1$. L'argument suivant de Kronecker montre que c'est le cas. Voir également l'exercice 22.

Proposition 6.4.4. $\varepsilon = +1$.

Preuve. Considérons le polynôme

$$f(x) = \sum_{j=1}^{p-1} \chi(j) x^j - \varepsilon \prod_{k=1}^{(p-1)/2} (x^{2k-1} - x^{p-(2k-1)}). \tag{2}$$

Alors $f(\zeta) = 0$ par (1) et $f(1) = 0$ par le lemme 2. Par le commentaire précédant la proposition 6.4.2 et le fait que $1 + x + \ldots + x^{p-1}$ and $x - 1$ sont premiers entre eux, on conclut que $x^p - 1 | f(x)$. Écrivons que $f(x) = (x^p - 1)h(x)$ et remplaçons x par e^z pour obtenir

$$\sum_{j=1}^{p-1} \chi(j) e^{jz} - \varepsilon \prod_{k=1}^{(p-1)/2} (e^{(2k-1)z} - e^{z(p-(2k-1))}) = (e^{pz} - 1)h(e^z). \tag{3}$$

On voit facilement que le coefficient de $z^{(p-1)/2}$ du côté gauche de (3) est

$$\frac{\sum_{j=1}^{p-1} \chi(j) j^{(p-1)/2}}{((p-1)/2)!} - \varepsilon \prod_{k=1}^{(p-1)/2} (4k - p - 2).$$

De l'autre côté par l'exercice 21, le coefficient de $z^{(p-1)/2}$ du côté droit de (3) est pA/B où $p \not| B$, A et B étant des nombres entiers. En égalant les coefficients, en multipliant par $B((p-1)/2)!$ et en réduisant modulo p, on obtient que

$$\begin{aligned}
\sum_{j=1}^{p-1} \chi(j) j^{(p-1)/2} &\equiv \varepsilon \left(\frac{p-1}{2}\right)! \prod_{k=1}^{(p-1)/2} (4k-2) \pmod{p} \\
&\equiv \varepsilon(2.4.6 \ldots p-1) \prod_{k=1}^{(p-1)/2} (2k-1) \\
&\equiv \varepsilon(p-1)! \\
&\equiv -\varepsilon(p)
\end{aligned}$$

en utilisant le théorème de Wilson (corollaire de la proposition 4.1.1).

Par la proposition 5.1.2, $j^{(p-1)/2} \equiv \chi(j) \pmod{p}$, ainsi on a

$$\sum_{j=1}^{p-1} \chi(j)^2 \equiv (p-1) \equiv -\varepsilon \pmod{p}$$

et donc

$$\varepsilon \equiv 1 \pmod{p}.$$

Puisque $\varepsilon = \pm 1$, on conclut finalement que $\varepsilon = 1$. Ceci conclut la démonstration.

Les résultats peuvent être énoncés de la façon suivante

Théorème 1. *La valeur de la somme quadratique de Gauss $g(\chi)$ est donnée par*

$$g(\chi) = \begin{cases} \sqrt{p}, & \text{si } p \equiv 1 \pmod{4}, \\ i\sqrt{p}, & \text{si } p \equiv 3 \pmod{4} \end{cases}$$

Traduction d'un extrait du livre Circulant matrices de Philip J. Davis (Denise Vella-Chemla, juin 2023)

(p. 27) : Matrice dite push

Parmi les matrices de permutation, la matrice

$$\pi = \begin{pmatrix} 0 & 1 & 0 & 0 & ... & 0 \\ 0 & 0 & 1 & 0 & ... & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & 0 & ... & ... & ... & 0 \end{pmatrix}. \tag{2.4.14}$$

joue un rôle fondamental dans la théorie des matrices circulantes. Elle correspond à la permutation de décalage *vers l'avant* $\sigma(1) = 2, \sigma(2) = 3, ..., \sigma(n-1) = n, \sigma(n) = 1$, c'est-à-dire au cycle $\sigma = (1, 2, 3, ...n)$ générant le groupe cyclique d'ordre n (π est pour "push"). On a

$$pi^2 = \begin{pmatrix} 0 & 0 & 1 & 0 & ... & 0 \\ 0 & 0 & 0 & 1 & ... & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & 0 & 0 & ... & 0 \end{pmatrix}. \tag{2.4.15}$$

correspondant à σ^2 pour lequel $\sigma^2(1) = 3, \sigma^2(2) = 4, \ldots, \sigma^2(n) = 2$. Similairement, pour π^k et σ^k. La matrice π^n correspond à $\sigma^n = I$, de telle façon que

$$\pi^n = I \tag{2.4.16}$$

Notons également que

$$\pi^T = \pi^* = \pi^{-1} = \pi^{n-1} \tag{2.4.17}$$

Une instance particulière de (2.4.13) est

$$\pi A \pi^T = (a_{i+1,j+1}) \tag{2.4.18}$$

où $A = (a_{i,j})$ et les indices sont pris mod n.

(p. 119 et suivantes)

4.4. n-gones imbriqués

(voir la section 1.4.) Soit $Z = (z_1, z_2, \ldots, z_n)^T$ désignant les sommets d'un n-gone et appliquons itérativement la transformation $C(= c_s)$ où

$$\begin{aligned} C &= \text{circ}(s, t, 0, 0, ..., 0) \\ &= sI + t\pi, \qquad s > 0, t > 0, s + t = 1. \end{aligned} \tag{4.4.1}$$

Les valeurs propres de C sont les nombres $\lambda_k = s + tw^{k-1}$, $k = 1, 2, \ldots, n$. Ces nombres sont les combinaisons linéaires strictement convexes de 1 et w^{k-1}. Donc, $\lambda_1 = 1$ et pour $k = 2, ..., n$, on a $|\lambda_k| < 1$. Voir la figure 4.4.1. En fait, ces nombres sont sur un cercle intérieur et tangent au cercle unité en $z = 1$. On a

$$
\begin{aligned}
|\lambda_k|^2 &= \left| s + t(\cos(\frac{2\pi(k-1)}{n} + i \sin \frac{2\pi(k-1)}{n}) \right|^2 \\
&= \left| s^2 + t^2 + 2st \cos \frac{2\pi(k-1)}{n} \right|^2, \qquad k = 1, 2, ..., n
\end{aligned}
\tag{4.4.2}
$$

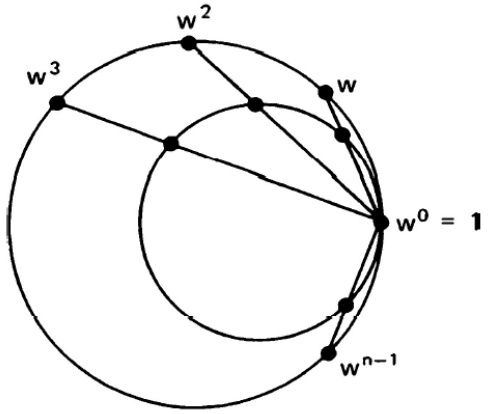


FIG. 4.4.1

Il est clair que les valeurs propres de valeurs proches de $\lambda_1 = 1$ sont λ_2 et $\lambda_n (= \overline{\lambda}_2)$ pour lesquelles

$$
| \lambda_2 |^2 = |\lambda_n|^2 = \left| s^2 + t^2 + 2st \cos \frac{2\pi}{n} \right|^2 \tag{4.4.3}
$$

À partir de (3.4.14), on a pour $r = 0, 1, ...,$

$$
C^r z = B_1 Z + \lambda_2^r B_2 Z + \ldots + \lambda_n^r B_n Z, \tag{4.4.4}
$$

donc

$$
\lim_{r \to \infty} C^r Z = B_1 Z. \tag{4.4.4$'$}
$$

Puisqu'à partir de (3.4.13), $B_1 = 1/n \text{ circ}(1, 1, ..., 1), B_1 Z = (1/n)(z_1 + z_2 + ... + z_n)(1, 1, \ldots, 1)^T$. Donc, lorsque $r \to \infty$, chaque composante de $C^r Z$ s'approche de la c.g. de Z avec une rapidité géométrique. Il est utile, par conséquent, de supposer que la c.g. est en $z = 0$, en éliminant le premier terme dans (4.4.4). Alors on suppose que

$$
z_1 + z_2 + \ldots + z_n = 0 \tag{4.4.5}
$$

Une analyse asymptotique plus poussée peut être menée selon la ligne de la *méthode des puissances* en analyse numérique pour le calcul des valeurs propres de la matrice. Écrivons

$$
C^r Z = \lambda_2^r B_2 Z + \lambda_n^r B_n Z + (\lambda_3^r B_3 + \ldots + \lambda_{n-1}^r B_{n-1}) Z. \tag{4.4.6}
$$

Alors, puisque $|\lambda_n| = |\lambda_2|$,

$$
\frac{C^r Z}{|\lambda_2|^r} = \frac{\lambda_2^r}{|\lambda_2|^r} B_2 Z + \frac{\lambda_n^r}{|\lambda_n|^r} B_n Z + \left(\frac{\lambda_3^r}{|\lambda_2|^r} B_2 + \ldots + \frac{\lambda_{n-1}^r}{|\lambda_2|^r} B_{n-1} \right) Z. \tag{4.4.7}
$$

Maintenant, puisque $|\lambda_3|, |\lambda_4|, \ldots, |\lambda_{n-1}| < |\lambda_2|$, le terme entre parenthèses approche 0 lorsque $r \to \infty$. On le désigne par $\varepsilon(r)$. (C'est un vecteur colonne). Soit

$$\lambda_2 = |\lambda_2| e^{i\theta}$$

$$\theta = \tan^{-1}\left(\frac{t \sin 2\pi/n}{s + t\cos 2\pi/n}\right). \tag{4.4.8}$$

$$\lambda_n = |\lambda_2| e^{-i\theta}$$

Donc,

$$\frac{c^r Z}{|\lambda_2|^r} = e^{ir\theta} B_2 Z + e^{-ir\theta} B_n Z + \varepsilon(r). \tag{4.4.9}$$

Écrivons

$$Y_r = e^{ir\theta} B_2 Z + e^{-ir\theta} B_n Z, \tag{4.4.10}$$

de telle façon que

$$\frac{C^r Z}{|\lambda_2|^r} = Y_r + \varepsilon(r). \tag{4.4.11}$$

Puisqu'à partir de (3.4.9) $B_k = F^* \Lambda_k F$, on a

$$\begin{aligned} Y_r &= e^{ir\theta} B_2 Z + e^{-ir\theta} B_n Z \\ &= F^* \mathrm{diag}(0, e^{ir\theta}, 0, \ldots, 0, e^{-ir\theta}) F Z. \end{aligned}$$

Par conséquent

$$\begin{aligned} \|Y_r\|^2 &= Y_r^* Y_r = Z^* F^* \mathrm{diag}(0,1,0,\ldots,0,1) F Z \\ &= \widehat{Z}^* \mathrm{diag}(0,1,\ldots,0,1) \widehat{Z} \\ &= |\widehat{z}_2|^2 + |\widehat{z}_n|^2 \\ &= \text{constante (en ce qui concerne } r). \end{aligned}$$

De ceci découle immédiatement que *si la seconde et la* $n^{\text{ième}}$ *composantes de* FZ*, la transformée de Fourier de* Z*, sont toutes deux non nulles, alors les* Y_r *sont une famille de* n*-gones non nuls de moment d'inertie constant.*

Dans ce cas, alors, la vitesse de convergence de $C^r Z$ est précisément $|\lambda_2|^{-r}, r \to \infty$. Notons à partir de (4.4.3) ou de la Figure 4.4.1 que lorsque $n \to \infty$, $\lambda_2 \to 1$, de telle façon que *plus il y a de sommets dans le* n*-gone, plus lente est la convergence.*

La séquence des n-gones $C^r Z/|\lambda_2|^r$ sera dite *normalisée* et on appellera famille Y_r l'"approche" par les n-gones normalisés. Cela présente un intérêt de regarder la nature géométrique des Y_r.

Lemme. Soit $Z = (z_1, z_2, ..., z_n)^T$. Soit

$$p_Z(u) = z_1 + z_2 u + z_3 u^2 + \ldots + z_n u^{n-1} \tag{4.4.12}$$

Pour $r = 1, 2, \ldots, n$, soit

$$k = n + 1 - r. \tag{4.4.13}$$

Alors

$$B_r Z = \frac{1}{n}(p_Z(w^k))(1, \overline{w}^k, \overline{w}^{2k}, \ldots, \overline{w}^{(n-1)k})^T. \tag{4.4.14}$$

En particulier,

$$B_2 Z = \frac{1}{n}(p_Z(\overline{w}))(1, w, w^2, \ldots, w^{n-1})^T, \tag{4.4.15}$$

$$B_n Z = \frac{1}{n}(p_Z(w))(1, w, \overline{w}, \overline{w}^2, \ldots, \overline{w}^{n-1})^T. \tag{4.4.16}$$

PREUVE. À partir de (3.4.12), $B_r = 1/n$ circ$(1, w^k, w^{2k}, \ldots, w^{(n-1)k})$. Par conséquent, chaque ligne de B_r est la ligne précédente multipliée par $\overline{w}^k$. Évident. Les identités devraient maintenant être évidentes.

Lemme. *Soit $z = x + iy, z' = x' + iy', \tau_1, \tau_2$ deux complexes.*

Alors

$$z' = \tau_1 \overline{z} + \tau_2 z \tag{4.4.17}$$

est une transformation affine du plan (x, y). Elle est non singulière si et seulement si $|\tau_1| \neq |\tau_2|$.

PREUVE. Écrivons $\tau_1 = \xi_1 + i\eta_1, \tau_2 = \xi_2 + i\eta_2$, où les ξ et les η sont réels. Alors la transformation (4.4.17) peut s'écrire

$$\begin{aligned} x' &= (\xi_1 + \xi_2)x + (\eta_1 - \eta_2)y \\ y' &= (\eta_1 + \eta_2)x + (\xi_2 - \xi_1)y. \end{aligned} \tag{4.4.18}$$

Ceci est une transformation affine du plan x, y. Le déterminant Δ de la transformation est

$$\Delta = \xi_2^2 - \xi_1^2 - \eta_1^2 + \eta_2^2 = |\tau_2|^2 - |\tau_1|^2$$

de telle façon que $\Delta \neq 0$ si et seulement si $|\tau_1| \neq |\tau_2|$.

Théorème 4.4.1. Si $|\widehat{z}_2| \neq |\widehat{z}_n|$, les n-gones Y_r sont non nuls, et de moment d'inertie constant. Ce sont les images affines de polygone régulier unité à n côtés, par conséquent, ils sont convexes.

PREUVE. On a

$$\begin{aligned} Y_r &= e^{ir\theta} B_2 Z + e^{-ir\theta} B_n Z \\ &= e^{ir\theta} \frac{1}{n} p_Z(w)(1, \overline{w}, \overline{w}^2, ..., \overline{w}^{n-1})^T + e^{-ir\theta} \frac{1}{n} p_Z(\overline{w})(1, w, w^2, ..., w^{n-1})^T. \end{aligned}$$

Par conséquent, si on écrit $\tau_1 = (1/n)e^{ir\theta} p_Z(w), \tau_2 = (1/n)e^{-ir\theta} p_Z(\overline{w})$, les sommets dans Y_r sont les images de $(1, w, w^2, \ldots, w^{n-1})$ sous $z' = \tau_1 \overline{z} + \tau_2 z$. Puisque $p_Z(w) = \widehat{z}_n$ et $p_Z(\overline{w}) = \widehat{z}_2$, il en découle que $|\tau_1| \neq |\tau_2|$. Ceci est une transformation affine non singulière et toutes les transformations de ce type envoient les figures convexes sur des figures convexes.

Pour une analyse plus poussée, on fait la supposition que θ est un multiple rationnel de 2π. Dans ce cas, on peut identifier les limites de la sous-séquence des figures normalisées $C^r Z/|\lambda_2|^r, r = 0, 1, 2, \ldots$.

Plutôt que de travailler généralement, on supposera que

$$s = t = 1/2. \tag{4.4.19}$$

Cela amène immédiatement à

$$|\lambda_2| = cos\frac{\pi}{n}, \qquad \theta = \frac{\pi}{n} \tag{4.4.20}$$

de telle façon que (4.4.9) devient

$$\frac{C^r Z}{(\cos \pi/n)^r} = e^{\pi i r/n} B_2 Z + e^{-\pi i r/n} B_n Z + \varepsilon(r). \tag{4.4.21}$$

Posons maintenant

$$r = 2jn + b, \qquad 0 \leq b \leq 2n - 1, \qquad j = 0, 1, \ldots. \tag{4.4.22}$$

Alors (4.4.21) devient

$$\frac{C^{2jn+b} Z}{(\cos \pi/n)^{2jn+b}} = e^{\pi i b/n} B_2 Z + e^{-\pi i b/n} B_n Z + \varepsilon(2jn + b). \tag{4.4.23}$$

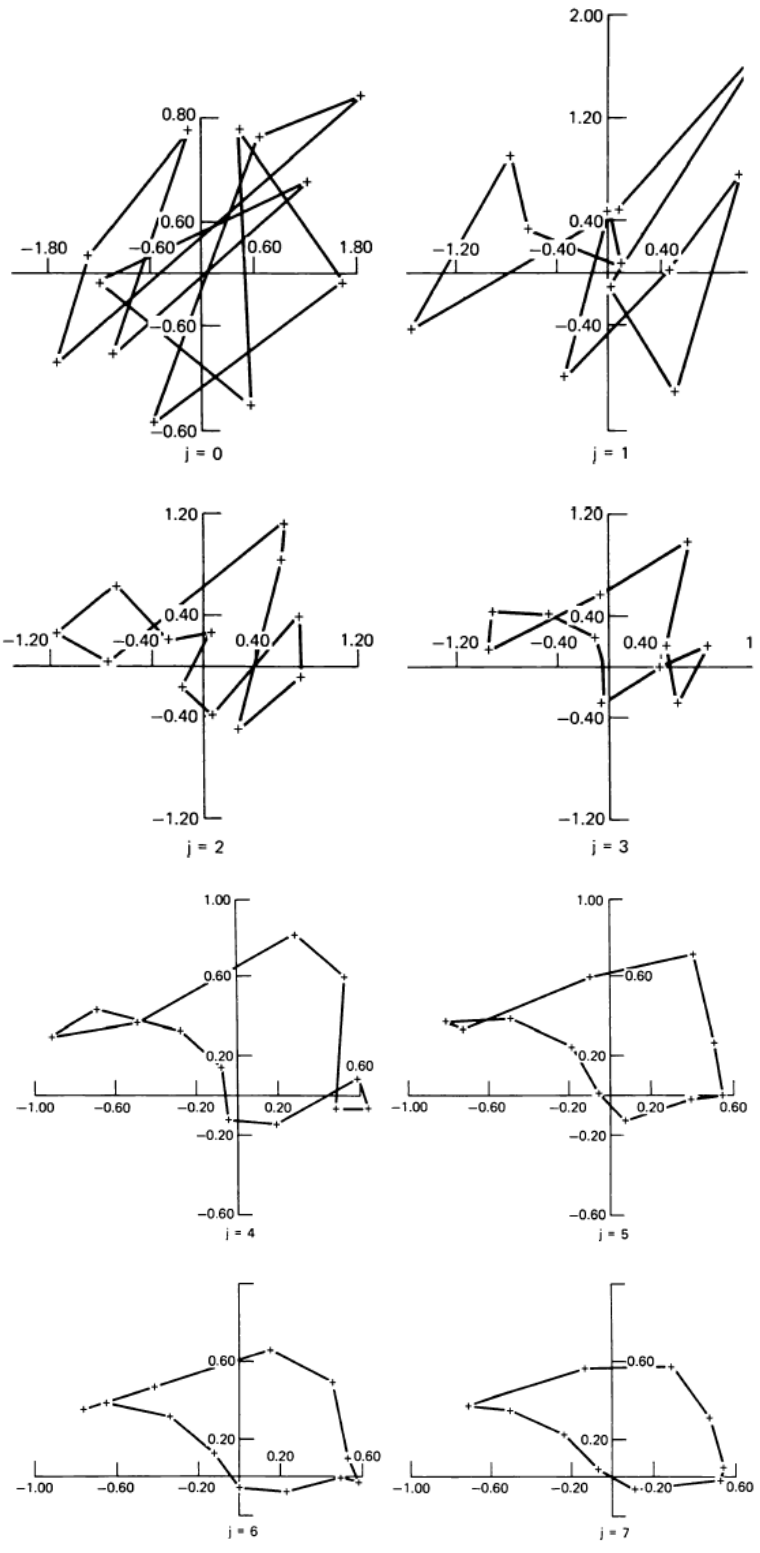
En écrivant

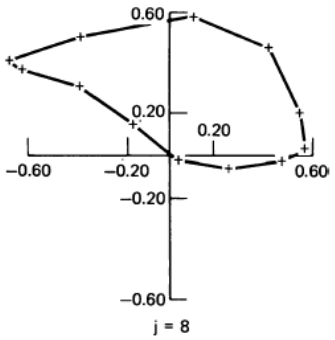
$$\begin{aligned} U_b &= e^{\pi i b/n} B_2 Z + e^{-\pi i b/n} B_n Z \\ &= F^* \mathrm{diag}(0, e^{\pi i b/n}, 0, 0, \ldots, 0, e^{-\pi i b/n}) F Z, \end{aligned} \tag{4.4.24}$$

on a maintenant

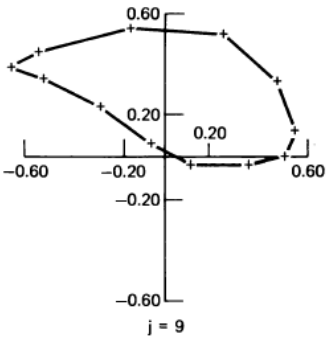
$$\lim_{j\to\infty} \frac{C^{2jn+b} Z}{(\cos \pi/n)^{2jn+b}} = U_b, \qquad b = 0, 1, 2, \ldots, 2n - 1, \tag{4.4.25}$$

de telle façon que les n-gones normalisés approchent les n-gones de limite $2n$, chacun des polygones étant est une transformation affine d'un n-gone régulier. Voir la figure 4.4.2.

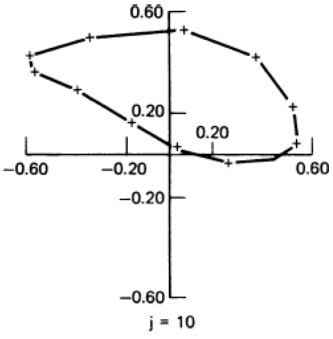

0.80
0.60
−1.80
−0.60
0.60
1.80
−0.60
−0.60
j = 0
2.00
1.20
0.40
−1.20
−0.40
0.40
−0.40
j = 1
1.20
0.40
−1.20
−0.40
0.40
1.20
−0.40
−1.20
j = 2
1.20
0.40
−1.20
−0.40
0.40
1
−0.40
−1.20
j = 3
1.00
0.60
0.20
0.60
−1.00
−0.60
−0.20
0.20
−0.20
−0.60
j = 4
1.00
0.60
0.20
−1.00
−0.60
−0.20
0.20
0.60
−0.20
−0.60
j = 5
0.60
0.20
0.20
0.60
−1.00
−0.60
−0.20
j = 6
0.60
0.20
−1.00
−0.60
−0.20
0.20
0.60
j = 7



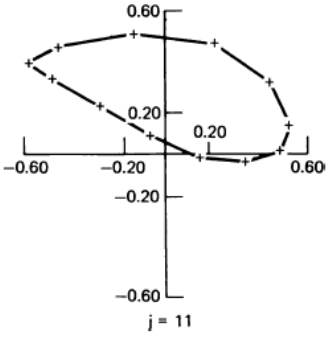
j = 8



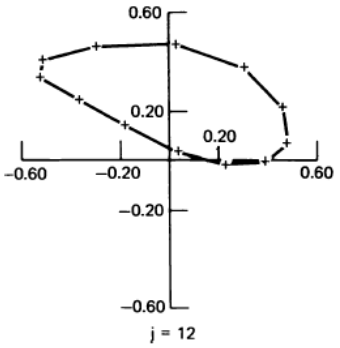
j = 9



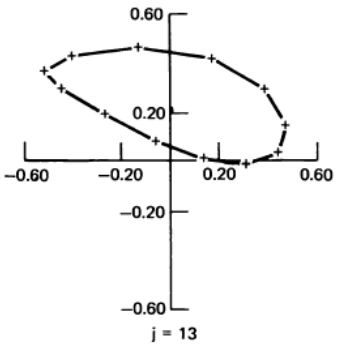
j = 10



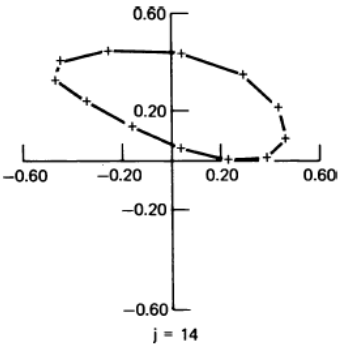
j = 11



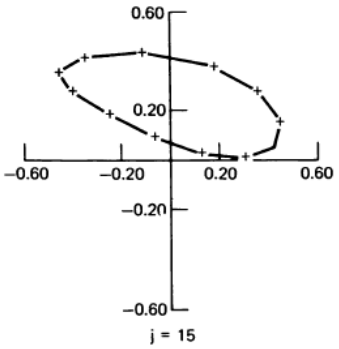
j = 12



j = 13



j = 14



j = 15

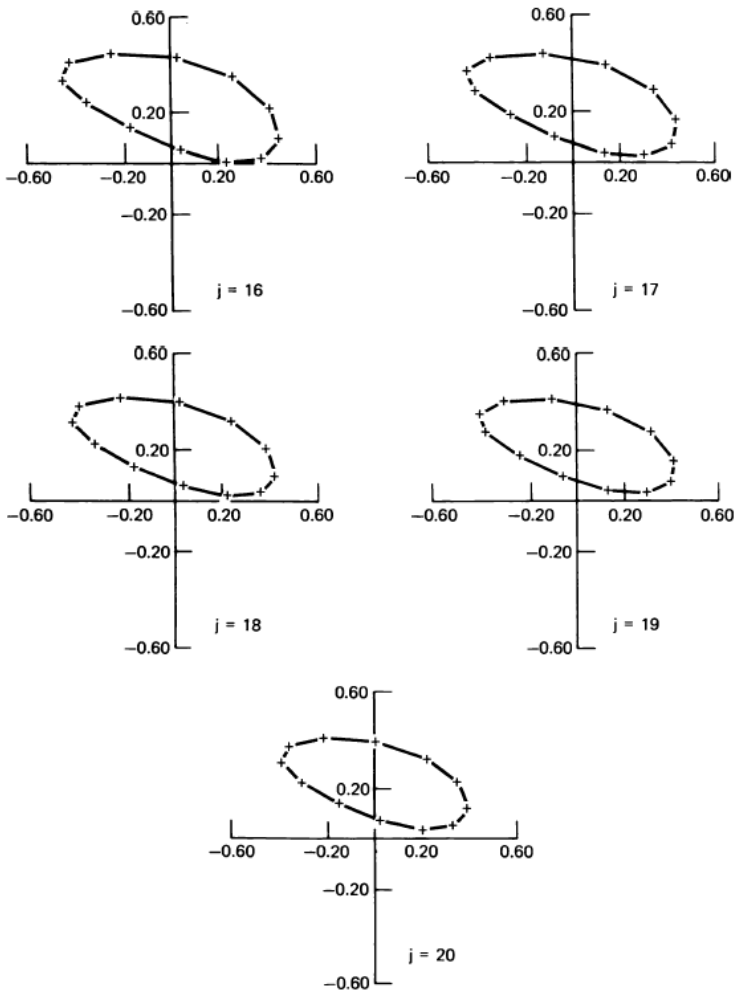


FIG. 4.4.2

Traduction du troisième chapitre du livre de Robert M. Gray, *Toeplitz and circulant matrices : a review*[1], Denise Vella-Chemla, juin 2023.

3. Matrices circulantes

Les propriétés des matrices circulantes sont bien connues et facilement démontrées ([15], p. 267,[6]). Puisque ces matrices sont utilisées à la fois pour approximer et pour expliquer le comportement des matrices de Toeplitz, il est instructif de présenter une version des démonstrations pertinentes ici.

3.1. Valeurs propres et vecteurs propres

Une matrice circulante C est une matrice de la forme

$$C = \begin{bmatrix} c_0 & c_1 & c_2 & \dots & \dots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & c_2 & \dots & \vdots \\ \vdots & c_{n-1} & c_0 & c_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & c_2 \\ \vdots & \ddots & \ddots & \ddots & \ddots & c_1 \\ c_1 & \dots & \dots & c_{n-1} & c_0 & \end{bmatrix}, \tag{3.1}$$

où chaque ligne est un décalage cyclique de la ligne au-dessus d'elle. La structure peut aussi être caractérisée en remarquant que l'entrée (k, j) de $C, C_{k,j}$, est donnée par

$$C_{k,j} = C_{(j-k) \bmod n},$$

qui permet de voir C comme un type particulier de matrices de Toeplitz.

Les valeurs propres ψ_k et les vecteurs propres $y^{(k)}$ de C sont les solutions de

$$Cy = \psi y \tag{3.2}$$

ou, de façon équivalente, des n équations aux différences

$$\sum_{k=0}^{m-1} c_{n-m+k} y_k + \sum_{k=m}^{n-1} c_{k-m} y_k = \psi y_m \; ; \qquad m = 0, 1, \dots, n-1. \tag{3.3}$$

En changeant la sommation au niveau des variables muettes, on obtient

$$\sum_{k=0}^{n-1-m} c_k y_{k+m} + \sum_{k=n-m}^{n-1} c_k y_{k-(n-m)} = \psi y_m \; ; \quad m = 0, 1, \dots, n-1. \tag{3.4}$$

On peut résoudre les équations aux différences comme on résout les équations différentielles - en devinant (avec espoir) une solution intuitive et en prouvant ensuite que c'en est bien une. Puisque l'équation est linéaire avec coefficients constants, une supposition raisonnable est $y_k = \rho^k$ (analogue aux équations différentielles $y(t) = e^{s\tau}$ invariantes en temps linéaire). La substitution dans (3.4) et l'élimination de ρ^m amène

[1] Référence : https://ee.stanford.edu/ gray/toeplitz.pdf

$$\sum_{k=0}^{n-1-m} c_k\rho^k + \rho^{-n}\sum_{k=n-m}^{n-1} c_k\rho^k = \psi.$$

Ainsi, si on choisit $\rho^{-n} = 1$, i.e., ρ est une des n racines complexes $n^{\text{ièmes}}$ de l'unité, alors on a une valeur propre

$$\psi = \sum_{k=0}^{n-1} c_k\rho^k \tag{3.5}$$

avec le vecteur propre correspondant

$$y = n^{-1/2}(1, \rho, \rho^2, \ldots, \rho^{n-1})', \tag{3.6}$$

où le symbole prime (') dénote la transposition où la normalisation est choisie pour donner l'énergie unité au vecteur propre. En choisissant ρ_m comme $n^{\text{ième}}$ racine de l'unité, $\rho_m = e^{-2\pi im/n}$, on a la valeur propre

$$\psi_m = \sum_{k=0}^{n-1} c_k e^{-2\pi imk/n} \tag{3.7}$$

et le vecteur propre

$$y^{(m)} = n^{-1/2}\left(1, e^{-2\pi im/n}, \ldots, e^{-2\pi i(n-1)/n}\right).$$

À partir de (3.7), on peut écrire

$$C = U\Psi U^*, \tag{3.8}$$

où

$$\begin{aligned} U &= \{y^{(0)}|y^{(1)}|\ldots|y^{(n-1)}\} \\ &= n^{-1/2}\{e^{-2\pi imk/n}\ ; m, k = 0, 1, \ldots, n-1\} \\ \Psi &= \{\psi_k\delta_{k-j}\} \end{aligned}$$

et où δ est le delta de Kronecker,

$$\delta_m = \begin{cases} 1 & \text{si } m = 0, \\ 0 & \text{sinon.} \end{cases}$$

Pour vérifier (3.8), appelons $a_{k,j}$ le $(k,j)^{\text{ième}}$ élément de $U\Psi U^*$ et observons que $a_{k,j}$ sera le produit de la $k^{\text{ième}}$ ligne de $U\Psi$, qui est $\{n^{-1/2}e^{-2\pi imk/n}\Psi_k\ ; m = 0, 2, ..., n-1\}$, fois la $j^{\text{ième}}$ ligne de U, $\{n^{-1/2}, e^{2\pi imj/n}\ ; m = 0, 2, ..., n-1\}$ de telle façon que

$$\begin{aligned} a_{k,j} &= n^{-1}\sum_{m=0}^{n-1} e^{2\pi im(j-k)/n}\psi_m \\ &= n^{-1}\sum_{m=0}^{n-1} e^{2\pi im(j-k)/n}\sum_{r=0}^{n-1} c_r e^{-2\pi imr/n} \qquad (3.9) \\ &= n^{-1}\sum_{r=0}^{n-1} c_r\sum_{m=0}^{n-1} e^{2\pi im(j-k-r)/n}. \end{aligned}$$

Mais on a

$$\sum_{m=0}^{n-1} e^{2\pi i m(j-k-r)/n} = \begin{cases} n & \text{si } k-j = -r \bmod n \\ 0 & \text{sinon} \end{cases}$$

de telle façon que $a_{k,j} = c_{-(k-j) \bmod n}$. Par conséquent, (3.8) et (3.1) sont équivalents. De plus, (3.9) montre que n'importe quelle matrice exprimable sous la forme (3.8) est une matrice circulante.

Il devrait aussi être familier à ceux qui ont une formation d'ingénierie standard que ψ_m dans (3.7) est simplement la transformée de Fourier discrète (DFT) de la séquence c_k et (3.8) peut être interprétée comme une combinaison de la formule d'inversion de Fourier et de la formule de décalage cyclique de Fourier.

Puisque C est unitairement similaire à une matrice diagonale, ceci est normal. Notons que toutes les matrices circulantes ont le même ensemble de vecteurs propres.

3.2 Propriétés

Le théorème suivant résume les propriétés dérivées dans la section précédente qui concernent les valeurs propres et les vecteurs propres de matrices circulantes et fournit quelques implications faciles.

Théorème 3.1. Soit $C = \{c_{k-j}\}$ et $B = \{b_{k-j}\}$ des matrices circulantes ayant pour valeurs propres

$$\psi_m = \sum_{k=0}^{n-1} c_k e^{-2\pi i m k/n}$$

$$\beta_m = \sum_{k=0}^{n-1} b_k e^{-2\pi i m k/n} ,$$

respectivement.

(1) C et B commutent et

$$CB = BC = U^* \gamma U \quad ,$$

où $\gamma = \{\psi_m \beta_m \delta_{k,m}\}$, et CB est aussi une matrice circulante.

(2) $C + B$ est une matrice circulante et

$$C + B = U^* \Omega U$$

où $\Omega = \{(\psi_m + \beta_m)\delta_{k,m}\}$

(3) Si $\psi_m \neq 0 \; ; m = 0, 1, ..., n-1$, alors C est non singulière et

$$C^{-1} = U^* \Psi^{-1} U$$

de telle façon que l'inverse de C peut être construite d'une manière évidente.

Preuve. On a $C = U^*\Psi U$ et $B = U^*\Phi U$ où Ψ et Φ sont des matrices diagonales avec pour éléments $\psi_m\delta_{k,m}$ et $\beta_m\phi_{k,m}$, respectivement.

(1) $$\begin{aligned} CB &= U^*\Psi U U^*\Phi U \\ &= U^*\Psi\Phi U \\ &= U^*\Phi\Psi U = BC \end{aligned}$$
Puisque $\Psi\Phi$ est diagonale, (3.9) implique que CB est une matrice circulante.

(2) $$C + B = U^*(\Psi + \Phi)U.$$

(3) $$\begin{aligned} C^{-1} &= (U^*\Psi U)^{-1} \\ &= U^*\Psi^{-1}U \end{aligned}$$
si Ψ est non singulière.

Les matrices circulantes sont une classe de matrices particulièrement gérables puisque les inverses, les produits, et les sommes sont aussi des matrices circulantes et par conséquent sont évidentes à construire et normales. De plus, les valeurs propres de telles matrices peuvent facilement être trouvées exactement.

Dans le prochain chapitre, on verra que certaines matrices circulantes approximent asymptotiquement les matrices de Toeplitz et par conséquent, des résultats similaires à ceux du théorème 3.1 seront asymptotiquement vérifiés par les matrices de Toeplitz.

Références

[6] P. J. Davis, *Circulant Matrices*, Wiley-Interscience, NY, 1979.

[15] P. Lancaster, *Theory of Matrices*, Academic Press, NY, 1969.

Pensées impulsées (Denise Vella-Chemla, juin 2023)

On voudrait noter ici une toute petite idée suite à la traduction de la dernière note d'Alain Connes et Caterina Consani intitulée *Riemann-Roch pour l'anneau* $\mathbb{Z}$[1] et de la retranscription du texte d'André Weil en référence de l'article en question, et intitulé *Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques* ([3])[2] .

On retrouve deux extraits de textes d'André Weil.

Un extrait de *De la métaphysique aux mathématiques* ([1])

> Heureusement pour les chercheurs, à mesure que les brouillards se dissipent sur un point, c'est pour se reformer sur un autre. Une grande partie du colloque de Tokyo s'est déroulée sous le signe des analogies entre la théorie des nombres et la théorie des fonctions algébriques. Là, nous sommes encore en pleine métaphysique. C'est de ces analogies, parce que j'en ai quelque expérience personnelle, que je voudrais parler ici, avec l'espoir, vain peut-être, de donner aux lecteurs "honnêtes gens" de cette revue quelque idée des méthodes de travail en mathématique.
>
> Dès l'enseignement élémentaire, on fait voir aux élèves que la division des polynômes (à une variable) ressemble beaucoup à la division des entiers et conduit à des lois toutes semblables. Pour les uns comme pour les autres, il y a un plus grand commun diviseur, dont la détermination se fait par division successive. À la décomposition des nombres entiers en facteurs premiers correspond la décomposition des polynômes en facteurs irréductibles ; aux nombres rationnels correspondent les fonctions rationnelles, qui, elles aussi, peuvent toujours se mettre sous forme de fractions irréductibles ; celles-ci s'ajoutent par réduction au plus petit commun dénominateur, etc. Il est donc tout naturel de penser qu'il y a analogie entre les nombres algébriques (racines d'équations dont les coefficients sont des nombres entiers) et les fonctions algébriques d'une variable (racines d'équations dont les coefficients sont des polynômes à une variable).
>
> Le fondateur de la théorie des fonctions algébriques d'une variable aurait sans doute été Galois s'il avait vécu ; c'est ce que permettent de penser les indications qu'on trouve sur ce sujet dans sa célèbre lettre-testament, écrite à la veille de sa mort, d'où on peut conclure qu'il touchait déjà à quelques-unes des principales découvertes de Riemann. Peut-être aurait-il donné à cette théorie une allure algébrique, conforme à l'esprit des travaux contemporains d'Abel et de ses propres recherches d'algèbre pure.
>
> Au contraire, Riemann, l'un des moins algébristes sans doute parmi les grands mathématiciens du XIXème siècle, mit la théorie sous le signe du "transcendant" (mot qui, pour le mathématicien, s'oppose à "algébrique", et désigne tout ce qui appartient en propre au continu). Les méthodes très puissantes mises en œuvre par Riemann

[1] traduction de l'article arxiv du 2 juin 2023 https://arxiv.org/pdf/2306.00456.pdf à l'adresse http://denise.vella.chemla.free.fr/trad-2306-00456-fr.pdf.

[2] à l'adresse http://denise.vella.chemla.free.fr/transc-Weil-analogie.pdf.

amenèrent presque du premier coup la théorie à un degré d'achèvement qui n'a guère été dépassé. Mais elles ne tiennent aucun compte des analogies avec les nombres algébriques, et ne peuvent être transposées telles quelles en vue de l'étude de ceux-ci, étude qui relève traditionnellement de l'arithmétique ou de la théorie des nombres, et qui, du vivant déjà de Riemann, était, en voie de développement rapide.

C'est Dedekind, ami intime de Riemann, mais algébriste consommé, qui devait le premier tirer parti des analogies en question et en faire un instrument de recherche. Il appliqua avec succès, aux problèmes traités par Riemann par voie transcendante, les méthodes qu'il avait lui-même créées et mises au point en vue de l'étude arithmétique des nombres algébriques ; et il fit voir qu'on peut retrouver ainsi la partie proprement algébrique de l'œuvre de Riemann.

À première vue, les analogies ainsi mises en évidence restaient superficielles, et ne paraissaient pas pouvoir porter sur les problèmes les plus profonds de l'une ni de l'autre théorie. Hilbert alla plus loin dans cette voie, à ce qu'il semble ; mais, s'il est probable que ses élèves subirent l'influence de ses idées sur ce sujet, il n'en est resté quelque trace que dans un compte rendu obscur qui n'a même pas été reproduit dans ses Œuvres complètes. Les lois non écrites de la mathématique moderne interdisent, en effet, de publier des vues métaphysiques de cette espèce. Sans doute est-ce mieux ainsi ; autrement on serait accablé d'articles encore plus stupides, sinon plus inutiles, que tous ceux qui encombrent à présent nos périodiques. Mais il est dommage que les idées de Hilbert n'aient été développées par lui nulle part. Il y avait loin encore, cependant, de l'arithmétique, où règne le discontinu, à la théorie des fonctions au sens classique. Or, en disant que les fonctions algébriques sont racines d'équations dont les coefficients sont des polynômes, j'ai volontairement omis un point important: ces polynômes eux-mêmes ont des coefficients mais ceux-ci, quels sont-ils ? Lorsqu'on traite de la division des polynômes dans l'enseignement élémentaire, il va sans dire que les coefficients sont des "nombres" : nombres "réels" (rationnels ou non, mais donnés en tout cas, si on veut, par un développement décimal), ou, à un niveau un peu plus élevé, nombres "réels ou imaginaires", ou, comme on dit, "nombres complexes". C'est exclusivement de nombres complexes qu'il s'agit dans la théorie riemannienne.

Mais, du point de vue de l'algébriste pur, tout ce qu'on demande aux "nombres" en question, c'est qu'ils se laissent combiner entre eux au moyen des quatre opérations (ce que l'algébriste exprime en disant qu'ils forment un "corps"). Si on n'en suppose pas plus sur leur compte, on obtient une théorie des fonctions algébriques, fort riche déjà (comme en témoigne le volume récent et déjà classique qu'a publié Chevalley sur ce sujet), mais qui ne l'est pas assez, pour que les analogies avec les nombres algébriques puissent être poursuivies jusqu'au bout.

Heureusement il s'est trouvé un domaine intermédiaire entre l'arithmétique et la théorie riemannienne, et qui possède, avec chacune de ces deux dernières théories, des ressemblances beaucoup plus étroites qu'elles n'en ont entre elles ; il s'agit des fonctions algébriques "sur un corps fini".

Comme on le savait depuis Gauss, s'il ne s'agit que de pouvoir faire les quatre opérations, il suffit d'un nombre fini d'éléments. Il suffit par exemple d'en avoir deux, qu'on nommera 0 et 1, et pour lesquels on posera par convention la table d'addition et la table de multiplication que voici[a] :

$$\begin{array}{lll} 0+0=0 & 0+1=1+0=1 & 1+1=0 \\ 0\times 0=0 & 0\times 1=1\times 0=0 & 1\times 1=1 \end{array}$$

Quelque paradoxale que puisse paraître au profane la règle $1+1=0$, quelque tentant qu'il soit de dire que c'est là un pur jeu de l'esprit qui ne répond à aucune "réalité", un tel système est monnaie courante pour le mathématicien ; et Galois en étendit beaucoup l'usage en construisant les "imaginaires de Galois".

Prenant donc les coefficients de nos polynômes dans un "corps de Galois", on construit des fonctions algébriques dont la théorie remonte à Dedekind mais s'est particulièrement développée depuis la thèse d'Artin. Pour dire en quoi elle consiste, il faudrait entrer dans des détails beaucoup trop techniques qui n'auraient pas leur place ici. Mais on peut, je crois, en donner une idée imagée en disant que le mathématicien qui étudie ces problèmes a l'impression de déchiffrer une inscription trilingue. Dans la première colonne se trouve la théorie riemannienne des fonctions algébriques au sens classique. La troisième colonne, c'est la théorie arithmétique des nombres algébriques. La colonne du milieu est celle dont la découverte est la plus récente ; elle contient la théorie des fonctions algébriques sur un corps de Galois.

Ces textes sont l'unique source de nos connaissances sur les langues dans lesquels ils sont écrits ; de chaque colonne, nous n'avons bien entendu que des fragments ; la plus complète et celle que nous lisons le mieux, encore à présent, c'est la première. Nous savons qu'il y a de grandes différences de sens d'une colonne à l'autre, mais rien ne nous en avertit à l'avance. À l'usage, on se fait des bouts de dictionnaire, qui permettent de passer assez souvent d'une colonne à la colonne voisine.

C'est ainsi qu'on avait déchiffré depuis longtemps, dans la dernière colonne, le début d'un paragraphe intitulé "fonction zéta". Vers la fin de ce paragraphe, on croit lire une phrase très mystérieuse ; elle dit que tous les zéros de la fonction se trouvent sur une certaine droite. Jamais on n'a pu savoir s'il en est bien ainsi, ou s'il y a eu erreur de lecture. C'est le célèbre problème de l'"hypothèse de Riemann", qui dans quelques mois sera tout juste centenaire.

La principale découverte d'Artin, dans sa thèse, c'est qu'il y a, dans la seconde colonne, un paragraphe intitulé aussi "fonction zéta", et qui est à peu de chose près une traduction de celui qu'on connaissait déjà ; notre dictionnaire s'en est trouvé beaucoup enrichi. Artin aperçut aussi, dans cette colonne, la phrase sur l'hypothèse de Riemann ; elle lui parut tout aussi mystérieuse que l'autre. Ce nouveau problème, à première vue, ne semblait pas plus facile que le précédent. En réalité, nous savons maintenant que la première colonne contenait déjà tous les éléments de sa solution. Il n'était que de traduire, d'abord en

[a] Remarque de la scribe : dans l'algèbre booléenne qu'utilisent les informaticiens, $1+1=1$, ci-dessous, sont fournis les règles de l'addition et de la multiplication de $\mathbb{Z}/2\mathbb{Z}$

théorie “abstraite” des fonctions algébriques, puis dans le langage “galoisien” de la seconde colonne, des résultats obtenus depuis longtemps par Hurwitz en “riemannien”, et que les géomètres italiens avaient ensuite traduits dans leur propre langage. Mais les meilleurs spécialistes des théories arithmétique et “galoisienne” ne savaient plus lire le riemannien, ni à plus forte raison l'italien ; et il fallut vingt ans de recherches avant que la traduction fut mise au point et que la démonstration de l'hypothèse de Riemann dans la seconde colonne fut complètement déchiffrée.

Si notre dictionnaire était suffisamment complet, nous passerions aussitôt de là à la troisième colonne, et l'hypothèse de Riemann, la vraie, se trouverait démontrée, elle aussi. Mais nos connaissances n'atteignent pas jusque là ; bien des déchiffrements patients seront encore nécessaires avant que la traduction puisse être faite. Au cours du colloque auquel il a été fait allusion plus haut, il a été beaucoup discuté de “métaphysique” à propos de ces problèmes ; un jour celle-ci fera place à une théorie mathématique dans le cadre de laquelle ils trouveront leur solution. Peut-être, comme c'était le cas pour Lagrange, ne nous manque-t-il, pour franchir ce pas décisif, qu'une notion, un concept, une “structure”. D'ingénieux philologues ont bien trouvé le secret des archives de Nestor et de celles de Minos. Combien de temps faudra-t-il encore pour que notre pierre de Rosette, à nous autres arithméticiens, rencontre son Champollion ?

Petit encart de la scribe : cette référence à la pierre de Rosette nous ramène à la lecture d'un ancien roman intitulé *Le Secret de Champollion*, de Jean-Michel Riou et qui raconte, sous une forme épistolaire, la quête de Champollion pour déchiffrer les hiéroglyphes. Il s'agit d'établir un dictionnaire vers un langage que l'on ne connaît pas. On peut considérer qu'on essaie par les recherches sur la conjecture de Goldbach ou l'hypothèse de Riemann d'établir un dictionnaire entre des espaces que l'on comprendrait déjà vers l'espace des nombres premiers, dont on ne connaît pas encore la véritable nature.

Un extrait de *L'avenir des mathématiques* ([2])

Ce qui précède met déjà en évidence, non seulement la vitalité de l'arithmétique moderne, mais aussi les liens étroits qui, aujourd'hui, comme au temps d'Euler et au temps de Jacobi, l'unissent aux parties les plus profondes de la théorie des groupes et de la théorie des fonctions. Cette unité essentielle, dont les manifestations sont si diverses et multiples, se retrouve sur bien d'autres points. L'introduction par Hermite des variables continues dans la théorie des nombres a abouti à l'étude systématique des groupes discontinus de nature arithmétique au moyen des groupes continus dans lesquels ils se laissent plonger, des espaces riemanniens symétriques associés à ces groupes, des propriétés différentielles et topologiques de leurs domaines fondamentaux (ou plutôt, dans le langage moderne, de leurs espaces quotients), et des fonctions automorphes qui y appartiennent. L'œuvre de Siegel, continuant la grande tradition de Dirichlet, d'Hermite, de Minkowski, nous a ouvert ici des voies toutes nouvelles. D'un côté, nous rejoignons par là Fermat, Lagrange

> et Gauss, la représentation des nombres par les formes, et les genres de formes quadratiques. En même temps commence à se préciser à nos yeux le principe si fécond d'après lequel l'aspect global d'un problème arithmétique peut, en certaines circonstances, se reconstituer à partir de ses aspects locaux. Par exemple, nous voyons à maintes reprises, chez Siegel, le nombre de solutions de tel problème arithmétique dans le corps des nombres rationnels exprimé au moyen des nombres définis par les problèmes locaux correspondants, densités de solutions dans le corps réel et dans les corps p-adiques pour toutes les valeurs du nombre premier p c'est là un principe, analogue au théorème des résidus sur la surface de Riemann d'une courbe algébrique, auquel il y a lieu de rattacher aussi les célèbres "séries singulières" qui apparaissent dans l'application de la méthode de Hardy-Littlewood aux problèmes de la théorie analytique des nombres. Est-il possible d'en donner un énoncé général, qui permette d'un seul coup d'obtenir tous les résultats de cette nature, de même que la découverte du théorème des résidus a permis de calculer par une méthode uniforme tant d'intégrales et de séries qu'on ne traitait auparavant que par des procédés disparates ? Ce n'est pas là encore, semble-t-il, un problème pour l'avenir immédiat ; il n'en est que plus important d'en préparer la solution par l'examen de cas particuliers bien choisis. C'est le même principe qui fournira peut-être un jour la raison profonde de l'existence des produits eulériens, dont les recherches de Hecke viennent seulement de nous révéler l'extrême importance en théorie des nombres et en théorie des fonctions ; ici, ce sont les classes mêmes des formes quadratiques, et non pas seulement comme avec Siegel leurs genres, que nous commençons à atteindre ; en même temps, nous nous trouvons au cœur de la théorie des fonctions modulaires, que ces travaux ont renouvelée entièrement, et de la théorie des fonctions thêta. Ce domaine est encore pour nous si mystérieux, les questions qui s'y posent sont si nombreuses et si fascinantes, que toute tentative pour les classer par ordre d'importance serait prématuré.

On a différents ensembles (celui des réels, celui des complexes, celui des entiers p-adiques de Hensel, celui des polynômes du second degré, celui des polynômes de degré 3 munis de certaines fonctions et on essaie de trouver un ensemble "prototypal"[3] dont les trois ensembles sus-cités (et potentiellement d'autres) seraient autant d'instances différentes.

On doit aussi trouver une (ou des) fonction entre chacun des ensembles et le prototype qui préserve les structures.

Références

[1] André Weil, Œuvres scientifiques / Collected papers, vol. 2, (1951-1964), De la métaphysique aux mathématiques, Springer-Verlag, 1960 (a), p. 408.

[2] _____, Œuvres scientifiques / Collected papers, vol. 1, (1926-1951), L'avenir des mathématiques, Springer-Verlag, 1947 (a), p. 359.

[3] _____, Œuvres scientifiques / Collected papers, vol. 1, (1926-1951), Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques, Springer-Verlag, 1939 (a), p. 236.

[3] Pour les informaticiens, la notion de prototype correspondrait peut-être à la notion d'objet des *langages orientés objet* ou bien à la notion de type, auxquels sont associées les fonctions pouvant agir en leur sein.

[1939a] Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques

André Weil

On connaît diverses analogies entre les corps de nombres algébriques et les corps de fonctions algébriques d'une variable ; le but de cette note est, par des moyens tout élémentaires, de préciser en quelques points cette analogie.

Soit K un corps de nombres algébriques, de degré n. Comme on sait, on est conduit à introduire dans l'étude de K des éléments qui correspondent aux points de la surface de Riemann d'un corps de fonctions algébriques d'une variable, et que pour cette raison nous appellerons les "points" de K : on fait correspondre un tel "point" P à toute représentation isomorphe et partout dense de K dans un "corps local" $\mathrm{K_P}$ qui peut être, soit le corps des nombres réels, soit le corps des nombres complexes, soit un corps de nombres P-adiques (au sens de Hensel) ; bien entendu, deux représentations de K ne devront pas être considérées comme distinctes si elles se déduisent l'une de l'autre par un isomorphisme des corps locaux correspondants. Si $\mathrm{K_P}$ est le corps des nombres réels, P s'appellera un point réel à l'infini de K ; si $\mathrm{K_P}$ est le corps des nombres complexes, P s'appellera un point imaginaire à l'infini de K ; si $\mathrm{K_P}$ est un corps P-adique, P correspondra à un idéal premier $\mathfrak{p}$ de K.

Soit α un élément de K ; soit α_{P} l'élément de $\mathrm{K_P}$ qui correspond à α dans la représentation de K dans $\mathrm{K_P}$ définie par P. Nous poserons :

$I_{\mathrm{P}}(\alpha) = \log|\alpha_{\mathrm{P}}|$ si P est un point réel à l'infini ;

$I_{\mathrm{P}}(\alpha) = 2\log|\alpha_{\mathrm{P}}|$ si P est un point imaginaire à l'infini ;

$I_{\mathrm{P}}(\alpha) = -n\cdot\log \mathrm{N}(\mathfrak{p})$ si P est un point de K correspondant à l'idéal premier $\mathfrak{p}$, celui-ci figurant avec l'exposant n dans l'expression de l'idéal principal (α) comme produit de puissances d'idéaux premiers distincts.

Les théorèmes élémentaires connus sur la norme montrent qu'on a, avec ces notations :

$$\sum_{\mathrm{P}} I_{\mathrm{P}}(\alpha) = 0,$$

la sommation étant étendue à tous les points P de K. Bien entendu, $I_{\mathrm{P}}(\alpha)$ ne diffère de zéro que pour un nombre fini de points P de K, de sorte que la somme du premier membre ne comprend qu'un nombre fini de termes non nuls. Cette relation doit être considérée comme analogue arithmétique du théorème algébrique suivant : soit K un corps de fonctions algébriques d'une variable ; x étant un élément de K, et P un point de la surface de Riemann de K, soit $I_{\mathrm{P}}(x)$ l'ordre de x au point P, c'est-à-dire l'entier égal à n si x a en P un pôle d'ordre n, à $-n$ si x a en P un zéro d'ordre n, et à 0 si x n'est ni nul, ni infini en P ; on aura :

$$\sum_{\mathrm{P}} I_{\mathrm{P}}(x) = 0,$$

égalité qui peut être considérée comme un cas particulier du théorème de Cauchy, puisqu'elle résulte de l'égalité :

$$\int d(\log\ x) = 0,$$

lorsque l'intégrale est étendue à un contour formé de $2g$ rétrosections (g étant le *genre* de K).

Considérons maintenant, dans le corps de fonctions algébriques K, le théorème de Riemann-Roch. Celui-ci peut être énoncé sous la forme suivante[1]. Supposons donné, pour chaque point P, un entier n, de telle façon que n_{P} ne diffère de zéro que pour des points P en nombre fini ; soit $n = \sum n_{\mathrm{P}}$ (la sommation étant étendue à tous les points P). Le théorème de Riemann-Roch indique combien il y a d'éléments linéairement indépendants du corps K qui satisfassent, quel que soit P, à la condition

$$I_{\mathrm{P}}(x) \leq n_{\mathrm{P}}$$

En particulier, il indique que, dès que n est assez grand (et, d'une manière précise, dès que $n > 2g - 2$), ce nombre est $n - g + 1$.

Revenons à un corps K de nombres algébriques ; supposons donné pour tout "point" P de K, un nombre réel n_{P}, de façon que n_{P} ne diffère de zéro que pour des points P en nombre fini, et que de plus, si P correspond à un idéal premier $\mathfrak{p}$ de K, n_{P} soit de la forme $\nu(\mathfrak{p}) \cdot \log \mathrm{N}(\mathfrak{p})$, le facteur $\nu(\mathfrak{p})$ étant entier. Posons $n = \sum n_{\mathrm{P}}$. Soit N le nombre des éléments α de K qui satisfont, quel que soit P, à la condition :

$$I_{\mathrm{P}}(\alpha) \leq n_{\mathrm{P}}.$$

Cette condition, si on l'applique d'une part à tous les points P correspondant à des idéaux premiers $\mathfrak{p}$ de K, donne

$$\alpha \in \mathfrak{a} = \prod \mathfrak{p}^{-\nu(\mathfrak{p})}$$

où le second membre ne comprend, en vertu de la définition de n_{P} et de $\nu(\mathfrak{p})$, qu'un nombre fini de facteurs différents de 1, et a donc un sens bien défini. D'autre part, la même condition, appliquée aux points à l'infini de K, donne, pour chaque point réel à l'infini

$$|\alpha_{\mathrm{P}}| \leq e^{n_{\mathrm{P}}}$$

et, pour chaque point imaginaire à l'infini:

$$|\alpha_{\mathrm{P}}|^2 \leq e^{n_{\mathrm{P}}}$$

Si, alors, on désigne par $\alpha_1, \alpha_2, ..., \alpha_n$ une base de l'idéal $\mathfrak{a}$, de sorte que tout élément de $\mathfrak{a}$ soit de la forme :

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n,$$

N apparaîtra comme le nombre de points $(x_1, x_2, \ldots, x_n))$ à coordonnées entières qui se trouvent dans un domaine de l'espace à n dimensions défini par certaines inégalités élémentaires. Nous nous contenterons ici de l'évaluation assez grossière de N qui est fournie par le volume de ce domaine, volume qu'il est facile de calculer élémentairement. On trouve ainsi :

$$\log N = n - \log(2^{-r_1-r_2}\pi^{-r_2}\sqrt{|d|}) + \varepsilon,$$

où r_1 est le nombre des points réels à l'infini de K, r_2 le nombre des points imaginaires à l'infini de K, d le discriminant de K, et où ε est aussi petit qu'on veut dès que, les $\nu(\mathfrak{p})$ étant supposés fixes,

[1] Cf. A. Weil, Zur algebraischen Theorie der algebraischen Funktionen, Journal de Crelle, t. 179 (1938), p. 129.

chacun des nombres n_{P} relatifs aux points à l'infini de K est suffisamment grand.

Pour avoir une formule entièrement analogue au théorème de Riemann-Roch, il faut observer de plus que les racines de l'unité dans K, et elles seules, satisfont à la condition $I_P(\alpha) = 0$ quel que soit P : elles jouent donc le rôle que jouent les constantes dans un corps de fonctions algébriques. Si, dans un corps K de fonctions algébriques, un élément x satisfait en tout point P à la condition $I_{\mathrm{P}}(x) \leq n_{\mathrm{P}}$, il en sera de même de même de cx si c est une constante arbitraire : on a le droit de voir dans ce facteur constant arbitraire l'origine du terme $+1$ du théorème de Riemann-Roch. De même, si, dans un corps de nombres K, un élément α satisfait quel que soit P à la condition $I_{\mathrm{P}}(\alpha) \leq n_{\mathrm{P}}$, le produit de α par une racine de l'unité contenue dans K y satisfait aussi. Cela conduit à poser, en désignant par w le nombre de racines de l'unité contenues dans K :

$$g = \log(2^{-r_1-r_2}\pi^{-r_2} \cdot w\sqrt{|d|}),$$

et à écrire la formule ci-dessus sous la forme:

$$\log \mathrm{N} = n - g + \log w + \varepsilon;$$

le nombre g, qui apparaît ainsi comme le "*genre*" du corps K, joue, comme on sait, un rôle important dans la théorie de la fonction zêta de ce corps. On est conduit à penser, en même temps, que le rôle joué par la quantité $g - 1$ dans la théorie des corps de fonctions sera joué en arithmétique par $g - \log w$; ce qu'on peut confirmer par la remarque suivante. Soit K′ un corps contenant K, non ramifié par rapport à K, et de degré relatif f; s'il s'agit de corps de fonctions algébriques d'une variable, les genres g, g' de K, K′, sont liés entre eux par la relation :

$$g' - 1 = f(g - 1) ;$$

dans le cas arithmétique, le genre étant défini comme ci-dessus, on vérifie facilement que l'on a :

$$g' - \log w' = f(g - \log w).$$

Nous allons maintenant montrer qu'à côté de la formule :

$$\sum_{\mathrm{P}} I_{\mathrm{P}}(\alpha) = 0$$

qui est une traduction des résultats classiques sur les normes, l'on peut mettre une formule non moins élémentaire relative aux traces. Soit α un élément de K ; pour simplifier le langage dans ce qui va suivre, on supposera que α engendre K, c'est-à-dire que, n étant le degré de K, α est racine d'une équation *irréductible* de degré n, à coefficients rationnels :

$$F(t) = t^n - t \cdot t^{n-1} + \ldots = 0$$

Par rapport au corps des nombres réels $\mathrm{F}(t)$ se décompose en r_1 facteurs du premier degré, et r_2 facteurs du second degré, correspondant respectivement aux points à l'infini réels et imaginaires de K. Posons, si P est un point réel à l'infini de K, $\mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}}) = \alpha_{\mathrm{P}}$; si P est un point imaginaire à l'infini, $\mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}}) = \alpha_{\mathrm{P}} + \overline{\alpha}_{\mathrm{P}}$ (la barre dénotant suivant l'usage l'imaginaire conjugué). On aura donc l'expression suivante de la trace r de α :

$$r = \sum_{\mathrm{P}} \mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}})$$

la sommation étant étendue aux points à l'infini de K.

Soit de même p un nombre premier rationnel ; k désignant le corps des nombres rationnels, on désignera par k_{P} le corps *p-adique* correspondant à p. Le polynome $\mathrm{F}(t)$ se décomposera, par rapport à k_{P}, en autant de facteurs que p possède dans K de diviseurs premiers ; chacun de ceux-ci définira un point P de K, et le corps K_{P} contiendra k_{P} ; on désignera par $\mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}})$ la trace de α_{P} par rapport au corps k_{P} : c'est un nombre de k_{P}, et le facteur de $\mathrm{F}(t)$ correspondant à P, s'il est de degré m, commencera par les termes $t^m - \mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}}) \cdot t^{m-1} + ...$ On aura donc :

$$r = \sum_{\mathrm{P}} \mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}})$$

la sommation étant étendue cette fois à tous les points P correspondant aux idéaux premiers de K qui divisent p.

Mais, si u est un nombre quelconque de k_{P}, il existe des entiers rationnels $a,\ b$ tels que $u - a \cdot p^{-b}$ soit un entier de k_{P} ; le nombre $u' = a \cdot p^{-b}$ est bien déterminé, modulo 1, par cette condition : il détermine donc un élément du groupe additif des nombres réels modulo 1, qu'on appellera la partie polaire de u. En particulier, désignons par $t_{\mathrm{P}}(\alpha)$ la partie polaire de $\mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}})$; posons

$$r' = \sum_{\mathrm{P}} t_{\mathrm{P}}(\alpha_{\mathrm{P}})$$

la sommation étant étendue cette fois aux points P correspondant à tous les idéaux premiers de K ; $t_{\mathrm{P}}(\alpha_{\mathrm{P}})$ étant nul chaque fois que α_{P} est entier, c'est-à-dire chaque fois que $I_{\mathrm{P}}(\alpha_{\mathrm{P}}) \leq 0$, la somme du second membre ne contient qu'un nombre fini de termes non nuls. Quel que soit le nombre premier p, le nombre rationnel $r - r'$ est entier dans k_{P} : $r - r'$ est donc entier rationnel, c'est-à-dire que $r \equiv r' \pmod 1$.

Posons alors, chaque fois que P est un point à l'infini de K, $t_{\mathrm{P}}(\alpha_{\mathrm{P}}) = -\mathrm{T}_{\mathrm{P}}(\alpha_{\mathrm{P}}) \pmod 1$. La combinaison des résultats ci-dessus donne la formule que nous avions en vue :

$$\sum_{\mathrm{P}} t_{\mathrm{P}}(\alpha_{\mathrm{P}}) \equiv 0 \pmod 1$$

la sommation étant étendue à tous les points de K.

Cette formule, bien entendu, reste vraie même si α n'engendre pas K.

Soit maintenant ω un élément de K ; l'application de la formule ci-dessus à $\omega\alpha$ donne :

$$\sum_{\mathrm{P}} t_{\mathrm{P}}(\omega_{\mathrm{P}}\alpha_{\mathrm{P}}) \equiv 0.$$

Si, ω étant laissé fixe, on pose $f_{\mathrm{P}}(\alpha_{\mathrm{P}}) = t_{\mathrm{P}}(\omega_{\mathrm{P}}\alpha_{\mathrm{P}})$, f_{P} est un caractère du groupe additif des nombres de K_{P} (c'est-à-dire une représentation continue de ce groupe dans le groupe additif des nombres réels modulo 1). On a ainsi une infinité de relations entre des caractères $f_{\mathrm{P}}(\alpha_{\mathrm{P}})$. Réciproquement, supposons qu'on ait fait correspondre, à tout point P de K, un caractère $f_{\mathrm{P}}(\alpha_{\mathrm{P}})$ du groupe additif

des nombres de K_P, de telle manière que, pour α entier dans K, les $f_P(\alpha_P)$ soient tous nuls à l'exception d'un nombre fini d'entre eux, et qu'ils soient liés, quel que soit α dans K, par la relation

$$\sum_P f_P(\alpha_P) \equiv 0.$$

Il est facile de montrer que dans ces conditions il existe un nombre ω de K tel que l'on ait, quel que soit P :

$$f_P(\alpha_P) \equiv t_P(\omega_P \alpha_P)$$

Autrement dit, nous avons trouvé toutes les relations de la forme indiquée entre caractères locaux des nombres de K. Cela montre que la relation :

$$\sum_P t_P(\omega_P \alpha_P) \equiv 0$$

doit être considérée comme l'analogue arithmétique de la relation (cas particulier du théorème de Cauchy dans la théorie des fonctions algébriques) :

$$\int x\omega = 0,$$

où x est un élément quelconque d'un corps de fonctions algébriques K, ω une différentielle appartenant au même corps, et où l'intégrale est prise le long d'un contour formé de $2g$ rétrosections.

Riemann-Roch pour l'anneau $\mathbb{Z}$

Alain Connes, Caterina Consani

Résumé : On montre que le fait de travailler sur la base absolue $\mathbb{S}$ (la version catégorique du spectre de la sphère) au lieu de $\mathbb{S}[\pm 1]$ améliore notre formule de Riemann-Roch précédente pour $\overline{\operatorname{Spec}\mathbb{Z}}$. La formule rend égales la caractéristique d'Euler (de valeur entière) du diviseur d'Arakelov et la somme du degré du diviseur (en utilisant les logarithmes en base 2) et du nombre 1, confirmant ainsi notre compréhension de l'anneau $\mathbb{Z}$ comme un anneau de polynômes en une variable sur la base absolue $\mathbb{S}$, notamment $\mathbb{S}[X], 1+1 = X + X^2$.

1. Introduction

Dans [3], on a prouvé une formule de Riemann-Roch pour $\overline{\operatorname{Spec}\mathbb{Z}}$ s'appliquant à toute extension sphérique $\mathbb{S}[\pm 1] := \mathbb{S}[\mu_{2,+}]$ de la base absolue $\mathbb{S}$. La preuve de ce résultat est basée sur le fait de voir l'anneau $\mathbb{Z}$ comme un anneau de polynômes[1] avec des coefficients dans $\mathbb{S}[\pm 1]$ et le générateur $3 \in \mathbb{Z}$. Dans le présent article, on montre qu'en travaillant sur la base absolue $\mathbb{S}$ elle-même, on obtient la formule suivante de Riemann-Roch.

Théorème 1.1. *Soit D un diviseur d'Arakelov sur $\overline{\operatorname{Spec}\mathbb{Z}}$. Alors*[2]

$$\dim_{\mathbb{S}} H^0(D) - \dim_{\mathbb{S}} H^1(D) = \left\lceil \deg_2 D \right\rceil' + 1. \tag{1.1}$$

Ici $\lceil x \rceil'$ dénote la fonction continue à droite qui coïncide avec la fonction plafond(x) pour $x > 0$ non entier, et avec $-$plafond$(-x)$ pour $x < 0$ non entier (voir la Figure 1).

La preuve de (1.1) suit les mêmes lignes que celles de la preuve de la formule de Riemann-Roch dans [3], et voit $\mathbb{Z}$ comme un anneau de polynômes[3] sur $\mathbb{S}$ de générateur -2. Cela améliore considérablement ce résultat précédent comme suit :

1. Le terme $\mathbf{1}_L$ faisant intervenir l'ensemble exceptionnel L dans la formule précédente est maintenant éliminé.

2. La formule (1.1) présente une analogie parfaite avec la formule de Riemann-Roch vérifiée par les courbes de genre 0.

3. Le diviseur canonique $K = -2\{2\}$ est de degré entier $\deg_2(K) = -2$.

Quand on travaille sur la base absolue $\mathbb{S}$, on est amené à une notion très naturelle de $\mathbb{S}$-module associé à un diviseur d'Arakelov comme expliqué dans la Section 2.

Recherche financée par la Fondation Simons.

AC : Collège de France, Paris, France.
IHÉS, Bures-sur-Yvette, France
CC : Département de mathématiques, Université Johns Hopkins, Baltimore, USA

Référence : https://arxiv.org/pdf/2306.00456.pdf .

[1] Plus précisément tout entier peut être mis sous la forme $P(X)$ où P est un polynôme à coefficients dans $\{-1, 0, 1\}$ et $X = 3$, la présentation est donnée par $1 + 1 = X - 1$

[2] On utilise la notation $\deg_2 := \deg / \log 2$

[3] Tout entier peut être mis de manière unique sous la forme $P(X)$ où P est un polynôme à coefficients dans $\{0, 1\}$ et $X = -2$, la présentation est $1 + 1 = X + X^2$

2. Travailler sur la base absolue $\mathbb{S}$

On dénote par Γ^{op} l'opposée de la catégorie de Segal (voir [4] chap. 2 et [1]), elle a un objet k_+ pour chaque entier $k > 0$, l'ensemble pointé $\{*, 1, \dots, k\}$, et les morphismes sont des morphismes d'ensembles pointés. Les foncteurs covariants $\Gamma^{\mathrm{op}} \longrightarrow \mathfrak{Sets}_*$ et leurs transformations naturelles déterminent la catégorie $\Gamma\mathfrak{Sets}_*$ des Γ-sets (aussi appelés $\mathbb{S}$-modules). Quand on travaille sur l'algèbre monoïdale sphérique $\mathbb{S}[\pm 1]$ du monoïde multiplicatif (pointé) $\{\pm 1\}$, le $\mathbb{S}[\pm 1]$-module naturel associé à une norme sur un groupe abélien A est ($k \in \mathbb{N}$, $\lambda \in \mathbb{R}$)

$$\|HA\|_\lambda(k_+) := \{a \in A^k \mid \sum |a_j| \leq \lambda\}. \tag{2.1}$$

La formule ci-dessus s'applique en la place archimédienne, pour les sous-groupes $A \subset \mathbb{R}$ et avec $|\cdot|$ dénotant la valeur absolue euclidienne. Si $\mathbb{S}[\pm 1]$ est remplacé par la base $\mathbb{S}$, il y a une définition plus basique d'un $\mathbb{S}$-module associé à un sous-ensemble arbitraire $X \subset A$ contenant $0 \in A$.

Lemme 2.1. *Soit A un monoïde abélien avec $0 \in A$. Soit $X \subset A$ un sous-ensemble de A contenant 0. La condition suivante définit un sous-foncteur du $\mathbb{S}$-module HA*

$$(HA)_X(k_+) := \{a \in A^k \mid \textstyle\sum_Z a_j \in X,\ \forall Z \subset k_+\} \subset X^k. \tag{2.2}$$

Preuve : Par construction $(HA)_X(k_+)$ est un sous-ensemble de $HA(k_+)$ contenant le point de $a_j = 0$, $\forall j$. Soit $\phi : k_+ \to m_+$ une application préservant le point de base $*$, on montrera que $\phi_*((HA)_X(k_+)) \subset (HA)_X(m_+)$. Soit $a \in (HA)_X(k_+)$. Pour tout $\ell \in m_+$, $\ell \neq *$, on a

$$\phi_*(a)(\ell) = \sum_{\phi^{-1}(\ell)} a_j = \sum_{Z_\ell} a_j, \qquad Z_\ell := \phi^{-1}(\ell).$$

Il découle de (2.2) que $\phi_*(a)(\ell) \in X$ pour tout ℓ et ceci pour tout sous-ensemble pointé $Z' \subset m_+$

$$\sum_{\ell \in Z'} \phi_*(a)(\ell) = \sum_Z a_j \in X, \qquad Z = \cup_{\ell \in Z'} Z_\ell.$$

Cela prouve que $\phi_*((HA)_X(k_+)) \subset (HA)_X(m_+)$. □

La proposition suivante montre que pour $X = [-\lambda, \lambda] \subset \mathbb{R}$ un intervalle symétrique, le $\mathbb{S}$-module $(H\mathbb{R})_X$ est un module sur la $\mathbb{S}$-algèbre $\|H\mathbb{R}\|_1$.

Proposition 2.2. *Soit $\lambda > 0$, $X = [-\lambda, \lambda] \subset \mathbb{R}$ un intervalle symétrique et $(H\mathbb{R})_X$ comme dans (2.2). Alors*

$$(H\mathbb{R})_X(k_+) = \{a \in \mathbb{R}^k \mid \textstyle\sum_{a_j > 0} a_j \leq \lambda,\ \sum_{a_j < 0}(-a_j) \leq \lambda\} \tag{2.3}$$

De plus, l'action de modules de la $\mathbb{S}$-algèbre $H\mathbb{R}$ sur elle-même par multiplication induit une action de la $\mathbb{S}$-algèbre $\|H\mathbb{R}\|_1$ sur le module $(H\mathbb{R})_X$.

Preuve : La condition (2.3) est remplie par tous les éléments de $(H\mathbb{R})_X(k_+)$ puisqu'elle fait intervenir des sommes sur les sous-ensembles de k_+. Inversement si $a \in \mathbb{R}^k$ vérifie (2.3), soit $Z \subset k_+$, appelons

$$Z_+ := \{j \in Z \mid a_j > 0\}, \quad Z_- := \{j \in Z \mid a_j < 0\}$$

On a $0 \leq \sum_{Z_+} a_j \leq \lambda$, $0 \geq \sum_{Z_-} a_j \geq -\lambda$ et par conséquent $-\lambda \leq \sum_Z a_j \leq \lambda$.

Pour prouver la seconde assertion, soit $Y = k_+, Y' = k'_+$ des ensembles finiment pointés et considérons l'application donnée par le produit

$$m : \|H\mathbb{R}\|_1(Y) \wedge (H\mathbb{R})_X(Y') \to (H\mathbb{R})(Y \wedge Y')$$

Elle associe à $(\alpha_i) \in \|H\mathbb{R}\|_1(Y)$, $\sum|\alpha_i| \leq 1$ et $(a_j) \in (H\mathbb{R})_X(Y')$ la double indexation $b := (b_{i,j})$, $b_{i,j} = \alpha_i a_j$ et on a besoin de montrer que $b \in (H\mathbb{R})_X(Y \wedge Y')$. Soit

$$Y_+ = \{i \in Y \mid \alpha_i > 0\},\ Y_- = \{i \in Y \mid \alpha_i < 0\},\ Y'_+ = \{j \in Y' \mid a_j > 0\},\ Y'_- = \{j \in Y' \mid a_j < 0\}$$

Par la règle des signes, les couples (i,j) pour lesquels $b_{i,j} > 0$ forment l'union $Y_+ \times Y'_+ \cup Y_- \times Y'_-$ de telle façon qu'on obtient

$$\sum_{b_{i,j}>0} b_{i,j} = \sum_{Y_+ \times Y'_+} \alpha_i a_j + \sum_{Y_- \times Y'_-} (-\alpha_i)(-a_j) = \sum_{Y_+} \alpha_i \sum_{Y'_+} a_j + \sum_{Y_-}(-\alpha_i) \sum_{Y'_-}(-a_j) \leq \lambda$$

en utilisant (2.3) pour les sommes sur les a_j ainsi que l'inégalité $\sum_{Y_+} \alpha_i + \sum_{Y_-}(-\alpha_i) \leq 1$ (puisque $\sum|\alpha_i| \leq 1$). On traite de manière similaire la somme sur les $b_{i,j}$ négatifs. □

En général, soit $\sigma \in \mathrm{Hom}_{\Gamma^{\mathrm{op}}}(k_+, 1_+)$ avec $\sigma(\ell) = 1\ \forall \ell \neq *$ et $\delta(j,k) \in \mathrm{Hom}_{\Gamma^{\mathrm{op}}}(k_+, 1_+)$, $\delta(j,k)(\ell) := 1$ si $\ell = j$, $\delta(j,k)(\ell) := *$ if $\ell \neq j$.

Étant donné un $\mathbb{S}$-module $\mathcal{F}$ et des éléments $x, x_j \in (1_+)$, $j = 1, \ldots, k$, on écrit

$$x = \textstyle\sum_j x_j \iff \exists z \in (k_+) \text{ s.t. } (\sigma)(z) = x,\ (\delta(j,k))(z) = x_j,\ \forall j. \tag{2.4}$$

Une relation de tolérance $\mathcal{R}$ sur un ensemble X est une relation réflexive et symétrique sur X. De façon équivalente, $\mathcal{R}$ est un sous-ensemble $\mathcal{R} \subset X \times X$ qui est symétrique et qui contient la diagonale. On dénotera par $\mathcal{T}$ la catégorie des relations de tolérance $(X, \mathcal{R})$. Les morphismes dans $\mathcal{T}$ sont définis par

$$\mathrm{Hom}_{\mathcal{T}}((X,\mathcal{R}),(X',\mathcal{R}')) := \{\phi : X \to X',\ \phi(\mathcal{R}) \subset \mathcal{R}'\}.$$

On dénote par $\mathcal{T}_*$ la catégorie pointée sous l'objet $\{*\}$ munie de la relation triviale. Un $\mathbb{S}$-module tolérant est un foncteur covariant pointé $\Gamma^{\mathrm{op}} \longrightarrow \mathcal{T}_*$ ([3]). On rappelle ci-dessous la définition de leur dimension.

Définition 2.1 [3] Soit $(E, \mathcal{R})$ un $\mathbb{S}$-module tolérant. Un sous-ensemble $F \subset E(1_+)$ engendre $E(1_+)$ si les deux conditions suivantes sont satisfaites

1. $\forall x, y \in F,\ x \neq y \implies (x,y) \notin \mathcal{R}$
2. Pour tout $x \in E(1_+)$, il existe $\alpha_j \in \{0,1\}$, $j \in F$ et $y \in E(1_+)$ tel que $y = \sum_F \alpha_j j \in E(1_+)$ au sens de (2.4), et $(x,y) \in \mathcal{R}$.

La dimension $\dim_{\mathbb{S}}(E, \mathcal{R})$ est définie comme la cardinalité minimale d'un ensemble générateur F.

3. Dimension de H^0 sur $\mathbb{S}$

Soit $m \in \mathbb{N}$, et $I_m = [-m, m] \cap \mathbb{Z}$. Le prochain lemme découle de (2.4) et de la définition 2.1.

Lemme 3.1. *La dimension* $\dim_{\mathbb{S}}((\mathbb{Z})_{I_m})$ *est la plus petite cardinalité d'un sous-ensemble* $G \subset I_m$ *tel que pour tout* $j \in I_m$*, il existe un sous-ensemble* $Z \subset G$ *avec* $\sum_Z i = j$ *et* $\sum_{Z'} i \in I_m$ *pour tout* $Z' \subset Z$*.*

Le nombre d'éléments de I_m est $2m+1$ et le nombre de sous-ensembles de G is $2^{\#G}$, par conséquent, on a les inégalités de base

$$\#G \geq \log_2(2m+1) > \log_2(2m), \qquad \dim_{\mathbb{S}}((\mathbb{Z})_{I_m}) \geq \lceil \log_2(m) \rceil + 1. \tag{3.1}$$

Ici $x \mapsto \lceil x \rceil$ dénote la fonction plafond qui associe à x le plus petit entier $> x$. Pour $m = 1$ on a besoin de deux éléments générateurs $\{-1, 1\}$, alors que pour $m = 2$ on choisit les trois éléments $\{-2, 1, 2\}$. Pour $m = 3$ on prend les trois éléments $\{-3, 1, 2\}$ alors que pour $m = 4$, on prend les 4 éléments $\{-3, -1, 1, 3\}$.

En général, on utilise le résultat suivant.

Lemme 3.2. *Soit $n \in \mathbb{N}$ et $I := [-a, a] \subset \mathbb{Z}$, où $2^{n-1} \leq a < 2^n$.*

(i) Si $n > 4$, il existe n éléments distincts $\alpha_j \in (0, a)$ tels que $\sum \alpha_j = a$ et tels que tout élément $z \in [0, a]$ peut s'écrire comme une somme partielle $z = \sum_Z \alpha_j$.

(ii) Le nombre minimal de $\mathbb{S}$-générateurs de $(H\mathbb{Z})_I$ est $n + 1$.

Preuve :

(i) On a $\sum_0^{n-1} 2^j = 2^n - 1 \geq a$ et $\sigma := \sum_0^{n-2} 2^j = 2^{n-1} - 1 < a$. L'idée est d'adjoindre à l'ensemble $T := \{2^j \mid 0 \leq j \leq n-2\}$, dont la cardinalité est $n-1$ et dont la somme est $\sigma < a$, un autre élément $a - \sigma$ de telle façon que la somme complète soit a. Le premier essai consiste à prendre $F = T \cup \{a - \sigma\}$. Supposons d'abord que $a - \sigma \notin T$. Les sommes partielles obtenues à partir de F sont l'union de l'intervalle $[0, \sigma]$ et de l'intervalle $[a - \sigma, a]$ et ces deux intervalles couvrent $[0, a]$, puisque $a - \sigma + \sigma = a$ alors que $a - \sigma \leq \sigma + 1$. Si $a - \sigma \in T$, on a pour un certain $k \geq 0$ que $a = \sigma + 2^k$. Pour éviter la répétition, on adopte les règles suivantes pour $2^{n-1} \leq a < 2^n$

1. Si $a = 2^{n-1}$, on pose $F := \{2^j \mid 0 \leq j \leq n-3\} \cup \{2^{n-2} - 2\} \cup \{3\}$
2. Si $a \neq 2^{n-1}$ et $a - \sigma \in T$, on pose $F := \{2^j \mid 0 \leq j \leq n-3\} \cup \{2^{n-2} - 1\} \cup \{a - \sigma + 1\}$
3. Si $a \neq 2^{n-1}$ et $a - \sigma \notin T$, on pose $F := T \cup \{a - \sigma\}$

Puisque par hypothèse $n > 4$, on a $2^{n-2} - 2 > 2^{n-3}$, donc dans le cas 1, on obtient $\#F = n$ et la somme des éléments de F est $a = 2^{n-1}$. Les sommes partielles des éléments de $\{2^j \mid 0 \leq j \leq n-3\}$ couvrent l'intervalle $J = [0, 2^{n-2} - 1]$. En ajoutant $2^{n-2} - 2$ aux éléments de J, on obtient l'intervalle $J + 2^{n-2} - 2 = [2^{n-2} - 2, 2^{n-1} - 3]$ dont l'union avec J est $[0, 2^{n-1} - 3]$, alors en mettant l'élément $3 \in F$, on voit que les sommes partielles couvrent $[0, a]$.

Dans le cas 2, on obtient de façon similaire $\#F = n$ puisque $a - \sigma + 1 \notin T$ et la somme des éléments de F est $\sigma + a - \sigma = a$. Les sommes partielles d'éléments de $\{2^j \mid 0 \leq j \leq n-3\}$ couvrent l'intervalle $J = [0, 2^{n-2} - 1]$ et en utilisant $2^{n-2} - 1$ ajouté aux éléments de J, on obtient l'intervalle $J + 2^{n-2} - 1 = [2^{n-2} - 1, 2^{n-1} - 2]$ dont l'union avec J est $J' = [0, 2^{n-1} - 2] = [0, \sigma - 1]$. En ajoutant $a - \sigma + 1$ à J', on obtient l'intervalle $J" = [a - \sigma + 1, a]$. Puisque $a - \sigma \in T$, on a $a - \sigma \leq 2^{n-2}$, par conséquent $a - \sigma + 1 \leq \sigma - 1$, de telle façon que le plus petit élément de $J"$ appartient à J' et $J' \cup J" = [0, a]$.

Dans le cas 3, les sommes partielles d'éléments de F couvrent $[0, a]$ comme expliqué ci-dessus.

(ii) Soit k le nombre minimal de $\mathbb{S}$-générateurs de $(H\mathbb{Z})_I$. Par (3.1), on a $k \geq n + 1$. Il reste à montrer qu'il existe un ensemble générateur de cardinalité $n+1$. On suppose d'abord que $n > 4$ et par conséquent, par (i), appelons $\alpha_j \in (0, a)$ les n éléments distincts vérifiant (i). Soit $F = \{-a\} \cup \{\alpha_j\} \subset [-a, a]$. Par construction $\#F = n + 1$. Pour montrer que F est un ensemble $\mathbb{S}$-générateur de $(H\mathbb{Z})_I$, on a besoin de vérifier les conditions du lemme 3.1. Par construction, la somme des éléments positifs de F est a et la somme de ses éléments négatifs est $-a$ par conséquent, toute somme partielle d'éléments de F appartient à $I = [-a, a]$. De plus, les

sommes partielles des éléments positifs de F couvrent l'intervalle $[0, a]$ par (i), et en utilisant l'élément $-a$, on couvre $I = [-a, a]$.

Pour $n \leq 4$, on a $a \leq 15$ et on peut faire la liste des ensembles générateurs de cardinalité $n+1$ comme suit

$$\{-1,1\},\{-3,1,2\},\{-6,1,2,3\},\{-7,1,2,4\},\{-10,1,2,3,4\},\{-11,1,2,3,5\}$$
$$\{-12,1,2,3,6\},\{-13,1,2,3,7\},\{-14,1,2,4,7\},\{-15,1,2,4,8\}$$

Ces ensembles sont du même type que ceux construits pour $n > 4$; pour les autres valeurs, on a

$$\{-3,-1,1,3\},\{-4,-1,2,3\},\{-7,-1,1,2,5\},\{-8,-1,1,3,5\}.$$

La valeur $a = 2$ nécessite 3 générateurs $\{-2,1,2\}$ et c'est la seule pour laquelle l'ensemble F des générateurs ne peut pas être choisi de telle façon que la somme de ses éléments positifs soit a et que la somme de ses éléments négatifs soit $-a$. On vérifie néanmoins que tous les éléments peuvent être obtenus comme une somme admissible. □

Théorème 3.3. *Soit D un diviseur d'Arakelov sur $\overline{\operatorname{Spec}\mathbb{Z}}$. Si $\deg(D) \geq 0$, on a*

$$\dim_{\mathbb{S}} H^0(D) = \left\lceil \deg_2 D \right\rceil + 1. \tag{3.2}$$

Preuve : On peut supposer que $D = \delta\{\infty\}$ où $\delta = \deg(D) > 0$. On a $H^0(D) = (H\mathbb{Z})_I$ où $I = [-e^\delta, e^\delta]$, en utilisant la relation classique entre le degré du diviseur et le sous-ensemble compact associé dans les adèles[4]. Soit $n \in \mathbb{N}$, $n \geq 1$, tel que $2^{n-1} \leq e^\delta < 2^n$. La partie entière a de e^δ vérifie $2^{n-1} \leq a < 2^n$ et on a $H^0(D) = (H\mathbb{Z})_{[-a,a]}$. Par conséquent, par le lemme 3.2, on obtient $\dim_{\mathbb{S}} H^0(D) = n+1$. Par définition $\deg_2 D := \deg D / \log 2$. Les conditions $2^{n-1} \leq e^\delta < 2^n$ signifient que $n - 1 \leq \deg_2 D < n$ et montrent que le plus petit entier $> \deg_2 D$ est égal à n, ce qui prouve (3.2). □

4. Dimension de H^1 sur $\mathbb{S}$

On définit la suite d'entiers suivante :

$$j(n) := \tfrac{1}{3}(-2)^n - \tfrac{1}{2}(-1)^n + \tfrac{1}{6} \qquad n \in \mathbb{N}. \tag{4.1}$$

Les premières valeurs de $j(n)$ sont alors : $0, 1, -2, 5, -10, 21, -42, 85, -170, 341, -682, 1365, -2730, \ldots$

Lemme 4.1. *Soit $G(n) = \{(-2)^j \mid 0 \leq j < n\}$. L'application σ de l'ensemble des sous-ensembles de $G(n)$ vers $\mathbb{Z}$ définie par $\sigma(Z) := \sum_Z j$ est en bijection avec l'intervalle $\Delta(n) := [j(k), j(k)+2^n-1]$ où $k = k(n) := 2E(n/2)+1$, ($E(x)$ = la partie entière de x).*

Preuve : L'application σ est injective et couvre un intervalle $[a, b]$. La borne inférieure a est la somme des puissances $a = \sum_{0 \leq \ell < \frac{n-1}{2}} (-2)^{2\ell+1}$ et la borne supérieure est la somme des puissances $b = \sum_{0 \leq \ell < \frac{n}{2}} (-2)^{2\ell}$. On liste des premiers intervalles comme suit

$$\Delta(1) = [0,1],\quad \Delta(2) = [-2,1],\quad \Delta(3) = [-2,5],\quad \Delta(4) = [-10,5],\quad \Delta(4) = [-10,21],\ldots$$ □

On renvoie le lecteur à [3], Appendice A, B, pour l'interprétation de $H^1(D)$ en termes du $\mathbb{S}$-module tolérant $(U(1), d)_\lambda$, $\lambda = e^{\deg D}$. Au niveau 1, la relation de tolérance sur le groupe abélien $\mathbb{R}/\mathbb{Z}$ est donnée par la condition $d(x, y) \leq \lambda$.

Proposition 4.2. *Soit $U(1)$ le groupe abélien $\mathbb{R}/\mathbb{Z}$ muni de la métrique canonique d de longueur 1.*

[4] Notons que $e^{\deg D} = 2^{\deg_2(D)}$

Soit $\lambda \in \mathbb{R}_{>0}$, $U(1)_\lambda$ le $\mathbb{S}$-module tolérant $(U(1), d)_\lambda$. Alors

$$\dim_{\mathbb{S}} U(1)_\lambda = \begin{cases} m & \text{if } 2^{-m-1} \leq \lambda < 2^{-m}, \\ 0 & \text{if } \lambda \geq \frac{1}{2}. \end{cases} \tag{4.2}$$

Preuve : Pour $\lambda \geq \frac{1}{2}$, tout élément de $U(1)_\lambda = (\mathbb{R}/\mathbb{Z}, d)_\lambda$ est à distance $\leq \lambda$ de 0, par conséquent on peut prendre $F = \varnothing$ comme ensemble générateur puisque, par convention, $\sum_\varnothing = 0$. Ainsi $\dim_{\mathbb{S}} U(1)_\lambda = 0$. Ensuite, on suppose $\lambda < \frac{1}{2}$. Soit $F \subset U(1)$ un ensemble générateur et posons $k = \#F$. On voit facilement qu'il y a au plus 2^k éléments de la forme $\sum_F \alpha_j j$, $\alpha_j \in \{0, 1\}$. Les sous-ensembles $\{x \in U(1) \mid d(x, \sum_F \alpha_j j) \leq \lambda\}$ couvrent $U(1)$, et puisque chacun d'eux à comme mesure 2λ, on obtient l'inégalité $2\lambda \cdot 2^k \geq 1$. Ainsi $k \geq \frac{-\log\lambda - \log 2}{\log 2}$. Quand $\frac{-\log\lambda - \log 2}{\log 2} = m$ est un entier, on a $\lambda = 2^{-m-1}$. Posons $F(m) = \{(-2)^{-j} \mid 1 \leq j \leq m\}$. La distance minimale entre deux éléments de $F(m)$ est la distance entre 2^{-m+1} et -2^{-m} qui est égale à $3 \cdot 2^{-m} = 6\lambda$. Montrons que $F(m)$ est un ensemble générateur. Par le lemme 4.1, tout entier q dans l'intervalle $\Delta(m)$ peut s'écrire comme $q = \sum_{i=0}^{m-1} \alpha_i (-2)^i$, avec $\alpha_i \in \{0, 1\}$. On obtient alors

$$q \cdot (-2)^{-m} = \sum_{i=0}^{m-1} \alpha_i (-2)^{i-m} = \sum_{j=1}^{m} \alpha_{m-j} (-2)^{-j}.$$

Soit $y \in \mathbb{R}/\mathbb{Z}$, faire monter y à un élément x de l'intervalle $(-2)^{-m}[j(k(m)), j(k(m)) + 2^m)$ qui est connexe de longueur 1 et est un domaine fondamental pour l'action de $\mathbb{Z}$ par translation. Alors il existe un entier $q \in \Delta(m)$ tel que $|(-2)^m x - q| \leq \frac{1}{2}$. Par conséquent, $d(x, q \cdot (-2)^{-m}) \leq 2^{-m-1} = \lambda$. Cela prouve que $F(m)$ est un ensemble générateur (voir la définition 2.1) et on en déduit que $\dim_{\mathbb{S}} U(1)_\lambda = m$. Supposons maintenant que $\frac{-\log\lambda - \log 2}{\log 2} \in (m, m+1)$, où m est un entier, i.e. que $\lambda \in (2^{-m-2}, 2^{-m-1})$. Pour tout ensemble générateur F de cardinalité k, on a $k \geq \frac{-\log\lambda - \log 2}{\log 2} > m$ de telle façon que $k \geq m + 1$. Le sous-ensemble $F(m+1) = \{(-2)^{-j} \mid 1 \leq j \leq m+1\}$ remplit la première condition de la définition 2.1 puisque la distance minimale entre deux éléments de $F(m+1)$ est $3 \cdot 2^{-m-1}$ qui est plus grand que $\lambda < 2^{-m-1}$. Comme montré ci-dessus, le sous-ensemble $F(m+1)$ est générateur pour $\lambda = 2^{-m-2}$ et a fortiori pour $\lambda > 2^{-m-2}$. Ainsi on obtient $\dim_{\mathbb{S}} U(1)_\lambda = m + 1$ et (4.2) est démontré. □

5. Formule de Riemann-Roch

On peut maintenant formuler le résultat principal de cet article

Théorème 5.1. *Soit D un diviseur d'Arakelov sur $\overline{\operatorname{Spec}\mathbb{Z}}$. Alors*

$$\dim_{\mathbb{S}} H^0(D) - \dim_{\mathbb{S}} H^1(D) = \left\lceil \deg_2 D \right\rceil' + 1 \tag{5.1}$$

où $\lceil x \rceil'$ est la fonction continue à droite qui coïncide avec plafond(x) pour $x > 0$ non entier et avec $-$plafond$(-x)$ pour $x < 0$ non entier (voir Figure 1).

Preuve : Pour $\deg_2 D \geq 0$, on a $\lambda = e^{\deg D} \geq 1$ et par conséquent par (4.2), on obtient $\dim_{\mathbb{S}} H^1(D) = 0$, de telle façon que (5.1) découle du théorème 3.3. Pour $\deg_2 D < 0$, on a $\dim_{\mathbb{S}} H^0(D) = 0$ puisque l'ensemble vide est un ensemble générateur. Pour $\deg_2 D \in [-m-1, -m)$ où $m \in \mathbb{N}$, on a, par (4.2), $\dim_{\mathbb{S}} H^1(D) = m$. Par conséquent, le côté gauche de (5.1) is $-m$ alors que le côté droit est égal à

$$\left\lceil \deg_2 D \right\rceil' + 1 = -m$$

par définition de la fonction $\lceil x \rceil'$ comme fonction continue à droite qui coïncide avec plafond(x) pour $x > 0$ non entier et avec $-$plafond$(-x)$ pour $x < 0$ non entier. □

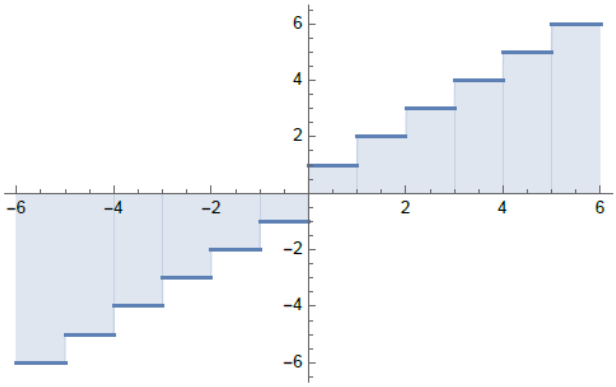


FIG 1 : Graphique de $\dim_{\mathbb{S}} H^0(D) - \dim_{\mathbb{S}} H^1(D) - 1$ comme une fonction de $\deg_2 D$

Remerciements. La seconde auteure est en partie financée par la subvention de la fondation Simons n° 691493.

Bibliographie

[1] A. Connes, C. Consani, *Absolute algebra and Segal's Gamma sets*, J. Number Theory 162 (2016), 518–551.

[2] A. Connes, C. Consani, *On Absolute Algebraic Geometry, the affine case*, Advances in Mathematics, 390, Paper No. 107909 (2021), 44 pp.

[3] A. Connes, C. Consani, *Riemann-Roch for* $\overline{\mathrm{Spec}\,\mathbb{Z}}$. À paraître dans le Bulletin des Sciences Mathématiques.

[4] B. Dundas, T. Goodwillie, R. McCarthy, *The local structure of algebraic K-theory.* Algebra and Applications, 18. Springer-Verlag London, Ltd., London, 2013.

[5] A. Weil *Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques*, Oeuvres scientifiques/Collected papers I. 1926–1951. Springer, Heidelberg, 2014.

Histoire de l'IHÉS et de sa fondation par Léon Motchane

Louis Michel

Léon Motchane est né le 10 juin 1900 dans une famille russo-suisse à Saint-Pétersbourg et y a grandi. Au moment de la Révolution de 1917, tout en poursuivant ses études de mathématiques et de physique, il s'implique dans une organisation de jeunes étudiants vouée à apaiser les souffrances de la population. L'année suivante, il rejoint sa mère et son frère aîné en Suisse, où il poursuit ses études et travaille à temps partiel comme ébéniste. Lorsque son père rejoint la famille un an plus tard, Léon peut passer un an comme assistant en physique à l'Université de Lausanne.

À partir de 1921, il doit travailler pour subvenir aux besoins de ses parents. Il travaille d'abord à Berlin comme impresario d'artistes, puis dans les assurances. Il s'installe en France pour y séjourner en 1924, dont il devient citoyen en 1938. De nombreuses activités variées l'occupent, s'étendant parfois au-delà de la France ; il a été cadre dans plusieurs entreprises.

Il est marié et père de deux fils : Didier, aujourd'hui conseiller maître à la Cour des comptes; et Jean Loup, physicien à Paris 7. Il n'a pas oublié son penchant mathématique ; il a rejoint la Société Mathématique de France et a publié en mathématiques. Il est aussi un bon pianiste et joueur d'échecs.

Au début de la Seconde Guerre mondiale, il s'est porté volontaire pour servir. Affecté à l'artillerie, il devient aspirant officier à l'école de Fontainebleau. Après avoir été démobilisé à l'été 1940 après la chute de la France, il rejoint immédiatement la Résistance, où ses fonctions sont principalement dans le renseignement ; il est blessé au combat le 13 août 1944. Pour ses services, il reçoit la Croix de Guerre et la Médaille de la Résistance avec rosette. Parallèlement, il travaille aux fameuses Editions de Minuit qui font paraître sous son pseudonyme Thimerais deux ouvrages clandestins de théorie sociologique : *Elements of Doctrine* (février 1944) et *Patient Thought* (juillet 1943). Ses amis retrouvent sa nature évoquée dans ses paroles d'introduction :

> *La pensée, sous la pression des jours qui passent, tend vers l'immédiat. Les obstacles à la reprise d'après-guerre semblent lointains ; néanmoins ils sont déjà présents et doivent être pris en compte. Les difficultés ne peuvent être surmontées sans une réflexion patiente. Les soucis quotidiens ne doivent pas nous occulter la continuité de la vie, qui rend les efforts d'aujourd'hui responsables des résultats de demain.*

Sa foi en l'avenir reposait sur un attachement absolu à la justice sociale et à la solidarité.

Après la guerre, tout en élargissant ses propres activités professionnelles, il s'intéresse de plus en plus à la science. Encouragé par Paul Montel, il publie des notes dans les Comptes-Rendus de l'Académie des Sciences, en mathématiques puis en physique théorique. Il soutient sa thèse de doctorat d'État en décembre 1954 ; elle s'intitulait *Propriétés invariantes en convergence simple* et le comité était composé de Paul Montel, Arnaud Denjoy, Jean Favard et Gustave Choquet. Motchane

Version éditée d'un discours du 8 octobre 1998 à l'occasion du quarantième anniversaire de la fondation de l'Institut des Hautes Études Scientifiques. Référence: L'intelligence mathématique, vol. 21, n° 2 1999.

a eu de nombreux contacts scientifiques en France et à l'étranger.

Quand a-t-il conçu le projet de fonder un institut scientifique ? Peut-être dès 1949. Alors qu'il rend visite à son frère Alexandre, ingénieur dans le New Jersey, Alexandre le présente à Robert Oppenheimer, le directeur de l'Institute for Advanced Study de Princeton. À partir de là, Motchane et Oppenheimer ont développé des relations profondes et amicales. Motchane rendait régulièrement visite à Oppenheimer et lui écrivait pour lui demander conseil. Lors de sa première visite à l'IAS, Léon Motchane a rencontré Cécile Morette (plus tard DeWitt) qui y travaillait alors ; pour elle aussi, il avait de nombreuses questions sur le fonctionnement de l'Institut, et des remarques sur la manière dont la France pouvait utiliser une telle institution.

Certes l'IAS a servi de modèle à l'IHÉS, mais il faut faire ressortir des différences dans leur organisation. Il ne s'agissait pas pour un bienfaiteur de créer une fondation scientifique dotée d'une large dotation. Au XX$^{\text{ième}}$ siècle, la France a eu quelques instituts de recherche fondamentale créés par des dons de philanthropes (pour la plupart étrangers), mais dans le même domaine scientifique, le seul était l'Institut Henri Poincaré, et qui est géré par les universités parisiennes. et le Comité National de Recherches Scientifiques. Pour trouver un cas plus comparable à I'IHÉS, il faut remonter plus de cent ans en arrière, à l'Institut Pasteur !

La vision de Motchane semblait inévitablement utopique. Il souhaitait fonder un institut de recherche fondamentale en "Mathématiques, Physique Théorique et Méthodologie des Humanités". Il n'imposerait qu'une seule exigence à ses professeurs, qu'ils soient en résidence pendant six mois. Ils seraient permanents (c'est-à-dire nommés à vie) et égaux (en particulier avec un salaire égal). Le directeur serait nommé pour huit ans, renouvelable (deux fois au maximum) pour quatre ans. Le comité scientifique serait composé du directeur, des professeurs permanents et d'un nombre restreint de scientifiques cooptés par eux pour des mandats d'au plus six ans. Toutes les décisions scientifiques (et dans le cadre du budget qui comprenait la nomination des professeurs) seraient prises par le Comité Scientifique et ne pourraient être renversées par le Conseil d'Administration. À l'expiration du mandat d'un administrateur, le successeur serait choisi par le Comité scientifique ; le Conseil d'Administration n'avait que le pouvoir d'entériner ou de refuser leur choix. Et l'Institut devrait fonctionner sur les dons des entreprises aux termes de la loi de 1901.

Ce projet impossible, Motchane l'a réalisé. Il fallait un optimisme inébranlable, fondé sur une profonde réflexion et sur une connaissance approfondie du monde scientifique et des milieux d'affaires ; et il a fallu de grandes compétences de négociation. L'association a été constituée le 27 juin 1958 par une assemblée de tous les futurs membres du Conseil d'Administration. Elle s'est déroulée dans le bureau de son premier président, Joseph Pérès, Doyen de la vaste Faculté des Sciences de l'Université de Paris[1]. Le projet de statuts, minutieusement rédigé par Léon Motchane

[1]En plus de Léon Motchane et de son conseiller juridique Jean Robert, le groupe était constitué de représentants de sept grands groupes - Renault, Esso Standard, Shell France, Pétrole BP, Gaz de France, Compagnie générale de TSF (dont Maurice Ponte fut un ardent supporter de l'IHÉS), et les Tréfileries du Havre - et de deux personnes philantropes : un représentant d'Edmond de Rothschild, et Gabrielle Reinach, qui léguera plus tard l'ensemble de son patrimoine à l'IHES, lui permettant d'ajouter une aile au bâtiment scientifique, 3 agences gouvernementales comme le CEA (dont le PDG Francis Perrin était un véritable allié), EDF, la Banque de France, la Caisse des Dépôts et Consignations ; de grosses entreprises comme Pont-à-Mousson, dont le président honoraire André Grandpierre succéda à Pérés en 1962 comme président du Conseil d'Administration.

et son conseiller juridique, fut approuvé à l'unanimité. Motchane a été choisi comme directeur de l'IHÉS, poste qu'il a conservé jusqu'à sa retraite en 1971.

Tout au long de ces 13 années, à force de talent pour les relations humaines, et aidé de quelques membres du Conseil d'Administration, Motchane grossit les rangs des supporters. Non sans difficultés. La constitution en organisme de service public, indispensable au fonctionnement de l'IHÉS, fut obtenue en 1961. À cette occasion, deux dirigeants de compagnies pétrolières voulurent nommer des représentants du Conseil d'Administration au Comité scientifique pour statuer sur les activités des professeurs et visiteurs de l'IHÉS. Motchane est resté fidèle aux principes qu'il avait établis, mais cela lui a coûté l'appui des deux compagnies pétrolières. Dans certains cas, il est arrivé qu'un membre industriel manquant de dévotion envers l'IHÉS soit également remplacé à son poste au Conseil d'Administration et le soutien de son entreprise a cessé.

La première crise financière eut lieu en 1965. La menace n'était pas seulement que les progrès remarquables des sept premières années seraient stoppés, mais que le projet pourrait disparaître ! Le Premier ministre Pompidou est alerté et s'engage à organiser un financement régulier de l'État ; cela est rapidement devenu la source principale. Motchane, puis Grand-Pierre, le deuxième président du Conseil d'Administration, ont tenté d'obtenir des subventions de l'étranger, mais celles-ci n'ont pas duré. La plus ancienne subvention étrangère et toujours en cours est celle de la SRC anglaise (depuis 1970) ; un certain nombre d'autres ont été lancées pendant le mandat de directeur de Nicholaas Kuiper (1971-1985). À l'heure actuelle, les apports étrangers couvrent environ un sixième du budget et les donateurs français un seizième. Toutes les ressources de l'IHÉS sont constituées de fonds engagés pour quelques années seulement.

Passons maintenant à l'histoire scientifique de l'IHÉS. Elle débute dans deux bureaux loués à la Fondation Thiers (dans le XVI$^{\text{ième}}$ arrondissement de Paris), l'un pour le directeur et la secrétaire (Annie Rolland), l'autre pour les deux premiers professeurs permanents : Jean Dieudonné (français, mais résidant alors aux États-Unis) et Alexander Grothendieck (alors âgé de 32 ans, apatride scolarisé en France). Un séminaire hebdomadaire de géométrie algébrique a été lancé en 1959, se réunissant dans une salle de la Fondation Thiers et attirant 20 à 30 mathématiciens, des jeunes étudiants de l'École Normale Supérieure aux professeurs confirmés. À cela s'ajoutent en 1960-61 le séminaire de Claude Chevalley (en visite à l'année) et des conférences (tenues sur différents sites) par des visiteurs de courte durée : M. Atiyah, S. S. Chern, H. Grauert, H. Hironaka, J. Tits, A. Weil,... En 1960 paraissent les Publications Mathématiques de l'IHÉS, qui deviennent rapidement une revue mathématique exceptionnelle.

Ce début brillant n'a pas été égalé par la physique théorique. Fort de très bons conseils, Motchane offrit en décembre 1959 la première chaire de physique à Murray Gell-Mann (prix Nobel 1969), qui effectuait un séjour de plusieurs mois au Collège de France. Il a imposé plusieurs conditions ; il a fallu six mois au directeur pour le rencontrer, et un an de plus à Gell-Mann pour décliner l'offre. Motchane a également invité un bon nombre de visiteurs, mais les physiciens ont leurs propres habitudes de travail, et pour autant que je sache, seuls trois d'entre eux ont accepté de visiter cet institut sans campus : E. Caianello, A. Wightman et G. Källen.

Tout cela change à l'automne 1962, lorsque l'IHÉS s'installe dans le magnifique domaine de Bois-

Marie, un parc de 10 hectares à Bures-sur-Yvette. Oppenheimer, Peierls et Weisskopf étaient alors les physiciens membres du comité scientifique. Je suis devenu le premier professeur permanent de physique. Harry Lehmann est arrivé alors aussi et est resté trois ans. On lui avait proposé un poste de professeur permanent, mais il a rapidement décidé de ne pas démissionner de sa chaire à Hambourg et donc de ne pas accepter le titre de professeur à l'IHÉS. (Il fut plus tard le représentant d'une fondation allemande au Conseil d'Administration). Soit dit en passant, Alain Connes est compté parmi les professeurs, même s'il a décliné l'offre du titre lors de son adhésion au Collège de France ; son bureau et la plupart de ses activités sont ici ; il est répertorié par l'IHÉS comme "Professeur Léon Motchane" et a les mêmes responsabilités que les professeurs permanents. La liste des visiteurs en physique théorique est vite devenue très importante en quantité et en qualité.

En mathématiques, René Thom avait été approché des années plus tôt, mais n'est venu qu'en 1963. Le séminaire Grothendieck a conservé son grand prestige et les "éléments de Géométrie algébrique" (publiés dans la "revue bleue" de l'IHÉS) est devenu un monument des mathématiques. Le premier professeur permanent étranger fut le physicien David Ruelle, arrivé en 1964. Depuis, dix autres professeurs ont été recrutés, dont deux seulement français, Alain Connes et Thibault Damour.

À noter qu'à l'exception de Dieudonné, les professeurs de l'IHES ont été recrutés entre 25 et 40 ans (le plus souvent entre 30 et 33 ans). Tant par ses membres permanents que par ses membres invités, l'IHÉS est une institution internationale ; depuis 1980, c'est officiellement une fondation française.

Léon Motchane fit construire en 1967 une résidence, l'Ormaille à Bures, pour héberger les visiteurs et leurs familles. L'IHÉS n'avait pas les moyens d'acheter la résidence, mais a obtenu un bail de 25 ans. L'Institut a obtenu un prêt pour rendre possible l'achat de la propriété, afin de conserver une caractéristique essentielle du mode de vie de ses membres. Les enfants des membres sont très bien accueillis par les écoles, et leurs amitiés scolaires ouvrent des amitiés familiales avec des voisins français non scientifiques. Les résidences, le déjeuner à l'Institut et le thé tous les jours à 4 heures sont un mode de vie copié de l'IAS à Princeton ; ils sont bien adaptés à la vie scientifique de l'IHÉS et à l'intensité des échanges entre ses membres.

Dans sa vision prophétique, Motchane parlait de collaboration entre les mathématiciens et les physiciens théoriques. Au cours de son mandat, tout ce qu'on peut dire de cette collaboration, c'est qu'il s'agissait plutôt d'une coexistence ; mais depuis lors, l'IHÉS est devenu le seul endroit au monde où les deux disciplines ont les interactions les plus intenses, les plus profondes et les plus productives.

Aller plus loin dans la riche histoire scientifique de l'IHÉS serait trop long. Il y a à tout moment six professeurs, six visiteurs CNRS de longue durée et trente ou quarante autres visiteurs, et leurs réalisations et leur influence sont grandes. Un aperçu de l'historique se trouve dans les rapports annuels des administrateurs : L. Motchane, N. Kuiper, M. Berger, J.-P. Bourguignon. Il existe déjà une thèse de Princeton, de David Aubin, portant le titre assez sarcastique "*Une histoire culturelle des catastrophes et du chaos autour de l'Institut des Hautes Études Scientifiques de France*" ; cette thèse décrit et analyse une partie de l'activité scientifique de l'Institut dans la décennie commençant un peu avant 1970. Permettez-moi de donner une statistique qui peut être impressionnante même pour les non- scientifiques : l'IHÉS est unique en ce que les deux tiers de ses

professeurs de mathématiques (6 des 9 qu'il a nommés depuis sa fondation) ont une médaille Fields. Parmi ceux-ci, seul René Thom l'avait déjà avant de rejoindre l'IHÉS. Alexander Grothendieck, Pierre Deligne, Alain Connes, Jean Bourgain et Maxim Kontsevich ont obtenu la médaille Fields alors qu'ils étaient professeurs à l'IHÉS. Maxim Kontsevich et Mikhaïl Gromov sont désormais professeurs permanents de mathématiques, Dennis Sullivan ayant récemment démissionné. Les professeurs de physique sont David Ruelle, Thibault Damour et Michael Douglas ; les anciens détenteurs du titre sont Jürg Fröhlich, Oscar Lanford et moi-même.

Léon Motchane a pris sa retraite en 1971. Annie Rolland, qui, en tant que Secrétaire générale, avait mis tant de devouement, de goût et de soin à organiser le cadre de la vie de l'Institut, prit sa retraite en même temps que Léon Motchane et devint Madame Motchane. Les jeunes mariés ont vécu plusieurs années près d'Aix-en-Provence, pour laisser le successeur de Motchane s'essayer à diriger seul l'IHÉS. De retour à Paris, Léon Motchane a encore apporté une aide précieuse à l'IHÉS en tant que Vice-Président (plus tard Président Honoraire) du Conseil d'Administration. Il a eu le plaisir de voir tout son projet se réaliser tel qu'il l'avait conçu à l'exception de la section sur la Méthodologie des Humanités. René Thom a fait quelques pas dans cette direction, mais la section n'a jamais été créée.

La vie de l'Institut est le meilleur souvenir de Léon Motchane. Les scientifiques. du monde entier, et tous les Français, peuvent lui être reconnaissants de ce qu'il a fait pour la patrie et pour la science. Dans le parc, près de la bibliothèque, un très beau buste de lui[2] rappelle à ceux qui l'ont connu et à tous que Léon Motchane fut le créateur de l'IHÉS.

Louis Michel est né en France en 1923 et a étudié la physique à l'École Polytechnique de Paris de 1943 à 1946 (interrompu par le service dans l'armée française en 1944-45). Il a travaillé à l'étranger pendant plusieurs années à partir de 1948, à l'Université de Manchester, à l'Institut Bohr de Copenhague et à l'Institute for Advanced Study de Princeton. De retour en France en 1955, il enseigne à Lille et à Paris, Léon Motchane prend sa retraite en 1971. puis est nommé professeur permanent à l'IHÉS en 1962. A l'IHÉS il a accueilli des collaborateurs du monde entier. Il a lui-même effectué de nombreuses visites aux États-Unis, en Europe, en Amérique du Sud et en Asie ; depuis 1990, il passe trois mois par an au Technion de Haïfa. Il divise son travail en deux périodes : d'abord, jusqu'en 1976, l'étude des interactions fondamentales (en particulier des effets relativistes de la polarisation des particules) : puis depuis 1976, l'étude de la symétrie dans tous les domaines de la physique et de la géométrie des réseaux. Le professeur Michel et son épouse ont six enfants adultes et dix petits-enfants, qui vivent presque tous assez près pour se retrouver au domicile Michel à Bures-sur-Yvette pour le souper dominical.

[2]Buste réalisé à l'occasion des 40 ans de l'Institut par Richard Rysanek, sculpteur résidant à Bures-sur-Yvette.

Le silence de Bourbaki se perpétue
Une interview de Pierre Cartier

Marjorie Senechal

18 juin 1997

Nicolas Bourbaki, 1935-????

Si vous êtes un mathématicien travaillant aujourd'hui, vous avez presque certainement été influencé par Bourbaki, au moins dans le style et l'esprit, et peut-être dans une plus grande mesure que vous ne le pensez. Mais si vous êtes étudiant, vous n'avez peut-être jamais entendu parler de ça, de lui, ou d'eux. Qu'est-ce qu'est Bourbaki, ou bien qui est, ou qui était Bourbaki ?

Cochez tous les items qui s'appliquent. Bourbaki est, ou était, selon le cas ::

- le découvreur (ou l'inventeur, si vous préférez) de la notion de structure mathématique. Va-t-il encore parler ? Peut-il encore parler ?
- l'un des grands mouvements abstractionnistes du XXe siècle ;
- une communauté de mathématiciens petite mais extrêmement influente ;
- un collectif qui n'a pas publié depuis quinze ans.

La réponse est : *tout ce qui précède*, et ce sont quatre fils étroitement tissés d'un chapitre important de l'histoire intellectuelle. Est-il temps d'écrire ce chapitre ? L'histoire de Bourbaki est-elle terminée ?

Bourbaki est né à Paris en 1935 lorsqu'un petit groupe de mathématiciens de l'École Normale Supérieure, mécontents des cours qu'ils dispensaient, décidèrent de les reformuler. La plupart des mathématiciens ont vécu cette expérience à un moment ou à un autre, mais l'ampleur du mécontentement de Bourbaki a grandi rapidement et sans limite. Dès 1939, écrivant en tant que collectif anonyme sous le pseudonyme de Nicolas Bourbaki, ils commencent à publier une série d'ouvrages destinés à transformer la théorie et la pratique des mathématiques elles-mêmes. Dès ses débuts, Bourbaki était un fervent partisan de l'unité et de l'universalité des mathématiques, et s'est consacré à démontrer les deux en refondant toutes les mathématiques en un tout unifié. Ses objectifs étaient une formalisation totale et une parfaite rigueur. Dans les années d'après-guerre, Bourbaki s'est métamorphosé de rebelle à membre de l'establishment.

Les propres règles de Bourbaki prévoyaient explicitement l'auto-renouvellement : de temps en temps, de jeunes mathématiciens étaient invités à se joindre et des membres plus âgés démissionnaient, conformément à la "retraite" obligatoire à cinquante ans. Or Bourbaki a maintenant près de vingt ans de plus que n'importe lequel de ses membres. Le séminaire Bourbaki qui existe de longue date est toujours bien vivant et il se tient à Paris, mais la voix de Bourbaki elle-même, telle qu'elle

Référence : The mathematical intelligencer, Springer-Verlag, New-York, vol. 20, n° 1, p.22, 1998.
Traduction : Denise Vella-Chemla, mai 2023, aidée de Google Lens, et Google traduction.

s'exprime à travers ses livres, est restée silencieuse pendant quinze ans.

Bourbaki parlera-t-il encore ? Peut-il parler à nouveau ?

Pierre Cartier a été membre de Bourbaki de 1955 à 1983. Né à Sedan, en France en 1932, il est diplômé de l'École Normale Supérieure de Paris, où il a étudié sous la direction d'Henri Cartan. Sa thèse, soutenue en 1958, portait sur la géométrie algébrique ; depuis lors, il a contribué à de nombreux domaines des mathématiques, y compris la théorie des nombres, la théorie des groupes, les probabilités et la physique mathématique. Le professeur Cartier a enseigné à Strasbourg pendant une décennie à partir de 1961, après quoi il a rejoint le CNRS, le Centre National de la Recherche Scientifique. Depuis 1971, il est professeur à l'IHÉS (Institut des Hautes Études Scientifiques) de Bures-sur Yvette, et a enseigné à l'École Polytechnique et à l'École Normale, où il anime entre autres un séminaire d'épistémologie. En 1979, il reçoit le prix Ampère de l'Académie française des sciences. Le professeur Cartier a participé à divers programmes pour aider les pays en développement, dont le Chili, le Vietnam et l'Inde, à développer la science chez eux ; il est également éditeur d'un livre sur l'art et les mathématiques. Peu de personnes sont mieux qualifiées pour discuter du silence de Bourbaki. Nous lui sommes reconnaissants d'avoir accepté de faire cette interview pour les lecteurs de *The Mathematical Intelligencer.*

L'Interview

Senechal : *S'il vous plaît, parlez-nous d'abord de votre propre lien avec Bourbaki.*

Cartier : Autant que je m'en souvienne, ma première rencontre avec Bourbaki remonte à juin 1951. J'étais élève en première année à l'École Normale, Henri Cartan y était mon professeur de mathématiques et à sa demande Bourbaki m'a invité à participer à leur réunion à Pelvoux, dans les Alpes. Je me souviens que nous avons discuté de beaucoup de choses, notamment d'un texte écrit par Laurent Schwartz sur les fondements des groupes de Lie ; c'était l'une des premières ébauches de la série bien connue de Bourbaki sur les groupes de Lie. Ce n'était pas beaucoup d'années après l'invention de Schwartz des distributions, qui l'a rendu célèbre. Il faut comprendre que les élèves de mathématiques à l'École Normale étaient tous élèves à la fois d'Henri Cartan et de Laurent Schwartz (qui a quitté Nancy pour Paris en 1952). Nous avons assisté à leurs séminaires et cours et essayé d'utiliser leurs nouveaux outils dans tous les sens. François Bruhat et moi avons été parmi les premiers à comprendre l'importance des distributions dans la théorie des groupes de Lie et leurs représentations. Bruhat a consacré sa thèse à ces sujets et n'a publié mes propres contributions que bien plus tard.

Pour moi, c'était très important d'être exposé de l'intérieur. J'ai été surpris de voir toutes ces personnes formidables que j'avais connues de loin. J'ai été accepté très librement. Il a fallu trois ou quatre ans de plus avant que je ne sois officiellement accepté comme membre. Dans les années cinquante et soixante, il y avait un spectre continu depuis l'intérieur du noyau Bourbaki jusqu'à l'extérieur. Le travail qui était imprimé dans les livres, ce qui était rapporté dans le séminaire et le travail des étudiants étaient étroitement liés, et je pense que c'est une des raisons du grand succès des mathématiques françaises à cette époque. Bien sûr, ces temps étaient très différents. L'échelle était beaucoup plus petite. Il y avait alors une dizaine de doctorats par an en mathématiques en

France (contre trois cents aujourd'hui).

Lors de cette première rencontre, j'étais ce qu'ils appellent un *cobaye*, un cochon d'Inde. J'étais très enthousiaste à ce sujet. Tout d'abord, c'était la première fois que je voyais des mathématiques modernes. Je viens d'une petite ville, d'une situation difficile à cause de la guerre. J'avais été élève dans une école secondaire très provinciale, très désuète. Certains de mes professeurs étaient très bons mais bien sûr ils étaient très éloignés de la science moderne. Les mathématiques qu'on m'enseignait étaient la géométrie classique, de manière synthétique et inculte. J'ai eu la chance d'avoir un professeur de physique imaginatif, et donc au début je voulais être physicien. Puis j'ai été élève au Lycée Saint-Louis à Paris avant d'être admis à l'École Normale, et j'ai suivi des cours particuliers de physique avec un professeur très particulier, Pierre Aigrain. (Diplômé de l'Académie navale, il était en 1950 professeur adjoint de physique ; il est finalement devenu secrétaire d'État aux sciences sous le président Giscard.) Habituellement, un étudiant brillant termine le programme en deux ans, mais j'ai réussi à le terminer en un. Mais les mathématiques et la physique qu'on m'enseignait étaient totalement démodées à cette époque, totalement. Je me souviens que, dans un cours qui s'appelait Physique générale à la Sorbonne, le professeur faisait une déclaration solennelle : "Messieurs", il ne mentionnait pas les dames mais il y avait très peu d'élèves filles, "dans ma classe, ce que certains appellent "l'hypothèse atomique", n'a pas sa place." C'était en 1950, cinq ans après Hiroshima ! Alors je suis allé voir Aigrain et j'ai dit : "Qu'est-ce que je fais ?" et il a dit: "Eh bien, bien sûr, tu dois obtenir ton diplôme, mais je vais t'enseigner la physique correctement." Cela montre ce qu'était l'université française à l'époque. Pour comprendre l'influence de Bourbaki, il faut comprendre cela. Bourbaki est tombé dans le vide. Beaucoup de gens ont discuté des raisons pour lesquelles il en était ainsi ; Je ne pense pas que ce soit le lieu pour en reparler. Mais évidemment dans les années 50, au début des années 50, l'enseignement des sciences était très pauvre. Il a fallu environ cinq ou six ans à Bourbaki pour renverser tout le système. En 1957 ou 1958, la subversion était presque totale, à Paris.

Senechal : *Mais Bourbaki a commencé dans les années trente...*

Cartier : Le premier livre a été publié en 1939, mais il y a eu la guerre, qui a retardé les choses, et aussi André Weil était aux États-Unis, Claude Chevalley était aux États-Unis, et Laurent Schwartz a dû se cacher pendant la guerre parce qu'il était juif. Bourbaki a survécu pendant la guerre avec seulement Henri Cartan et Jean Dieudonné. Mais tout le travail qui avait été fait dans les années trente s'est épanoui dans les années cinquante. Je me souviens que nous, les jeunes mathématiciens, étions vraiment impatients d'aller à la librairie pour acheter les nouveaux livres. Et à cette époque Bourbaki publiait au moins un ou deux tomes chaque année.

Quand je suis officiellement devenu membre de Bourbaki en 1955, je devais respecter la règle selon laquelle tout le monde devait partir à 50 ans, et je suis donc parti en 1983, alors que j'avais presque 51 ans. J'ai consacré près de 30 ans de ma vie, et au moins un tiers de mon travail, à Bourbaki. Les habitudes de travail de Bourbaki impliquaient de très nombreux avant-projets d'un livre avant sa publication. À l'époque, nous avions trois réunions par an, une semaine à l'automne, une semaine au printemps et deux semaines à l'été, ce qui représente déjà un mois de dur labeur, dix ou douze heures par jour. Les livres publiés comprenaient environ 10 000 pages, ce qui signifie environ 1 000 à 2 000 pages de rapports préliminaires et de brouillons rédigés chaque année. J'estime avoir

contribué à environ 200 pages par an pendant tout ce temps avec Bourbaki.

Senechal : *Combien de personnes faisaient-elles partie du groupe, à cette époque ?*

Cartier : Environ 12. C'était toujours un petit groupe bien délimité. Le séminaire était différent, beaucoup plus ouvert. Mais encore, dans les années 1950, si vous regardez la table des matières des volumes du séminaire, environ la moitié des communications étaient écrites par des membres de Bourbaki ; à cette époque, l'interaction entre le séminaire et le groupe était très forte. Maintenant ce n'est plus vrai : c'est toujours une série distinguée mais elle est généralement écrite par des gens qui n'ont aucun lien direct avec l'institution Bourbaki. Mais à cette époque, les gens publiaient dans la série de séminaires une partie de leurs découvertes, ou des récits préliminaires des idées de Bourbaki qui parurent plus tard dans les livres.

J'étais typiquement un membre de la troisième génération. On peut dire qu'il y en a eu quatre. La première génération était constituée des pères : André Weil, Henri Cartan, Claude Chevalley, Jean Delsarte et Jean Dieudonné, les personnes qui ont fondé le groupe dans les années trente. (D'autres personnes se sont jointes au début, mais sont parties bientôt.) Puis il y a eu une deuxième génération, des personnes invitées à rejoindre pendant ou juste après la guerre : Godement, et Sammy Eilenberg. La troisième génération comprenait Armand Borel, Alexandre Grothendieck, François Bruhat, moi-même, Serge Lang et John Tate.

Senechal : *Ces générations différaient-elles dans leurs attitudes ou leurs perspectives ?*

Cartier : Ils étaient très différents. Je pense qu'ils sont devenus de plus en plus pragmatiques et de moins en moins dogmatiques.

Senechal : *Et comment cela s'est-il manifesté dans l'œuvre de Bourbaki ?*

Cartier : Dès le début, le traité Bourbaki a été conçu comme comprenant deux parties. La première partie est sur les fondations et se compose de six livres, sur la théorie des ensembles, l'algèbre, la topologie générale, le calcul élémentaire, les espaces vectoriels topologiques et la théorie de l'intégration (de Lebesgue). Les quatre derniers de ces livres donnent les fondements de l'analyse, tels que perçus par Bourbaki, avec un fort penchant vers l'analyse fonctionnelle. La deuxième partie, en deçà de projets plus ambitieux, consiste en deux séries très réussies, sur les groupes de Lie et sur l'algèbre commutative. En regardant la liste des membres de Bourbaki des deuxième et troisième générations, on se rend compte que certains des plus grands experts mondiaux de l'époque étaient là, et cela explique l'ampleur et la profondeur de la deuxième partie de l'œuvre de Bourbaki.

L'ancienne génération avait appris les mathématiques à l'ancienne. Ce sont eux qui ont remanié les mathématiques. La deuxième génération avait déjà été exposée au nouvel enseignement. Ma génération, la troisième génération, n'a pas eu à prouver que la nouvelle méthode était meilleure que l'ancienne parce qu'on nous enseignait essentiellement avec la nouvelle méthode. Je pense que j'étais juste à la frontière, car au lycée, on m'enseignait encore selon l'ancienne méthode, mais quand je suis allé à Paris, j'ai été exposé à la nouvelle pensée. Et donc nous étions de moins en moins dogmatiques, car nous n'avions rien à prouver. Le noyau des mathématiques françaises

s'était rendu à Bourbaki. Bourbaki avait déjà pris le pouvoir, non seulement sur le plan intellectuel mais aussi sur le plan académique. Il était clair que d'un point de vue institutionnel, Bourbaki avait gagné.

Si vous regardez les volumes sur les groupes de Lie, vous verrez que les derniers ont des chapitres auxquels on ne s'attend pas chez Bourbaki. C'est devenu de plus en plus explicite ; il y a des tableaux et des dessins. Je pense que c'était essentiellement l'influence d'une personne, Armand Borel. Il aimait citer Shaw, "C'est le caractère national suisse, ma chère dame", et très souvent lors d'une discussion, il disait : "Je suis le paysan suisse."

Bien sûr, à cette époque, la géométrie différentielle était en plein essor, et cela avait toujours été un grand défi pour Bourbaki. Il faut se rappeler que le père d'Henri Cartan était Élie Cartan, le géomètre, et que les Bourbaki ne reconnaissaient qu'un seul parrain, Élie Cartan, et avaient beaucoup d'aversion pour tous les autres mathématiciens français des années trente. Bourbaki ne s'est réconcilié avec Poincaré qu'après une longue lutte. Quand j'ai rejoint le groupe dans les années 50, ce n'était pas du tout à la mode de valoriser Poincaré. Il était démodé. Bien sûr, l'opinion sur Poincaré a complètement changé. Mais force est de constater que son style et celui de Bourbaki étaient totalement différents.

La quatrième génération était plus ou moins un groupe d'étudiants de Grothendieck. Mais à cette époque Grothendieck avait déjà quitté Bourbaki. Il a appartenu à Bourbaki pendant une dizaine d'années mais il est parti en colère. Les personnalités étaient très fortes à l'époque. Je me souviens qu'il y avait des affrontements très souvent. Il y avait aussi, comme d'habitude, un combat de générations, comme dans toute famille. Je pense qu'un petit groupe comme ça répétait plus ou moins les traits psychologiques d'une famille. Nous avons donc eu des affrontements entre générations, des affrontements entre frères, etc. Mais ils n'ont pas détourné Bourbaki de son objectif principal, même s'ils ont parfois été assez brutaux. Au moins, l'objectif était clair. Il y avait quelques personnes qui ne pouvaient pas supporter le fardeau de ce style psychologique, par exemple Grothendieck est parti et Lang a aussi abandonné.

Senechal : *Les objectifs sont-ils restés dans le temps ou ont-ils changé ?*

Cartier : Ils ont changé. La première génération devait d'abord créer un projet à partir de rien. Ils ont dû inventer une méthode. Puis dans les années quarante, on peut dire que la méthode était apparue et Bourbaki savait où aller : son but était de donner les bases des mathématiques. Ils devaient soumettre toutes les mathématiques au schéma de Hilbert ; ce que van der Waerden avait fait pour l'algèbre devait être fait pour le reste des mathématiques. Ce qui devait être inclus était plus ou moins clair. Les six premiers livres de Bourbaki comprennent les connaissances de base d'un étudiant diplômé moderne.

Le malentendu était que beaucoup de gens pensaient qu'il fallait l'enseigner comme cela était écrit dans les livres. Vous pouvez considérer les premiers livres de Bourbaki comme une encyclopédie des mathématiques, contenant toutes les informations nécessaires. C'est une bonne description. Si vous le considérez comme un manuel, c'est un désastre.

Senechal : *Étiez-vous au courant de cela lorsque vous étiez membre de Bourbaki ? Les gens de Bourbaki se sont-ils rendus compte que ce n'était pas un manuel ?*

Cartier : Plus ou moins, mais pas aussi clairement que maintenant. Il y a eu un malentendu à ce sujet, je suppose parce que nous n'avions pas de manuels. Je me souviens très bien de la manière dont j'ai appris l'algèbre et la topologie. Quand j'étais étudiant, chaque fois que Bourbaki publiait un nouveau livre, je l'achetais ou l'empruntais à la bibliothèque et je l'apprenais. Pour moi, pour les gens de ma génération, c'était un manuel. Mais le malentendu était que ce devrait être un manuel pour tout le monde. C'était la grande catastrophe.

Quoi qu'il en soit, à ce moment-là, la portée du projet était plus ou moins claire. Mais que devrait faire Bourbaki après cela ? La seconde génération disposait d'une méthode existante, et n'avait plus qu'à développer un projet aux contours clairement délimités. La troisième génération devait aller au-delà, entrer dans le monde ouvert, ce qui signifiait, à l'époque, la géométrie de manière générale : géométrie algébrique, géométrie différentielle, plusieurs variables complexes, groupes de Lie, espaces de modules, etc.

Je pense que je suis responsable de l'idée que Bourbaki devrait consacrer un chapitre spécial à la géométrie des groupes cristallographiques. Les raisons en sont clairement énoncées dans l'introduction de la série sur les groupes de Lie. Coxeter a été le premier à comprendre la relation entre les groupes de Lie et les groupes cristallographiques et leur classement. Certes, les gens qui travaillaient sur les groupes de Lie étaient, par esprit, plus géométriques et plus pragmatiques que les autres. Mais je me souviens que j'ai dû me battre assez fort pour convaincre mes collègues de Bourbaki que la prééminence devait être donnée aux groupes cristallographiques.

Senechal : *Quelle était l'opinion de Bourbaki sur Coxeter ?*

Cartier : Je pense qu'à partir des années 60, les gens ont réalisé l'importance de son travail. Borel avait beaucoup d'idées semblables et Jacques Tits a également joué un rôle. Tits était beaucoup plus proche dans l'esprit, dans sa façon de faire des mathématiques, de Coxeter que de Bourbaki. Il n'était pas formellement membre de Bourbaki mais il a eu une longue collaboration avec nous. On a donc pu le remercier, dans les livres, pour sa collaboration sans enfreindre la règle de l'anonymat. Tits a été très généreux : il nous a fourni de nombreux volumes publiés pour la première fois dans Bourbaki. Mais bien sûr, il avait une façon très différente de penser les mathématiques.

Dans la deuxième génération et la troisième génération, les deux séries principales étaient l'algèbre commutative (avec la géométrie algébrique en arrière-plan) d'une part, et les groupes de Lie d'autre part. Et il y a une évidente différence de style et d'accent, malgré le fait qu'alors, Bourbaki était vraiment un collectif et que tout le monde contribuait à chaque livre, plus ou moins. Serre était le maître des deux côtés ; il n'était pas un expert des groupes de Lie au départ mais il en est devenu un. Serre était le leader naturel de la deuxième génération car, comme Weil pour la première génération, il était le seul à avoir une approche vraiment universelle des mathématiques. Mais aucun d'eux n'était analyste. Certes, le contenu de Bourbaki portait beaucoup plus sur l'algèbre, la géométrie algébrique, que sur l'analyse.

À la quatrième génération, l'objectif était moins visible. Grothendieck avait développé son propre programme, en dehors de Bourbaki, donc le besoin d'un Bourbaki était moins évident. Et il y avait aussi un manque de compréhension globale des mathématiques. Les membres étaient devenus plus spécialisés dans leurs intérêts.

Il y a eu diverses tentatives au sein du groupe pour se concentrer sur de nouveaux projets. Par exemple, pendant un certain temps, l'idée était que l'on devait développer la théorie de plusieurs variables complexes, et de nombreux brouillons ont été rédigés. Mais il n'a jamais mûri, je pense en partie parce qu'il était trop tard. Il y avait déjà beaucoup de bons manuels au sujet de la théorie de plusieurs variables dans les années soixante-dix, par Grauert et d'autres personnes. À la fin des années 70, la méthode de Bourbaki était si bien comprise que tout le monde savait écrire dans cet esprit. Il y avait toute une génération de manuels et de livres qui étaient sous son influence. Bourbaki s'est retrouvé sans tâche, et il a donc décidé de consacrer une partie de son énergie à la révision de ses propres livres, la soi-disant "Nouvelle édition". La révision était en grande partie achevée ; il s'agissait de révisions vraiment approfondies.

Senechal : *Les révisions incluent-elles un changement de style?*

Cartier : Non, non. Mais par exemple, la section sur la topologie des espaces métriques a été beaucoup plus développée et approfondie, les preuves ont été améliorées et il y a un petit volume qui a tenté de combler le fossé entre la théorie des probabilités et la façon dont Bourbaki a présenté Lebesgue dans la théorie de l'intégration. C'était une tentative de corriger un point de vue manifestement erroné de Bourbaki.

Senechal : *Quels autres domaines des mathématiques voyez-vous maintenant comme ayant été laissés de côté ?*

Cartier : Tout d'abord l'analyse, bien qu'il y ait un texte de calcul élémentaire, un très bon livre, c'était l'influence de Jean Delsarte. Il n'y a essentiellement aucune analyse au-delà des fondements : rien sur les équations aux dérivées partielles, rien sur les probabilités. Il n'y a rien non plus sur la combinatoire, rien sur la topologie algébrique, rien sur la géométrie concrète. Et Bourbaki n'a jamais sérieusement considéré la logique. Dieudonné lui-même était très véhément contre la logique.

Tout ce qui touche à la physique mathématique est totalement absent du texte de Bourbaki. Au séminaire Bourbaki, j'ai contribué à une longue série d'articles mettant l'accent sur des questions de physique mathématique. Mais j'étais le seul, et mes contributions n'étaient pas toujours acceptées sans combat.

Mais même dans les domaines des mathématiques qui n'ont pas été considérés par Bourbaki, en rétrospective sur les trente dernières années, il est évident que leur développement a été très marqué par l'esprit Bourbaki.

Senechal : *Y avait-il un préjugé contre la physique, ou Bourbaki n'y a-t-il tout simplement pas pensé ?*

Cartier : Eh bien, bien sûr, il y avait un fort parti pris contre, pour la plupart des gens. Au début, je suppose que j'étais un peu hétérodoxe au sein du groupe Bourbaki. J'avais un intérêt de longue date pour la physique mathématique. II y a quelques années, lors d'une discussion avec André Weil, juste après qu'il ait publié ses propres mémoires, j'ai dit : "Vous avez mentionné qu'en 1926 vous étiez à Gottingen... en 1926 quelque chose s'est passé à Gottingen". Et Weil a demandé : "Que s'est-il passé à Göttingen?" et j'ai dit "Oh ! La mécanique quantique !" Et Weil a dit : "Je ne sais pas ce que c'est." Il était élève de Hilbert en 1926 et Hilbert lui-même s'intéressait à la mécanique quantique, Max Born était là, Heisenberg était là, et d'autres, mais apparemment André Weil n'y prêtait aucune attention. J'ai récemment eu l'occasion de donner une conférence publique sur la philosophie de l'espace d'Hermann Weyl, j'ai donc lu attentivement la littérature à son sujet. Il y a une nécrologie d'Hermann Weyl écrite par Chevalley et Weil. Ils le louent, pour de bonnes raisons, mais il n'y a aucune mention de ses travaux en physique, pas même de ses travaux en relativité générale. De toute évidence, les deux meilleurs livres de Weyl sont son livre sur la relativité générale et son livre sur la mécanique quantique !

Senechal : *La dernière publication de Bourbaki remonte à 1983. Pourquoi ne publie-t-il plus rien maintenant ?*

Cartier : Il y a plusieurs raisons à cela. D'abord, il y a eu un clash entre Bourbaki et son éditeur, au sujet des droits d'auteur et des droits de traduction, qui s'est soldé par une longue et désagréable procédure judiciaire. Lorsque l'affaire a été réglée en 1980, Bourbaki a été autorisé à conclure un accord avec un nouvel éditeur. En utilisant le travail intensif effectué dans les années soixante-dix dans le but de réviser les anciennes éditions, nous avons pu les republier dans une nouvelle édition. Nous avons complété la série existante par deux ou trois volumes supplémentaires, mais alors... silence.

Au-delà de l'objectif facile d'une "édition définitive", Bourbaki a lutté dans les années 70 et 80 pour formuler de nouvelles orientations. J'ai déjà mentionné un projet raté sur la théorie à plusieurs variables complexes. Il y eut des tentatives de théorie de l'homotopie, de théorie spectrale des opérateurs, de théorème de l'indice, de géométrie symplectique. Mais aucun de ces projets n'a dépassé le stade préliminaire.

Bourbaki n'a pas pu trouver de nouvelle issue car on avait une vision dogmatique des mathématiques : tout devait être placé dans un cadre sécurisé. C'était tout à fait raisonnable pour la topologie générale et l'algèbre générale, qui étaient déjà solidifiées vers 1950. La plupart des gens conviennent maintenant que vous avez besoin de bases générales pour les mathématiques, du moins si vous croyez en l'unité des mathématiques. Mais je crois maintenant que cette unité doit être organique, alors que Bourbaki défendait un point de vue structurel.

Conformément aux vues de Hilbert, Bourbaki pensait que la théorie des ensembles fournissait ce cadre général dont on avait cruellement besoin. Si vous avez besoin de quelques bases logiques, les catégories sont un outil plus flexible que la théorie des ensembles. Le fait est que les catégories offrent à la fois un fondement philosophique général qui est la partie encyclopédique, ou taxonomique, et un outil mathématique très efficace, à utiliser dans des situations mathématiques. Que la théorie des ensembles et les structures soient, en revanche, plus rigides, on peut le voir en lisant le dernier

chapitre de la théorie des ensembles de Bourbaki, avec un effort monstrueux pour formuler des catégories sans catégories.

> Pour lui, il était important de voir les questions dans leur ensemble, de voir la nécessité d'une preuve, ses implications globales. Quant à la rigueur, tous les membres de Bourbaki y tenaient : le mouvement Bourbaki est né essentiellement parce que la rigueur manquait aux mathématiciens français, par rapport aux Allemands, c'est-à-dire aux hilbertiens. La rigueur consistait à se débarrasser d'une accumulation de détails superflus. À l'inverse, le manque de rigueur donnait à mon père l'impression d'une épreuve où l'on marchait dans la boue, où il fallait ramasser une sorte de crasse pour avancer. Une fois cette saleté retirée, on pouvait accéder à l'objet mathématique, sorte de corps cristallisé dont l'essence est sa structure. Quand cette structure avait été construite, il disait que c'était un objet qui l'intéressait, quelque chose à regarder, à admirer, peut-être à retourner, mais certainement pas à transformer. Pour lui, la rigueur en mathématiques consistait à fabriquer un nouvel objet qui pouvait ensuite rester inchangé.
>
> La façon dont mon père travaillait, il semble que c'était ça qui comptait le plus, cette production d'un objet qui ensuite devenait inerte-mort, vraiment. Il ne devait plus être altéré ni transformé. Non pas qu'il y ait eu une connotation négative à cela. Mais je dois ajouter que mon père était probablement le seul membre de Bourbaki qui considérait les mathématiques comme un moyen de mettre à mort des objets à des fins esthétiques.
>
> Extrait de "Claude Chevalley décrit par sa fille" (1988)
> dans *Nicolas Bourbaki : Faits et légendes.*

Il est étonnant que la théorie des catégories ait été plus ou moins l'idée originale de Bourbaki. Les deux fondateurs étaient Eilenberg et MacLane. MacLane n'a jamais été membre de Bourbaki, mais Eilenberg l'était, et MacLane était proche d'esprit. Le premier manuel sur l'algèbre homologique qui a été publié était de Cartan-Eilenberg, lorsque les deux étaient très actifs à Bourbaki. Citons aussi Grothendieck, qui a très largement développé les catégories. J'ai utilisé des catégories de manière consciente ou inconsciente dans une grande partie de mon travail, tout comme la plupart des membres de Bourbaki. Mais parce que la façon de penser était trop dogmatique, ou du moins la présentation dans les livres était trop dogmatique, Bourbaki ne pouvait s'accommoder d'un changement d'orientation, une fois le processus de publication lancé.

Je pense que les années 80 étaient une limite naturelle. Sous la pression d'André Weil, Bourbaki a insisté pour que chaque membre prenne sa retraite à cinquante ans, et je me souviens qu'à quatre-vingts ans, j'ai dit, en plaisantant, que Bourbaki devait prendre sa retraite à cinquante ans.

Senechal : *Il semble que cela se soit plus ou moins produit.*

Cartier : Oui, je pense que l'une des principales raisons est que son objectif déclaré, fournir les bases de toutes les mathématiques existantes, a été atteint. Mais aussi, si vous avez un format aussi rigide, il est très difficile d'intégrer de nouveaux développements. Si ce qui est considéré comme important ne change pas, c'est toujours possible. Mais bien sûr, après cinquante ans, ce qui est considéré comme important avait changé.

Senechal : *En diriez-vous un peu plus là-dessus ?*

Cartier : André Weil aimait parler de l'air du temps, de l'air du temps. Ce n'est pas un hasard si Bourbaki a duré du début des années 30 aux années 80, alors que le système soviétique a duré de 1917 à 1989. André Weil n'aime pas cette comparaison. Il dit à plusieurs reprises : "Je n'ai jamais été communiste !". On dit en plaisantant que le XXe siècle a duré de Sarajevo 1914 à Sarajevo 1989. Le XXe siècle, de 1917 à 1989, a été un siècle d'idéologie, l'âge idéologique.

Senechal : *Par idéologie, entendez-vous l'idée d'un schéma directeur qui puisse servir à tous les usages et pour toujours ?*

Cartier : *Une solution finale.* Il y a de bonnes raisons de détester cette expression, mais c'est dans l'esprit des gens qu'on pourrait arriver à une solution finale. Il y a un livre de H.G. Wells intitulé *A Modern Utopia*, qui devrait être réimprimé. Par hasard, je le lisais juste au moment de l'effondrement du système soviétique. Comme vous le savez, H.G. Wells était certainement très amical envers la révolution d'Octobre 1917, il était un ami des Soviétiques, certes. Mais il avait un esprit très vif et il avait une vision historique si fine qu'il pouvait envisager des développements.

Même s'il était enthousiasmé par cette nouvelle ère, il a compris que la solution finale n'existe pas et que c'était une erreur de considérer qu'on peut atteindre un tel état d'équilibre social historique que désormais la société restera telle qu'elle est pour toujours. Wells s'est très bien opposé à cette idée. Si vous lisez ses livres, vous verrez cela comme l'une de ses obsessions.

Hilbert, je pense, reflétait ce Zeitgeist. Il y a un enregistrement de sa voix ; dans le livre de Constance Reid sur Hilbert, il y en a une disquette, un enregistrement d'un discours que Hilbert a prononcé en Allemagne dans les années trente. C'est très idéologique. À l'époque, Hilbert vieillissait et ses vues étaient donc idylliques, se solidifiant.

Si vous mettez côte à côte le manifeste des surréalistes et l'introduction de Bourbaki, ainsi que d'autres manifestes de l'époque, ils se ressemblent beaucoup. Ma fille traduit actuellement un livre sur la naissance de la cinématographie, et dans un chapitre sur les futuristes italiens, il y a une affirmation très similaire. En science, en art, en littérature, en politique, en économie, en affaires sociales, c'était le même esprit. L'objectif déclaré de Bourbaki était de créer une nouvelle mathématique. Il n'a cité aucun autre texte mathématique. Bourbaki est autosuffisant. Bien sûr, à l'époque, les communistes de l'Union soviétique affirmaient la même chose. Nous savons maintenant que c'était un mensonge, et que les dirigeants savaient à l'époque qu'ils mentaient. Certes Bourbaki ne mentait pas, mais quand même, l'esprit était le même. C'était le temps de l'idéologie : Bourbaki devait être le Nouvel Euclide, il écrirait un manuel pour les 2000 prochaines années.

Senechal : *Pourquoi y a-t-il un manque d'illustration visuelle dans la plupart des œuvres de Bourbaki ?*

Cartier : Je pense que la meilleure réponse serait la description de Chevalley donnée par sa fille [voir encadré]. Les Bourbaki étaient des puritains, et les puritains s'opposent fortement aux représentations picturales des vérités de leur foi. Le nombre de protestants et de juifs dans le groupe Bourbaki était écrasant. Et vous savez que les protestants français surtout sont très proches des

juifs dans l'esprit. J'ai des origines juives et j'ai été élevé dans la lignée des huguenots. Nous sommes un peuple de la Bible, de l'Ancien Testament, et beaucoup de huguenots en France sont plus épris de l'Ancien Testament que du Nouveau Testament. Parfois, nous adorons Jaweh plus que Jésus.

Alors, quelles étaient les raisons ? La philosophie générale telle que développée par Kant, certainement. Bourbaki est le fruit de la philosophie allemande, Bourbaki a été fondée pour développer et propager les vues philosophiques allemandes dans la science. André Weil a toujours aimé la science allemande et il citait toujours Gauss. Tous ces gens, avec leurs propres goûts et leurs propres opinions personnelles, étaient des partisans de la philosophie allemande.

Et puis il y a eu l'idée qu'il y a une opposition entre l'art et la science. L'art est fragile et mortel, parce qu'il fait appel aux émotions, au sens visuel et aux analogies tacites.

Mais je pense que cela fait aussi partie de la tradition euclidienne. Dans Euclide, vous trouvez quelques dessins mais on sait que la plupart d'entre eux ont été ajoutés après Euclide, dans des éditions ultérieures. La plupart des dessins de l'original sont des dessins abstraits. Vous faites un raisonnement sur certaines proportions et vous dessinez des segments, mais ils ne sont pas destinés à être des segments géométriques, juste des représentations de certaines notions abstraites. Aussi Lagrange affirmait-il fièrement, dans son manuel de mécanique : "Vous ne trouverez aucun dessin dans mon livre !" L'esprit analytique faisait partie de la tradition française et de la tradition allemande. Et je suppose que c'était aussi dû à l'influence de gens comme Russell, qui affirmaient qu'ils pouvaient tout prouver formellement - que la soi-disant intuition géométrique n'était pas fiable en matière de preuve.

Encore une fois, les abstractions et le mépris de Bourbaki pour la visualisation s'inscrivaient dans une mode globale, comme l'illustrent les tendances abstraites de la musique et de la peinture de cette période.

Senechal : *Les membres de Bourbaki appréciaient-ils la musique abstraite et l'art abstrait ?*

Cartier : Je ne pense pas qu'ils aient eu beaucoup de goût pour la musique ou l'art abstrait. On pourrait dire qu'ils avaient dans l'ensemble des goûts bourgeois classiques. Bourgeois instruit, pas philistins. Par exemple, Cartan et Dieudonné étaient des amoureux et des praticiens de la musique, mais ils étaient très classiques. Cartan certes, dans son éducation protestante, aimait beaucoup Bach, et Dieudonné était un assez bon pianiste, au niveau amateur, mais assez bon, et il avait une mémoire fantastique. Il connaissait des centaines et des centaines de pages de partitions par cœur et pouvait suivre chaque note. Je me souviens que j'ai eu quelques occasions d'aller à la salle de concert avec lui. C'était fascinant, il regardait la partition dans sa main et s'exclamait "OH !" si l'orchestre sautait une note ! Il consacra les six derniers mois de sa vie, lorsqu'il décida que sa vie mathématique était terminée, qu'il avait écrit son dernier livre, et qu'il se retira chez lui, pour écouter des enregistrements et suivre les partitions et les notes.

Il est intéressant de savoir que les révolutionnaires en mathématiques n'étaient pas des révolutionnaires dans d'autres domaines. Je suppose que la seule personne dans le groupe Bourbaki qui était

vraiment consciente des liens de l'idéologie Bourbaki avec d'autres idéologies était Chevalley. Il a été membre de divers groupes d'avant-garde, tant en politique qu'en arts. En tant qu'éditeur du travail de Chevalley, j'ai décidé, à la demande de sa fille, d'inclure un volume spécial sur son travail en dehors des mathématiques. Il avait écrit diverses brochures et diverses notes : Catherine Chevalley devra travailler dur pour collecter ces choses et nous les publierons dans le cadre de ses œuvres collectées.

Chevalley était le seul à percevoir le lien entre Bourbaki et le reste, et c'est peut-être pourquoi, dans les années 70, il était plus critique que les autres. Dans les années 70, une personne sensée pouvait déjà voir la fin d'une longue tendance historique, et je pense qu'il y était très sensible. Les mathématiques étaient la partie la plus importante de sa vie, mais il n'a tracé aucune frontière entre ses mathématiques et le reste de sa vie. Peut-être que c'était parce que son père était ambassadeur, donc il avait plus de contacts avec d'autres personnes.

Senechal : *Pouvez-vous préciser les principales raisons du déclin de Bourbaki ?*

Cartier : Comme je l'ai dit, dans les années 80, il n'y avait plus d'objectif déclaré, si ce n'est la longue bataille juridique. Je pense que c'était l'un des cas du siècle ! Nous avons engagé un célèbre avocat qui s'était battu pour les héritiers de Picasso et de Fujita. Nous avons survécu artificiellement : nous devions gagner cette bataille. Mais ce fut une victoire à la Pyrrhus. Comme d'habitude dans les batailles juridiques, les deux parties ont perdu et l'avocat s'est enrichi. Dans la gloire et dans la poche.

En un sens, Bourbaki est comme un dinosaure, la tête trop éloignée de la queue. Quand Dieudonné fut le scribe de Bourbaki, pendant de nombreuses années, chaque mot imprimé venait de sa plume. Bien sûr, il y avait eu de nombreux brouillons et versions préliminaires, mais la version imprimée était toujours de la plume de Dieudonné. Et avec sa mémoire fantastique, il connaissait chaque mot. Je me souviens, c'était une blague, on pouvait dire "Dieudonné, c'est quoi ce résultat sur untel ?" et il se dirigeait vers l'étagère, décrochait le livre et l'ouvrait à la bonne page. Après Dieudonné (et un intermède de Samuel et Dixmier) j'étais le secrétaire de Bourbaki, et c'était mon devoir de faire la majeure partie de la relecture, je pense que j'ai relu cinq à dix mille pages. J'ai une bonne mémoire visuelle. Je ne me comparerais pas à Dieudonné, mais il fut un temps où je connaissais la plupart des imprimés de Bourbaki. Mais personne après moi n'a pu le faire. Ainsi Bourbaki a perdu la conscience de son propre corps, les 40 volumes publiés.

Et comme je l'ai déjà dit, Bourbaki était plus ou moins comme une famille. La deuxième, la troisième ou la quatrième génération de toute famille ou de tout groupe social suit des schémas sociologiques définis. Ma propre famille était typique. Mon grand-père était un self-made man, un homme d'affaires très prospère. Mon père et mon oncle se sont lancés dans l'entreprise, mais ils n'étaient pas si dévoués au combat. Et les gens de ma génération, eh bien, je suppose que j'ai pris la bonne décision de ne pas m'y engager. En effet, les gens de ma génération qui ont poursuivi les affaires de notre famille n'ont pas si bien réussi, parce qu'ils n'avaient rien contre quoi se battre.

Mais ce sont les raisons internes. Bien sûr, le monde extérieur a aussi une influence. Que le monde mathématique extérieur ait changé est évident. Nous savons tous que ce que Staline n'a jamais pu

réaliser avec son armée, conquérir le monde, l'effondrement de l'Union soviétique l'a réalisé pour les mathématiques. Les mathématiciens russes ont apporté un style différent à l'Occident, une façon différente de regarder les problèmes, un sang neuf.

C'est une autre époque, avec des valeurs différentes. Je n'ai aucun regret : je pense que cela valait la peine de vivre au XXe siècle.

Senechal : Comment décririez-vous votre parcours avec Bourbaki ?

Cartier : J'ai été personnellement très heureux parce que quand j'ai atteint l'âge de la retraite normale de Bourbaki, j'ai eu la très heureuse opportunité d'être sollicité pour prononcer la conférence au nom de Vladimir Drinfel'd au Congrès international des mathématiciens à Berkeley en 1986 (Drinfel'd a été empêché de venir pour des raisons politiques). Ce fut un grand défi et un grand honneur pour moi ; son article est l'un des articles les plus importants des Proceedings. Du jour au lendemain, cela a changé ma vie mathématique. J'ai pensé : "C'est ce que je dois faire maintenant.". Bien sûr je connaissais le matériau de base mais la perspective était nouvelle. Je ne peux pas prétendre que dans les quelques heures que j'ai eues pour préparer la conférence, j'ai pu vraiment la maîtriser, mais j'en ai assez compris pour pouvoir expliquer aux gens : "C'est nouveau, c'est important.".

Quand j'ai commencé en mathématiques, la tâche principale d'un mathématicien était de mettre de l'ordre et de faire une synthèse du matériau existant, pour créer ce que Thomas Kuhn appelait la science normale. Les mathématiques, dans les années 1940 et 1950, traversaient ce que Kuhn appelle une période de solidification. Dans une science donnée, il y a des moments où vous devez prendre tout le matériau existant et créer une terminologie unifiée, des normes unifiées et former les gens dans un style unifié. Le but des mathématiques, dans les années 50 et 60, était de créer une nouvelle ère de science normale. Maintenant, nous sommes à nouveau au début d'une nouvelle révolution. Les mathématiques connaissent des changements majeurs. Nous ne savons pas exactement où cela ira. Il n'est pas encore temps de faire la synthèse de tout cela, peut-être dans vingt ou trente ans sera-t-il l'heure d'un nouveau Bourbaki. Je me considère très chanceux d'avoir eu deux vies, une vie de science normale et une vie de révolution scientifique.

Bibliographie

1. *Nicolas Bourbaki, Faits et légendes*, Michèle Chouchan, Éditions du Choix, Argenteuil, 1995.
2. Nicholas Bourbaki, Collective Mathematician : an interview with Claude Chevalley, Denis Guedj, traduit par Jeremy Gray, *The Mathematical Intelligencer, vol. 7, n° 2, 18-22, 1985.*
3. *Les Mathématiques et l'Art*, Pierre Cartier, Institut des Hautes Études Scientifiques, preprint IHÉS/M/93/33.
4. The Continuing Silence of a Poet, A. B. Yehoshua, dans *The continuing silence of a poet : collected stories*, Penguin books, 1991.

Comment une valeur propre de matrice peut permettre de distinguer les nombres premiers des nombres composés ? (Denise Vella-Chemla, 21.5.2023)

1. Exposition du problème

On revient à une matrice par blocs (idéalement infinie mais on va ici considérer des matrices de taille finie), notée M_k dans la suite, contenant sur sa diagonale des matrices circulantes de taille 2, 3, 4, ..., k. On avait eu l'idée de cette matrice en juillet 2019 pour "simuler le crible d'Ératosthène"[1]. On écrit M_5 ci-dessous pour illustrer.

$$M_5 = \begin{pmatrix} \boxed{\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}} & 0 & 0 & 0 \\ 0 & \boxed{\begin{matrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{matrix}} & 0 & 0 \\ 0 & 0 & \boxed{\begin{matrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{matrix}} & 0 \\ 0 & 0 & 0 & \boxed{\begin{matrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{matrix}} \end{pmatrix}$$

Dans la note de 2019, on avait utilisé cet opérateur (cette matrice) pour distinguer les nombres premiers des nombres composés par le fait suivant : si la trace de la puissance de matrice $\mathrm{Tr}(M^p)$ est égale à p, alors p est un nombre premier.

La matrice M_k est une matrice carrée de taille $n \times n$ avec $n = \dfrac{k(k+1)}{2} - 1$. Comme elle ne contient que des 0 et des 1 et que chaque ligne et chaque colonne ne contient qu'un seul 1, cette matrice est une matrice de permutation.

Les mini-matrices circulantes, sur la diagonale de M_k sont les matrices de permutation des groupes cycliques C_2, C_3, C_4, ..., C_k. Si on observe la diagonale de chacune de ces petites matrices, par exemple, la diagonale de la matrice 3×3, lorsqu'on l'élève à différentes puissances correspondant aux entiers successifs

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^4 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^5 = \ldots,$$

[1] Voir http://denise.vella.chemla.free.fr/enstransfotrace.pdf.

on comprend que suivant l'exposant de la matrice (la puissance à laquelle on l'élève), une fois sur 3, pour les $3k$, les 3 chiffres 1 se retrouveront sur la diagonale, et la puissance de la matrice en question aura pour trace 3. Cette cyclicité correspond au fait de "barrer un nombre sur 3" dans l'algorithme du crible d'Ératosthène pour trouver les nombres premiers.

Il en est de même pour la matrice "géante" contenant *toutes* les mini-matrices circulantes parce toutes les matrices autres que la matrice p lorsque p est un nombre premier ont leur diagonale pleine de 0 (et la trace étant la somme des éléments diagonaux, elle ne cumulera rien pour les petites matrices circulantes en question) quand on est sur une puissance M^q avec $q \neq p$.

On fait calculer par programme les valeurs propres des matrices $(M_k)^k$ pour k les entiers successifs. On constate que la liste des valeurs propres de $(M_p)^p$ pour p un nombre premier est le cumul des listes des racines de l'unité pour $2 \leq k \leq p$ alors que pour les nombres composés, la liste des valeurs propres contient de nombreux 1, ainsi que "quelques" complexes racines de l'unité.

2. Tentative d'explication

La trace de la matrice $\mathrm{Tr}((M_k)^k)$ est égale à $\sigma(k) - 1$, où $\sigma(k)$ dénote la somme des diviseurs de k. En effet, par la cyclicité des sous-matrices, l'élévation à la puissance k de la matrice M_k "ramène" les 1 sur la diagonale seulement pour les diviseurs de k et l'opérateur trace, qui calcule la somme des éléments diagonaux de $(M_k)^k$, qui ici compte les 1 qui sont revenus sur la diagonale, en compte d pour un diviseur d de k dans la matrice $(M_k)^k$ (*rappel* : la matrice $(M_k)^k$ est de taille $\left(\frac{k(k+1)}{2} - 1\right) \times \left(\frac{k(k+1)}{2} - 1\right)$).

Le déterminant de cette même matrice est égal à -1 pour les nombres de la forme $4k+3$ et 1 pour les nombres de la forme $4k+1$, $4k$ et $4k+2$[2].

Voyons les valeurs propres ; écrivons les premières listes : on sépare par ci par là les valeurs propres par des ";" bleus au lieu d'utiliser les ",", pour bien séparer certains groupes de valeurs propres que l'on pense devoir être "lues ensembles".

$$2 \to [1, 1]$$

$$3 \to [1, -1 \ ; \ 1, 1, 1]$$

$$4 \to [-\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i \ ; \ -\tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i \ ; \ 1, 1, 1 \ ; \ 1, 1, 1, 1]$$

$$5 \to [1, -1 \ ; \ -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i, -\tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i, 1 \ ; \ -1, i, -i, 1 \ ; \ 1, 1, 1, 1, 1]$$

$$6 \to [-0.80 + 0.587i, -0.80 - 0.587i, 0.30 + 0.95i, 0.30 - 0.95i, 1 \ ; \ 1, -1, 1, -1 \ ; \ 1, 1 \ ; \ 1, 1, 1 \ ; \ 1, 1, 1, 1, 1, 1]$$

$$7 \to [1, -1 \ ; \ -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i, -\tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i, 1 \ ; \ -1, i, -i, 1 \ ; \ -0.80 + 0.587i, -0.80 - 0.587i, 0.30 + 0.95i, 0.30 - 0.95i, 1 \ ; \ -1, -\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i, -\tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i, \tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i, \tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i, 1 \ ; \ 1, 1, 1, 1, 1, 1, 1]$$

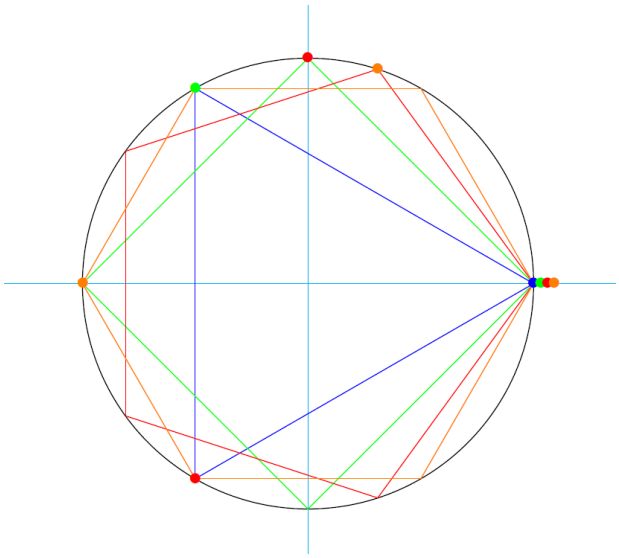
[2] On rappelle que Gauss remplaçait les $4k+3$ par des -1 dans les Recherches arithmétiques, dans sa démonstration de la loi de réciprocité quadratique.

On voit que ce n'est que pour les nombres premiers que la liste des valeurs propres est la liste des racines $k^{\text{ièmes}}$ de l'unité du plus petit polygone au plus grand en commençant par le polygone à 2 côtés (de sommets 1 et -1).

Ainsi, les nombres premiers ont des images qui sont des listes emboîtées : la liste des valeurs propres de la puissance p de leur matrice M_p (dont on rappelle qu'elle est de taille $\frac{p(p+1)}{2} - 1$) contient toutes les racines de l'unité pour $2 \leq k \leq p$. Les nombres composés n'ont pas ce genre d'image.

Regardons les valeurs propres pour le nombre composé 6 dans la liste fournie précédemment : on voit les $2 + 3 + 6 = \sigma(6) - 1 = 11$ occurrences de la valeur propre 1 correspondant aux 1 sur la diagonale de la sixième puissance de M_6, les autres valeurs propres sont celles du pentagone (car $6 \equiv 1 \pmod 5$).

Ci-dessous, le cercle unité sur lequel ont été positionnées les racines de l'unité des polygones réguliers ayant de 3 à 6 côtés.



3. Tentative de théorisation

La matrice M_k, qui contient toutes les circulantes sur sa diagonale, présente l'avantage, lorsqu'on l'élève à des puissances successives, de faire agir *simultanément* chacune des petites matrices circulantes indépendamment. Dans la suite, on notera les petites circulantes C_x pour ne pas se mélanger les pinceaux[3] avec la grosse matrice M_k.

La matrice M_k est une matrice de permutation :

- elle fait agir la mini-matrice C_2 sur les nombres de 1 à 2 ;
- elle fait agir la mini-matrice C_3 sur les nombres de 3 à 5 ;
- elle fait agir la mini-matrice C_4 sur les nombres de 6 à 9 ;

[3] C'est le cas de le dire..., puisque la théorie de tout ça en anglais parle de "shuffle".

- etc ;
- elle fait agir la mini-matrice C_k sur les nombres de $\frac{(k-1)k}{2}$ à $\frac{k(k+1)-2}{2}$.

Voyons les puissances des matrices circulantes indépendamment les unes des autres :

- $(C_k)^{0 \pmod k} = \mathrm{Id}_k$;
- $(C_k)^{+1 \pmod k} = C_k$;
- $(C_k)^{-1 \pmod k} = (C_k)^*$; il se trouve que dans le cas des matrices de permutations (ici cycliques), la transposée est également l'inverse. ;
- si k est pair, $(C_k)^{\frac{k}{2} \pmod m}$ est une matrice symétrique qui contient deux moitiés de diagonales, une au nord-est et une au sud-ouest (par exemple $(C_4)^6 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$.

4. Littérature

On peut se reporter à l'article 41 des Recherches arithmétiques de Gauss [1] pour trouver une démonstra-tion au sujet de permutations ainsi qu'aux manuscrits de Galois [2].

Valentin Bahier (à Toulouse) ou Nadia Lafrenière (à Montréal) ont présenté deux thèses sur les opérateurs de mélange aléatoires ([3], [4]).

5. Lien avec la conjecture de Goldbach

On a vu [5] qu'un nombre premier incongru à n (un nombre pair ≥ 6) selon tout module premier $\leq \lfloor \sqrt{n} \rfloor$ est un décomposant de Goldbach de n.

La reformulation de cette conjecture en terme de matrices est :

Conjecture de Goldbach :

$\forall n \geq 6, \exists p, p$ est un décomposant de Goldbach de n, i.e. p est premier et $n-p$ est premier.

$\forall n \geq 6, \exists p, \forall q$ premier, $2 \leq q \leq \lfloor \sqrt{n} \rfloor, (M_q)^p \neq (M_q)^n$.

On utilise la caractérisation trouvée pour les nombres premiers en terme de trace, on obtient :

$$\forall n \geq 6, \exists p \text{ tel que } \mathrm{Tr}(M_p)^p = p$$
$$\text{et } \forall q \text{ tel que }, 2 \leq q \leq \lfloor \sqrt{n} \rfloor \text{ et } \mathrm{Tr}(M_q)^q) = q,$$
$$\text{on a } (M_q)^p \neq (M_q)^n.$$

On peut préférer $(M_p)^p = \mathrm{Id}_p$ plutôt que $\mathrm{Tr}(M_p)^p = p$.

Illustration sur un exemple

Dans la table ci-dessous, on montre les puissances (exposants entêtes des colonnes) des matrices (dénomination choisie indiquée entêtes de ligne) qui montrent que 3 et 7 sont des décomposants de Golbach de 20. Pour alléger le tableau, on note ci-dessous les matrices de 20 :

$$(M_3)^{20} = \begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix}, \quad (M_5)^{20} = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix}, \quad (M_7)^{20} = \begin{pmatrix} & & & & & & 1 \\ 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \end{pmatrix}$$

Table des puissances impaires des matrices d'indices impaires :

	3	5	7	9
M_3	$\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$	$\begin{pmatrix} & & 1 \\ 1 & & \\ & 1 & \end{pmatrix}$	$\begin{pmatrix} 1 & & \\ & & 1 \\ 1 & & \end{pmatrix}$	$\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$
M_5	$\begin{pmatrix} & & 1 & & \\ & & & & 1 \\ 1 & & & & \\ & 1 & & & \\ & & & 1 & \end{pmatrix}$	$\begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{pmatrix}$	$\begin{pmatrix} & & 1 & & \\ & & & 1 & \\ & & & & 1 \\ 1 & & & & \\ & 1 & & & \end{pmatrix}$	$\begin{pmatrix} & & & & 1 \\ 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \end{pmatrix}$
M_7	$\begin{pmatrix} & & 1 & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & & 1 \\ 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \end{pmatrix}$	$\begin{pmatrix} & & & & & & 1 \\ 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \end{pmatrix}$	$\begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & 1 \end{pmatrix}$	$\begin{pmatrix} & & & 1 & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & 1 \\ 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \end{pmatrix}$
M_9	$(7,8,9,1,2,3,4,5,6)$	$(5,6,7,8,9,1,2,3,4)$	$(3,4,5,6,7,8,9,1,2)$	$(1,2,3,4,5,67,8,9)$

Note : Pour la ligne des puissances $9^{\text{ièmes}}$, on utilise la notation standard des permutations (voir la diapositive 4/29 du diaporama de Nadia Lafrenière [6]). On a que $(M_x)^y = (x-y+1, \ldots, x, 1, \ldots, x-y)$.

Références.

[1] Carl Friedrich Gauss, Recherches arithmétiques, Brunswick, 1802, voir l'édition Jacques Gabay, Paris ici https://gallica.bnf.fr/ark:/12148/bpt6k29060d.

[2] Évariste Galois, Manuscrits, publiés par Jules Tannery, 1908, Gauthier-Villars, Paris ici https://gallica.bnf.fr/ark:/12148/bpt6k9610625f.

[3] Nadia Lafreniere, Thèse de doctorat, *Valeurs propres des opérateurs de mélange symétrisés*, 2019, Montréal, https://nadialafreniere.github.io/these.pdf.

[4] Valentin Bahier, Thèse de doctorat, *Spectre de matrices de permutation aléatoires*, 2018, http://thesesups.ups-tlse.fr/3973/1/2018TOU30069.pdf.

[5] Denise Vella-Chemla, *Réécrire* (aidée de Leila Schneps), http://denise.vella.chemla.free.fr/jade1.pdf.

[6] Nadia Lafrenière, *Derangements : Solving Problems by Counting (Certain Types Of) Permutations*, Dartmouth College, https://nadialafreniere.github.io/talks/Derangements.pdf

Comment une valeur propre de matrice peut permettre de distinguer les nombres premiers des nombres composés ? (Denise Vella-Chemla, 21.5.2023)

On revient à une matrice, notée M dans la suite, contenant sur sa diagonale des matrices circulantes de taille 2, 3, 4, etc. On avait eu l'idée de cette matrice en juillet 2019 pour "simuler le crible d'Eratosthène"[1].

$$M = \begin{pmatrix}
0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 1 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 1 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 0 & 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 1 & 0 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 1 & 0 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 1 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 1 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 0 & 1 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 1 & 0 & 0 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}$$

Dans la note de 2019, on avait utilisé cet opérateur (cette matrice) pour distinguer les nombres premiers des nombres composés par le fait suivant : si $\mathrm{Tr}(M^p) = p$, alors p est un nombre premier.

Au rang k, la matrice est une matrice carrée de taille $n \times n$ avec $n = \frac{k(k+1)}{2} - 1$. Comme elle ne contient que des 0 et des 1 et que chaque ligne et chaque colonne ne contient qu'un seul 1, cette matrice est une matrice de permutation.

Les mini-matrices cycliques sur la diagonale de M sont les matrices de permutation des groupes cycliques C_2, C_3, C_4, etc. Si on observe la diagonale de chacune de ces petites matrices, par exemple, la diagonale de la matrice 3×3, lorsqu'on les élève à différentes puissances correspondant aux entiers successifs

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^4 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^5 = \dots,$$

on comprend que suivant l'exposant de la matrice (la puissance à laquelle on l'élève), une fois sur 3, pour les puissances multiples de 3, les 3 chiffres 1 se retrouveront sur la diagonale, et la puissance de

[1] Voir http://denise.vella.chemla.free.fr/enstransfotrace.pdf.

la matrice en question aura pour trace 3. Cette cyclicité correspond au fait de “barrer un nombre sur 3” dans l'algorithme de criblage d'Ératosthène pour trouver les nombres premiers.

Il en est de même pour la matrice “géante” contenant *toutes* les mini-matrices circulantes parce toutes les matrices autres que la matrice p lorsque p est un nombre premier ont leur diagonale pleine de 0 quand on est sur une puissance M^q avec $q \neq p$.

Ci-dessous, le programme qui élève M aux diverses puissances successives et en calcule une valeur propre.

```
import math
import numpy as np
import numpy.linalg as alg

for k in range(2,50):
      print(k,end='')
      m=int(k*(k+1)/2-1)
      a = np.zeros((m,m))
      for u in range(k-1):
            i = int(((u+1)**2+3*(u+1)-2)/2)
            j = int(((u+3)**2-3*(u+3))/2)
            a[i,j] = 1
      for u in range(m-1):
            a[u,u+1] = 1
      for u in range(k-2):
            i = int(((u+1)**2+3*(u+1)-2)/2)
            j = int(((u+1)**2+3*(u+1)-2)/2+1)
            a[i,j] = 0
      grise = alg.matrix_power(a,k)
      valpropres = alg.eigvals(grise)
      print(valpropres[2:3])
      if (np.trace(grise) == k):
            print(k, 'est un nombre premier.'),
```

On utilise la bibliothèque python numpy.alg pour calculer l'une des valeurs propres des matrices pour un rang variant de 2 à 100.

```
2[] 2 est un nombre premier.
3[1.]  3 est un nombre premier.
4[1.+0.j]
5[-0.5+0.8660254j] 5 est un nombre premier.
6[0.30901699+0.95105652j]
7[-0.5+0.8660254j] 7 est un nombre premier.
```

```
8[-0.22252093+0.97492791j]
9[-1.+0.j]
10[-0.5+0.8660254j]
11[-0.5+0.8660254j] 11 est un nombre premier.
12[0.30901699+0.95105652j]
13[-0.5+0.8660254j] 13 est un nombre premier.
14[-0.74851075+0.66312266j]
15[-1.+0.j]
16[-0.80901699+0.58778525j]
17[-0.5+0.8660254j] 17 est un nombre premier.
18[-0.70710678-0.70710678j]
19[-0.5+0.8660254j] 19 est un nombre premier.
20[-0.5+0.8660254j]
21[-1.+0.j]
22[-0.90096887+0.43388374j]
23[-0.5+0.8660254j] 23 est un nombre premier.
24[-0.65486073+0.75574957j]
25[-0.5+0.8660254j]
26[-0.92977649+0.36812455j]
27[-1.+0.j]
28[-0.93969262+0.34202014j]
29[-0.5+0.8660254j] 29 est un nombre premier.
30[-0.90096887-0.43388374j]
31[-0.5+0.8660254j] 31 est un nombre premier.
32[-0.95413926+0.29936312j]
33[-1.+0.j]
34[-0.95949297+0.28173256j]
35[-0.5+0.8660254j]
36[-0.85021714+0.52643216j]
37[-0.5+0.8660254j] 37 est un nombre premier.
38[-0.96773295+0.25197806j]
39[-1.+0.j]
40[-0.87947375+0.47594739j]
41[-0.5+0.8660254j] 41 est un nombre premier.
42[-0.95105652-0.30901699j]
43[-0.5+0.8660254j] 43 est un nombre premier.
44[-0.97607588+0.21743018j]
45[-1.+0.j]
46[-0.9781476+0.20791169j]
47[-0.5+0.8660254j] 47 est un nombre premier.
48[-0.9172113+0.39840109j]
49[-0.5+0.8660254j]
```

Si l'on prend la seconde valeur propre, on trouve que pour les rangs correspondant aux nombres premiers, mais pas seulement pour ces rangs-là, la seconde valeur propre est le complexe $0.5 + \frac{\sqrt{3}}{2}\, i$,

correspondant à l'angle $\frac{\pi}{3}$ sur le cercle trigonométrique. On est "ennuyée" par le fait que pour les rangs 10, 25, 35 ou 49, la seconde valeur propre est aussi égale au complexe en question.

De ce fait, on décide de s'intéresser à une valeur propre "ultérieure", par exemple la $11^{\text{ième}}$ et là, surprise, les rangs qui sont des nombres premiers semblent être les seuls rangs pour lesquels la $11^{\text{ième}}$ valeur propre est égale à $e^{\frac{-2i\pi}{5}}$, mais en y regardant bien, 49 n'est pas discriminé des nombres premiers.

Le résultat du programme :

```
2[] 2 est un nombre premier.
3[] 3 est un nombre premier.
4[]
5[1.+0.j] 5 est un nombre premier.
6[1.+0.j]
7[0.30901699+0.95105652j] 7 est un nombre premier.
8[-0.80901699-0.58778525j]
9[-0.80901699-0.58778525j]
10[1.+0.j]
11[0.30901699+0.95105652j] 11 est un nombre premier.
12[0.41541501+0.909632j]
13[0.30901699+0.95105652j] 13 est un nombre premier.
14[0.88545603+0.46472317j]
15[0.6234898+0.78183148j]
16[0.66913061-0.74314483j]
17[0.30901699+0.95105652j] 17 est un nombre premier.
18[-0.80901699-0.58778525j]
19[0.30901699+0.95105652j] 19 est un nombre premier.
20[-0.87947375+0.47594739j]
21[-1.66533454e-16+1.j]
22[0.07473009-0.9972038j]
23[0.30901699+0.95105652j] 23 est un nombre premier.
24[-0.80901699+0.58778525j]
25[-0.96592583-0.25881905j]
26[-0.18738131-0.98228725j]
27[-0.35460489+0.93501624j]
28[-0.28680323-0.95798951j]
29[0.30901699+0.95105652j] 29 est un nombre premier.
30[1.+0.j]
31[0.30901699+0.95105652j] 31 est un nombre premier.
32[-0.44039415-0.89780454j]
33[-0.55557023+0.83146961j]
34[-0.5-0.8660254j]
35[-0.9829731-0.18374952j]
```

```
36[0.44573836-0.89516329j]
37[0.30901699+0.95105652j] 37 est un nombre premier.
38[-0.59463318-0.80399713j]
39[-0.67728157+0.73572391j]
40[0.24548549-0.96940027j]
41[0.30901699+0.95105652j] 41 est un nombre premier.
42[0.30901699+0.95105652j]
43[0.30901699+0.95105652j] 43 est un nombre premier.
44[-0.6940742-0.71990347j]
45[-0.75574957+0.65486073j]
46[-0.7193398-0.69465837j]
47[0.30901699+0.95105652j] 47 est un nombre premier.
48[-0.06824241-0.99766877j]
49[0.30901699+0.95105652j]
```

On constate que 10, 25, 35 ont été "discriminés" des nombres premiers en prenant une valeur propre d'indice plus élevé, mais 49 s'envoie toujours sur le même complexe (en l'occurrence $e^{\frac{2i\pi}{5}}$) que les nombres premiers. Alors, on prend la $22^{\text{ième}}$ valeur propre et enfin, le nombre 49 s'avère ne pas avoir la même image que les nombres premiers (pour eux, c'est le complexe correspondant à l'angle 77.14 degrés) ; le résultat du programme est :

```
2[] 2 est un nombre premier.
3[] 3 est un nombre premier.
4[]
5[] 5 est un nombre premier.
6[]
7[1.+0.j] 7 est un nombre premier.
8[1.+0.j]
9[-0.90096887-0.43388374j]
10[-0.90096887+0.43388374j]
11[-0.22252093+0.97492791j] 11 est un nombre premier.
12[-0.90096887-0.43388374j]
13[-0.22252093+0.97492791j] 13 est un nombre premier.
14[-0.5-0.8660254j]
15[-0.22252093+0.97492791j]
16[-0.90096887-0.43388374j]
17[-0.22252093+0.97492791j] 17 est un nombre premier.
18[-0.27366299-0.96182564j]
19[-0.22252093+0.97492791j] 19 est un nombre premier.
20[0.54694816-0.83716648j]
21[1.+0.j]
22[-0.90096887-0.43388374j]
23[-0.22252093+0.97492791j] 23 est un nombre premier.
```

```
24[0.41541501+0.909632j]
25[0.25881905+0.96592583j]
26[0.96858316-0.24868989j]
27[0.74851075-0.66312266j]
28[1.+0.j]
29[-0.22252093+0.97492791j] 29 est un nombre premier.
30[0.22252093-0.97492791j]
31[-0.22252093+0.97492791j] 31 est un nombre premier.
32[0.68896692+0.72479279j]
33[0.38268343-0.92387953j]
34[0.58005691+0.81457595j]
35[-0.27366299+0.96182564j]
36[-0.90096887+0.43388374j]
37[-0.22252093+0.97492791j] 37 est un nombre premier.
38[0.37285648+0.92788903j]
39[0.08257935-0.99658449j]
40[-0.90096887+0.43388374j]
41[-0.22252093+0.97492791j] 41 est un nombre premier.
42[-0.95105652-0.30901699j]
43[-0.22252093+0.97492791j] 43 est un nombre premier.
44[0.10937121+0.99400098j]
45[-0.14231484-0.98982144j]
46[0.0348995+0.99939083j]
47[-0.22252093+0.97492791j] 47 est un nombre premier.
48[0.8544194-0.51958395j]
49[-0.99144486-0.13052619j]
```

On n'a pas encore d'explication d'un tel phénomène mais il reste surprenant car on n'a au départ "mis aucune information" dans la matrice M : elle contient *toutes* les matrices circulantes jusqu'à un certain rang, un peu comme une factorielle contient tous les entiers jusqu'à l'un certain d'entre eux.

Ce qui est étonnant dans le fait que telle valeur propre (par exemple la $22^{\text{ième}}$), qui a permis de discriminer les nombres premiers des nombres composés inférieurs à 50, soit la même pour deux nombres premiers, par exemple prenons $p_1 = 11$ et $p_2 = 37$ (pour tous les nombres premiers en fait), c'est le fait qu'on pense avoir calculé deux choses différentes : dans un cas la $22^{\text{ième}}$ valeur propre de la $11^{\text{ième}}$ puissance d'une matrice de taille $\frac{11 \times 12}{2} - 1$ et dans l'autre cas, la $22^{\text{ième}}$ valeur propre de la $37^{\text{ième}}$ puissance d'une matrice de taille $\frac{37 \times 38}{2} - 1$; il faudrait dans un premier temps au moins comprendre cela, peut-être ce partage d'une valeur propre de même rang est-il dû au fait que la première matrice est sous-matrice haute gauche de la seconde. On n'a pas d'explication parce qu'on imagine que les racines des nouveaux facteurs intégrés au polynôme caractéristique (par exemple les racines de $(x^k - 1)$), au fur et à mesure de l'augmentation de la taille de la matrice, devraient s'intercaler entre les racines des polynômes caractéristiques des niveaux inférieurs (les racines des produits successifs de $x^{k'} - 1$ avec $k' < k$.

Explication : la trace de la matrice $\mathrm{Tr}(M^k)$ est égal à $\sigma(k)$, la somme des diviseurs de k diminuée de 1. En effet, par la cyclicité des sous-matrices, l'élévation à la puissance "ramène les 1 sur la diagonale" et l'opérateur trace, qui calcule la somme des éléments diagonaux de M^k, qui ici compte les 1 qui sont revenus sur la diagonale, en compte d pour un diviseur d de k dans la matrice M^k (*rappel* : la matrice M^k est de taille $\left(\frac{k(k+1)}{2}-1\right)\times\left(\frac{k(k+1)}{2}-1\right)$).

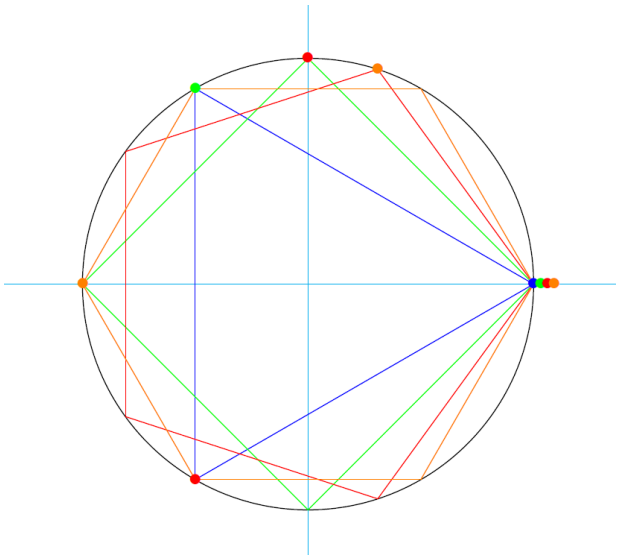
Le déterminant de cette même matrice est égal à -1 pour les nombres de la forme $4k+3$ et 1 pour les nombres de la forme $4k+1$, $4k$ et $4k+2$[2].

Voyons les valeurs propres ; écrivons les premières listes : on sépare par ci par là les valeurs propres par des ";" bleus au lieu d'utiliser les ",", pour bien séparer les groupes de 2, 3, 4, 5, etc. valeurs propres.

$2 \to [1, 1]$
$3 \to [1, -1 \ ; \ 1, 1, 1]$
$4 \to [-\frac{1}{2}+\frac{\sqrt{3}}{2}i \ ; \ -\frac{1}{2}-\frac{\sqrt{3}}{2}i \ ; \ 1, 1, 1 \ ; \ 1, 1, 1, 1]$
$5 \to [1, -1 \ ; \ -\frac{1}{2}+\frac{\sqrt{3}}{2}i, -\frac{1}{2}-\frac{\sqrt{3}}{2}i, 1 \ ; \ -1, i, -i, 1 \ ; \ 1, 1, 1, 1, 1]$
$6 \to [-0.80+0.587i, -0.80-0.587i \ ; \ 0.30+0.95i, 0.30-0.95i, 1 \ ; \ 1, -1, 1, -1 \ ; \ 1, 1, 1, 1, 1 \ ; \ 1, 1, 1, 1, 1, 1]$
$7 \to [1, -1 \ ; \ -\frac{1}{2}+\frac{\sqrt{3}}{2}i, -\frac{1}{2}-\frac{\sqrt{3}}{2}i, 1 \ ; \ -1, i, -i, 1 \ ; \ -0.80+0.587i, -0.80-0.587i,$
$0.30+0.95i, 0.30-0.95i, 1 \ ; \ -1, -\frac{1}{2}+\frac{\sqrt{3}}{2}i, -\frac{1}{2}-\frac{\sqrt{3}}{2}i, \frac{1}{2}+\frac{\sqrt{3}}{2}i, \frac{1}{2}-\frac{\sqrt{3}}{2}i], 1 \ ; \ 1, 1, 1, 1, 1, 1, 1]$

On voit que ce n'est que pour les nombres premiers que la liste des valeurs propres est la liste des racines $k^{\text{ièmes}}$ de l'unité dans l'ordre du plus petit polygone au plus grand en commençant par le polygone à 2 côtés (de sommets 1 et -1). C'est pour cette raison que la $22^{\text{ième}}$ valeur propre est toujours la même pour les nombres premiers et pas pour les nombres composés. Peut-être faut-il le démontrer, ou peut-être que c'est trivial.

Ci-dessous, le cercle unité sur lequel ont été positionnées les racines de l'unité des polygones réguliers ayant de 3 à 6 côtés.



[2] On rappelle que Gauss remplaçait les $4k+3$ par des -1 dans les Recherches arithmétiques, dans sa démonstration de la loi de réciprocité quadratique.

II. Un mémoire sur la théorie des matrices.

Arthur Cayley, Esq., F.R.S.

Reçu le 10 décembre 1857, lu le 14 janvier 1858.

Le terme matrice peut être utilisé dans un sens plus général, mais dans le présent mémoire, je considère seulement des tableaux carrés et rectangulaires, et le terme matrice, utilisé sans précision, doit être compris comme signifiant une matrice carrée ; dans ce sens restreint, un ensemble de quantités arrangées sous la forme d'un carré,

$$\begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}$$

est appelé une matrice. La notion d'une telle matrice surgit naturellement d'une notation abrégée pour un ensemble d'équations linéaires, par exemple les équations

$$\begin{aligned} X &= ax + by + cz, \\ Y &= a'x + b'y + c'z, \\ Z &= a''x + b''y + c''z, \end{aligned}$$

peuvent être plus simplement représentées par

$$(X, Y, Z) = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} (x, y, z)$$

et la considération d'un tel système d'équations amène à la plupart des notions fondamentales de la théorie des matrices. On verra que les matrices (en ne considérant seulement que celles du même ordre) se comportent comme des objets particuliers ; elles peuvent être ajoutées, multipliées ou composées ensemble, etc. : la loi de l'addition des matrices est précisément similaire à celle pour l'addition des quantités algébriques ordinaires ; en ce qui concerne leur multiplication, il y a une particularité telle que les matrices ne peuvent être échangées[1] ; il est néanmoins possible de former les puissances (positive ou négative, entière ou fractionnaire) d'une matrice, et par conséquent, de parvenir à appliquer une fonction rationnelle et entière, ou plus généralement n'importe quelle fonction algébrique d'une matrice. J'obtiens le théorème remarquable qu'une matrice quelconque satisfait une équation algébrique de son propre ordre, le coefficient de la plus grande puissance étant l'unité, et les autres puissances, des fonctions des termes de la matrice, le dernier coefficient étant en fait le déterminant sous forme condensée ; la règle de formation de cette équation peut être énoncée sous la forme condensée suivante, qui sera compréhensible après une lecture de ce mémoire, le déterminant, formée de la matrice diminuée de la matrice considérée comme une quantité unique[2] multipliée par la matrice unité, sera égal à zéro. Le théorème montre que toute fonction rationnelle

Philosophical Transactions of the Royal Society of London, 1858, Vol. 148 (1858), pp. 17-37.

Esq. F.R.S = Esquire Fellowship of the Royal Society ; trad. : a le titre de Membre de la Société royale.

[1] on dit maintenant "ne commutent pas".

[2] On les appelle maintenant scalaire.

et entière (ou en effet, toute fonction rationnelle) d'une matrice peut être considérée comme une fonction rationnelle et entière, dont le degré est au plus égal à celui de la matrice, diminué d'une unité ; cela montre même que dans un certain sens, on a la même chose par rapport à n'importe quelle fonction algébrique d'une matrice quelle qu'elle soit. Une des applications du théorème est de trouver une expression générale des matrices qui peuvent être échangées[3] avec une certaine matrice, et je ne suis pas entré dans ce domaine plus avant qu'en montrant comment certaines des notions applicables à celles-ci peuvent s'étendre aux matrices rectangulaires.

1. Pour la concision, les matrices écrites complètement seront en général d'ordre 3, mais on doit comprendre que les définitions, les raisonnements et les conclusions s'appliquent à n'importe quel degré. Et quand deux matrices ou plus sont dites en connexion l'une avec l'autre, cela implique toujours (à moins que le contraire ne soit explicitement écrit) que les matrices sont du même ordre.

2. Notation

$$\begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} (x, y, z)$$

représente l'ensemble des fonctions linéaires

$$((a, b, c \,\}\, x, y, z), (a', b', c' \,\}\, x, y, z), (a'', b'', c'' \,\}\, x, y, z)),$$

de telle façon qu'en appelant celles-ci (X, Y, Z), on a

$$(X, Y, Z) = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} (x, y, z)$$

et, comme remarqué au-dessus, cette formule amène à la plupart des notions fondamentales de la théorie.

3. Les quantités (X, Y, Z) seront identiquement nulles, si tous les termes de la matrice sont nulles, et on peut dire que

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

est la matrice nulle.

À nouveau, (X, Y, Z) sera égal à (x, y, z), si la matrice est

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

et on appelle cette dernière la matrice unité. On peut parler, bien sûr, quand il est nécessaire de distinguer, disons, de la matrice zéro, ou (suivant le cas) de la matrice unité *de tel ordre*. Les

[3] commuter

matrices nulles peuvent être représentées par 0 et la matrice unité par 1.

4. Les équations

$$(X,Y,Z) = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} (x,y,z), \qquad (X',Y',Z') = \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix} (x,y,z),$$

donnent

$$(X+X',Y+Y',Z+Z') = \begin{pmatrix} a+\alpha & b+\beta & c+\gamma \\ a'+\alpha' & b'+\beta' & c'+\gamma' \\ a''+\alpha'' & b''+\beta'' & c''+\gamma'' \end{pmatrix} (x,y,z)$$

et cela amène à

$$\begin{pmatrix} a+\alpha & b+\beta & c+\gamma \\ a'+\alpha' & b'+\beta' & c'+\gamma' \\ a''+\alpha'' & b''+\beta'' & c''+\gamma'' \end{pmatrix} = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} + \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix}$$

selon la règle d'addition des matrices ; pour la soustraction on procède de façon similaire.

5. Une matrice n'est pas modifiée par addition ou soustraction de la matrice nulle, c'est-à-dire qu'on a $M \pm 0 = M$.

L'équation $L = M$, qui exprime que les matrices L, M sont égales, peut aussi s'écrire sous la forme $L - M = 0$, i. e. la différence de deux matrices égales est la matrice nulle.

6. L'équation $L = -M$, écrite sous la forme $L + M = 0$, exprime que la somme de deux matrices L, M est égale à la matrice nulle, les matrices ainsi reliées sont dites être *opposées* l'une à l'autre ; en d'autres termes, une matrice dont les termes sont égaux ou opposés en signe aux termes d'une matrice donnée est appelée l'opposée de la matrice en question.

7. Il est clair qu'on a $L + M = M + L$, c'est-à-dire que l'opération d'addition est commutative, et de plus, que $(L + M) + N = L + (M + N) = L + M + N$, c'est-à-dire que l'opération d'addition est aussi associative.

8. L'équation

$$(X,Y,Z) = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} (mx,my,mz)$$

écrite sous la forme :

$$(X,Y,Z) = m \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} (x,y,z) = \begin{pmatrix} ma & mb & mc \\ ma' & mb' & mc' \\ ma'' & mb'' & mc'' \end{pmatrix} (x,y,z)$$

donne

$$m \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} = \begin{pmatrix} ma & mb & mc \\ ma' & mb' & mc' \\ ma'' & mb'' & mc'' \end{pmatrix}$$

comme règle de multiplication d'une matrice par une quantité unique[4]. Le scalaire m peut être écrit soit avant soit après la matrice, et l'opération est par conséquent commutative. On a clairement $m(L+M) = mL + mM$, ou que l'opération est distributive.

9. Les matrices L et mL peuvent être dites similaires l'une à l'autre ; en particulier, si $m = 1$, elles sont égales, et si $m = -1$, elles sont opposées.

10. On a, en particulier,

$$m \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} m & 0 & 0 \\ 0 & m & 0 \\ 0 & 0 & m \end{pmatrix}$$

ou bien en remplaçant la matrice du côté gauche par l'unité, on peut écrire

$$m = \begin{pmatrix} m & 0 & 0 \\ 0 & m & 0 \\ 0 & 0 & m \end{pmatrix}$$

La matrice du côté droit est dite scalaire m en la considérant comme *intervenant dans la matrice unité.*

11. Les équations

$$(X, Y, Z) = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} (x, y, z), \qquad (x, y, z) = \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix} (\xi, \eta, \zeta),$$

donnent

$$(X, Y, Z) = \begin{pmatrix} A & B & C \\ A' & B' & C' \\ A'' & B'' & C'' \end{pmatrix} (\xi, \eta, \zeta) = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix} (\xi, \eta, \zeta)$$

et par conséquent, en substituant à la matrice

$$\begin{pmatrix} A & B & C \\ A' & B' & C' \\ A'' & B'' & C'' \end{pmatrix}$$

sa valeur, on obtient

$$\begin{pmatrix} (a, b, c \,\}\, \alpha, \alpha', \alpha'') & (a, b, c \,\}\, \beta, \beta', \beta'') & (a, b, c \,\}\, \gamma, \gamma', \gamma'') \\ (a', b', c' \,\}\, \alpha, \alpha', \alpha'') & (a', b', c' \,\}\, \beta, \beta', \beta'') & (a', b', c' \,\}\, \gamma, \gamma', \gamma'') \\ (a'', b'', c'' \,\}\, \alpha, \alpha', \alpha'') & (a'', b'', c'' \,\}\, \beta, \beta', \beta'') & (a'', b'', c'' \,\}\, \gamma, \gamma', \gamma'') \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{pmatrix}$$

[4] un scalaire.

comme règle de multiplication ou composition de deux matrices. On doit observer que l'opération n'est pas commutative ; les facteurs matriciels que l'on compose peuvent être distingués comme le premier composant (ou davantage), et le second composant ou le composant matriciel le plus proche et la règle de composition est comme suit, par exemple n'importe quelle *ligne* de la matrice composée est obtenue en combinant les *lignes* de la première matrice ou des composantes matricielles suivantes successivement avec les *colonnes* de la seconde matrice ou de la matrice la plus proche.

12. Une matrice composée, soit comme première soit comme seconde matrice, avec la matrice nulle donne la matrice nulle. Le cas où l'un quelconque des termes de la matrice donnée est infini est bien sûr exclus.

13. Une matrice n'est pas altérée par sa composition, soit comme premier soit comme second composant avec la matrice unité. Elle est composée soit comme premier soit comme deuxième composant avec un scalaire m considéré comme une matrice unité dans laquelle tous les 1 serait remplacés par la quantité m : ceci est en fait la règle déjà mentionnée pour la multiplication d'une matrice par un scalaire, règle qui peut ainsi être vue comme un cas particulier de la multiplication de deux matrices.

14. On peut de la même manière multiplier ou composer ensemble trois matrices ou plus : l'ordre d'arrangement des facteurs est bien sûr accessoire et on peut les distinguer comme étant le premier ou le plus éloigné, le second, le troisième, etc., et le dernier ou le plus proche, et les remplacer par une matrice unique, et etc. jusqu'à ce que toutes les matrices aient été composées ensemble, le résultat étant indépendant de la manière dont la composition est effectuée ; c'est-à-dire qu'on a $L.MN = LM.N = LMN, LM.NP = L.MN.P$, etc. : l'opération de multiplication, bien qu'elle ne soit pas commutative, comme cela a déjà été noté, est un opération associative.

15. On arrive alors à la notion de puissance entière et positive L^p d'une matrice L, et on doit observer que les différentes puissances de la même matrice commutent. Il est clair également que p et q étant des entiers positifs, on a $L^p.L^q = L^{p+q}$, qui est le théorème des exposants pour les puissances entières positives d'une matrice.

16. La dernière équation mentionnée, $L^p.L^q = L^{p+q}$, supposée être vrai pour toutes les valeurs quels que soient les exposants p et q, amène à la notion de puissances d'une matrice pour n'importe quelle forme, quel que soit l'exposant. En particulier, $L^p.L^0 = L^p$ ou $L^0 = 1$, c'est-à-dire, la $0^{\text{ième}}$ puissance d'une matrice est la matrice unité. Et alors en posant $p = 1, q = -1$, ou $p = -1, q = 1$, on a $L.L^{-1} = L^{-1}.L = 1$; c'est-à-dire, L^{-1}, ou, comme on peut l'appeler, la matrice inverse ou réciproque, est une matrice qui, composée soit comme premier soit comme second composant avec la matrice originale, donne la matrice unité.

17. On peut arriver à la notion d'inverse ou de matrice réciproque, directement à partir de l'équation

$$(X, Y, Z) = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} (x, y, z)$$

en fait, l'équation donne

$$(x,y,z) = \begin{pmatrix} A & A' & A'' \\ B & B' & B'' \\ C & C' & C'' \end{pmatrix} (X,Y,Z) = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}^{-1} (X,Y,Z),$$

et on a, pour la détermination des coefficients de la matrice inverse ou réciproque les équations

$$\begin{pmatrix} A & A' & A'' \\ B & B' & B'' \\ C & C' & C'' \end{pmatrix} \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} \begin{pmatrix} A & A' & A'' \\ B & B' & B'' \\ C & C' & C'' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

qui sont équivalentes, et l'une ou l'autre d'entre elles est suffisante pour déterminer complètement la matrice inverse ou réciproque. Il est connu que si ∇ dénote le déterminant, c'est-à-dire si

$$\nabla = \begin{vmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{vmatrix}$$

alors les termes de la matrice inverse ou réciproque sont donnés par les équations :

$$A = \frac{1}{\nabla} \begin{vmatrix} 1 & 0 & 0 \\ 0 & b' & c \\ 0 & b'' & c'' \end{vmatrix}, \qquad B = \frac{1}{\nabla} \begin{vmatrix} 0 & 1 & 0 \\ a' & 0 & c' \\ a'' & 0 & c'' \end{vmatrix}, \text{etc.}$$

ou, ce qui est la même chose, la matrice inverse ou réciproque est donnée par l'équation

$$\begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}^{-1} = \frac{1}{\nabla} \begin{pmatrix} \partial_a \nabla & \partial_{a'} \nabla & \partial_{a''} \nabla \\ \partial_b \nabla & \partial_{b'} \nabla & \partial_{b''} \nabla \\ \partial_c \nabla & \partial_{c'} \nabla & \partial_{c''} \nabla \end{pmatrix}$$

où bien sûr les différentiations doivent dans tous les cas être réalisées comme si les termes a, b, etc. étaient tous des quantités arbitraires.

18. La formule montre, ce qui est clair en effet *a priori*, que les notions de matrice inverse ou réciproque échouent ensemble quand le déterminant s'évanouit : la matrice est dans ce cas dite indéterminée, et on doit comprendre qu'en l'absence de mention expresse, le cas particulier en question est fréquemment exclus des considérations. On doit ajouter que la matrice nulle est indéterminée ; et que le produit de deux matrices peut être nul, seulement si les matrices sont des matrices unités ou si les deux sont indéterminées.

19. La notion de matrice inverse ou de matrice réciproque une fois établie, les autres puissances négatives entières de la matrice originale sont des puissances entières positives de la matrice inverse ou réciproque, et la théorie à propos de telles puissances négatives entières peut être considérée

comme connue. La discussion ultérieure des puissances fractionnaires d'une matrice sera résumée par la suite.

20. La puissance entière positive L^m de la matrice L peut bien sûr être multipliée par n'importe quelle matrice de même degré ; un tel facteur cependant ne commute en général pas avec L ; et pour préserver autant que possible l'analogie avec l'algèbre ordinaire des fonctions algébriques, on peut restreindre l'attention au cas où le facteur est un scalaire, et une telle convertibilité existe par conséquent. On a de cette manière une matrice cL^m, et par addition de n'importe quel nombre de tels termes, on obtient une fonction rationnelle et entière de la matrice L.

21. Le théorème général auquel il a été fait référence précédemment sera mieux compris par un développement complet d'un cas particulier. Imaginons la matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

et formons le déterminant

$$\begin{vmatrix} a-M & b \\ c & d-M \end{vmatrix}.$$

L'expression développée de ce déterminant est

$$M^2 - (a+d)M^1 + (ad-bc)M^0 \ ;$$

les valeurs de M^2, M^1, M^0 sont

$$\begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{pmatrix}, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

et en substituant ces valeurs, le déterminant devient égal à la matrice nulle, on a notamment

$$\begin{aligned} \begin{vmatrix} a-M & b \\ c & d-M \end{vmatrix} &= \begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{pmatrix} - (a+d)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (ad-bc)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} (a^2+bc)-(a+d)a+(ad-bc) & b(a+d)-(a+d)b \\ c(a+d)-(a+d)c & d^2+bc-(a+d)d+ad-bc \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

c'est-à-dire

$$\begin{vmatrix} a-M & b \\ c & d-M \end{vmatrix} = 0$$

où la matrice du déterminant est

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} - M\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

c'est-à-dire que c'est la matrice originale, diminuée de la matrice unité dont les 1 sont remplacés par un même scalaire. Et ceci, c'est le théorème général, qui est que le déterminant, ayant pour matrice une matrice donnée moins la même matrice considérée comme une matrice unité dont les

1 sont remplacés par un scalaire est égal à zéro.

22. La représentation symbolique suivante du théorème vaut, je pense, la peine d'être notée : soit la matrice M, considérée comme un scalaire, représentée par $\widetilde{M}$, alors en dénotant la matrice identité par 1, $\widetilde{M}.1$ représentera la matrice M, considérée comme une matrice unité dont les 1 sont remplacés par un scalaire. Selon des principes de notation identiques, $\widetilde{1}.M$ représentera, ou peut être considérée comme représentant, simplement la matrice M, et le théorème est

$$\text{Det.}(\widetilde{1}.M - \widetilde{M}.1) = 0.$$

23. J'ai vérifié le théorème, dans le cas le plus simple, d'une matrice d'ordre 3, par exemple si M est une telle matrice, considérons

$$M = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

alors le déterminant s'évanouit, ou bien on a

$$\begin{vmatrix} a - M & b & c \\ d & e - M & f \\ g & h & i - M \end{vmatrix} = 0,$$

ou, en développant,

$$M^3 - (a + e + i)M^2 + (ei + ia + ae - fh - cg - bd)M - (aei + bfg + cdh - afh - bdi - ceg) = 0$$

mais je n'ai pas trouvé nécessaire d'entreprendre le travail de l'établissement d'une preuve formelle dans le cas général d'une matrice de n'importe quel degré.

24. Si l'on ne fait qu'énoncer la forme générale du résultat, on voit que toute matrice satisfait une équation algébrique de son propre ordre, ce qui est dans de nombreux cas la matière du théorème.

25. Il découle directement de cela que toute fonction rationnelle et entière, ou en effet toute fonction rationnelle d'une matrice peut être exprimée comme une fonction rationnelle et entière d'un ordre au plus égal à celui de la matrice, moins l'unité. Mais il est important de considérer à quel niveau ou dans quel sens un théorème semblable est vrai par rapport aux fonctions irrationnelles d'une matrice. Si on avait seulement l'équation satisfaite par la matrice elle-même, une telle extension[5] ne pourrait pas être faite ; mais on a, outre l'équation du même ordre satisfaite par la fonction irrationnelle de la matrice, et au moyen de ces deux équations, et de l'équation par laquelle la fonction irrationnelle de la matrice est déterminée, on peut exprimer la fonction irrationnelle comme une fonction rationnelle et entière de la matrice, d'un ordre égal au plus à celui de la matrice, moins une unité ; une telle expression fera pourtant intervenir *les coefficients de l'équation satisfaite par la fonction irrationnelle* qui sont des fonctions (en nombre égal à l'ordre de la matrice) des coefficients supposés inconnus, de la fonction irrationnelle elle-même. La transformation n'est jamais une transformation importante, comme celle de réduire le nombre de quantités inconnues de n^2 (si n est l'ordre de la matrice) à n. Pour compléter la solution, il est nécessaire de comparer la valeur

[5] aux fonctions irrationnelles

obtenue comme ci-dessus, avec la valeur supposée de la fonction irrationnelle, ce qui amènera à des équations pour la détermination des n quantités inconnues.

26. Comme illustration, considérons la matrice donnée

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

et cherchons à trouver la matrice $L = \sqrt{M}$. Dans ce cas, M satisfait l'équation

$$M^2 - (a+d)M + ad - bc = 0;$$

et de la même manière si

$$L = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

alors L satisfait l'équation

$$L^2 - (\alpha + \delta)L + \alpha\delta - \beta\gamma = 0\ ;$$

et à partir de ces deux équations, et de l'équation rationalisée $L^2 = M$, il devrait être possible d'exprimer L sous la forme d'une fonction linéaire de M : en fait, en substituant à L dans la dernière équation sa valeur ($= M$), on trouve directement

$$L = \frac{1}{\alpha + \delta}[M + (\alpha\delta - \beta\gamma)],$$

qui est l'expression requise, faisant intervenir comme il se doit les coefficients $\alpha + \delta, \alpha\delta - \beta\gamma$ de l'équation dans L. Il n'y a pas de difficulté à compléter la solution ; écrivons pour résumer $\alpha + \delta = X, \alpha\delta - \beta\gamma = Y$, alors on a

$$L = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \dfrac{a+Y}{X} & \dfrac{b}{X} \\ \dfrac{c}{X} & \dfrac{d+Y}{X} \end{pmatrix}$$

et par conséquent en formant les valeurs de $\alpha + \delta$ et $\alpha\delta - \beta\gamma$,

$$X = \frac{a + d + 2Y}{X},$$

$$Y = \frac{(a+Y)(d+Y) - bc}{X^2},$$

et en mettant également $a + d = P, ad - bc = Q$, on trouve sans difficulté

$$X = \sqrt{P} + 2\sqrt{Q},$$

$$Y = \sqrt{Q},$$

et les valeurs de $\alpha, \beta, \gamma, \delta$ sont par conséquent connues. Le signe de $\sqrt{Q}$ est le même dans les deux formulæ, et est par conséquent le même dans les quatre solutions, c'est-à-dire que la racine $\sqrt{M}$ a

quatre valeurs.

27. Pour illustrer cela plus avant, supposons qu'à la place de M, on ait la matrice

$$M^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} a^2 + bc & b(a+d) \\ c(a+d) & d^2 + bc \end{pmatrix},$$

de telle façon que $L^2 = M^2$, on trouve

$$P = (a+d)^2 - 2(ad - bc), Q = (ad - bc)^2,$$

et par conséquent $Q = \pm(ad - bc)$. En prenant le signe positif, on a

$$Y = ad - bc, X = \pm(a + d),$$

et ces valeurs donnent simplement

$$L = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm M,$$

Mais en prenant le signe négatif

$$Y = -ad + bc, X = \pm\sqrt{(a-d)^2 + 4bc},$$

et en retenant X pour dénoter cette racine, on trouve

$$L = \begin{pmatrix} \dfrac{a^2 - ad + 2bc}{X} & \dfrac{b(a+d)}{X} \\ \dfrac{c(a+d)}{X} & \dfrac{d^2 - ad + 2bc}{X} \end{pmatrix}$$

qui peut aussi s'écrire

$$L = \frac{a+d}{X} \begin{pmatrix} a & b \\ c & d \end{pmatrix} - \frac{2(ad-bc)}{X} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

ou, ce qui est la même chose

$$L = \frac{a+d}{X} M - \frac{2(ad-bc)}{X} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

et il est facile de vérifier *a posteriori* que cette valeur en fait donne $L^2 = M^2$. On peut remarquer que si

$$M^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^2 = 1$$

la formule mentionnée en dernier échoue, car on a $X = 0$; on verra présentement que l'équation $L' = 1$ admet d'autres solutions outre $L = \pm 1$. L'exemple montre comment les valeurs des puissances fractionnaires d'une matrice doivent être recherchées.

28. Il y a une difficulté apparente liée à l'équation satisfaite par une matrice, qu'il convient d'expliquer. Supposons, comme précédemment,

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

de telle façon que M satisfasse l'équation

$$\begin{vmatrix} a - M & b \\ c & d - M \end{vmatrix} = 0$$

ou

$$M^2 - (a + d)M + ad - bc = 0,$$

et dénotons par $X_{'}, X_{''}$, les quantités scalaires, racines de l'équation

$$\begin{vmatrix} a - X & b \\ c & d - X \end{vmatrix}$$

ou

$$X^2 - (a + d)X + ad - bc = 0.$$

L'équation satisfaite par la matrice peut être écrite

$$(M - X_{'} \between M - X_{''}) = 0,$$

dans laquelle $X_{'}, X_{''}$, doivent être considérées comme des matrices scalaires, et il pourrait sembler à première vue que l'on doive avoir l'un des facteurs simples égal à zéro, ce qui n'est pas le cas de manière évidente, car une telle égalité signifierait que le matrice parfaitement indéterminée M serait égale à une matrice scalaire. L'explication est que chacun des facteurs simples est une matrice indéterminée, en fait $M - X$, représente la matrice

$$\begin{pmatrix} a - X_{'} & b \\ c & d - X_{'} \end{pmatrix}$$

et le déterminant de cette matrice est égal à zéro. Le produit de deux facteurs est ainsi égal à zéro sans que l'un ou l'autre des facteurs ne soit nul.

29. Une matrice satisfait, nous l'avons vu, une équation de son propre ordre, faisant intervenir les coefficients de la matrice ; supposons que la matrice doive être déterminée pour satisfaire une certaine autre équation, dont les coefficients sont des quantités scalaires données. Il pourrait sembler à première vue que nous puissions éliminer la matrice entre les deux équations, et ainsi obtenir une équation qui serait la seule condition que les coefficients de la matrice devraient satisfaire ; ceci est trivialement faux, car plus de conditions doivent être nécessaires, et on voit que si nous devions alors procéder pour compléter la solution en trouvant la valeur de la matrice commune aux deux équations, nous devrions trouver que la matrice est égale dans tous les cas à une matrice scalaire, ce qui ne peut clairement pas être le cas. L'explication est similaire à celle de la difficulté dont on a dit de se méfier précédemment, les équations doivent contenir un, et un seul, facteur commun, et il est possible alors qu'elles soient satisfaites toutes les deux, et il est possible que le facteur commun ne s'évanouisse même pas. La condition nécessaire semble être que l'une des équations devraient être

un facteur de l'autre ; dans le cas où l'équation supposée est d'un ordre égal ou supérieur à celui de la matrice, alors si cette équation contient comme facteur l'équation qui est toujours satisfaite par la matrice, l'équation supposée sera satisfaite identiquement et la condition est suffisante aussi bien que nécessaire : dans l'autre cas, lorsque l'équation supposée est d'un ordre inférieur à celui de la matrice, la condition est nécessaire, mais elle n'est pas suffisante.

30. L'équation satisfaite par la matrice peut être de la forme $M^n = 1$; la matrice dans ce cas est dite périodique du $n^{\text{ième}}$ ordre. Les considérations précédentes s'appliquent à la théorie des matrices périodiques ; ainsi, par exemple, supposons qu'il soit nécessaire de trouver une matrice d'ordre 2, qui est périodique du second ordre. En écrivant

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

on a

$$M^2 - (a+d)M + ad - bc = 0$$

et l'équation supposée est

$$M^2 - 1 = 0.$$

Ces équations seront identiques si

$$a + d = 0, \qquad ad - bc = -1,$$

c'est-à-dire que, ces équations étant satisfaites, l'équation $M^2 - 1 = 0$ devant l'être, sera identique à l'équation qui est toujours satisfaite, et sera donc elle-même satisfaite. Et d'une façon semblable, la matrice M d'ordre 3 satisfera la condition $M^3 - 1 = 0$, ou sera périodique du troisième ordre, si seulement $M^3 - 1$ contient un facteur

$$M^2 - (a+d)M + ad - bc$$

et etc.

31. Mais supposons qu'on ait besoin de trouver une matrice d'ordre 3,

$$M = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

qui soit périodique du second ordre. En écrivant pour résumer

$$\begin{vmatrix} a - M & b & c \\ d & e - M & f \\ g & h & i - M \end{vmatrix} = -(M^3 - AM^2 + BM - C),$$

la matrice ici satisfait

$$M^3 - AM^2 + BM - C = 0$$

et, comme précédemment, l'équation supposée est $M^2 - 1 = 0$. Ici, si on a $1 + B = 0, A + C = 0$, le côté gauche contiendra le facteur $(M^2 - 1)$, et l'équation prendra la forme $(M^2 - 1)(M + C) = 0$,

et on devrait alors avoir $M^2 - 1 = 0$, en supposant que $M + C$ n'est pas une matrice indéterminée. Mais $M + C$ dénotant la matrice

$$\begin{pmatrix} a+C & b & c \\ d & e+C & f \\ g & h & i+C \end{pmatrix}$$

dont le déterminant est $C^3 + AC^2 + BC + C$, qui est égal à zéro en vertu des équations $1 + B = 0, A + C = 0$, on ne peut, par conséquent, à partir de l'équation $(M^2 - 1)(M + C) = 0$, déduire l'équation $M^2 - 1 = 0$. C'est comme ça devrait être, car les deux conditions ne sont pas suffisantes, en fait l'équation

$$M^2 = \begin{pmatrix} a^2 + bd + cg & ab + be + ch & ac + bf + ci \\ da + ed + fg & db + e^2 + fh & dc + ef + fi \\ ga + hd + ig & gb + he + ih & gc + hf + i^2 \end{pmatrix} = 1$$

donne neuf équations, qui sont pourtant satisfaites par les valeurs suivantes, dans lesquelles interviennent en réalité quatre coefficients arbitraires ; on peut dire que la matrice est égale à

$$k = \begin{pmatrix} \dfrac{\alpha}{\alpha+\beta+\gamma} & \dfrac{-(\beta+\gamma)\frac{\nu}{\mu}}{\alpha+\beta+\gamma} & \dfrac{-(\beta+\gamma)\frac{\nu}{\mu}}{\alpha+\beta+\gamma} \\ \dfrac{-(\gamma+\alpha)\mu\nu^{-1}}{\alpha+\beta+\gamma} & \dfrac{\beta}{\alpha+\beta+\gamma} & \dfrac{-(\gamma+\alpha)\frac{\lambda}{\mu}}{\alpha+\beta+\gamma} \\ \dfrac{-(\alpha+\beta)\mu\nu^{-1}}{\alpha+\beta+\gamma} & \dfrac{-(\alpha+\beta)\frac{\nu}{\lambda}}{\alpha+\beta+\gamma} & \dfrac{\gamma}{\alpha+\beta+\gamma} \end{pmatrix}$$

de telle façon qu'il y a en tout quatre relations (et pas seulement deux) entre les coefficients de la matrice.

32. Plutôt que l'équation $M^n - 1 = 0$, qui est celle d'une matrice périodique, il est plus pratique dans de nombreux cas, et c'est un peu la même chose, de considérer une équation $M^n - k = 0$, où k est un scalaire. La matrice peut dans ce cas être dite périodique à un facteur près.

33. Deux matrices L, M commutent quand $LM = ML$. Si la matrice M est donnée, cette égalité fournit un ensemble d'équations linéaires entre les coefficients de L de cardinal le nombre de coefficients, mais ces équations ne peuvent pas être toutes indépendantes, car il est clair que si L est une fonction rationnelle et entière quelconque de M (les coefficients étant des quantités uniques), alors L commutera avec M ; ou bien ce qui est apparemment (mais seulement apparemment) plus général, si L est n'importe quelle fonction algébrique de M (les coefficients étant toujours des quantités uniques), alors L commutera avec M. Mais quelle que soit la forme de la fonction, elle peut être réduite à une fonction rationnelle et entière d'un ordre égal à celui de M, diminué de 1, et on a ainsi l'expression générale pour les matrices commutant avec une matrice donnée, i.e. toute telle matrice est une fonction rationnelle et entière (les coefficients étant des quantités uniques) de la matrice donnée, l'ordre étant celui de la matrice donnée, diminué de 1. En particulier, la forme

générale de la matrice L qui commute avec une matrice donnée M d'ordre 2, est $L = \alpha M + \beta$, ou bien, ce qui est la même chose, les matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

commutent si $a' - d' : b' : c' = a - d : b : c$.

34. Deux matrices L, M anti-commutent quand $LM = -ML$; c'est une relation beaucoup moins importante que la commutativité ordinaire, car on doit remarquer qu'on ne peut en général trouver une matrice L qui anti-commute avec une matrice donnée M. En fait, en considérant M comme donnée, l'égalité fournit un ensemble d'équations linéaires entre les coefficients de L en nombre égal au nombre de coefficients ; et dans ce cas, les équations sont indépendantes, et on peut éliminer tous les coefficients de L, et on arrive ainsi à une relation qui doit être satisfaite par les coefficients de la matrice donnée M. Ainsi, supposons que les matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

anti-commutent, on a

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$
$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} aa' + b'c & a'b + b'd \\ c'a + d'c & c'b + d'd \end{pmatrix}$$

et les conditions d'anti-commutativité sont

$$\begin{aligned} 2aa' + bc' + b'c &= 0 \\ b'(a+d) + b(a'+d') &= 0 \\ c'(a+d) + c(a'+d') &= 0 \\ 2dd' + bc' + b'c &= 0 \end{aligned}$$

En éliminant a', b', c', d', la relation entre a, b, c, d est

$$\begin{vmatrix} 2a & c & b & . \\ b & a+d & . & b \\ c & . & a+d & c \\ . & c & b & 2d \end{vmatrix} = 0$$

qui est équivalente à

$$(a+d)^2(ad - bc) = 0$$

En excluant le cas $ad - bc = 0$, qui impliquerait que la matrice est indéterminée, on a $a + d = 0$. Le système de conditions résultant est

$$a + d = 0, \qquad a' + d' = 0, \qquad aa' + bc' + b'c + dd' = 0,$$

dont les deux premières équations impliquent que les matrices sont respectivement périodiques du second ordre à un facteur près.

35. On peut noter que si les matrices composées LM et ML sont similaires, elles sont soit égales soit opposées ; c'est-à-dire que les matrices L, M soit commutent soit anti-commutent.

36. Deux matrices telles que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

sont dites formées l'une à partir de l'autre par transposition, et on note ça par le symbole tr.[6] ; ainsi on peut écrire

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \text{tr.} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

L'effet de deux transpositions successives est bien sûr de ramener à la matrice originale.

37. Il est facile de voir que si M est une matrice quelconque, alors

$$(\text{tr. } M)^p = \text{tr.}(M^p),$$

et en particulier,

$$(\text{tr. } M)^{-1} = \text{tr.}(M^{-1}),$$

38. Si L, M sont deux matrices quelconques,

$$\text{tr.}(LM) = \text{tr.}M.\ \text{tr.}L,$$

et similairement pour trois matrices ou plus L, M, N, etc.,

$$\text{tr.}(LMN) = \text{tr.}N.\ \text{tr.}M.\ \text{tr.}L, \text{etc.}$$

40[7]. Une matrice telle que

$$\begin{pmatrix} a & h & g \\ h & b & f \\ g & f & c \end{pmatrix}$$

qui n'est pas modifiée par transposition, est dite symétrique.

41. Une matrice telle que

$$\begin{pmatrix} 0 & \nu & -\mu \\ -\nu & 0 & \lambda \\ \mu & -\lambda & 0 \end{pmatrix}$$

qui par transposition est changée en son opposée est dite antisymétrique.

42. Il est facile de voir qu'une matrice quelconque peut être exprimée comme la somme d'une matrice symétrique et d'une matrice antisymétrique ; par conséquent, la forme

$$\begin{pmatrix} a & h+\nu & g-\mu \\ g-\nu & b & f+\lambda \\ g+\mu & f-\lambda & c \end{pmatrix}$$

[6] Actuellement, la notation standard est plutôt M^{T} pour la transposée tandis que tr dénote la trace.

[7] *Remarque de la traductrice* : il n'y a pas d'article 39 dans l'article original.

qui peut évidemment représenter toute matrice quelle qu'elle soit d'ordre 3 est la somme des deux matrices mentionnées juste avant.

43. Les formules suivantes, bien qu'étant un peu plus que des exemples de la composition de matrices transposées peuvent être notées,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{pmatrix}$$

qui montre qu'une matrice composée à sa transposée donne une matrice symétrique. Il n'en découle pas cependant, et ce n'est pas un fait, qu'une matrice et sa transposée commutent. Et également

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a^3+bcd+a(b^2+c^2) & c^3+abd+c(a^2+d^2) \\ b^3+acd+b(a^2+d^2) & d^3+abc+d(b^2+c^2) \end{pmatrix}$$

qui est une forme remarquablement symétrique. Il n'est pas nécessaire d'aller plus loin, puisqu'il est clair que

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \left(\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right)^2$$

44. Dans tout ce qui précède, on a utilisé fréquemment des matrices d'ordre 2, mais essentiellement pour illustrer la théorie générale ; mais il vaut la peine de développer la théorie de telles matrices. Je rappelle les propriétés fondamentales qui ont été obtenues, par exemple, on a montré que la matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

satisfait l'équation

$$M^2 - (a+d)M + ad - bc = 0,$$

et que les deux matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

commuteront si

$$a' - d' : b' : c' = a - d : b : c$$

et qu'elles seront antisymétriques si

$$a + d = 0, \qquad a' + d' = 0, \qquad aa' + bc' + b'c + dd' = 0,$$

les deux premières de ces équations étant les conditions pour que les deux matrices soient respectivement périodiques du second ordre à un facteur près.

45. On peut noter en passant que si L, M sont des matrices antisymétriques d'ordre 2, et si ces matrices sont également telles que $L^2 = -1, M^2 = -1$, alors en utilisant le fait que $N = LM = -ML$, on obtient

$$L^2 = -1, \qquad M^2 = -1, \qquad N^2 = -1,$$
$$L = MN = -NM, \qquad M = NL = -LN, \qquad N = LM = -ML,$$

qui est un système de relations précisément similaire à celui de la théorie des quaternions.

46. Les puissances entières de la matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

sont obtenues avec une grande facilité à partir de l'équation quadratique ; ainsi on a, d'abord pour les puissances positives,

$$\begin{aligned} &M^2 = (a+d)M - (ad-bc), \\ &M^3 = [(a+d)^2 - (ad-bc)]M - (a+d)(ad-bc), \\ &\text{etc.,} \end{aligned}$$

par conséquent également, les conditions sur l'ordre que la matrice soit à un facteur près périodique d'ordres 2, 3, etc. sont

$$\begin{aligned} a+d &= 0, \\ (a+d)^2 - (ad-bc) &= 0, \\ &\text{etc. ;} \end{aligned}$$

et pour les puissances négatives, on a

$$(ad-bc)M^{-1} = -M + (a+d),$$

qui est équivalent à la forme ordinaire

$$(ad-bc)M^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

et les autres puissances négatives de M peuvent être obtenues par des multiplications successives par M^{-1}.

Un accent sépare reprouver de réprouver (Denise Vella-Chemla, fin mai 2023)

Ci-dessous la traduction de différentes notes, afférentes à la preuve topologique de Furstenberg de l'infinitude de l'ensemble des nombres premiers.

Sur l'infinitude de l'ensemble des nombres premiers

Harry Furstenberg, Université Yeshiva

Dans cette note, nous souhaiterions proposer une preuve "topologique" élémentaire de l'infinitude de l'ensemble des nombres premiers. On introduit une topologie dans l'espace des entiers S, en utilisant les progressions arithmétiques (de $-\infty$ à $+\infty$) comme base. Il n'est pas difficile de vérifier que cela en fait effectivement un espace topologique. En fait, dans cette topologie, on peut montrer que S est normal et même mesurable. Chaque progression arithmétique est aussi bien fermée qu'ouverte, puisque son complémentaire est l'union des autres progressions arithmétiques (de même raison). Il en résulte que n'importe quel nombre fini de progressions arithmétiques est fermé. Considérons l'ensemble $A = \bigcup A_p$, où A_p contient tous les multiples de p et où p couvre l'ensemble des nombres premiers ≥ 2. Les seuls nombres n'appartenant pas à A sont -1 et 1 et puisque l'ensemble $\{-1, 1\}$ n'est clairement pas un ensemble ouvert, A ne peut pas être fermé. Par conséquent A n'est pas une union finie d'ensembles fermés, ce qui prouve qu'il existe une infinité de nombres premiers.

Une preuve topologique du théorème d'Euclide[1]

Publié le 11 mai 2023

Théorème d'Euclide : Il y a une infinité de nombres premiers.

La preuve d'Euclide de ce résultat est classique. Elle est souvent décrite comme étant une preuve par contradiction mais, en fait, Euclide nous montre comment, étant donnée une liste de nombres premiers jusqu'à un certain nombre, l'on peut construire, à l'aide d'un processus fini, un nouveau nombre premier ; ainsi, la preuve est constructive.

Dans un récent article du magazine Quanta, Anna Kramer (2023) s'est intéressée à la raison qui pousse les mathématiciens à chercher de nouvelles preuves de résultats anciens dont on connaît la véracité. Un exemple qu'elle considère est le théorème d'Euclide sur l'infinitude de l'ensemble des nombres premiers. Des centaines de démonstrations de ce théorème ont été trouvées, la plus remarquable d'entre elles étant la preuve de 1955 de Hillel Furstenberg, qui utilise une topologie d'ensembles de points.

Contrairement à la preuve classique d'Euclide, la preuve de Furstenberg est une preuve par contradiction. Cette démonstration a été publiée en 1955, alors que Furstenberg étant encore un étudiant de premier cycle à l'Université Yeshiva de New York.

[1]Traduction d'un article du blog "That's maths", ici https://thatsmaths.com/2023/05/11/a-topological-proof-of-euclids-theorem/

La démonstration de Furstenberg

Furstenberg définit une topologie $\mathcal{O}$ sur les entiers $\mathbb{Z}$, la topologie des entiers régulièrement espacés, en utilisant comme base les séquences arithmétiques (doublement infinies)

$$S(a,b) = \{an + b | n \in \mathbb{Z}\} = a\mathbb{Z} + b.$$

Un sous-ensemble $U \subseteq \mathbb{Z}$ est ouvert si et seulement s'il est l'union de séquences arithmétiques $S(a,b)$ pour $a \neq 0$, ou si c'est l'ensemble vide. Il est clair que U est ouvert si et seulement si, pour tout $x \in U$, il existe un certain entier non nul a tel que $S(a,x) \subseteq U$.

On démontre facilement que $\mathcal{O}$ vérifie les axiomes d'une topologie :

- par définition, $\varnothing$ est ouvert. $\mathbb{Z}$ est égal à la séquence $S(1,0)$, et est donc ouvert ;
- toute union d'ensembles ouverts est ouverte : pour toute collection d'ensembles ouverts U_i, et x dans leur union U, quels que soient les nombres a_i pour lesquels $S(a_i,x) \subseteq U_i$, on a également $S(a_i,x) \subseteq U$;
- l'intersection de deux ensembles ouverts est ouverte : soient U_1 et U_2 des ensembles ouverts et $x \in U_1 \cap U_2$, avec les nombres a_1 et a_2 tels que $x \in S(a_1,x) \cap S(a_2,x)$. Soit a le plus petit commun multiple de a_1 et a_2. Alors $S(a,x) \subseteq S(a_i,x) \subseteq U_i$.

Deux propriétés-clés de la topologie $\mathcal{O}$ sont utilisées dans la démonstration :

1. Tout ensemble ouvert non vide contient une suite infinie ; par conséquent, aucun ensemble fini non vide n'est ouvert. Donc le complémentaire de n'importe quel ensemble vérifiant cela ne peut pas être fermé.
2. Les ensembles de base $S(a,b)$ sont à la fois ouverts et fermés. Ils sont ouverts par définition et on peut écrire
$$S(a,b) = \mathbb{Z} \setminus \bigcup_{n=1}^{a-1} S(a, b+n)$$
de telle façon que $S(a,b)$ est le complémentaire d'un ensemble ouvert.

Maintenant, Furstenberg observe que les seuls entiers qui ne sont pas multiples entiers de nombres premiers sont $+1$ et -1. Par conséquent,

$$\bigcup_{p \text{ premier}} S(p,0) = \mathbb{Z} \setminus \{-1, +1\}. \tag{1}$$

Maintenant, la première propriété ci-dessus - que le complémentaire d'un ensemble fini non vide ne peut être fermé - implique que l'ensemble $\mathbb{Z}\setminus\{-1,+1\}$ ne peut pas être fermé. Par la seconde propriété, les ensembles $S(p,0)$ sont fermés. Mais, s'il y avait seulement un nombre fini de tels nombres premiers, l'union finie $\bigcup_p S(p,0)$ des ensembles fermés serait aussi fermée. Donc (1) impliquerait l'égalité entre un ensemble fermé (sur la gauche) et un ensemble non fermé (sur la droite).

Cette contradiction nous oblige à aboutir à la conclusion qu'**il y a une infinité de nombres premiers.**

L'argument ci-dessus est essentiellement celui qui a été présenté par Furstenberg, et est similaire à la preuve donnée dans l'article de Wikipedia "la preuve de Furstenberg de l'infinitude de l'ensemble des nombres premiers."

Discussion

Mercer (2009) a donné une variation de la preuve de Furstenberg qui évite le langage topologique. Cela montre que les techniques essentielles utilisées dans la preuve sont arithmétiques, et ne nécessitent pas d'idées topologiques avancées. Pourtant, la preuve de Mercer n'a pas le côté direct de la preuve de Furstenberg (bien que ceci soit grandement une affaire de goût).

Furstenberg était encore au lycée quand sa preuve a été publiée. Elle n'a que douze lignes et est d'une grande élégance selon les mathématiciens. Bien sûr, on doit reconnaître que la preuve originale d'Euclide était également remarquable par son élégance, et était constructive, alors que la preuve topologique de Furstenberg est une preuve par contradiction.

Furstenberg a eu une carrière brillante, et il a apporté sa contribution à plusieurs disciplines. En 1955, il a reçu son diplôme du Lycée Yeshiva après avoir reçu une licence et une maîtrise. Il avait déjà publié un certain nombre d'articles avec sa *Note sur un type de forme indéterminée* (1953) et *Sur l'infinitude de l'ensemble des nombres premiers* (1955) apparues ensemble dans le mensuel American Mathematical Monthly.

Furstenberg a étudié à l'Université de Princeton pour sa thèse, supervisée par Salomon Bochner, et a reçu son doctorat en 1958. Cette thèse a été publiée en 1960 sous le titre *Processus stationnaires et théorie de la prédiction.* Furstenberg a travaillé à l'Institut de technologie du Massachusetts (MIT), et au département de mathématiques de l'Université du Minnesota, où il faisait partie du groupe travaillant en théorie des probabilités. En 1965, il fut recruté comme Professeur de mathématiques à l'Université hébraïque de Jérusalem. Furstenberg resta à l'Université hébraïque jusqu'à l'année de sa retraite en 2003.

Furstenberg reçut de nombreuses récompenses pour son travail mathématique : le prix Israël, une récompense de l'état d'Israël qui est la plus haute récompense reçue dans ce pays, en 1993 et, la même année, le prix Harvey, remis annuellement par Technion à Haifa, "pour ses travaux révolutionnaires en théorie ergodique et probabilités, groupes de Lie et dynamique topologique". En 2007, il a reçu le prix Wolf "pour ses profondes contributions à la théorie ergodique, aux probabilités, à la dynamique topologique, à l'analyse des espaces symétriques et des flots homogènes".

Références

1. Furstenberg, Harry Furstenberg, 1955, On the Infinitude of Primes. *Amer. Math. Monthly*, **62** (5), pg. 353 (1 page).
2. Golomb, Solomon W., 1959, A Connected Topology for the Integers *Amer. Math. Monthly*, 66 (8), pp. 663-665.

3. Anna Kramer, 2023, Why Mathematicians Re-Prove What They Already Know. Quanta Magazine.
4. Mercer, Idris D., 2009, On Furstenberg's Proof of the Infinitude of Primes. *Amer. Math. Monthly*, 116 (4), pp. 355-356.
5. Biographie MacTutor d'Hillel Furstenberg.
6. article Wikipedia : *Furstenberg's proof of the infinitude of primes.*

Traduction de l'article de Golomb en référence ci-dessus.

Une topologie connexe pour les nombres entiers

Solomon W. Golomb
Laboratoire de propulsion à réaction - Institut de technologie de Californie

On obtient une topologie D pour les entiers positifs quand les progressions arithmétiques $(an + b)$ avec $(a, b) = 1$ sont prises comme bases pour les ensembles ouverts. Elles forment une base parce que l'intersection de deux telles progressions est du même type, ou vide, comme on le vérifie aisément. Notons que tout ensemble ouvert non vide, étant l'union de progressions arithmétiques, doit être infini. Cette topologie fournit une preuve intéressante du

Théorème 1. Le nombre de nombres premiers est infini.

Preuve. Si p est un nombre premier, la progression $\{np\}$ est fermée, puisque son complémentaire est $\{np + 1\} \cup \{np + 2\} \cup ... \cup \{np + (p - 1)\}$, une union d'ensembles ouverts. Considérons l'union $X = \bigcup_p \{np\}$ étendue sur tous les nombres premiers. Si c'est une union finie d'ensembles fermés, alors X est fermée. Mais le complémentaire de X est $\{1\}$, qui n'est ni vide ni infini. Puisque le complémentaire de X n'est pas ouvert, X ne peut pas être fermé, l'union n'est pas une union finie, et le nombre de nombres premiers est infini.

(Une preuve similaire, dans une topologie plus forte et non connexe, a été donnée par Furstenberg [2].)

Théorème 2. La topologie D est de Hausdorff.

Preuve. Étant donnés deux entiers positifs distincts s et t, choisir un nombre premier p (par le théorème 1) qui est supérieur à $\max(s, t)$. Alors $\{pn + s\}$ et $\{pn + t\}$ sont des ensembles ouverts disjoints qui séparent s et t.

Théorème 3. La topologie D est connexe.

Preuve. Supposons que les entiers puissent être représentés comme l'union de deux ensembles disjoints non vides O_1 et O_2. Soit $\{a_1n + b_1\}$ un ensemble base dans O_1, et soit $\{a_2n + b_2\}$ un ensemble base dans O_2. Soit α un multiple de a_1. Si α était dans O_2, on aurait $\alpha = An_0 + B$, où $\{An + B\} \subset O_2$. Puisque $(A, B) = 1$, on devrait avoir $(\alpha, A) = 1$, et par conséquent $(a_1, A) = 1$. Mais alors $\{a_1n + b_1\}$ et $\{An + B\}$ devraient s'intersecter infiniment souvent, ce qui contredirait

la disjonction de O_1 et O_2. Donc tous les multiples de a_1 doivent appartenir à O_1. Similairement, les multiples de a_2 doivent appartenir à O_2. Mais alors les multiples communs de a_1 et a_2 doivent appartenir à la fois à O_1 et O_2, ce qui contredit la disjonction.

L'auteur a récemment appris qu'une preuve de la connexité de la topologie D, sans référence à la théorie des nombres a été présentée par Morton Brown au meeting d'avril 1953 de l'American Mathematical Society à New York [1].

THÉORÈME 4. La topologie D n'est pas régulière.

Preuve. Supposons que des recouvrements ouverts sont donnés pour l'ensemble fermé $\{2n\}$ et pour l'ensemble qui lui est extérieur $\{1\}$. Tout recouvrement ouvert de $\{1\}$ n'intersectant pas $\{2n\}$ doit inclure une progression $\{en+1\}$, où e est un nombre pair. C'est à dire, $e \in \{2n\}$. Soit $\{an+b\}$ l'élément du recouvrement ouvert $\{2n\}$ qui contient e, de telle façon que $e = an_0 + b$. Puisque $(a,b) = 1$, on a $(a,e) = 1$, où $\{an+b\}$ intersecte $\{en+1\}$ infiniment souvent. Donc l'ensemble $\{2n\}$ et le point $\{1\}$ ne peuvent avoir de voisinages disjoints ouverts.

THÉORÈME 5. La topologie D n'est pas compacte.

Preuve. L'union $\bigcup_p \{np-1\}$ étendue sur tous les nombres premiers est un recouvrement ouvert infini pour les entiers positifs. Puisque l'omission d'une quelconque progression $\{nq-1\}$ laisse le nombre $q-1$ non couvert, la propriété de Heine-Borel échoue.

En fait, la topologie D n'est même pas localement compacte, parce que tout espace de Hausdorff localement compact est régulier. Pour une preuve de cela, ainsi que des définitions les plus basiques de la topologie des ensembles de points, le lecteur est renvoyé à [5]. Le théorème de Dirichlet qui énonce que toute progression $\{an+b\}$ avec $(a,b) = 1$ contient une infinité de nombres premiers, a une formulation élégante en fonction de la topologie D.

THÉORÈME 6. Le théorème de Dirichlet est équivalent à l'assertion que les nombres premiers sont un sous-ensemble dense des entiers dans la topologie D.

Preuve. Supposons d'abord la validité du théorème de Dirichlet. Alors tout ensemble ouvert non vide contient des nombres premiers, de telle façon que les nombres premiers sont un sous-ensemble dense des nombres entiers. Inversement, supposons que les nombres premiers forment un sous-ensemble dense. Alors tout ensemble ouvert non vide, et en particulier toutes les progressions $\{an+b\}$ avec $(a,b) = 1$, doivent contenir des nombres premiers. Il est bien connu [4] que si toute telle progression contient au moins un nombre premier, alors toute telle progression contient une infinité de nombres premiers. (Dans la terminologie topologique : "si la fermeture de l'ensemble des nombres premiers, c'est l'ensemble des entiers, alors l'ensemble dérivé des nombres premiers est l'ensemble des entiers.").

Il semble peu probable qu'une preuve topologique complète du théorème de Dirichlet puisse être donnée selon ces lignes sans l'introduction de nouvelles idées et méthodes puissantes.

Un autre fait familier rendu possible par la formulation topologique est le

Théorème 7. Dans la topologie D, l'intérieur de l'ensemble des nombres premiers est vide.

Preuve. S'il y avait un ensemble ouvert constitué seulement complètement de nombres premiers, il y aurait une progression $\{an + b\}$ avec $1 \leq b \leq a$ constituée entièrement de nombres premiers. Mais avec $n_0 = a + b + 1$, $an_0 + b = (a + b)(a + 1)$, qui est composé.

Il est intéressant de considérer également la topologie D' pour les entiers positifs, qui a pour base ces progressions $\{an + b\}$ avec $(a, b) = 1$ pour tout $n > N$.

(Ici N peut prendre toutes les valeurs.) Cette topologie est clairement plus forte que D, bien que les théorèmes 1 à 7 soient encore valides dans D'. De plus, certains théorèmes reliés au crible d'Ératosthène sont valides dans D'. En particulier,

Théorème 8. L'ensemble des entiers positifs m tels que $6m-1$ et $6m+1$ est une paire de "nombres premiers jumeaux" est fermé dans D'.

Preuve. On sait [3] que les nombres m en question sont précisément ces nombres entiers positifs *non* exprimables sous la forme $6ab \pm a \pm b$ pour tout $a \geq 1$ et $b \geq 1$. Par conséquent le complémentaire de notre ensemble est $\bigcap_{b\geq 1}\{(6b \pm 1)a \pm b\}$, où chaque progression est restreinte aux $a \geq 1$, et est ouverte parce que $(6b \pm 1, b) = 1$. L'union est ouverte dans D', parce que c'est une union d'ensembles ouverts. Par conséquent, les entiers m pour lesquels $6m - 1$ et $6m + 1$ sont tous les deux des nombres premiers forment un ensemble fermé.

Références

1. M. Brown, A countable connected Hausdorff space, Bull. Amer. Math. Soc., vol. 59, 1953, p. 367.
2. H. Furstenberg, On the infinitude of primes, this MONTHLY, vol. 62, 1955, p. 353.
3. S. Golomb, Problem E 969, this MONTHLY vol. 58, 1951, p. 338.
4. R. Spira, Problem E 1218, this MONTHLY, vol. 63, 1956, p. 342.
5. J. L. Kelley, General Topology, New York, 1955.

Traduction de l'article de Mercer en référence plus haut.

Sur la preuve de Furstenberg de l'infinitude de l'ensemble des nombres premiers

Idris D. Mercer

Théorème. Il y a une infinité de nombres premiers.

La démonstration d'Euclide de ce théorème est un morceau classique des mathématiques. Et bien qu'une seule preuve suffise à établir la vérité du théorème, de nombreuses générations de mathématiciens se sont amusées à trouver des preuves alternatives. Voir, par exemple, [2], ou le

chapitre 1 soit de [1] soit de [4].

Il y a une preuve particulièrement surprenante, due à Furstenberg en 1955 [3], qui utilise, parmi toutes choses, le langage topologique ! Dans cette note, nous donnons une variante de la preuve de Furstenberg qui évite le langage topologique et par conséquent, selon l'opinion du présent auteur, exhibe mieux la "véritable raison" pour laquelle l'approche de Furstenberg marche.

DÉFINITION. Si m et r sont des entiers avec $m \geq 1$, on dénote par $r + m\mathbb{Z}$ l'ensemble des entiers congrus à r mod m, donc par exemple,

$$2 + 7\mathbb{Z} = 9 + 7\mathbb{Z} = -5 + 7\mathbb{Z} = \{\ldots, -12, -5, 2, 9, 16, \ldots\}.$$

On appelle un tel ensemble une progression arithmétique, ou PA en abrégé.

Notation. Pour $m \geq 2$, l'ensemble des entiers non divisibles par m est

$$(1 + m\mathbb{Z}) \cup \ldots \cup ((m-1) + m\mathbb{Z}).$$

qu'on abrège en $\mathrm{NM}(m)$ (les initiales de "non multiples" de m).

ASSERTION 1. *Une intersection finie de* PA *est soit vide soit infinie.*

Preuve. Si x appartient à $r_i + m_i\mathbb{Z}$ pour $1 \leq i \leq k$, alors il en est de même de $x + y$ où y est n'importe quel multiple commun des m_i.

ASSERTION 2. *Si $\mathcal{S}$ est une collection quelconque d'ensembles, alors une intersection finie d'unions finies d'ensembles dans $\mathcal{S}$ est également une union d'intersections finies d'ensembles dans $\mathcal{S}$.*

Preuve. Ceci énonce juste le fait que l'intersection se distribue sur l'union. Par exemple, on a

$$\begin{aligned}(R) \cap (U \cup V) \cap (W \cup X) \quad &= (R \cap U \cap W) \cup (R \cap U \cap X) \\ &\cup (R \cap V \cap W) \cup (R \cap V \cap X) \\ &\cup (S \cap U \cap W) \cup (S \cap U \cap X) \\ &\cup (S \cap V \cap W) \cup (S \cap V \cap X) \\ &\cup (T \cap U \cap W) \cup (T \cap U \cap X) \\ &\cup (T \cap V \cap W) \cup (T \cap V \cap X)\end{aligned}$$

□

Preuve du théorème. Si $p_1, \ldots, p_k$ étaient tous des nombres premiers, on aurait

$$\{-1, +1\} = \mathrm{NM}(p_1) \cap \mathrm{NM}(p_2) \cap \ldots \cap \mathrm{NM}(p_k),$$

qui est une intersection finie d'unions finies de PA et par conséquent, par l'assertion 2, une union finie d'intersections finies de PA, qui par l'assertion 1 doit être soit vide soit infinie. Ceci est une contradiction. □

Références

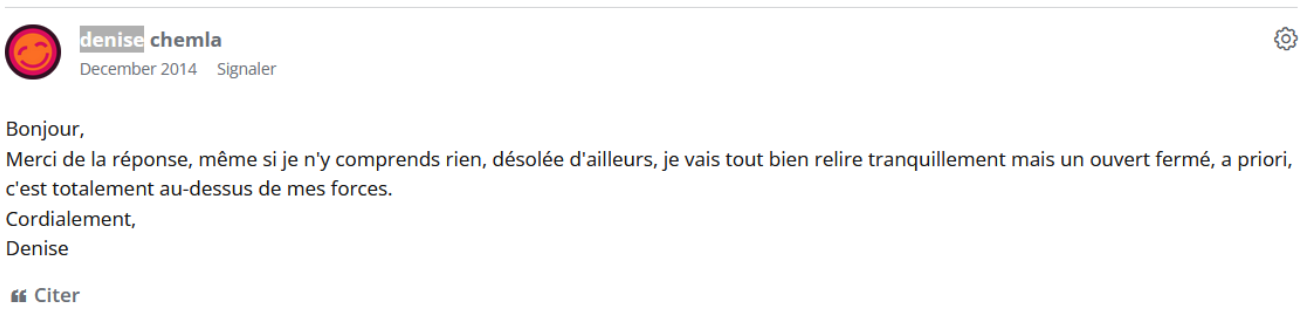
1. M. Aigner and G. M. Ziegler, Proofs from The Book, Springer-Verlag, New York, 1998.
2. C. K. Caldwell, Proofs that there are infinitely many primes (2007), available at http://primes.utmedu/notes/proofs/infinite.
3. H. Furstenberg, On the infinitude of primes, this MONTHLY 62 (1955) 353.
4. P. Ribenboim, The New Book of Prime Number Records, 3rd ed., Springer-Verlag, New York, 1996.

181 Wychwood Avenue, Toronto, ON, Canada M6C 2T4 idmercer@yorku.ca

---

Posté sur le forum les-mathematiques.net ici :

https://les-mathematiques.net/vanilla/index.php?p=/discussion/991521/absurde-et-tiers-exclu/p1



denise chemla
December 2014 Signaler

Bonjour,
Merci de la réponse, même si je n'y comprends rien, désolée d'ailleurs, je vais tout bien relire tranquillement mais un ouvert fermé, a priori, c'est totalement au-dessus de mes forces.
Cordialement,
Denise

❝ Citer

Décomposants de Goldbach et preuve par 9 (Denise Vella-Chemla, 8.5.2023)

En se remémorant de vieux souvenirs d'enfance, on cherche par programme si les nombres pairs, à partir de 56, ont toujours un décomposant de Goldbach qui vérifierait, ainsi que son complémentaire à n, un nombre pair considéré, certaines propriétés quant à la somme de ses chiffres.

On peut se reporter à cette transcription en LaTeX d'un extrait d'encyclopédie datant de 1856 pour se rappeler ce qu'est la preuve par 9 http://denise.vella.chemla.free.fr/transc-Montferrier-preuve-par-9.pdf.

On note $sc_9(x)$ la somme des chiffres de x. Le fait qui nous intéresse ici est que $sc_9(x+y) = sc_9(x) + sc_9(y)$.

La preuve par 9 "écrase" les nombres : deux nombres qui ont les mêmes chiffres[1] mais pas dans le même ordre, ont la même somme des chiffres. De même d'un nombre et d'un autre dans lequel on intercalerait des 9 par ci par là entre ses chiffres (comme 1234 et 1992394), etc.

Par programme jusqu'à 10^6, on trouve pour tous les :

- $18x+2$ (exemples : 56, 74) un décomposant de Goldbach et son complémentaire, tous les deux de somme des chiffres 1, i.e. deux nombres de la forme $18k+1$ (exemples : 19, 37) ; on a notamment la décomposition $56 = 19 + 37$;
- $18x+4$ (exemples : 58, 76) un décomposant de Goldbach et son complémentaire, tous les deux de somme des chiffres 2, i.e. deux nombres de la forme $18k+11$ (exemples : 11, 29) ; on a notamment la décomposition $58 = 11 + 47$) ;
- $18x+8$ (exemples : 62, 80) un décomposant de Goldbach et son complémentaire, tous les deux de somme des chiffres 4, i.e. deux nombres de la forme $18k+13$ (exemples : 13, 31) ; on a notamment la décomposition $80 = 13 + 67$) ;
- $18x+10$ (exemples : 64, 82) un décomposant de Goldbach et son complémentaire, tous les deux de somme des chiffres 5, i.e. deux nombres de la forme $18k+5$ (exemples : 5, 23) ; on a notamment la décomposition $64 = 5 + 59$) ;
- $18x+14$ (exemples : 68, 86) un décomposant de Goldbach et son complémentaire, tous les deux de somme des chiffres 7, i.e. deux nombres de la forme $18k+7$ (exemples : 7, 43) ; on a notamment la décomposition $68 = 7 + 61$) ;
- $18x+16$ (exemples : 70, 88) un décomposant de Goldbach et son complémentaire, tous les deux de somme des chiffres 8, i.e. deux nombres de la forme $18k+17$ (exemples : 17, 53) ; on a notamment la décomposition $70 = 17 + 53$) ;

Il faut avoir à l'esprit qu'après tout, c'est assez ridicule de s'intéresser aux décompositions faisant intervenir deux nombres de même somme de chiffres, cette coïncidence de la somme ayant lieu parce qu'on utilise un système décimal de numération et parce que dans ce système, on fait des paquets

[1] Les chiffres sont aux nombres ce que les lettres sont aux mots.

de 10, 10 se trouvant être congru à l'unité modulo 9, mais dans un autre système de numération, il en serait autrement.

Les résultats du programme jusqu'à 10^6 (15 méga) sont à trouver ici :
http://denise.vella.chemla.free.fr/sommechif1M.txt[2].

Il semblerait qu'on ne trouve jamais de décompositions de Goldbach (à partir de 56) vérifiant les contraintes qu'on souhaite pour les nombres pairs multiples de 3. Pour eux on cherchera, peut-être, les décompositions de la forme $n = p + q$ avec $sc_9(p) = 1$ ou $sc_9(q) = 1$.

On a ainsi une espèce de périodicité qui fait retrouver la même sorte de décomposants de Goldbach tous les 9 nombres pairs. Cette périodicité permet de chercher les décomposants de Goldbach dans des progressions arithmétiques et il faudrait vraisemblablement utiliser les résultats au sujet du plus petit nombre premier appartenant à une progression arithmétique. On note pour mémoire les résultats démontrés fournis par la littérature dans la section suivante.

Plus petit nombre premier dans une progression arithmétique

(*On traduit un extrait d'un article de Heath-Brown ici*) : Le théorème classique de Dirichlet énonce que toute progression arithmétique $a \pmod q$ avec $(a, q) = 1$ ((a, q) est la notation habituelle pour le plus grand commun diviseur de a et q, on dit également, si $(a, q) = 1$ que a et q sont premiers entre eux) contient une infinité de nombres premiers (*Pour les progressions qui nous intéressent (dans lesquelles on cherche les décomposants de Goldbach), on a* $\varphi(18) = 6$ *et les nombres 1, 5, 7, 11, 13 et 17 dans les progressions* $18k + 1, 18k + 5, 18k + 7, 18k + 11, 18k + 13, 18k + 17$ *sont premiers à 18, bien sûr (sinon, elles ne permettraient pas de trouver des nombres premiers).*)

Il est alors naturel de se demander quel est le premier (i.e. le plus petit) d'entre eux, notons le $P(a, q)$?

En ce qui concerne les majorations, le résultat le plus important est celui de Yu. V. Linnik[3] qui a démontré que

$$P(a, q) \ll q^L \qquad \text{pour une certaine constante absolue } L$$

R. Heath-Brown[4] démontre (théorème 6, p. 5) qu'on peut prendre $L = 5.5$.

[2]jusqu'à 10 millions, le fichier de 150 méga est là :
http://denise.vella.chemla.free.fr/sommechif10M.txt.

[3]Yu. V. Linnik, *On the least prime in an arithmetic progression I. The basic theorem*, Rec. Math. (Mat. Sbornik), N. S., 15 (57), 1944, 139-178, et Yu. V. Linnik, *On the least prime in an arithmetic progression II. The Deuring-Heilbronn phenomenon*, Rec. Math. (Mat. Sbornik), N. S., 15 (57), 1944, 347-368

[4]Roger Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, 1992, Proc. London Math. Soc., vol. 64, n° 3, p. 265-338.

Annexe à la proposition denitac.pdf (Denise Vella-Chemla, 23.7.2019)

On cherche à décomposer un nombre pair n en somme de 2 nombres premiers $p_1 + p_2$.

On ne peut pas faire référence à $\zeta(-1)$ comme on l'a fait dans [1]. On peut cependant, pour obtenir une minoration du nombre de décomposants de Goldbach de n, utiliser le cardinal $\left|\mathcal{P}_{\frac{n}{2}}\right|$ de l'ensemble des nombres premiers inférieurs ou égaux à $\frac{n}{2}$ et le multiplier par le produit $\prod_{p\leq\sqrt{n}}\left(1-\frac{1}{p}\right)$ qui compte combien de chances a le nombre premier p_1 de ne pas partager son reste avec n selon chaque module p inférieur à $\sqrt{n}$ (le fait de ne pas partager son reste avec n permet à p_1 d'avoir un complémentaire à n (appelé p_2) qui est premier également).

La minoration[1] de $\pi(x)$ (le nombre de nombres premiers inférieurs à x) par $\frac{x}{\log x}$ est fournie dans [2], page 69, pour $x \geq 17$ (Corollaire 1, (3.5), du Théorème 2, dont la démonstration est fournie au paragraphe 7 de [2]).

On a en conséquence $|\mathcal{P}_{\frac{n}{2}}| > \frac{\frac{n}{2}}{\log\left(\frac{n}{2}\right)}$.

La minoration de $\prod_{p\leq\sqrt{n}}\left(1-\frac{1}{p}\right)$ est également fournie dans [2], page 70 (c'est le corollaire (3.27) du Théorème 7 dont la démonstration est fournie au paragraphe 8 de [2], avec γ la constante d'Euler-Mascheroni).

$$(3.27) \qquad \frac{e^{-\gamma}}{\log x}\left(1-\frac{1}{\log^2 x}\right) < \prod_{p\leq x}\left(1-\frac{1}{p}\right) \quad \text{pour } 1 < x.$$

En multipliant ces expressions ensemble, on obtient que le nombre de décomposants de Goldbach de n doit être supérieur à :

$$\frac{n/2}{\log(n/2)}\frac{e^{-\gamma}}{\log\sqrt{n}}\left(1-\frac{1}{\log^2\sqrt{n}}\right)$$

qui est strictement supérieur à 1 à partir de 24.

Bibliographie

[1] http://denisevellachemla.eu/denitac.pdf.

[2] J. B. Rosser et L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, dedicated to Hans Rademacher for his seventieth birthday, Illinois J. Math., Volume 6, Issue 1 (1962), 64-94.

1. Cette minoration est à distinguer du Théorème des nombres premiers, prouvé indépendamment par Hadamard et La Vallée-Poussin, et qui fournit une tendance asymptotique pour $\pi(x)$.

Deux par classe (Denise Vella-Chemla, juillet 2022).

1. Caractérisation des décomposants de Goldbach de n supérieurs à $\sqrt{n}$[1]

Soit $n \in 2\mathbb{N}+6$ un entier pair supérieur à 6.

Pour tout $p \in \mathbb{P}^*$ premier impair inférieur à $\sqrt{n}$ (*i.e.* $3 \leq p \leq \sqrt{n}$), on définit l'ensemble :

$$F_n(p) = \{m \in 2\mathbb{N}+1 : 3 \leq m \leq n/2,\ m \not\equiv 0\ [p],\ m \not\equiv n\ [p]\}$$

L'intersection des ensembles $F_n(p)$ pour tout p premier compris entre 3 et $\sqrt{n}$ est notée :

$$D_n = \bigcap_{\substack{p\in\mathbb{P} \\ 3\leq p\leq\sqrt{n}}} F_n(p)$$

Nous allons montrer que D_n et son complémentaire $n-D_n$ ne contiennent que des nombres premiers.
Lemme 1 : Soit $m \in 2\mathbb{N}+1$ un entier impair. Si m n'est divisible par aucun nombre premier compris entre 3 et $\sqrt{m}$, alors il est premier.

Démonstration : Si m est composé, on a $m = pq$, où p est le plus petit nombre premier intervenant dans la factorisation de m en nombres premiers et où q est le produit de tous les autres facteurs. Puisque m est impair, $p \geq 3$, et puisque $q \geq p$ (q étant le produit d'entiers $\geq p$), $m = pq \geq pp = p^2$ et donc $\sqrt{m} \geq p$ (la fonction racine carrée étant croissante). On a ainsi montré que si m impair est composé, il est divisible par un premier compris entre 3 et $\sqrt{m}$. Le lemme s'obtient par contraposition. □

Lemme 2 : $D_n \subseteq \mathbb{P}$

Démonstration : Soit $m \in D_n$. Alors $m \in F_n(p)$ pour tout p premier compris entre 3 et $\sqrt{n}$. Par conséquent, m est impair et m n'est divisible par aucun nombre premier p compris entre 3 et $\sqrt{n}$ (puisque $m \not\equiv 0\ [p]$), et donc *a fortiori* par aucun premier compris entre 3 et $\sqrt{m}$ (car $m \leq n/2 \implies m \leq n \implies \sqrt{m} \leq \sqrt{n}$). D'après le lemme 1, m est donc premier. □

Lemme 3 : $n - D_n \subseteq \mathbb{P}$

Démonstration : Soit $m \in D_n$. Alors $m \in F_n(p)$ pour tout p premier compris entre 3 et $\sqrt{n}$. Par conséquent, $n-m$ est impair (car m est impair et n pair) et $n-m$ n'est divisible par aucun nombre premier p compris entre 3 et $\sqrt{n}$ (puisque $m \not\equiv n\ [p]$), et donc *a fortiori* par aucun premier compris entre 3 et $\sqrt{n-m}$ (car $n - m \leq n \implies \sqrt{n-m} \leq \sqrt{n}$). D'après le lemme 1, $n-m$ est donc premier. □

Les ensembles D_n ne contiennent que des décomposants de Goldbach de n.

[1] Leila Schneps a démontré que la caractérisation de certains décomposants de Goldbach que je proposais était justifiée.

Lemme 4 : Soit $n \in 2\mathbb{N}+6$. Si $D_n \neq \varnothing$, alors n vérifie la conjecture de Goldbach.

Démonstration : Si $D_n \neq \varnothing$, il contient un entier p nécessairement premier (d'après le lemme 1), tel que $q = n-p$ est également premier (d'après le lemme 2), et donc $n = p+q$ vérifie la conjecture de Goldbach.

2. Minoration du nombre de décomposants de Goldbach

La caractérisation de la Section 1 suggère que $\frac{n}{2}\prod_{2<p\leqslant n}\left(1-\frac{2}{p}\right)$ doit minorer le nombre de décomposants de Goldbach d'un nombre pair : les "pires" des cas (ou cas "très criblants") adviennent lorsque le nombre pair est de la forme $2^k p$ avec p un nombre premier, car alors on élimine deux classes de congruences selon tout module premier inférieur à $\sqrt{n}$, et les cas "moins criblants" adviennent lorsque le nombre pair considéré a de nombreux diviseurs (comme le nombre 60 par exemple) car alors on ne doit éliminer qu'une seule classe de congruence au lieu de 2 selon chaque module premier divisant n.

On peut utiliser la formule 2.6 de [1] qui fournit l'estimation :

"(2.6)
$$\prod_{\alpha<p\leq x}\left(1-\frac{\alpha}{p}\right) = \exp\left\{\sum_{\alpha<p\leq x}\log\left(1-\frac{\alpha}{p}\right)\right\} \cong \exp\left\{c_1(\alpha)-\alpha\sum_{p\leq x}\frac{1}{p}\right\} \cong \frac{c(\alpha)}{(\log x)^\alpha},$$

où α est une constante réelle, habituellement prise comme étant égale à 1."

Il est expliqué dans le paragraphe suivant de l'article de Rosser et Schoenfeld qu'il est possible d'utiliser les constantes $c(\alpha)$ et $c_1(\alpha)$ parce que l'erreur absolue tend vers 0 lorsque x tend vers l'infini.

Pour avoir une idée de la constante $c(2)$, il est possible[2] de démontrer que

$$\left(\prod_{2<p\leqslant n} 1-\frac{2}{p}\right)^{-1} = \frac{1}{4}e^{2\gamma}\Pi_2^{-1}\log^2 n + O(e^{-c\sqrt{\log n}})$$

avec $e = 2.71828, \gamma = 0.5772156649, \Pi_2 = 0.6601618158$[3].

On choisit de minorer le nombre de décomposants de Goldbach de n en utilisant la minoration

$$\#\{3 \leq dg \leq n/2 \mid n = dg + (n-dg) \text{ avec } dg \text{ et } n-dg \text{ premiers}\} \geq \frac{n}{2}\frac{4\Pi_2}{e^{2\gamma}}\frac{1}{\log^2 n}$$

[2]Se reporter à https://math.stackexchange.com/questions/22411/computing-the-product-of-p-p-2-over-the-odd-primes?rq=1.

[3]Voir https://mathworld.wolfram.com/TwinPrimesConstant.html).

3. Résultats numériques.

On utilise le programme suivant :

```
import math

def prime(atester):
  k = 2 ;
  if (atester in [0,1]): return False ;
  if (atester in [2,3,5,7]): return True ;
  while (True):
    if ((k * k) > atester): return True
    else:
      if ((atester % k) == 0): return False
      else: k=k+1

for n in range(6,100002,2):
  moitie = int(n/2)
  #if prime(moitie):
  if True:
    print('')
    print(n)
    nbdg = 0
    for p in range(3, moitie+1,2):
      if prime(p) and prime(n-p):
        nbdg += 1
    print('nbdg ', nbdg)
    estimproddespmoinsdeuxsurp = 0.8324290656/(math.log(n)**2)
    print('produit des p moins 2 sur p',estimproddespmoinsdeuxsurp)
    res = n*estimproddespmoinsdeuxsurp/2
    print(' que multiplie n/2 ', res)
    if res < nbdg:
      print('min reussi')
    else:
      print('min rate')
```

FIGURE 1 : Programme de minoration du nombre de décomposants de Goldbach d'un nombre pair.

pour vérifier que la minoration est effective pour tout n un nombre pair compris entre 6 et 10^5.

Le résultat de ce programme est consultable à l'adresse http://denise.vella.chemla.free.fr/respgm-prod-un-moins-deux-sur-p.pdf.

Référence

[1] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math., 6 (1962) 64-94.

Probabilité d'obtenir une décomposition de Goldbach d'un nombre pair (Denise Vella-Chemla, août 2022)

1. Un exemple illustratif

Prenons l'exemple de la recherche des décomposants de Goldbach de l'entier pair $n = 98$.

$$S_{98} = \begin{cases} 98 \equiv 0 \pmod 2 \\ 98 \equiv 2 \pmod 3 \\ 98 \equiv 3 \pmod 5 \\ 98 \equiv 0 \pmod 7 \end{cases}$$

Appelons d_{98} un décomposant de Goldbach potentiel de $n = 98$. d_{98} peut être congru, hormis 0, à tout ce à quoi $n = 98$ n'est pas congru. Le signe $\vee$ dans le système ci-dessous est à lire comme un ou exclusif, son emploi étendu est à comprendre comme le fait de vérifier autant de systèmes de congruences que la combinatoire le permet.

$$S_{d_{98}} = \begin{cases} d_{98} \equiv 1 \pmod 2 \\ d_{98} \equiv 1 \pmod 3 \\ d_{98} \equiv 1 \vee 2 \vee 4 \pmod 5 \\ d_{98} \equiv 1 \vee 2 \vee 3 \vee 4 \vee 5 \vee 6 \pmod 7 \end{cases}$$

Remarque : on note que le fait de respecter le système de systèmes de congruences ci-dessus est une condition suffisante mais non nécessaire pour obtenir un décomposant de Goldbach de n. La démonstration de la validité de cette caractérisation des décomposants de Goldbach d'un nombre pair n qui sont supérieurs à la racine carrée de n est fournie en section 2.

Comme on le comprend aisément, les modules qui ne divisent pas n "éliminent davantage de classes de congruences" (au nombre de 2 par module premier inférieur à $\sqrt{n}$) que les modules qui divisent n. Plaçons-nous dans le pire des cas, où l'on élimine deux classes de congruences par module premier inférieur à $\sqrt{n}$, on trouve tout de même

$$\prod_{\substack{p \text{ premier} \\ 3 \leq p \leq \sqrt{n}}} (p-2)$$

classes de congruences *différentes* par l'application du théorème des restes chinois à chacun des systèmes de congruences combinatoirement trouvé (voir $S_{d_{98}}$ ci-dessus). Ces solutions sont inférieures à $D = \prod_{\substack{p \text{ premier} \\ 3 \leq p \leq \sqrt{n}}} p$.

Serait-il possible de "rater l'intervalle visé", i.e. que toutes les solutions soient supérieures à n, comprises entre n et D ? À la section 3, on verra que la probabilité d'obtenir au moins une solution inférieure à n tend très vite vers 1.

2. Caractérisation des décomposants de Goldbach de n supérieurs à $\sqrt{n}$[1]

Soit $n \in 2\mathbb{N} + 6$ un entier pair supérieur à 6.

[1] Leila Schneps a démontré que la caractérisation de certains décomposants de Goldbach proposée était valide.

Pour tout $p \in \mathbb{P}^*$ premier impair inférieur à $\sqrt{n}$ (*i.e.* $3 \leq p \leq \sqrt{n}$), on définit l'ensemble :

$$F_n(p) = \{m \in 2\mathbb{N}+1 : 3 \leq m \leq n/2,\ m \not\equiv 0\ [p],\ m \not\equiv n\ [p]\}$$

L'intersection des ensembles $F_n(p)$ pour tout p premier compris entre 3 et $\sqrt{n}$ est notée :

$$D_n = \bigcap_{\substack{p \in \mathbb{P} \\ 3 \leq p \leq \sqrt{n}}} F_n(p)$$

Nous allons montrer que D_n et son complémentaire $n - D_n$ ne contiennent que des nombres premiers.
Lemme 1 : Soit $m \in 2\mathbb{N}+1$ un entier impair. Si m n'est divisible par aucun nombre premier compris entre 3 et $\sqrt{m}$, alors il est premier.

Démonstration : Si m est composé, on a $m = pq$, où p est le plus petit nombre premier intervenant dans la factorisation de m en nombres premiers et où q est le produit de tous les autres facteurs. Puisque m est impair, $p \geq 3$, et puisque $q \geq p$ (q étant le produit d'entiers $\geq p$), $m = pq \geq pp = p^2$ et donc $\sqrt{m} \geq p$ (la fonction racine carrée étant croissante). On a ainsi montré que si m impair est composé, il est divisible par un premier compris entre 3 et $\sqrt{m}$. Le lemme s'obtient par contraposition. □

Lemme 2 : $D_n \subseteq \mathbb{P}$

Démonstration : Soit $m \in D_n$. Alors $m \in F_n(p)$ pour tout p premier compris entre 3 et $\sqrt{n}$. Par conséquent, m est impair et m n'est divisible par aucun nombre premier p compris entre 3 et $\sqrt{n}$ (puisque $m \not\equiv 0\ [p]$), et donc *a fortiori* par aucun premier compris entre 3 et $\sqrt{m}$ (car $m \leq n/2 \implies m \leq n \implies \sqrt{m} \leq \sqrt{n}$). D'après le lemme 1, m est donc premier. □

Lemme 3 : $n - D_n \subseteq \mathbb{P}$

Démonstration : Soit $m \in D_n$. Alors $m \in F_n(p)$ pour tout p premier compris entre 3 et $\sqrt{n}$. Par conséquent, $n-m$ est impair (car m est impair et n pair) et $n-m$ n'est divisible par aucun nombre premier p compris entre 3 et $\sqrt{n}$ (puisque $m \not\equiv n\ [p]$), et donc *a fortiori* par aucun premier compris entre 3 et $\sqrt{n-m}$ (car $n-m \leq n \implies \sqrt{n-m} \leq \sqrt{n}$). D'après le lemme 1, $n-m$ est donc premier. □

Les ensembles D_n ne contiennent que des décomposants de Goldbach de n.

Lemme 4 : Soit $n \in 2\mathbb{N}+6$. Si $D_n \neq \varnothing$, alors n vérifie la conjecture de Goldbach.

Démonstration : Si $D_n \neq \varnothing$, il contient un entier p nécessairement premier (d'après le lemme 1), tel que $q = n - p$ est également premier (d'après le lemme 2), et donc $n = p + q$ vérifie la conjecture de Goldbach. □

3. Probabilité $P(n,k,p)$ de tirer un nombre inférieur ou égal à k, sans remise, quand on tire uniformément p entiers parmi les n premiers entiers.

La probabilité[2] $P(n,k,p)$ de tirer tirer un nombre inférieur ou égal à k, sans remise, quand on tire uniformément p entiers parmi les n premiers entiers se calcule par la formule suivante :

$$P = \frac{k}{n} + \frac{n-k}{n}\left(\frac{k}{n-1} + \frac{n-k-1}{n-1}\left(\frac{k}{n-2} + \frac{n-k-2}{n-2}\left(\dots\left(\frac{k}{n-p+1}\right)\dots\right)\right)\right)$$

Le premier terme de la somme correspond au fait de trouver un nombre inférieur à k dès le premier tirage. Le deuxième terme de la somme correspond au fait d'avoir tiré un nombre supérieur à k lors du premier tirage, de ne pas avoir la possibilité de tirer à nouveau ce nombre, et de tenter sa chance sur les nombres restant, la probabilité restant uniforme sur les nombres restant, etc.

On calcule cette probabilité pour

$$p = \prod_{\substack{x \text{ premier} \\ 3 \leqslant x \leqslant \sqrt{k}}} (x-2)$$

et

$$n = \prod_{\substack{x \text{ premier} \\ 3 \leqslant x \leqslant \sqrt{k}}} x.$$

Le programme python utilisé est le suivant :

```python
import math

def P(n, k, p):
    assert(1 <= p and p <= n and k <= n-p)
    s, t = 0, 1
    for i in range(p):
        s += t*(k/(n-i))
        t *= (n-k-i)/(n-i)
    return s

for n, k, p in [(30, 26, 3),
                (210, 50, 15),
                (2310, 122, 135),
                (30030, 170, 1485),
                (510510, 290, 22275),
                (9699690, 362, 378675),
                (223092870, 530 , 7952175),
                (6469693230, 842, 214708725),
                (200560490130, 962, 6226553025)]:
    print(f'n = {n}, k = {k}, p = {p} : P_n(k,p) = {P(n, k, p)}')
```

```
n = 30, k = 26, p = 3 : P_n(k,p) = 0.9990147783251231
n = 210, k = 50, p = 15 : P_n(k,p) = 0.9856514594832753
n = 2310, k = 122, p = 135 : P_n(k,p) = 0.9994752040784769
n = 30030, k = 170, p = 1485 : P_n(k,p) = 0.999824267526177
n = 510510, k = 290, p = 22275 : P_n(k,p) = 0.9999976037996607
n = 9699690, k = 362, p = 378675 : P_n(k,p) = 0.9999994514468453
n = 223092870, k = 530, p = 7952175 : P_n(k,p) = 0.9999999955788792
n = 6469693230, k = 842, p = 214708725 : P_n(k,p) = 0.9999999997119475
n = 200560490130, k = 962, p = 6226553025 : P_n(k,p) = 0.9999999921336346
```

[2] Merci Jacques.

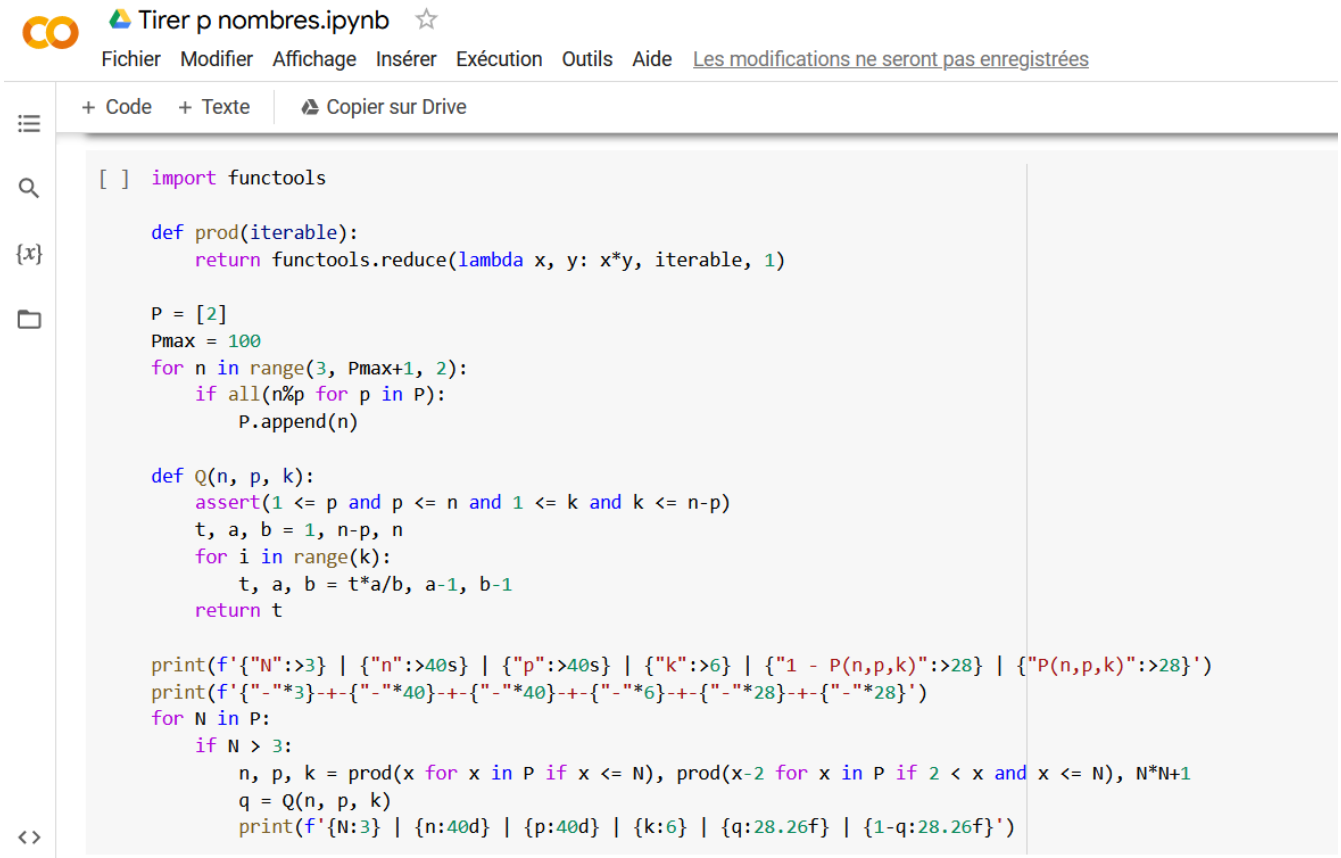
Fournissons ses résultats dans le tableau ci-dessous :

$N = \sqrt{k-1}$	n	k	p	$P(n,k,p)$
5	30	26	3	0.9990147783251231
7	210	50	15	0.9856514594832753
11	2310	122	135	0.9994752040784769
13	30030	170	1485	0.999824267526177
17	510510	290	22275	0.9999976037996607
19	9699690	362	378675	0.9999994514468453
23	223092870	530	7952175	0.9999999955788792
29	6469693230	842	214708725	0.9999999997119475
31	200560490130	962	6226553025	0.9999999921336346

Pour confirmer les résultats du programme, on utilise une fonction qui calcule la probabilité des événements complémentaires, i.e. la probabilité qu'au cours des p tirages sans remise réalisés selon la loi uniforme discrète dans l'intervalle $1..n$, tous les entiers tirés soient strictement supérieurs à $k$selon la formule

$$\overline{P(n,p,k)} = 1 - P(n,p,k) = \frac{n-p}{n}.\frac{n-p-1}{n-1}\ldots\frac{n-p-k+1}{n-k+1}.$$

La probabilité d'obtenir un décomposant de Goldbach d'un nombre pair est de 1 à partir du nombre premier 37 si l'on fixe la précision des calculs à 20 chiffres après la virgule.



Les résultats de ce programme sont fournis dans le tableau ci-dessous :

N	n	p	k	P(n,p,k)
5	30	3	26	0.99901477832512319832147796
7	210	15	50	0.98565145948327537173128121
11	2310	135	122	0.99947520407847800782974446
13	30030	1485	170	0.99982426752617770127073982
17	510510	22275	290	0.99999760379966495804637816
19	9699690	378675	362	0.99999945144687962805818415
23	223092870	7952175	530	0.99999995578856992750615 97
29	6469693230	214708725	842	0.99999999999954458651529876
31	200560490130	6226553025	962	0.99999999999993338661852249
37	7420738134810	217929355875	1370	1.00000000000000000000000000
41	304250263527210	8499244879125	1682	1.00000000000000000000000000
43	13082761331670030	348469040044125	1850	1.00000000000000000000000000
47	614889782588491410	15681106801985625	2210	1.00000000000000000000000000
53	32589158477190044730	799736446901266875	2810	1.00000000000000000000000000
59	1922760350154212639070	45584977473372211875	3482	1.00000000000000000000000000
61	117288381359406970983270	2689513670928960500625	3722	1.00000000000000000000000000
67	7858321551080267055879090	174818388610382432540625	4490	1.00000000000000000000000000
71	55794083012669896096741 5390	12062468814116387845303125	5042	1.00000000000000000000000000
73	40729680599249024150621323470	85643528580226353701652 1875	5330	1.00000000000000000000000000
79	32176447673406729078990845541 30	65945517006774292350272184375	6242	1.00000000000000000000000000
83	26706451568927585135562401799 2790	53415868775487176803720469343 75	6890	1.00000000000000000000000000
89	23768741896345550770650537601358310	46471805834673843819236808329062 5	7922	1.00000000000000000000000000
97	23055679639455184247531021473317560 70	44148215542940151628274967912609375	9410	1.00000000000000000000000000

Si tous étaient bien répartis, Denise Vella-Chemla, 25.3.2023

On calcule le produit des $p_k - 2$ (on élimine au maximum 2 classes de congruences modulo p_k, pour les non-diviseurs de n, pour p_k nombre premier impair ; concernant le nombre premier 2, il faut le considérer au dénominateur, pour éliminer les nombres pairs, mais pas au numérateur car 2-2 annule tout !) sur le produit des p_k et on le multiplie par les bornes de l'intervalle auquel appartient n (du carré du dernier p_k au carré du nombre premier suivant).

$\frac{1 \times 3 \times 5}{2 \times 3 \times 5 \times 7} = \frac{15}{210}$ pour les nombres compris entre 50 ($= 7^2 + 1$) et 120 ($= 11^2 - 1$);

$\frac{1 \times 3 \times 5 \times 9}{2 \times 3 \times 5 \times 7 \times 11} = \frac{135}{2310}$ pour les nombres compris entre 122 ($= 11^2 + 1$) et 168 ($= 13^2 - 1$);

$\frac{1 \times 3 \times 5 \times 9 \times 11}{2 \times 3 \times 5 \times 7 \times 11 \times 13} = \frac{1485}{30030}$ pour les nombres compris entre 170 ($= 13^2 + 1$) et 288 ($= 17^2 - 1$);

$\frac{1 \times 3 \times 5 \times 9 \times 11 \times 15}{2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17} = \frac{22275}{510510}$ pour les nombres compris entre 290 ($= 17^2 + 1$) et 360 ($= 19^2 - 1$);

Seul le fait que les solutions des systèmes d'incongruence soient toutes bien réparties dans l'intervalle source pourrait permettre de faire des calculs de proportion aux bornes successives, ces calculs donnent :

$\frac{15}{210} \times 50 = 3.57$ $\quad$ $\frac{15}{210} \times 120 = 8.57$

$\frac{135}{2310} \times 122 = 7.12$ $\quad$ $\frac{135}{2310} \times 168 = 9.81818181818$ (nombre rigolo à rapprocher du *Blues du bégayeur* de Dick Annegarn);

$\frac{1485}{30030} \times 170 = 8.4$ $\quad$ $\frac{1485}{30030} \times 288 = 14.2$

$\frac{22275}{510510} \times 170 = 12.65$ $\quad$ $\frac{22275}{510510} \times 360 = 15.7$

Petits décomposants de Goldbach (Denise Vella-Chemla, 18.4.2023)

Un nombre premier p compris entre 3 et $\sqrt{n}$ est un décomposant de Goldbach de n, un nombre pair supérieur ou égal à 6 (i.e. $n-p$ est un nombre premier également), s'il vérifie :

$$\forall q, 3 \leq q \leq \sqrt{n} \text{ et } q \text{ premier} \implies p \not\equiv n \pmod{q}.$$

En effet, l'assertion $p \not\equiv n \pmod{q}$ est équivalente à $n - p \not\equiv 0 \pmod{q}$ et cette dernière assertion entraîne que $n-p$ est un nombre premier (il n'est divisible par aucun nombre premier inférieur à sa racine carrée, puisque $a \not\equiv 0 \pmod{b}$ est équivalent au fait que $b \nmid a$). Ainsi, $n = p + (n-p)$ est une décomposition de n comme somme de deux nombres premiers, et n vérifie la conjecture de Goldbach.

Jusqu'à 100 000, 7,3 % des nombres pairs seulement ont comme plus petit décomposant de Goldbach un nombre qui est supérieur strictement à leur racine. La majorité des nombres semblent avoir chacun (du moins jusqu'à 10^8) un "petit" décomposant de Goldbach.

De 100 000 à 10^8, par programme, on ne trouve aucun nombre pair qui aurait comme plus petit décomposant de Goldbach un nombre premier supérieur à sa racine, c'est le cas par exemple pour le nombre pair $81099776 = 139 + 81099637$ avec $139 < \sqrt{81099776}$ $(= 9005,54...)$. En note, on fournit la liste des 70 nombres inférieurs à 100 000 ayant pour plus petit décomposant de Goldbach un nombre premier supérieur à leur racine[1].

Cette constatation amène à proposer le calcul suivant : si l'on pense que p à $\frac{1}{q}$ chances d'être congru à n modulo q, et que la probabilité d'être congru à n modulo q_1 *ou bien* à n modulo q_2 est la somme des probabilités $\frac{1}{q_1}$ et $\frac{1}{q_2}$, alors on obtient la probabilité pour l'ensemble des nombres premiers compris entre 3 et $\sqrt{n}$, qui sont au nombre de $\pi(\sqrt{n})$[2] de n'être, chacun, jamais congru à n selon tout module premier inférieur à $\sqrt{n}$ en ajoutant toutes les probabilités

$$S = \sum_{\substack{3 \leq q_k \leq \sqrt{n} \\ q_k \text{ premier}}} \left(1 - \frac{1}{q_k}\right)$$

Or on a $\sum_{\substack{3 \leq q_k \leq \sqrt{n} \\ q_k \text{ premier}}} \frac{1}{q_k} = \ln\ln\sqrt{n}$, ce qui permettrait d'obtenir pour S la valeur :

$$(\pi(\sqrt{n}) - 1) - \ln\ln\sqrt{n}$$

S est supérieur à 1 pour $n \geq 50$.

[1] Les 73 nombres pairs inférieurs à 100 000 ayant pour plus petit décomposant de Goldbach un nombre premier qui est supérieur à leur racine : 6, 8, 12, 18, 24, 30, 38, 98, 122, 126, 128, 220, 302, 332, 346, 488, 556, 854, 908, 962, 992, 1144, 1150, 1274, 1354, 1360, 1362, 1382, 1408, 1424, 1532, 1768, 1856, 1928, 2078, 2188, 2200, 2438, 2512, 2530, 2618, 2642, 3458, 3818, 3848, 4618, 4886, 5372, 5978, 6002, 6008, 7426, 9596, 9602, 10268, 10622, 11438, 11642, 12886, 13148, 13562, 14198, 14678, 16502, 18908, 21368, 22832, 23426, 23456, 43532, 54244, 63274.

[2] On utilise la notation $\pi(x)$ habituelle pour désigner le nombre de nombres premiers inférieurs ou égaux à x.

On avait, à la place de cette idée d'ajouter les probabilités, proposé à l'été 2019 d'utiliser plutôt une multiplication du nombre de nombres premiers inférieurs à $n/2$ (ce nombre de nombres premiers étant égal à $A = \dfrac{n/2}{\ln(n/2)}$) par le produit $B = \displaystyle\prod_{\substack{p \text{ premier} \\ p \leq \sqrt{n}}} \left(1 - \frac{1}{p}\right)$ dont Mertens a démontré qu'il est égal à $\dfrac{1}{e^{\gamma} \ln(p_{max})} \left(1 + O\left(\dfrac{1}{\ln p_{max}}\right)\right)$, ce théorème étant valable pour $n \geq 2$, où γ désigne la constante d'Euler-Mascheroni. Ce second produit B représente la probabilité qu'a chaque nombre premier, dont le nombre est compté par A, d'être congru à n selon un module premier inférieur à $\sqrt{n}$ (i.e. d'avoir le même reste, dans une division par un nombre premier inférieur à $\sqrt{n}$).

La formule pour la probabilité devient :

$$S' = \frac{n/2}{\ln(n/2)} \frac{1}{e^{\gamma} \ln(p_{max})} \left(1 + O\left(\frac{1}{\ln n}\right)\right)$$

qui est supérieur à 1 pour 6 et 8, inférieur à 1 jusqu'à 2422, puis semble repasser définitivement au-dessus de 1 à partir de ce nombre 2422.

Factorisations des nombres dont le plus petit décomposant de Goldbach est supérieur à leur racine (où l'on voit tout l'alea associé aux nombres premiers) :

$6 = 2 \times 3$
$8 = 2^3$
$12 = 2^2 \times 3$
$18 = 2 \times 3^2$
$24 = 2^3 \times 3$
$30 = 2 \times 3 \times 5$
$38 = 2 \times 19$
$98 = 2 \times 7^2$
$122 = 2 \times 61$
$126 = 2 \times 3^2 \times 7$
$128 = 2^7$
$220 = 2^2 \times 5 \times 11$
$302 = 2 \times 151$
$332 = 2^2 \times 83$
$346 = 2 \times 173$
$488 = 2^3 \times 61$
$556 = 2^2 \times 139$
$854 = 2 \times 7 \times 61$
$908 = 2^2 \times 227$
$962 = 2 \times 13 \times 37$
$992 = 2^5 \times 31$
$1144 = 2^3 \times 11 \times 13$
$1150 = 2 \times 5^2 \times 23$
$1274 = 2 \times 7^2 \times 13$
$1354 = 2 \times 677$
$1360 = 2^4 \times 5 \times 17$
$1362 = 2 \times 3 \times 227$
$1382 = 2 \times 691$
$1408 = 2^7 \times 11$
$1424 = 2^4 \times 89$
$1532 = 2^2 \times 383$
$1768 = 2^3 \times 13 \times 17$
$1856 = 2^6 \times 29$
$1928 = 2^3 \times 241$
$2078 = 2 \times 1039$
$2188 = 2^2 \times 547$
$2200 = 2^3 \times 5^2 \times 11$
$2438 = 2 \times 23 \times 53$
$2512 = 2^4 \times 157$
$2530 = 2 \times 5 \times 11 \times 23$
$2618 = 2 \times 7 \times 11 \times 17$
$2642 = 2 \times 1321$

$3458 = 2 \times 7 \times 13 \times 19$
$3818 = 2 \times 23 \times 83$
$3848 = 2^3 \times 13 \times 37$
$4618 = 2 \times 2309$
$4886 = 2 \times 7 \times 349$
$5372 = 2^2 \times 17 \times 79$
$5978 = 2 \times 7^2 \times 61$
$6002 = 2 \times 3001$
$6008 = 2^3 \times 751$
$7426 = 2 \times 47 \times 79$
$9596 = 2^2 \times 2399$
$9602 = 2 \times 4801$
$10268 = 2^2 \times 17 \times 151$
$10622 = 2 \times 47 \times 113$
$11438 = 2 \times 7 \times 19 \times 43$
$11642 = 2 \times 5821$
$12886 = 2 \times 17 \times 379$
$13148 = 2^2 \times 19 \times 173$
$13562 = 2 \times 6781$
$14198 = 2 \times 31 \times 229$
$14678 = 2 \times 41 \times 179$
$16502 = 2 \times 37 \times 223$
$18908 = 2^2 \times 29 \times 163$
$21368 = 2^3 \times 2671$
$22832 = 2^4 \times 1427$
$23426 = 2 \times 13 \times 17 \times 53$
$23456 = 2^5 \times 733$
$43532 = 2^2 \times 10883$
$54244 = 2^2 \times 71 \times 191$
$63274 = 2 \times 17 \times 1861$

Retour à l'indicatrice φ d'Euler (Denise Vella-Chemla, 29.4.2023)

On rappelle la définition suivante : A et B sont premiers l'un à l'autre si leur plus grand diviseur commun (pgcd) est égal à 1.

Si $n = p + (n-p)$ est une décomposition de Goldbach de n, un nombre pair supérieur à 4, alors p et $n-p$ sont deux nombres premiers. Considérons un nombre premier p supérieur à $\sqrt{n}$, il est premier au produit des nombres premiers inférieurs à $\sqrt{n}$. Son complémentaire à n également est premier à ce produit. Et le produit $p(n-p)$ est lui aussi premier au produit en question des nombres premiers inférieurs ou égaux à $\sqrt{n}$.

Cette constatation permet de trouver d'une façon particulière les décomposants de Goldbach p d'un nombre pair n (≥ 6) qui sont supérieurs à $\sqrt{n}$. On teste simplement que le produit $A = p(n-p)$ est premier à $B = \prod_{\substack{q \text{ premier} \\ 2 \leq q \leq \sqrt{n}}} q$. Si tel est le cas, p est un décomposant de Goldbach de n.

Pour n un nombre pair, on a $\left\lfloor \frac{n-2}{4} \right\rfloor$ nombres impairs qui sont des décomposants de Goldbach potentiels de n.

L'indicatrice d'Euler, $\varphi(k)$ compte le nombre de nombres inférieurs à k et premiers à k, i.e. le nombre de nombres qui ont pour pgcd avec k le nombre 1 (on dit aussi qui n'ont pas de facteur commun qui soit supérieur à 1 avec k).

Question 1 : peut-on dire que la probabilité pour un nombre inférieur à k d'être premier à k est égale à $\frac{\varphi(k)}{k}$?

Question 2 : peut-on dire qu'un certain nombre de nombres inférieurs à un entier donné k, ces nombres étant en quantité x, ont $x \times \frac{\varphi(k)}{k}$ chances à eux tous que l'un d'entre eux au moins soit premier à k ?

Si l'on pouvait répondre par l'affirmative à ces deux questions, cela serait très arrangeant, car on pourrait alors dire que les $\left\lfloor \frac{n-2}{4} \right\rfloor$ nombres impairs décomposants de Goldbach potentiels du nombre n ont à eux tous $\left\lfloor \frac{n-2}{4} \right\rfloor \times \frac{\varphi(\prod_{\substack{q \text{ premier} \\ 2 \leq q \leq \sqrt{n}}} q)}{\prod_{\substack{q \text{ premier} \\ 2 \leq q \leq \sqrt{n}}} q}$ chances que l'un d'entre eux soit premier à $\prod_{\substack{q \text{ premier} \\ 2 \leq q \leq \sqrt{n}}} q$, i.e. soit un décomposant de Goldbach de n et ce nombre de chances d'être un décomposant de Goldbach de n est supérieur strictement à 1 à partir de $n = 10$ et au-delà, semble-t-il par programme.

Retour à l'indicatrice φ d'Euler (Denise Vella-Chemla, 29.4.2023)

On rappelle la définition suivante : A et B sont premiers l'un à l'autre si leur plus grand diviseur commun (pgcd) est égal à 1.

Si $n = p + (n-p)$ est une décomposition de Goldbach de n, un nombre pair supérieur à 4, alors p et $n-p$ sont deux nombres premiers. Considérons un nombre premier p supérieur à $\sqrt{n}$, il est premier au produit des nombres premiers inférieurs à $\sqrt{n}$. Son complémentaire à n également est premier à ce produit. Et le produit $p(n-p)$ est lui aussi premier au produit en question des nombres premiers inférieurs ou égaux à $\sqrt{n}$.

Cette constatation permet de trouver d'une façon particulière les décomposants de Goldbach p d'un nombre pair n (≥ 6) qui sont supérieurs à $\sqrt{n}$. On teste simplement que le produit $A = p(n-p)$ est premier à $B = \prod_{\substack{q \text{ premier} \\ 2 \leq q \leq \sqrt{n}}} q$. Si tel est le cas, p est un décomposant de Goldbach de n.

Pour n un nombre pair, on a $\left\lfloor \frac{n-2}{4} \right\rfloor$ nombres impairs qui sont des décomposants de Goldbach potentiels de n.

L'indicatrice d'Euler, $\varphi(k)$ compte le nombre de nombres inférieurs à k et premiers à k, i.e. le nombre de nombres qui ont pour pgcd avec k le nombre 1 (on dit aussi qui n'ont pas de facteur commun qui soit supérieur à 1 avec k).

Question 1 : peut-on dire que la probabilité pour un nombre inférieur à k d'être premier à k est égale à $\frac{\varphi(k)}{k}$?

Question 2 : peut-on dire qu'un certain nombre de nombres inférieurs à un entier donné k, ces nombres étant en quantité x, ont $x \times \frac{\varphi(k)}{k}$ chances à eux tous que l'un d'entre eux au moins soit premier à k ?

Si l'on pouvait répondre par l'affirmative à ces deux questions, cela serait très arrangeant, car on pourrait alors dire que les $\left\lfloor \frac{n-2}{4} \right\rfloor$ nombres impairs décomposants de Goldbach potentiels du nombre n ont à eux tous $\left\lfloor \frac{n-2}{4} \right\rfloor \times \frac{\varphi(\prod_{\substack{q \text{ premier} \\ 2 \leq q \leq \sqrt{n}}} q)}{\prod_{\substack{q \text{ premier} \\ 2 \leq q \leq \sqrt{n}}} q}$ chances que l'un d'entre eux soit premier à $\prod_{\substack{q \text{ premier} \\ 2 \leq q \leq \sqrt{n}}} q$, i.e. soit un décomposant de Goldbach de n et ce nombre de chances d'être un décomposant de Goldbach de n est supérieur strictement à 1 à partir de $n = 10$ et au-delà, semble-t-il par programme.

Petits décomposants de Goldbach (Denise Vella-Chemla, 18.4.2023)

Un nombre premier p compris entre 3 et $\sqrt{n}$ est un décomposant de Goldbach de n, un nombre pair supérieur ou égal à 6 (i.e. $n-p$ est un nombre premier également), s'il vérifie :

$$\forall q, 3 \leq q \leq \sqrt{n} \text{ et } q \text{ premier} \implies p \not\equiv n \pmod{q}.$$

En effet, l'assertion $p \not\equiv n \pmod{q}$ est équivalente à $n - p \not\equiv 0 \pmod{q}$ et cette dernière assertion entraîne que $n-p$ est un nombre premier (il n'est divisible par aucun nombre premier inférieur à sa racine carrée, puisque $a \not\equiv 0 \pmod{b}$ est équivalent au fait que $b \nmid a$). Ainsi, $n = p + (n-p)$ est une décomposition de n comme somme de deux nombres premiers, et n vérifie la conjecture de Goldbach.

Jusqu'à 100 000, 7,3 % des nombres pairs seulement ont comme plus petit décomposant de Goldbach un nombre qui est supérieur strictement à leur racine. La majorité des nombres semblent avoir chacun (du moins jusqu'à 10^8) un "petit" décomposant de Goldbach.

De 100 000 à 10^8, par programme, on ne trouve aucun nombre pair qui aurait comme plus petit décomposant de Goldbach un nombre premier supérieur à sa racine, c'est le cas par exemple pour le nombre pair $81099776 = 139 + 81099637$ avec $139 < \sqrt{81099776}$ $(= 9005,54...)$. En note, on fournit la liste des 70 nombres inférieurs à 100 000 ayant pour plus petit décomposant de Goldbach un nombre premier supérieur à leur racine[1].

Cette constatation amène à proposer le calcul suivant : si l'on pense que p à $\frac{1}{q}$ chances d'être congru à n modulo q, et que la probabilité d'être congru à n modulo q_1 *ou bien* à n modulo q_2 est la somme des probabilités $\frac{1}{q_1}$ et $\frac{1}{q_2}$, alors on obtient la probabilité pour l'ensemble des nombres premiers compris entre 3 et $\sqrt{n}$, qui sont au nombre de $\pi(\sqrt{n})$[2] de n'être, chacun, jamais congru à n selon tout module premier inférieur à $\sqrt{n}$ en ajoutant toutes les probabilités

$$S = \sum_{\substack{3 \leq q_k \leq \sqrt{n} \\ q_k \text{ premier}}} \left(1 - \frac{1}{q_k}\right)$$

Or on a $\sum_{\substack{3 \leq q_k \leq \sqrt{n} \\ q_k \text{ premier}}} \frac{1}{q_k} = \ln\ln\sqrt{n}$, ce qui permettrait d'obtenir pour S la valeur :

$$(\pi(\sqrt{n}) - 1) - \ln\ln\sqrt{n}$$

S est supérieur à 1 pour $n \geq 50$.

[1] Les 73 nombres pairs inférieurs à 100 000 ayant pour plus petit décomposant de Goldbach un nombre premier qui est supérieur à leur racine : 6, 8, 12, 18, 24, 30, 38, 98, 122, 126, 128, 220, 302, 332, 346, 488, 556, 854, 908, 962, 992, 1144, 1150, 1274, 1354, 1360, 1362, 1382, 1408, 1424, 1532, 1768, 1856, 1928, 2078, 2188, 2200, 2438, 2512, 2530, 2618, 2642, 3458, 3818, 3848, 4618, 4886, 5372, 5978, 6002, 6008, 7426, 9596, 9602, 10268, 10622, 11438, 11642, 12886, 13148, 13562, 14198, 14678, 16502, 18908, 21368, 22832, 23426, 23456, 43532, 54244, 63274.

[2] On utilise la notation $\pi(x)$ habituelle pour désigner le nombre de nombres premiers inférieurs ou égaux à x.

On avait, à la place de cette idée d'ajouter les probabilités, proposé à l'été 2019 d'utiliser plutôt une multiplication du nombre de nombres premiers inférieurs à $n/2$ (ce nombre de nombres premiers étant égal à $A = \dfrac{n/2}{\ln(n/2)}$) par le produit $B = \displaystyle\prod_{\substack{p \text{ premier} \\ p \leq \sqrt{n}}} \left(1 - \frac{1}{p}\right)$ dont Mertens a démontré qu'il est égal à $\dfrac{1}{e^{\gamma} \ln(p_{max})} \left(1 + O\left(\dfrac{1}{\ln p_{max}}\right)\right)$, ce théorème étant valable pour $n \geq 2$, où γ désigne la constante d'Euler-Mascheroni. Ce second produit B représente la probabilité qu'a chaque nombre premier, dont le nombre est compté par A, d'être congru à n selon un module premier inférieur à $\sqrt{n}$ (i.e. d'avoir le même reste, dans une division par un nombre premier inférieur à $\sqrt{n}$).

La formule pour la probabilité devient :

$$S' = \frac{n/2}{\ln(n/2)} \frac{1}{e^{\gamma} \ln(p_{max})} \left(1 + O\left(\frac{1}{\ln n}\right)\right)$$

qui est supérieur à 1 pour 6 et 8, inférieur à 1 jusqu'à 2422, puis semble repasser définitivement au-dessus de 1 à partir de ce nombre 2422.

Factorisations des nombres dont le plus petit décomposant de Goldbach est supérieur à leur racine (où l'on voit tout l'alea associé aux nombres premiers) :

$6 = 2 \times 3$
$8 = 2^3$
$12 = 2^2 \times 3$
$18 = 2 \times 3^2$
$24 = 2^3 \times 3$
$30 = 2 \times 3 \times 5$
$38 = 2 \times 19$
$98 = 2 \times 7^2$
$122 = 2 \times 61$
$126 = 2 \times 3^2 \times 7$
$128 = 2^7$
$220 = 2^2 \times 5 \times 11$
$302 = 2 \times 151$
$332 = 2^2 \times 83$
$346 = 2 \times 173$
$488 = 2^3 \times 61$
$556 = 2^2 \times 139$
$854 = 2 \times 7 \times 61$
$908 = 2^2 \times 227$
$962 = 2 \times 13 \times 37$
$992 = 2^5 \times 31$
$1144 = 2^3 \times 11 \times 13$
$1150 = 2 \times 5^2 \times 23$
$1274 = 2 \times 7^2 \times 13$
$1354 = 2 \times 677$
$1360 = 2^4 \times 5 \times 17$
$1362 = 2 \times 3 \times 227$
$1382 = 2 \times 691$
$1408 = 2^7 \times 11$
$1424 = 2^4 \times 89$
$1532 = 2^2 \times 383$
$1768 = 2^3 \times 13 \times 17$
$1856 = 2^6 \times 29$
$1928 = 2^3 \times 241$
$2078 = 2 \times 1039$
$2188 = 2^2 \times 547$
$2200 = 2^3 \times 5^2 \times 11$
$2438 = 2 \times 23 \times 53$
$2512 = 2^4 \times 157$
$2530 = 2 \times 5 \times 11 \times 23$
$2618 = 2 \times 7 \times 11 \times 17$
$2642 = 2 \times 1321$

$3458 = 2 \times 7 \times 13 \times 19$
$3818 = 2 \times 23 \times 83$
$3848 = 2^3 \times 13 \times 37$
$4618 = 2 \times 2309$
$4886 = 2 \times 7 \times 349$
$5372 = 2^2 \times 17 \times 79$
$5978 = 2 \times 7^2 \times 61$
$6002 = 2 \times 3001$
$6008 = 2^3 \times 751$
$7426 = 2 \times 47 \times 79$
$9596 = 2^2 \times 2399$
$9602 = 2 \times 4801$
$10268 = 2^2 \times 17 \times 151$
$10622 = 2 \times 47 \times 113$
$11438 = 2 \times 7 \times 19 \times 43$
$11642 = 2 \times 5821$
$12886 = 2 \times 17 \times 379$
$13148 = 2^2 \times 19 \times 173$
$13562 = 2 \times 6781$
$14198 = 2 \times 31 \times 229$
$14678 = 2 \times 41 \times 179$
$16502 = 2 \times 37 \times 223$
$18908 = 2^2 \times 29 \times 163$
$21368 = 2^3 \times 2671$
$22832 = 2^4 \times 1427$
$23426 = 2 \times 13 \times 17 \times 53$
$23456 = 2^5 \times 733$
$43532 = 2^2 \times 10883$
$54244 = 2^2 \times 71 \times 191$
$63274 = 2 \times 17 \times 1861$

Matrices, Denise Vella-Chemla, avril 2023

On représente tout entier x par une matrice 2×2 de la forme $\begin{bmatrix} x & 0 \\ 1 & 0 \end{bmatrix}$.

On représente les fonctions $f : x \mapsto ax + b$ par des matrices 2×2 de la forme $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$.[1]

On cherche les décomposants de Goldbach de $n = 26$ supérieurs à $\sqrt{26} = 5, ...$
26 est un $2k$, 26 est un $3k + 2$, 26 est un $5k + 1$.

En effet, on a :

$$\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 13 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 26 & 0 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 8 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 26 & 0 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 5 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 5 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 26 & 0 \\ 1 & 0 \end{bmatrix}$$

On cherche les nombres qui ne sont ni des $2k$, ni des $3k$, ni des $5k$, ni des $3k + 2$, ni des $5k + 1$.
On cherche toutes les matrices de la forme $\begin{bmatrix} x & 0 \\ 1 & 0 \end{bmatrix}$ avec $3 \leq x \leq 13$, qui ne sont pas image d'une matrice $Y = \begin{bmatrix} y & 0 \\ 1 & 0 \end{bmatrix}$, i.e. qui ne sont pas égales à un produit matriciel de la forme MY avec $M \in \left\{ \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 5 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 5 & 1 \\ 0 & 1 \end{bmatrix} \right\}$.

Les matrices $\begin{bmatrix} 7 & 0 \\ 1 & 0 \end{bmatrix}$ et $\begin{bmatrix} 13 & 0 \\ 1 & 0 \end{bmatrix}$ vérifient les contraintes souhaitées. Un théorème d'algèbre matricielle garantit peut-être l'existence d'une matrice au moins dans le cas général.

[1] Dans le livre *Noncommutative geometry* d'Alain Connes, téléchargeable ici https://alainconnes.org/wp-content/uploads/book94bigpdf.pdf, il est question de matrices semblables à celles utilisées dans la présente note à la page 535 : *Consider P_K as a subgroup of $GL(2, K)$: $P_k = \left\{ \begin{bmatrix} 1 & b \\ 0 & a \end{bmatrix} ; a \in K^*, b \in K \right\}$* . Si l'on considère qu'à la page 536, les matrices de la forme $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ correspondraient aux nombres, on ne parvient pas à faire ce qu'on veut, i.e. obtenir $\begin{bmatrix} 1 & 26 \\ 0 & 1 \end{bmatrix}$ par multiplication, à droite ou à gauche de $\begin{bmatrix} 1 & 1 \\ 0 & 5 \end{bmatrix}$ par $\begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix}$; on obtient soit $\begin{bmatrix} 1 & 6 \\ 0 & 5 \end{bmatrix}$, soit $\begin{bmatrix} 1 & 26 \\ 0 & 5 \end{bmatrix}$ alors qu'on souhaiterait obtenir $\begin{bmatrix} 1 & 26 \\ 0 & 1 \end{bmatrix}$; les matrices pour les nombres qui nous permettent d'obtenir le résultat qu'on souhaite devraient être de la forme $\begin{bmatrix} 1 & x \\ 0 & 0 \end{bmatrix}$, on a forcément dû mal interpréter le texte.

Tous pour un, Denise Vella-Chemla, avril 2023

On s'acharne parce qu'on est sûre qu'il y a quelque chose de simple, que l'on n'a toujours pas compris, et qui fait que les décomposants de Goldbach sont ceux qu'ils sont, pour chaque nombre pair, pour une raison très précise, et que l'on cherche.

D'abord on pense à multiplier tous les décomposants de Goldbach entre eux, pour $n = 98$, sauf un, pour voir si on n'aurait pas une relation d'un des décomposants de Goldbach à tous les autres.

Pour 98, notre exemple fétiche, on a $98 = 19 + 79 = 31 + 67 = 37 + 61$.

Si l'on multiplie tous les décomposants sauf un, voici ce qu'on obtient :

- le produit de tous les décomposants de Goldbach (notés *dg* dans la suite) sauf 19 est égal à 370335331 qui est congru à 93 modulo 98 ;
- le produit de tous les *dg* sauf 31 est congru à 57 (mod 98) ;
- le produit de tous les *dg* sauf 37 est congru à 61 (mod 98) ;
- le produit de tous les *dg* sauf 61 est congru à 37 (mod 98) ;
- le produit de tous les *dg* sauf 67 est congru à 41 (mod 98) ;
- le produit de tous les *dg* sauf 79 est congru à 5 (mod 98).

Le couple (37,61) est dans une situation particulière par rapport aux autres couples de sommants : l'un des décomposants s'envoie sur son symétrique et inversement, par multiplication par tous les autres décomposants de Goldbach sauf lui-même. Ca semble intéressant.

On cherche si pour notre autre nombre pair fétiche 40, le même phénomène se produit : les *dg* sont 3, 11, 17, 23, 29, 37.

- le produit de tous les *dg* sauf 3 est congru à 13 (mod 40) ;
- le produit de tous les *dg* sauf 11 est congru à 29 (mod 40) ;
- le produit de tous les *dg* sauf 17 est congru à 7 (mod 40) ;
- le produit de tous les *dg* sauf 23 est congru à 33 (mod 40) ;
- le produit de tous les *dg* sauf 29 est congru à 11 (mod 40) ;
- le produit de tous les *dg* sauf 37 est congru à ? (mod 40).

Merci à Cédric Villani, pour la belle conférence qu'il a donnée à Clermont-Ferrand, le 13 janvier 2023, "Blaise Pascal, un génie clermontois", visionnable à l'adresse : https://www.youtube-nocookie.com/embed/MilmmZ0yCGo, à l'occasion des 400 ans de la naissance de Blaise Pascal.

Le couple (11,29) est dans la même situation particulière par rapport aux autres couples de sommants : 11 s'envoie sur 29 (resp. 29 s'envoie sur 11), si on le multiplie par le produit de tous les décomposants de Goldbach sauf lui-même. Ca semble confirmer ce qu'on a trouvé pour le nombre pair $n = 98$.

Alors, on revient à une vieille idée qui était de trouver un moyen de passer des décompositions de Goldbach des doubles de nombres premiers aux décompositions de Goldbach des doubles de nombres composés. On va d'abord se concentrer sur les décomposants de Goldbach des doubles de nombres premiers. On repense aux équations algébriques, aux relations invariantes de Galois, aux relations entre sommes et produits dans les coefficients des équations algébriques. On se dit que pour les doubles de nombres premiers, le nombre premier central est peut-être en relation avec tous les autres décomposants de Goldbach. Dans la droite ligne des calculs effectués pour $n = 98$ et $n = 40$, on fait les calculs suivants, pour les nombres pairs doubles de nombres premiers :

$10 = 3 + 7 = 5 + 5.Ona : 3 \times 7 = 21 = 1 \pmod{10}$ et 1 rend 5 fixe.

$14 = 3 + 11 = 7 + 7.Ona : 3 \times 11 = 33 = 5 \pmod{14}$ et 5 rend 7 fixe.

$22 = 3 + 19 = 5 + 17 = 11 + 11.Ona : 3 \times 19 \times 5 \times 17 = 4845 = 5 \pmod{22}$ et 5 rend 11 fixe.

Et enfin $26 = 3 + 23 = 7 + 19 = 13 + 13 : 3 \times 23 \times 7 \times 19 = 9177 = 25 \pmod{26}$ et 25 rend 13 fixe.

Problème : si on ajoute la décomposition $26 = 5 + 21$ comme s'il s'agissait d'une décomposition de Goldbach (alors que 21 est composé), comme $5 \times 21 = 1 \pmod{26}$, 13 est aussi rendu fixe par le nouveau produit alors que celui-ci contient une décomposition qui n'est pas une décomposition de Goldbach. Dommage, c'eut été si chouette.

Si tous étaient bien répartis, Denise Vella-Chemla, 25.3.2023

On calcule le produit des $p_k - 2$ (on élimine au maximum 2 classes de congruences modulo p_k, pour les non-diviseurs de n, pour p_k nombre premier impair ; concernant le nombre premier 2, il faut le considérer au dénominateur, pour éliminer les nombres pairs, mais pas au numérateur car 2-2 annule tout !) sur le produit des p_k et on le multiplie par les bornes de l'intervalle auquel appartient n (du carré du dernier p_k au carré du nombre premier suivant).

$\frac{1 \times 3 \times 5}{2 \times 3 \times 5 \times 7} = \frac{15}{210}$ pour les nombres compris entre 50 ($= 7^2 + 1$) et 120 ($= 11^2 - 1$);

$\frac{1 \times 3 \times 5 \times 9}{2 \times 3 \times 5 \times 7 \times 11} = \frac{135}{2310}$ pour les nombres compris entre 122 ($= 11^2 + 1$) et 168 ($= 13^2 - 1$);

$\frac{1 \times 3 \times 5 \times 9 \times 11}{2 \times 3 \times 5 \times 7 \times 11 \times 13} = \frac{1485}{30030}$ pour les nombres compris entre 170 ($= 13^2 + 1$) et 288 ($= 17^2 - 1$);

$\frac{1 \times 3 \times 5 \times 9 \times 11 \times 15}{2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17} = \frac{22275}{510510}$ pour les nombres compris entre 290 ($= 17^2 + 1$) et 360 ($= 19^2 - 1$);

Seul le fait que les solutions des systèmes d'incongruence soient toutes bien réparties dans l'intervalle source pourrait permettre de faire des calculs de proportion aux bornes successives, ces calculs donnent :

$\frac{15}{210} \times 50 = 3.57$ $\quad$ $\frac{15}{210} \times 120 = 8.57$

$\frac{135}{2310} \times 122 = 7.12$ $\quad$ $\frac{135}{2310} \times 168 = 9.81818181818$ (nombre rigolo à rapprocher du *Blues du bégayeur* de Dick Annegarn);

$\frac{1485}{30030} \times 170 = 8.4$ $\quad$ $\frac{1485}{30030} \times 288 = 14.2$

$\frac{22275}{510510} \times 170 = 12.65$ $\quad$ $\frac{22275}{510510} \times 360 = 15.7$

Projections, une façon marrante de voir la recherche des décomposants de Goldbach, Denise Vella-Chemla, mars 2023.

Dans la dernière modélisation qu'on a choisie, les nombres sont représentés par leurs restes modulaires dans un réseau de Minkowski à $d = \pi(\lfloor\sqrt{n}\rfloor)$ dimensions, on élimine les points des hyperplans contenant 0 et les points des hyperplans contenant n, et on souhaiterait être assuré qu'il reste un nombre $\leq n/2$ non éliminé dans le réseau de points après élimination des points de ces hyperplans.

Qu'est-ce qui permet de caractériser les points extérieurs à tous les hyperplans qu'on a dit "de coupure" (i.e. les points intérieurs aux sous-espaces convexes délimités par les hyperplans) ? Ils sont systématiquement différents de leurs projections sur les plans en question, puisqu'ils ne doivent pas appartenir à ces hyperplans.

Du coup, de façon marrante, on utilise des matrices de projections de l'espace affine ; prenons l'exemple de la recherche des décomposants de Goldbach du nombre 40 dans l'espace $2 \times 3 \times 5$. On rappelle qu'il a pour restes (0,1,0).

On a d'une part les matrices des projections sur les "hyperplans nuls" (respectivement $x = 0$, $y = 0$, $z = 0$). On ajoute une coordonnée fictive à tous les vecteurs pour gérer le côté affine de la chose. Les matrices des 3 projections en questions sont :

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

La matrice de projection sur le seul hyperplan autre que les hyperplans nuls à éliminer, ici le plan $y = 1$ est :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Et on a effectivement que les nombres 11 et 17 ne sont jamais égaux à leur image selon chacune des 4 projections ci-dessus.

Les programmes python à la va-vite sont là :
http://denise.vella.chemla.free.fr/pgm-marrant-py-40.pdf
http://denise.vella.chemla.free.fr/pgm-marrant-py-98.pdf

Leur résultat pour vérification est là :
http://denise.vella.chemla.free.fr/res-marrant-py-40.pdf
http://denise.vella.chemla.free.fr/res-marrant-py-98.pdf

Pour la recherche des décomposants de Goldbach de 98, on projette dans $2 \times 3 \times 5 \times 7$. Il faut éliminer en plus des hyperplans nuls les hyperplans 2 (mod 3) ($x_2 = 2$) et 3 (mod 5) ($x_3 = 3$) par

les matrices :

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Cette vision par les projections permettrait-elle d'assurer l'existence d'un point du réseau au moins qui n'est égal à aucune de ses images par les différentes projections à envisager (les projections orthogonales sur les hyperplans nuls, et les projections orthogonales sur les hyperplans contenant n) ?...

Bla-bla ce que je ne sais pas, Denise Vella-Chemla, mars 2023.

Dans la dernière modélisation qu'on a choisie, les nombres sont représentés par leurs restes modulaires dans un réseau de Minkowski à $d = \pi(\lfloor\sqrt{n}\rfloor)$ dimensions, on élimine des hyperplans et on souhaite montrer qu'après cette élimination d'hyperplans, il reste un nombre $\leq n/2$ à un croisement du réseau.

Combien y a-t-il de points extérieurs à tous les hyperplans (i.e. intérieurs aux sous-espaces convexes délimités par les hyperplans) ? Il y en a :

$$S = \prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \lfloor\sqrt{n}\rfloor}} p_k - \prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \lfloor\sqrt{n}\rfloor \\ p_k | n}} (p_k - 1) \prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \lfloor\sqrt{n}\rfloor \\ p_k \nmid n}} (p_k - 2).$$

On appelle A le produit $\prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \lfloor\sqrt{n}\rfloor \\ p_k | n}} (p_k - 1)$ et B le produit $\prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \lfloor\sqrt{n}\rfloor \\ p_k \nmid n}} (p_k - 2)$.

Si $n = 2p$ est le double d'un nombre premier (et vérifie trivialement la conjecture de Goldbach), le produit A est vide. Or ce produit est pair car 2 est le $p_k - 1$ de 3. Comme B ne contient que des termes impairs, S est impair et cela concorde avec le fait que p est ajouté à lui-même (une sorte de point-fixe d'une transformation à définir sur le réseau de Minkowski) dans la somme $n = p + p$.

Si n est le double d'un nombre composé, le produit A est pair (car comme dit $2 = 3 - 1$), et S est pair : toutes les sommes décompositions de Goldbach contiennent des sommants différents, i.e. sont de la forme $p + q$ avec $p < n/2$ et $q > n/2$.

On est très tenté de considérer comme transformations pertinentes pour la conjecture de Goldbach les symétries orthogonales par rapport aux hyperplans "de coupure" mais on ne voit toujours pas ce qui garantirait de trouver un décomposant $< n/2$ car l'ordre naturel sur les entiers est complètement bouleversé par l'écriture par les restes. Le seul ordre naturel dont on dispose sur les n-uplets de restes (qu'on les place ou pas sur un réseau de Minkowski, qui présente tout de même l'intérêt de fournir une image mentale géométrique du processus permettant de trouver, s'ils existent, les décomposants de Goldbach de n compris entre $\sqrt{n}$ et $n/2$), c'est l'ordre lexicographique et on ne sait pas comment l'utiliser pour remettre les entiers dans l'ordre ; enfin si, on sait qu'il faut appliquer le théorème des restes chinois pour trouver les entiers correspondant à un n-uplet de restes mais on ne sait pas garantir l'appartenance à un intervalle (l'intervalle $[3, n/2]$ en l'occurrence) de l'entier correspondant à un n-uplet de reste.

Polytopes et décomposants de Goldbach

Denise Vella-Chemla

mars 2023

Dans [1], on a caractérisé les décomposants de Goldbach de n (un nombre pair ≥ 6) supérieurs à $\sqrt{n}$[1] et $\leq n/2$.

Ils ne sont[2] :

1) pas $\equiv 0 \pmod{p_k}$ $\quad \forall p_k$ un nombre premier $\leq \sqrt{n}$ (cette première propriété en fait des nombres premiers) ;

2) pas $\equiv n \pmod{p_k}$ $\quad \forall p_k$ un nombre premier $\leq \sqrt{n}$ (cette seconde propriété en fait des nombres (appelons-les x) dont le complémentaire à n (i.e. $n-x$) est premier) ;

Pour avoir une appréhension géométrique de l'existence de décompositions de Goldbach pour n un nombre pair ≥ 6, on a l'idée de les placer dans un polytope entier de $\mathbb{R}_+^d$ avec $d = \lfloor \sqrt{n} \rfloor$. Un polytope est un polyèdre convexe borné, i.e. un sous-ensemble de $\mathbb{R}_+^d$ qui est l'intersection d'un nombre fini de demi-espaces fermés.

Ce polytope est de taille

$$\prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \lfloor \sqrt{n} \rfloor}} p_k.$$

On gradue ce polytope par un réseau de Minkowski de points entiers. Chaque direction du polytope correspond à un certain nombre premier $p_k \leq \sqrt{n}$. Les coordonnées possibles selon le nombre premier p_k (selon la direction correspondant à ce nombre premier) sont comprises entre 0 et $p_k - 1$. Un nombre est positionné à l'intersection de différentes droites en fonction de son appartenance aux différentes classes modulaires selon les nombres premiers inférieurs à sa racine. Sur un réseau à 3 dimensions[3], le nombre 40 sera positionné sur le point (0,1,0) (il a pour reste 0 quand on le divise par 2, il a pour reste 1 quand on le divise par 3, et il a pour reste 0 quand on le divise par 5). C'est le théorème des restes chinois qui permet de retrouver les nombres associés à un point du réseau de Minkowski graduant le polytope.

Ci-dessous, le réseau des nombres entiers ≤ 40, positionnés aux différents croisements du réseau de Minkowski dans un polytope de dimension 2, les dimensions correspondant aux nombres premiers

[1] dans toute la suite de cette note, l'expression "décomposant de Goldbach de n" sera à lire "décomposant de Goldbach de n supérieur à $\sqrt{n}$".

[2] Donnons un exemple simple pour illustrer la deuxième condition, selon le nombre premier 3 : si n est de la forme $3k+1$, un décomposant de Goldbach x de n (supérieur à $\sqrt{n}$) sera obligatoirement de la forme $3k+2$ (car si et x et n sont de la forme $3k+1$ tous les deux, leur différence est un $3k$ et donc $n-x$ est composé ; et inversement ; tandis que si n est de la forme $3k$, un décomposant de Goldbach de n peut être de l'une ou l'autre des deux formes $3k+1$ ou $3k+2$. En généralisant, si n est de la forme mp_k avec p_k un nombre premier, un décomposant de Goldbach de n peut être de toutes les formes possibles $np_k + i$ avec $1 \leq i \leq p_k - 1$ tandis que si n est de la forme $np_k + i$, un décomposant de Goldbach de n supérieur à $\sqrt{n}$ ne peut être que d'une des formes $mp_k + j$ avec $j \neq i$.

[3] Dans l'illustration ci-après, bien qu'il y ait 3 nombres premiers 2,3 et 5 qui soient $\leq \sqrt{40}$, on a "mélangé" dans le réseau plan les nombres pairs et les nombres impairs, même si, idéalement, ils devraient appartenir à deux sous-espaces différents.

3 et 5, et de taille 3×5 (on a projeté les pairs et les impairs d'un réseau de dimension 3 "au même étage") :

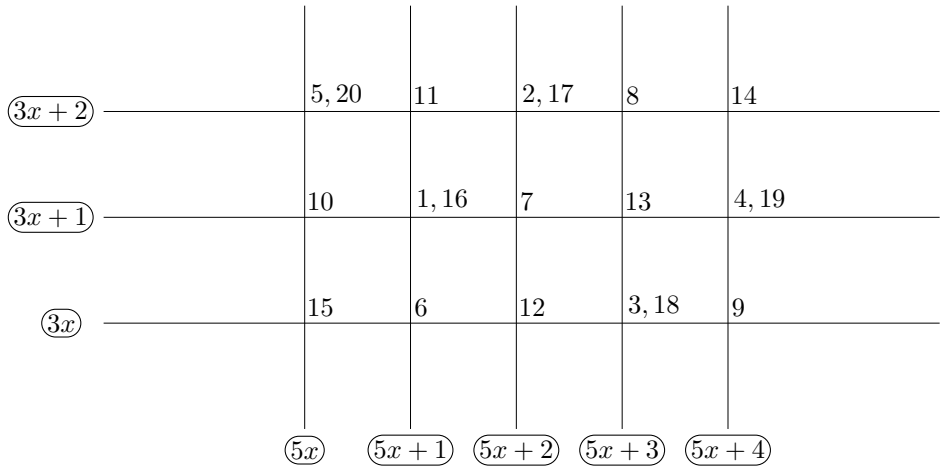


Figure 1 : positionnement des nombres dans le réseau de Minkowski
inclus dans le polytope de taille 3×5
pour illustrer la recherche des décomposants de Goldbach de 40

Les opérations 1) et 2) ci-dessus de criblage des nombres pour trouver de potentiels décomposants de Goldbach de n vont correspondre aux opérations géométriques ci-dessous, à effectuer dans le polytope :

1) les "divisibles" par un nombre premier quelconque sont sur les hyperplans bords[4] du polytope (cela correspond à la nullité de l'une de leur coordonnée) ;

2) les "congrus à n" selon un nombre premier quelconque sont éliminés en supprimant tout un hyperplan de l'espace ; par exemple l'hyperplan $x_3 = 2$ éliminera tous les nombres de reste 2 lorsqu'on les divise par $p_3 = 5$, si on appelle x_3 la coordonnée selon le nombre premier 5 ;

On symbolise sur le réseau l'élimination des hyperplans "nuls" (opération 1) par deux droites "au bord" et l'élimination des "congrus à 40" (opération 2) par une droite correspondant à un plan vertical, éliminant les $x_2 = 1$ (correspondant à $x \equiv 1 \pmod{p_2 = 3}$). Pour le nombre premier 5 qui divise 40, l'hyperplan bord et l'hyperplan $\equiv n \pmod 5$ sont confondus. On prend une même couleur pour des hyperplans parallèles (ici rouge pour le module 3 et bleu pour le module 5).

[4] En fait, il n'y a pas de bords, l'espace est un tore multi-dimensionnel (produit de cercles complexes sur lesquels sont positionnées les unités de la forme $e^{2i\pi m/p_k}$ avec m variant de 0 à $p_k - 1$) ; on peut aussi voir cet espace comme le produit cartésien des corps premiers $\mathbb{Z}/p_k\mathbb{Z}$, mais on se place dans $\mathbb{R}_+^d$ pour rendre l'exposé plus simple.

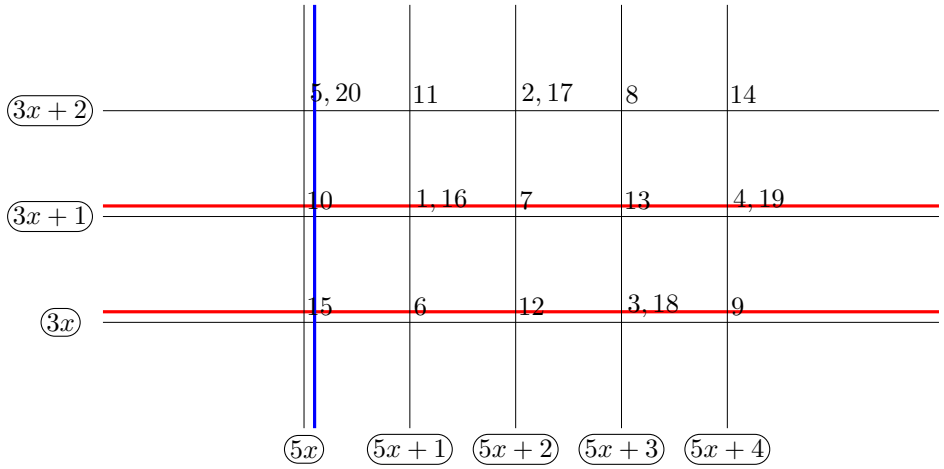


Figure 2 : positionnement des nombres dans le réseau de Minkowski
inclus dans le polytope de taille 3×5
pour illustrer la recherche des décomposants de Goldbach de 40

Cette modélisation étant choisie, quel problème géométrique se pose à nous qui pourrait empêcher l'existence d'un décomposant de Goldbach ?

D'abord, on voit qu'on se situe dans un espace bien plus grand que l'espace souhaité : on a dans le polytope tous les nombres de 1 à $\prod_{\substack{p_k \text{ premier} \\ 3 \leq p_k \leq \lfloor \sqrt{n} \rfloor}} p_k$. Or notre caractérisation d'un décomposant de Goldbach par [1] nécessite que ce nombre soit compris entre $\sqrt{n}$ et $n/2$.

Pour essayer de comprendre un peu mieux ce qui se passe, la première question à laquelle on doit répondre est : combien de croisements du réseau reste-t-il qui n'ont pas été éliminés une fois qu'on a éliminé les hyperplans contenant l'origine ainsi que les hyperplans contenant n ?

Il en reste :

(1)
$$\prod_{\substack{p_k \text{ premier} \\ 3 \leq p_k \leq \lfloor \sqrt{n} \rfloor \\ p \nmid n}} (p_k - 2) \times \prod_{\substack{p_k \text{ premier} \\ 3 \leq p_k \leq \lfloor \sqrt{n} \rfloor \\ p \mid n}} (p_k - 1)$$

Pour s'en convaincre, on peut analyser la grille de recherche des décomposants de Goldbach de 98 ci-après, ou relire la note de bas de page n° 2 de la page 1 :

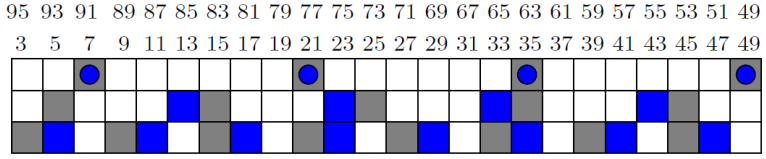


Figure 3 : visualisation des décomposants de Goldbach de $n = 98$. Les nombres ont été notés au-dessus de la grille. Seules les colonnes des nombres 19, 31 et 37 ne contiennent aucune case colorée. La ligne en bas de la grille montre la divisibilité par 3 (en gris, celle des nombres $\leq n/2$, en bleu, celle des nombres $\geq n/2$) ; la ligne médiane correspond à la divisibilité par 5 et la ligne en haut de la grille correspond à la divisibilité par 7.

Remarquons bien dans la visualisation par grille ci-dessus que comme le nombre premier 7 divise 98, les cases bleues et grises coïncident dans la ligne du haut : on élimine **un** nombre tous les $p_k = 7$ nombres dans la ligne du haut. Dans les deux autres lignes, on élimine **deux** nombres sur $p_k = 3$ ou bien 2 nombres sur $p_k = 5$ respectivement. On résumera cette idée par la phrase "Parmi les nombres premiers inférieurs ou égaux à $\sqrt{n}$, les nombres premiers intervenant dans la décomposition en facteurs premiers de n font éliminer moins de nombres que les autres nombres premiers.".

Revenons à la modélisation géométrique. On se pose le problème de l'existence d'un point "non éliminé" par tous les plans de coupe. La formule (1) bien comprise nous indique qu'il y a deux plans de coupe (le plan bord, contenant 0, et le plan contenant n) selon tout nombre premier ne divisant pas n, tandis qu'il n'y a qu'un seul plan de coupe pour les diviseurs de n (les deux plans de coupe de 0 et de n sont alors confondus).

Pour garantir l'existence d'un point au moins, on va montrer qu'on peut toujours trouver un petit carré composé de 4 mailles du réseau, qui ne sont touchées par aucun plan de coupe, ce qui garantit l'existence d'un point au croisement central de ces 4 carrés qui n'appartient à aucun plan de coupe, i.e. qui n'est pas éliminé par les hyperplans de coupe.

On cherche le carré de 4 mailles en question dans une projection plane de l'ensemble des points non éliminés :

- si n est de la forme $6p_mk$, seuls les hyperplans aux 2 bords sont éliminés sur le plan de taille $3 \times p_m$ avec $p_m > 3$, et on dispose donc d'un carré assez grand pour contenir un petit carré de 2×2 mailles du réseau, qui contient en son centre un point non éliminé par les coupes ;

- si n est de la forme $2p_mp_nk$, seuls les hyperplans aux 2 bords sont éliminés sur le plan de taille $p_m \times p_n$ avec $p_m \geq 3$ et $p_n \geq 3$, et on dispose donc d'un carré assez grand de 2×2 mailles du réseau, qui contient en son centre un point non éliminé par les coupes ;

- si n est de la forme $2p_m$, n vérifie trivialement la conjecture de Goldbach, on n'a pas besoin de se préoccuper de ce cas ;

- si n est de la forme $2p_m^k$, on ne sait pas quoi faire...

En admettant que l'existence d'un point au moins puisse être assurée selon le raisonnement présenté ci-dessus, on est confronté à un autre problème : le point dont on a pu prouver l'existence pourrait ne pas être compris entre $\sqrt{n}$ et $n/2$. Il nous faudrait être capable de garantir, plutôt que l'existence d'un seul point, l'existence d'une chaîne complète non coupée de points successifs en progression arithmétique, cette chaîne devant être assez longue pour contenir un point au moins qui soit compris entre $\sqrt{n}$ et $n/2$.

Dit autrement, on comprend bien que les "hyperplans de coupe" font perdre la propriété de convexité de l'ensemble des points intérieurs du réseau de Minkowski, alors que cette propriété de convexité des parties "entre" les plans de coupe, en apportant l'existence de chaînes de nombres successifs en progression arithmétique suffisamment longues, pourrait nous garantir de trouver un nombre aussi petit que désiré (i.e. $\leq n/2$).

Étudions deux directions de coupe et combinons-les pour comprendre plus précisément encore le processus de criblage par élimination d'hyperplans : dans la direction correspondant au nombre premier 5, on a 5 droites possibles, correspondant aux $5k$, aux $5k+1$, aux $5k+2$, aux $5k+3$, aux $5k+4$.

Si 5 divise n, on n'aura que l'hyperplan bord (contenant l'origine) à éliminer. On aura alors 4 points du réseau successifs qui seront restés contigus (non séparés par un plan de coupe) selon la direction 5.

Si 5 ne divise pas n, on aura l'hyperplan bord à éliminer ainsi que l'un des autres hyperplans. On se retrouvera alors soit avec 3 points non séparés par le plan de coupe, le plan de coupe étant collé au plan bord (nombres $5k+1$) ou opposé au plan bord (nombres $5k+4$) , soit avec 1 point tout seul et 2 points contigus de part et d'autre du plan de coupe (plan de coupe $5k+2$), soit l'inverse (plan de coupe $5k+3$). Modulo 7, un raisonnement similaire amène aux contiguités possibles de points non séparés par des plans de coupe suivantes 6, 5, 4+1 ou 1+4 et 2+3 ou 3+2.

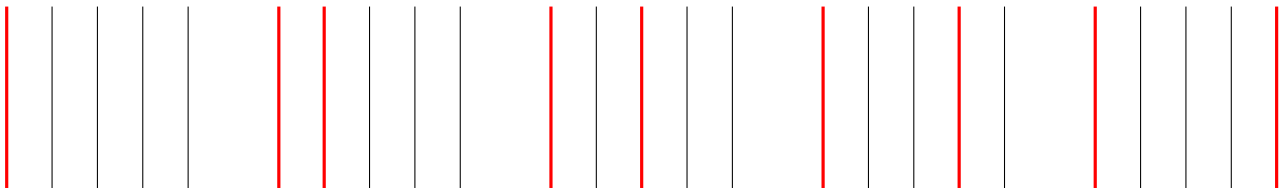


Figure 4 : les 5 positions possibles pour les 2 hyperplans (éventuellement confondus) $x \equiv 0 \pmod 5$ et $x \equiv n \pmod 5$; ils sont colorés en rouge.

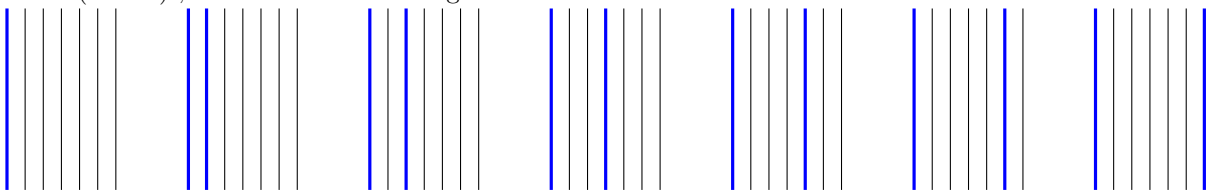
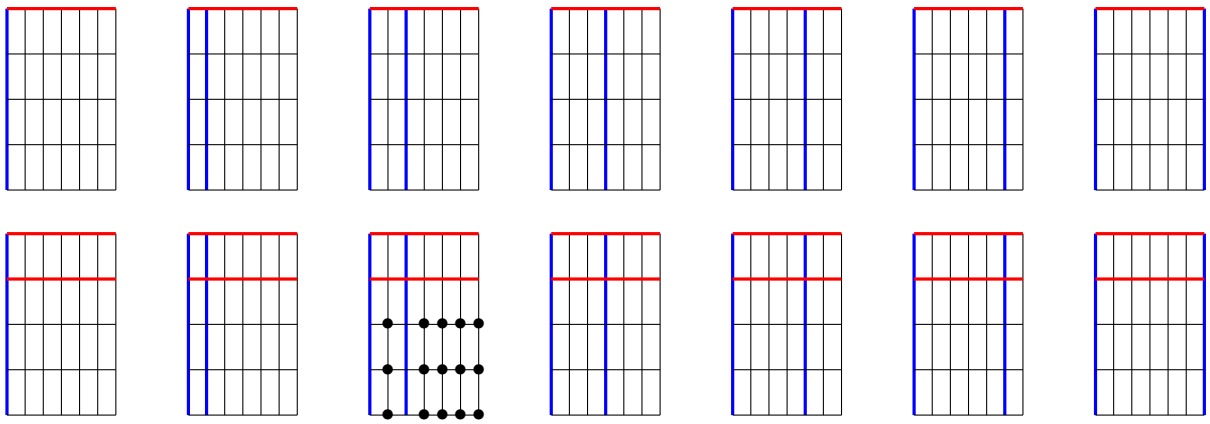


Figure 5 : les 7 positions possibles pour les 2 hyperplans (éventuellement confondus) $x \equiv 0 \pmod 7$ et $x \equiv n \pmod 7$; ils sont colorés en bleu.

En combinant les possibilités pour les plans de coupe selon 5 et 7 ci-dessus, on obtient 35 possibilités de "rectangles" modulo 5 et 7 dont les contiguités sont notées ci-dessous. Pour ne pas surcharger les dessins, pour deux grilles seulement, on a noté par des symboles • les points qui ne sont pas éliminés par les plans de coupe.



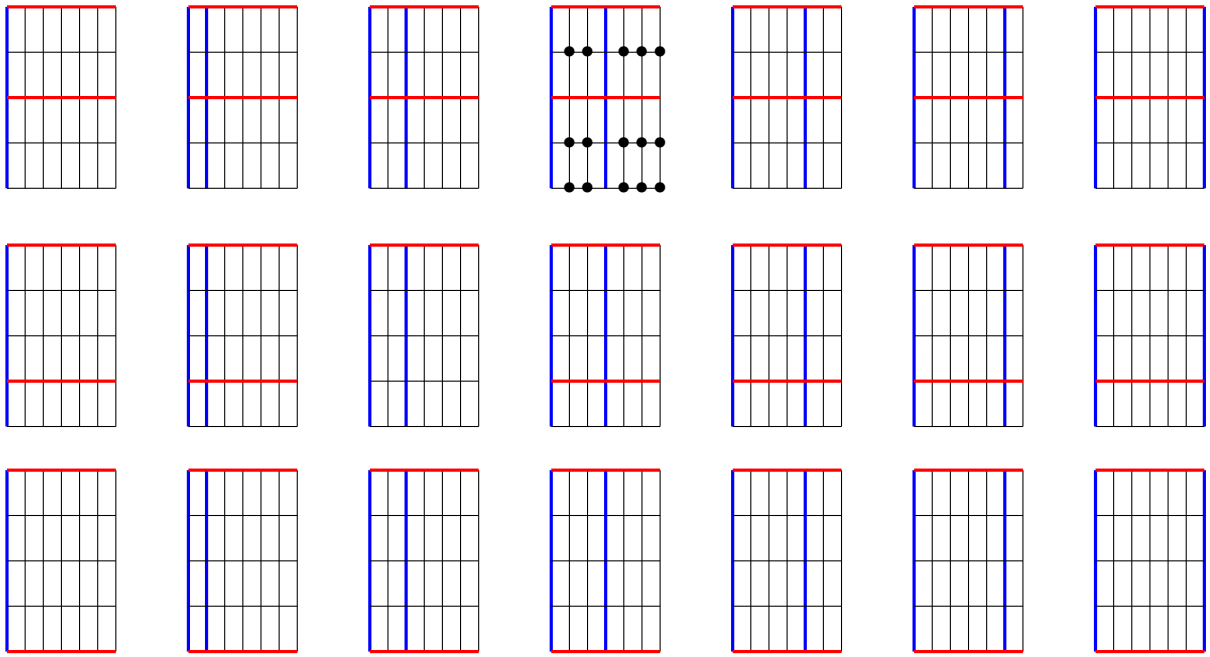


Figure 6 : les 35 positions possibles pour les hyperplans modulo 5 et 7.

On comprend à l'étude de ces cas particulier que les chaînes de longueur les plus grandes possibles, contenant des nombres non séparés par des plans de coupe, vont se trouver sur les rectangles de dimension les 2 plus grands diviseurs de n. En effet, pour les diviseurs en question, le seul hyperplan coupé est celui contenant l'origine et donc une chaîne de nombres "non séparés" d'un tel plan est au moins de longueur $\max\{p_k \text{ tel que } p_k|n\} - 1$.

On comprend également que, selon la direction d'un nombre premier p_k, dans les rectangles dont l'un des côtés est de longueur p_k, quel que soit la position du plan de coupe contenant n (i.e. que ce plan de coupe supprime les nombres de reste modulaire 1, 2, ..., ou $p_k - 1$ modulo p_k), on aura, d'un côté ou de l'autre de ce plan de coupe, des chaînes de longueur $\dfrac{p_k - 1}{2}$ dont la longueur sera maximum sur le rectangle considéré.

On ne sait pas pourquoi une telle longueur pourrait permettre de forcément atteindre un nombre compris entre 3 et $n/2$, qui est l'intervalle que l'on vise pour trouver un décomposant de Goldbach.

Référence

[1] Denise Vella-Chemla, Réécrire, 2019, http://denisevellachemla.eu/jade1.pdf.

Décomposants de Goldbach et géométrie des nombres

Denise Vella-Chemla

26 février 2023

1. Présentation de deux exemples pour appréhender la modélisation choisie

On situe le problème de la recherche des décomposants de Goldbach dans la géométrie des nombres de Minkowski. Regardons 2 exemples pour fixer les idées. On cherche les décomposants de Goldbach du nombre 40. On sait que certains d'entre eux, ceux qui sont supérieurs à la racine de 40, s'ils existent, ne sont divisibles par aucun nombre premier inférieur à $\sqrt{40}$ (pour être des nombres premiers) et ne partagent aucune classe de congruence avec 40 selon les modules premiers inférieurs à $\sqrt{40}$ (pour que leur complémentaire soit premier).

On représente les nombres sur un treillis de nombres de Minkowski ainsi : les nombres qui partagent un reste sont sur une même droite. On ne s'intéresse qu'aux restes dans les divisions par 3 ou 5, les deux seuls nombres premiers impairs inférieurs à $\sqrt{40}$. Il y a quelques points multiples car $3\times5 < \frac{n}{2}$.

Voici le treillis des nombres :

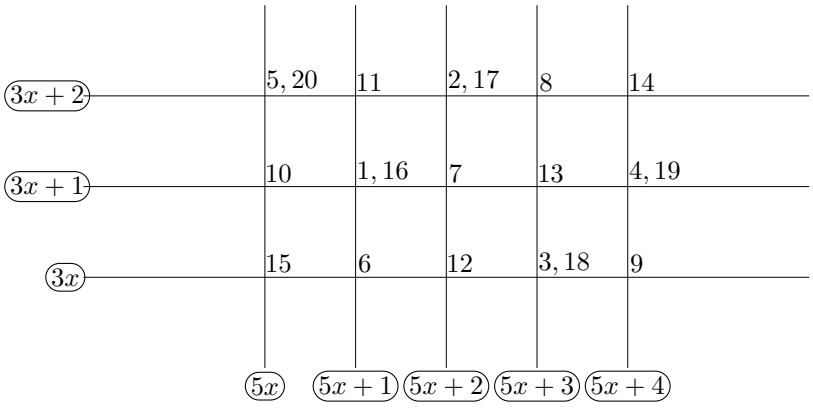


Figure 1 : positionnement des nombres dans un treillis de Minkowski pour illustrer la recherche des décomposants de Goldbach de 40

Les décomposants de Goldbach s'ils existent ne peuvent être sur les deux bords inférieur et gauche du rectangle des nombres étiquetés (nombres divisibles par 3 ou 5) et ne peuvent appartenir à aucune droite à laquelle 40 appartient. La droite éliminée ici est la droite des $3x+1$ ($40 \equiv 1 \pmod 3$).

On symbolise par la couleur les hyperplans (là des droites) éliminés par les congruences de $n = 40$ (on utilise le mélange de couleur vert pour le nombre 10 qui est à la fois un $5k$ et un $3k' + 1$ et le mélange de couleur violet pour le nombre 15 qui est à la fois un $3k$ et un $5k'$).

Voici le treillis des nombres, on a omis la direction correspondant au nombre premier 2, qui aurait permis d'éliminer les nombres pairs, pour éviter d'avoir à passer à la troisième dimension sur ce minuscule exemple, seuls les nombres impairs 11 et 17 n'appartiennent pas aux hyperplans (ici des droites) auxquelles 40 appartient, ainsi qu'aux hyperplans nuls. Ne restent que 11 et 17 qui sont bien les décomposants de Goldbach de 40 supérieurs à $\sqrt{40} = 6, ...$

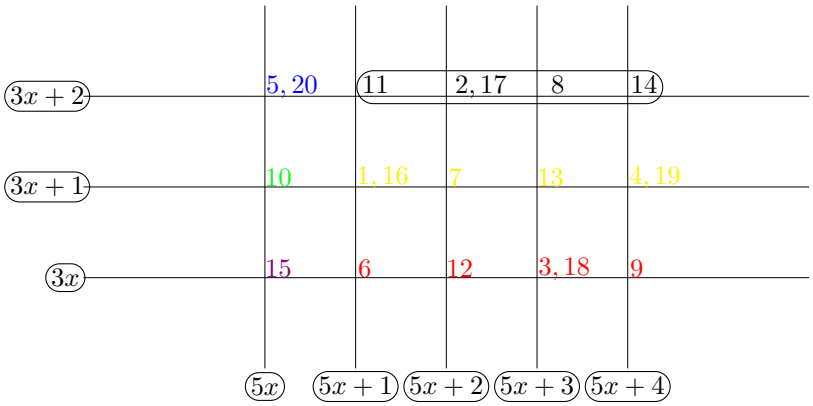


Figure 2 : décomposants de Goldbach de $n = 40$ en noir

Pour $n = 98$, on n'a plus de points multiples car $3 \times 5 \times 7 > \frac{n}{2}$. Pour des raisons de lisibilité, les nombres qui sont aux points entiers d'un réseau parallélépipède rectangle ont été représentés en séparant les différents "étages de l'immeuble" (les plans à troisième coordonnée constante, cette troisième coordonnée étant le reste modulaire d'un nombre selon le module 7). Les segments des hyperplans (ici des plans) auxquels 98 appartient ont été notés en rouge.

Les décomposants de Goldbach de 98 ne partagent aucun plan avec lui et ne peuvent appartenir aux "plans bords" qui contiennent les nombres divisibles par 3, 5 ou 7.

On imagine aisément comment le problème se généralise à un polytope de $\mathbb{Z}^d$ avec d le nombre de nombres premiers inférieurs à $\sqrt{n}$.
Le problème de la recherche d'un décomposant de Goldbach de n un nombre pair, qui soit supérieur à $\sqrt{n}$ s'est transformé en la recherche d'un point dans la grille de nombres de Minkowski :

> *n étant associé à un point de la grille des nombres, un décomposant de Goldbach de n, supérieur à $\sqrt{n}$, est un autre point D ($D \neq 1$ et de $D \neq n-1$) de la grille tel que D n'a aucune coordonnée nulle et D et n ont toutes leurs coordonnées différentes 2 à 2 (comme dans les exemples présentés, on a omis le module 2, il est également nécessaire que D soit impair et différent de 1 ou $n-1$).*

2. Détour par le premier chapitre du roman "Le Spectre d'Atacama" de Danye Chéreau, Alain Connes et Jacques Dixmier, 2018[1]

On résume ce qui nous intéresse ici dans le chapitre en question par la formule du nombre de cassures nécessaires pour couper une tablette de chocolat(de taille $m \times n$ en carrés de chocolat individuels ; ce nombre de cassures est égal à $nm - 1$. Voir l'extrait du chapitre en annexe.

[1] légèrement modifié.

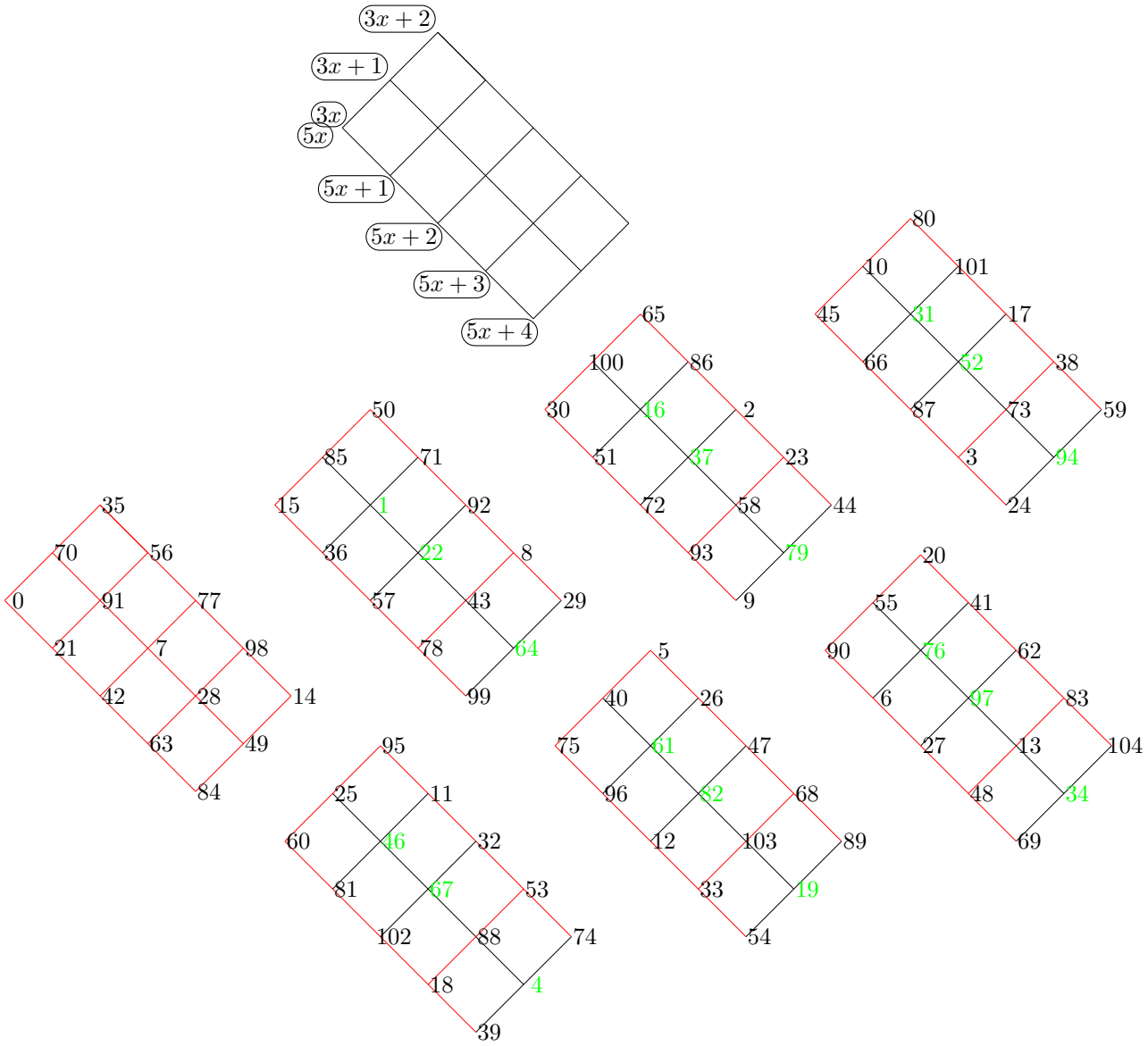


Figure 3 : en vert, nombres restant dans le treillis une fois éliminés :

- les nombres de reste nul dans une division par 3 (lignes rouges en bords inférieurs des étages du treillis),
- les nombres de reste nul dans une division par 5 (lignes rouges en bords gauches des étages du treillis),
- les nombres de reste nul dans une division par 7 (lignes rouges dans toute la "plaque" des $7x$),
- les nombres de reste identique au reste de 98 dans une division par 3 (lignes rouges $3x+2$ à chaque étage),
- les nombres de reste identique au reste de 98 dans une division par 5 (lignes rouges $5x+3$ à chaque étage),
- les nombres de reste identique au reste de 98 dans une division par 7 (déjà éliminés : lignes rouges dans toute la "plaque" des $7x$).

3. Retour au problème de la recherche des décomposants de Goldbach de n supérieurs à $\sqrt{n}$, vus comme les points intérieurs d'un treillis de Minkowski

On a vu que les décomposants de Goldbach sont les points intérieurs des régions obtenues en effec-

tuant au maximum deux cassures par direction[2], chaque direction correspondant à l'un des nombres premiers inférieurs à $\sqrt{n}$. Pour que les cassures correspondant au reste 0 selon tout module soient bien des cassures "dénombrables" (et non pas des bords, que l'on ne casse pas), on considère des parallélépipèdes dont les faces sont des rectangles de taille $(p_i+1)(p_j+1)$ avec p_i, p_j deux nombres premiers inférieurs à $\sqrt{n}$.

En généralisant l'exercice qu'Armand Lafforêt propose à la passagère de l'avion dans la section 2 à la dimension k, on a que la taille de la k-tablette (avec $k = \pi(\sqrt{n})$) est

$$\prod_{\substack{p_i \text{ premier} \\ p_i \leq \sqrt{n}}} (p_i + 1)$$

et que le nombre de cassures nécessaire pour, en fin de processus, n'avoir plus que des unités (i.e. ne plus avoir aucun point intérieur, à un croisement du maillage de Minkowski) est égal à

$$A = \prod_{\substack{p_i \text{ premier} \\ p_i \leq \sqrt{n}}} (p_i + 1) - 1.$$

Or le nombre de cassures maximum pour ne conserver que des décomposants de Goldbach de n supérieurs à $\sqrt{n}$ est égal à $B = 2 \times (\pi(\sqrt{n}) - 1)$ avec $\pi(x)$ la notation habituelle pour le nombre de nombres premiers inférieurs ou égaux à x.

Voyons dans un tableau les valeurs de A et B pour n allant du carré d'un nombre premier au carré du nombre premier suivant.

n	$k = \lfloor \sqrt{n} \rfloor$	$\pi(k) - 1$	$B = 2(\pi(k) - 1)$	$A = \prod_{\substack{p_i \text{ premier} \\ p_i \leq \sqrt{n}}} (p_i + 1) - 1$
de 10 à 24	3	1	2	$4 - 1 = 3$
de 26 à 48	5	2	4	$4 \times 6 - 1 = 23$
de 50 à 120	7	3	6	$4 \times 6 \times 8 - 1 = 191$
de 122 à 168	11	4	8	$4 \times 6 \times 8 \times 12 - 1 = 2304$
de 170 à 288	13	5	10	$4 \times 6 \times 8 \times 12 \times 14 - 1 = 32255$

Il y a ainsi de plus en plus de points de croisements du maillage qui ne sont pas "cassés", et qui, s'ils sont impairs, différents de 1 ou $n-1$ et inférieurs à $n/2$, sont autant de décomposants de Goldbach des nombres pairs considérés, ces points de croisements du maillage ayant été obtenus après avoir effectué deux cassures par direction, pour chaque direction correspondant à un nombre premier impair inférieur à $\sqrt{n}$.

On ne sait pas comment démontrer que l'un au moins des points qui n'étaient pas sur l'une des cassures (cassures pour éliminer les nombres de la forme $p_k \times x$ avec p_k un nombre premier inférieur ou égal à $\sqrt{n}$ - qui sont donc des nombres composés - et cassures pour éliminer les nombres appartenant à l'une des droites auxquelles n appartient - ces nombres ont leur complémentaire à n qui

[2]Pour la démonstration, se reporter à http://denise.vella.chemla.free.fr/jade1.pdf.

est composé) est forcément différent de 1, et est différent de $n-1$ et est inférieur à $n/2$, ce qui en fait un décomposant de Goldbach de n.

4. Ajout : la jolie multiplication par 16

On cherche dans ce treillis de taille $3 \times 5 \times 7$ une opération qui "fixerait" les $3k+1$ sur leur "ligne de nage" (en fait leur plan vertical ici), ainsi que les $5x+1$, les $5x+2$, les $5x+4$ dans leur couloir ou les $7x$ dans leur plan. On prend la multiplication par 16 (qui transforme un $7x$ en $7x$, un $3x+1$ en $3x'+1$, etc., dans la mesure où 16 est congru à l'unité mod 3 et 5). Cette multiplication par 16 transforme le triangle (64, 79, 4) en lui-même, ou bien son triangle symétrique (34, 19, 94) en lui-même en leur faisant subir une rotation de leurs sommets dans l'ordre énoncé. Il nous faudrait un argument qui assurerait l'existence d'un point (non congru à 0, non congru à n) sous prétexte qu'il serait fixe dans ce genre de transformation mais on n'arrive pas à trouver un tel argument (cf la démonstration de Don Zagier pour les nombres premiers $4k+1$ sommes de deux carrés).

On dessine cette multiplication par 16 "en petit", ci-dessous : elle laisse invariants les triangles (34, 19, 94), (64, 79, 4) mais également le triangle (31,76,61) ou le triangle (37,67,22). On a positionné dans ces triangles les décomposants qui interviennent dans les 3 décompositions de Goldbach de 98, $19+79 = 31+67 = 37+61$. Ils sont ainsi tous fixes par multiplication par 16^3. Malgré la découverte de ces transformations de triangles qui a été guidée par une intuition géométrique très classique, on n'a toujours pas l'argument qui assure l'existence d'un décomposant de Goldbach au moins.

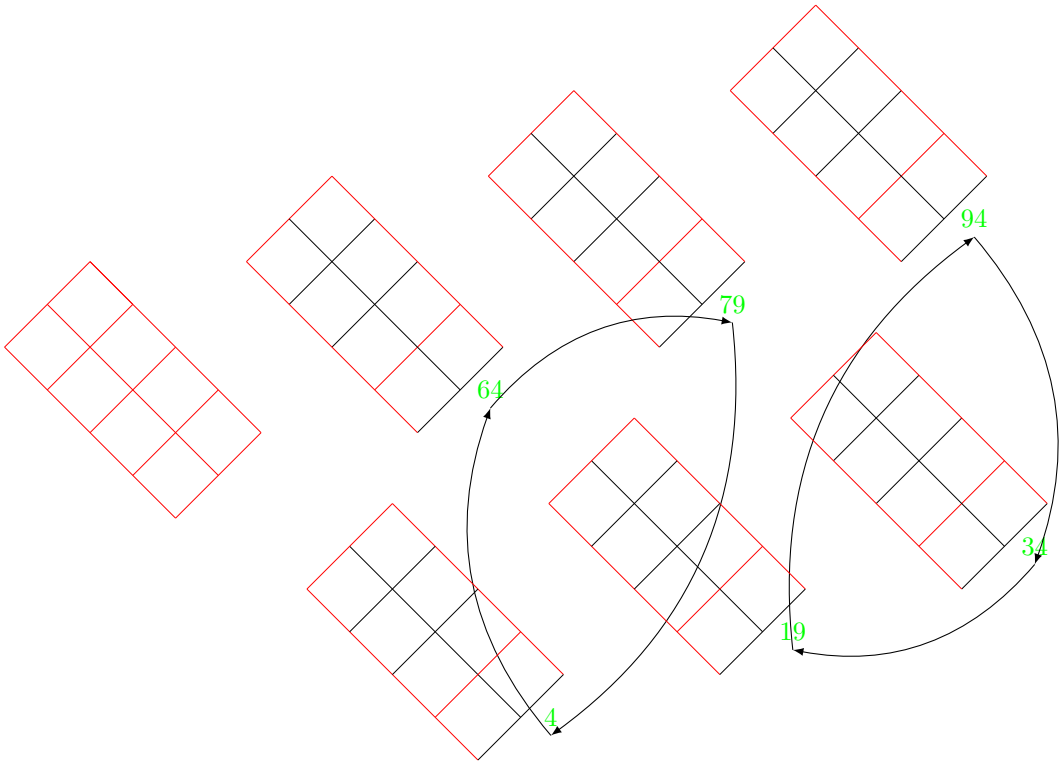


Figure 4 : deux petits triangles fixes par multiplication par 16.

Annexe : extrait du premier chapitre du roman "Le Spectre d'Atacama" de Danye Chéreau, Alain Connes et Jacques Dixmier, 2018[3]

- Votre tablette de chocolat, par exemple, pourrait m'aider à vous donner un avant-goût des maths. Supposez que je vous demande le nombre de cassures nécessaire pour découper la tablette en carrés de chocolat individuels.

Armand laisse sa voisine contempler sa tablette puis se mettre à couper une rangée de quatre carreaux. Et là elle s'amuse à réduire sa rangée en petits carreaux, mais reste perplexe.

- J'ai expérimenté avec une rangée de quatre carreaux, et j'ai constaté qu'il suffisait de trois cassures, dit-elle en lui tendant une nouvelle rangée.

- Effectivement. Si je prends cette rangée de quatre carreaux, dit-il joignant le geste à la parole, on voit qu'il suffit de trois cassures, mais on s'aperçoit aussi que, de toute façon, il faut toujours exactement trois cassures pour réduire une rangée de 4 carreaux en 4 carreaux individuels.

- Oui. Mais pour ma grande tablette en entier ?

- Si vous me permettez, je peux essayer de vous guider. Votre tablette est de longueur 6 et de largeur 4, et il est plus difficile de réfléchir au problème dans ce cas particulier que dans le cas général où longueur et largeur peuvent être choisies à loisir.

- D'accord. Si je comprends bien, vous me proposez de remplacer un problème particulier par de nombreux autres ? Je suis désolée, mais en quoi cela va-t-il être plus facile ?

- L'intérêt d'avoir généralisé le problème initial, c'est que l'on peut maintenant prendre des tablettes plus simples, et c'est exactement le geste que vous avez fait en prenant une rangée de quatre carreaux. Manifestement vous avez compris ce qui se passe pour une tablette d'une seule rangée.

Elle fait un nouvel essai, puis réfléchit quelques instants.

- Ah oui, cela devient plus clair. Il faudra quatre cassures pour une rangée de cinq carreaux. Et ce sera pareil pour toutes les tablettes avec une seule rangée de carreaux : il faudra une cassure de moins que le nombre de carreaux.

- Très bien, vous comprenez vite. Maintenant je vous laisse réfléchir à ce qui se passe pour une tablette de longueur 2 et de largeur 2. [...] Vous verrez qu'au bout d'un moment, après avoir pris suffisamment d'exemples, vous allez comprendre le cas général.

- Chiche !

- Je préfère ne pas vous donner la réponse tout de suite, car l'un des plaisirs des maths est de chercher et de trouver par soi-même. Divulguer trop tôt la réponse gâche le plaisir. La gourmande est ravie. Ses yeux brillent. L'envie de chercher la saisit. Il la laisse se concentrer sur le reste de sa tablette. [...]

[3] légèrement modifié.

- J'ai bien essayé toutes les manières de découper une tablette carrée de quatre carreaux, je constate qu'il faut toujours trois cassures. J'ai aussi essayé avec une tablette rectangulaire de trois carreaux par deux, ce qui fait six carreaux au total : il faut alors cinq cassures.

- Quelle intuition avez-vous à ce stade ?

- Eh bien, avec quatre carreaux il faut toujours trois cassures, quelle que soit la configuration des carreaux, avec cinq carreaux il faut quatre cassures, avec six carreaux c'est cinq. J'aurais donc tendance à dire que le nombre de cassures est égal au nombre de carreaux moins un, mais je ne vois pas trop comment en être sûre dans tous les cas.

- Effectivement, reprend Armand, le mathématicien fait ici une constatation : dans tous ces exemples, le nombre de cassures est indépendant de la manière de procéder et est égal au nombre de carreaux moins un.
  Voici comment il démontre que cela reste vrai dans le cas général : il va avancer comme on gravit une échelle. Il fait l'hypothèse que sa constatation est vraie, d'un point de vue mathématique, pour toutes les tablettes dont la taille, c'est-à-dire le nombre de carreaux, est plus petite que le nombre d'échelons, de marches, qu'il vient de gravir.

- Si je vous suis, j'ai atteint la sixième marche, puisque j'ai essayé toutes les tablettes jusqu'à six carreaux.

- Exactement. Et je vais vous expliquer comment on peut toujours passer à la marche suivante. Imaginons une tablette légèrement plus grande. Nous allons la casser en deux parties, peu importe où. Comme on a franchi les marches précédentes, on sait que pour chacune de ces deux parties le nombre de cassures est égal au nombre de carreaux moins un.

- Et si je vous suis toujours, on sait aussi que cela est vrai quelle que soit la manière de procéder dans chacune des deux parties.

- Oui! Récapitulons. La tablette initiale peut se voir comme la réunion des deux parties que nous avons séparées. Des cassures, il en faut donc le nombre de carreaux de la première partie moins 1 plus le nombre de carreaux de la deuxième partie moins 1, ce qui nous donne la somme du nombre de carreaux de chacune des parties moins 2. Or la somme du nombre de carreaux de chacune des parties n'est autre que le nombre total de carreaux de la tablette initiale. Mais n'oublions pas que nous avons au départ cassé la tablette en deux. Il faut donc ajouter cette première cassure au décompte, et là où nous soustrayions 2, nous ne devons donc plus retirer que 1. Finalement, on arrive ainsi au résultat final : il faut une cassure de moins que le nombre de carreaux de la tablette de départ. Cette manière de procéder en gravissant un à un les échelons est une méthode générale de démonstration qui s'appelle la récurrence.

- C'est fascinant. Mais il va quand même falloir que je joue avec ce truc de l'échelle pour me l'approprier.

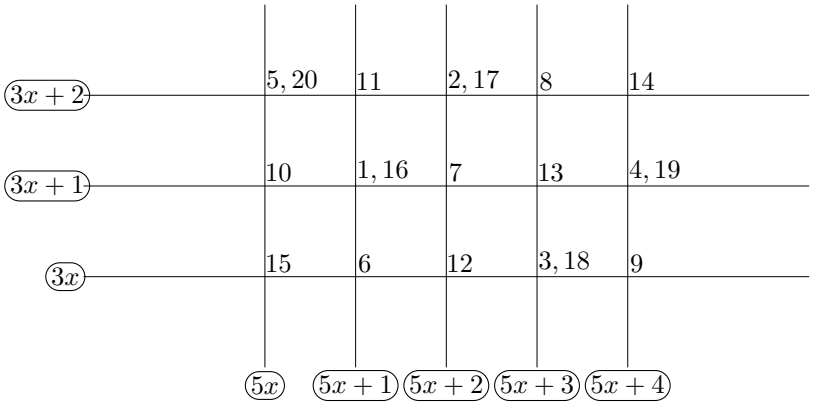
- Cet exemple illustre la démarche du mathématicien. Un problème peut paraître compliqué à première vue, mais lorsqu'on a le bon point de vue, lorsqu'on pense juste, on arrive au résultat presque sans effort. On sait que pour votre tablette de longueur 6 et de largeur 4, il faudra toujours 23 cassures !

Décomposants de Goldbach et géométrie des nombres (Denise Vella-Chemla, février 2023)

On situe le problème de la recherche des décomposants de Goldbach dans la géométrie des nombres de Minkowski. Regardons 2 exemples pour fixer les idées. On cherche les décomposants de Goldbach du nombre 40. On sait que certains d'entre eux, ceux qui sont supérieurs à la racine de 40, s'ils existent, ne sont divisibles par aucun nombre premier inférieur à $\sqrt{40}$ (pour être des nombres premiers) et ne partagent aucune classe de congruence avec 40 selon les modules premiers inférieurs à $\sqrt{40}$ (pour que leur complémentaire soit premier).

On représente les nombres sur un treillis de nombres de Minkowski ainsi : les nombres qui partagent un reste sont sur une même droite. On ne s'intéresse qu'aux restes dans les divisions par 3 ou 5, les deux seuls nombres premiers impairs inférieurs à $\sqrt{40}$. Il y a quelques points multiples car $3\times5 < \frac{n}{2}$.

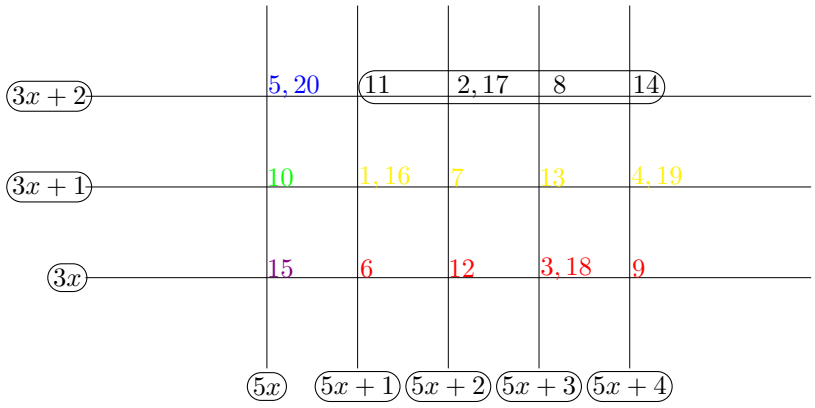
Voici le treillis des nombres :



Les décomposants de Goldbach s'ils existent ne peuvent être sur les deux bords inférieur et gauche du rectangle des nombres étiquetés (nombres divisibles par 3 ou 5) et ne peuvent appartenir à aucune droite à laquelle 40 appartient. La droite éliminée ici est la droite des $3x+1$ ($40 \equiv 1 \pmod 3$).

On symbolise par la couleur les hyperplans (là des droites) éliminés par les congruences de $n = 40$ (on utilise le mélange de couleur vert pour le nombre 10 qui est à la fois un $5k$ et un $3k' + 1$ et le mélange de couleur violet pour le nombre 15 qui est à la fois un $3k$ et un $5k'$).

Voici le treillis des nombres après application des filtres polarisants (on n'a pas utilisé de filtre polarisant pour éliminer les nombres pairs, pour éviter d'avoir à passer à la troisième dimension sur ce minuscule exemple), seuls les nombres impairs 11 et 17 n'ont pas été éliminés par les filtres polarisants qui éliminent les hyperplans (ici les droites) auxquelles 40 appartient. Ne restent que 11 et 17 qui sont bien les décomposants de Goldbach de 40 supérieurs à $\sqrt{40} = 6, ...$



Pour $n = 98$, on n'a plus de points multiples car $3 \times 5 \times 7 > \frac{n}{2}$. Pour des raisons de lisibilité, les nombres qui sont aux points entiers d'un réseau parallélépipède rectangle ont été représentés en séparant les différents "étages de l'immeuble" (les plans à troisième coordonnée constante, cette troisième coordonnée étant le reste modulaire d'un nombre selon le module 7). Les segments des hyperplans (ici des plans) auxquels 98 appartient[1] ont été notés en rouge.

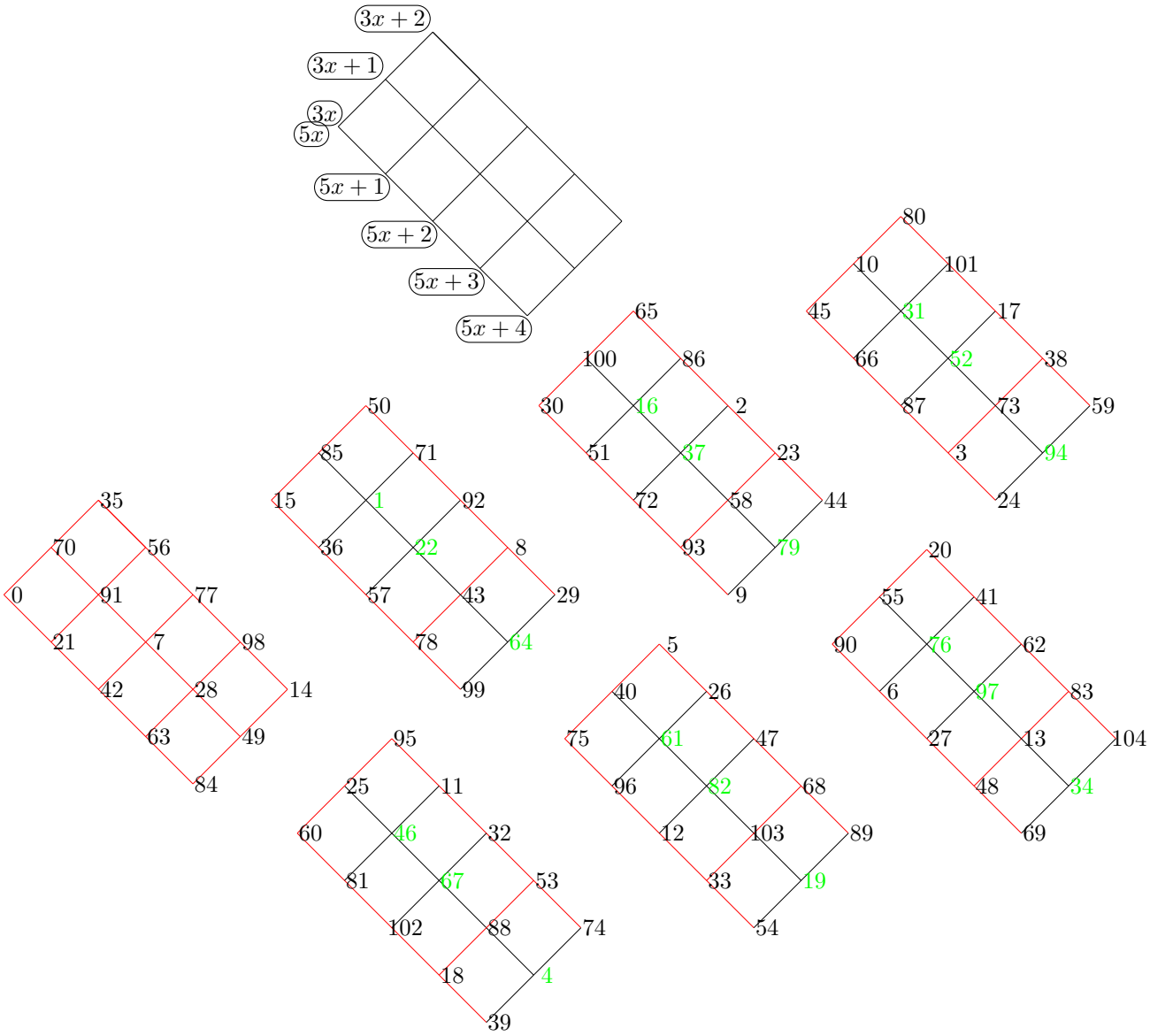
Les décomposants de Goldbach de 98 ne partagent aucun plan avec lui et ne peuvent appartenir aux "plans bords" qui contiennent les nombres divisibles par 3, 5 ou 7.

On imagine aisément comment le problème se généralise à un polytope de $\mathbb{Z}^d$ avec d le nombre de nombres premiers inférieurs à $\sqrt{n}$. L'existence d'au moins un point dans l'espace après élimination des hyperplans auquel n appartient provient sûrement de l'application du théorème de Blichfeldt, qui se situe dans la géométrie des nombres de Minkowski. On ne sait pas s'il est applicable : le fait d'éliminer des plans annihile la convexité du volume obtenu, même si les régions obtenues sont grandes. De plus, une solution doit être inférieure à la moitié du nombre pair considéré et on voit bien que les nombres sont tout mélangés (c'est pour cette raison qu'on ne peut pas appliquer une méthode comme le simplexe qui permettrait de situer les nombres inférieurs à la valeur souhaitée dans un demi-espace, d'un côté ou de l'autre d'un hyperplan).

On se contente de la démonstration probabiliste[2] qui dit que quand on choisit aléatoirement $\prod_{\substack{p_k \text{ premier} \\ p_k \leq \sqrt{n}}} (p_k - 2)$ nombres parmi $\prod_{\substack{p_k \text{ premier} \\ p_k \leq \sqrt{n}}} p_k$ nombres, on est très vite assuré que l'un d'entre eux au moins est inférieur à une valeur fixée (la valeur $\frac{n}{2}$ souhaitée).

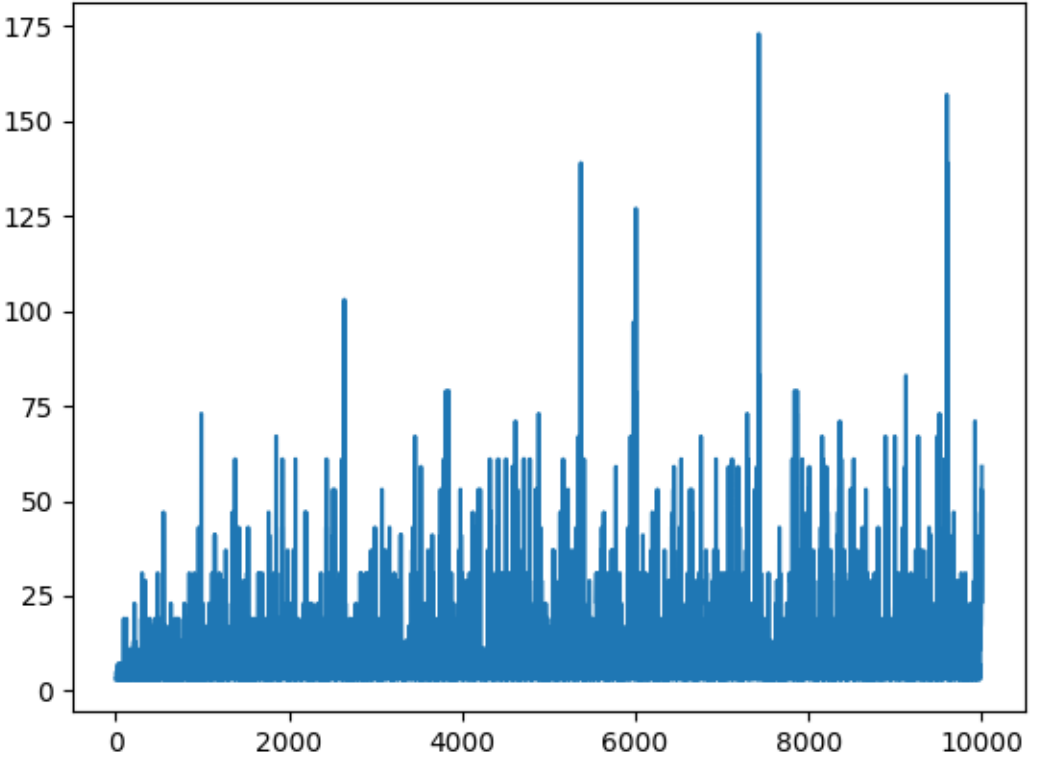
[1] à éliminer, comme par des filtres polarisants en photographie.

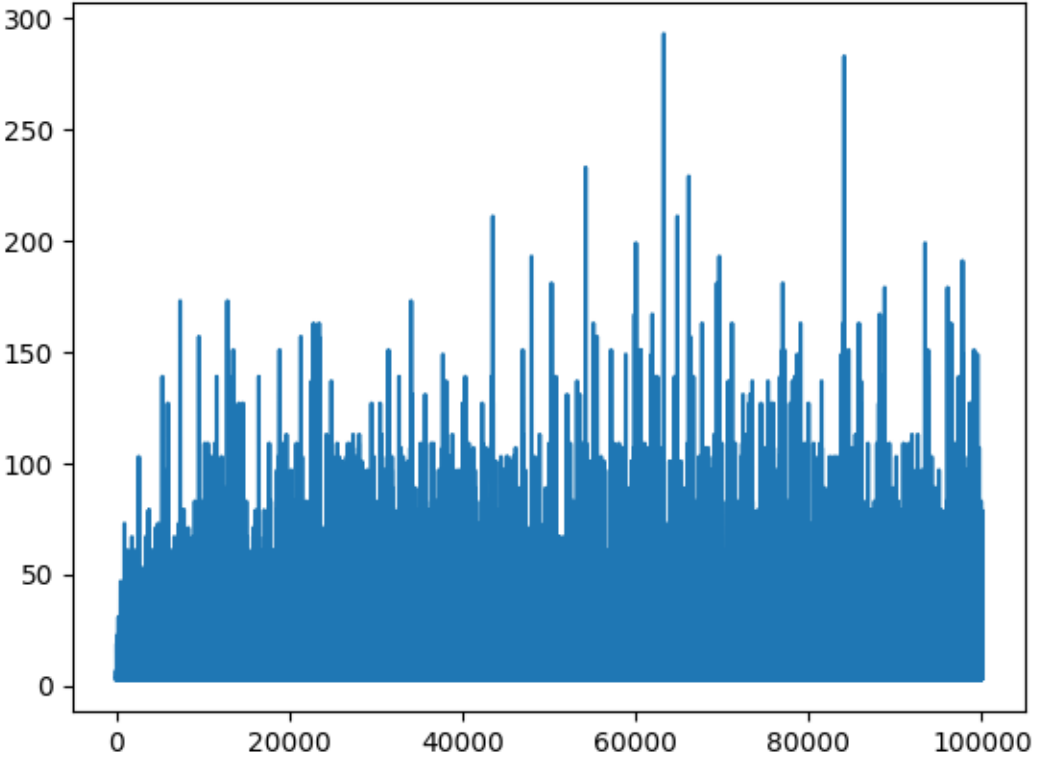
[2] https://hal.science/hal-03750889 (en anglais http://denise.vella.chemla.free.fr/proba-sans-deux-post-en.pdf).

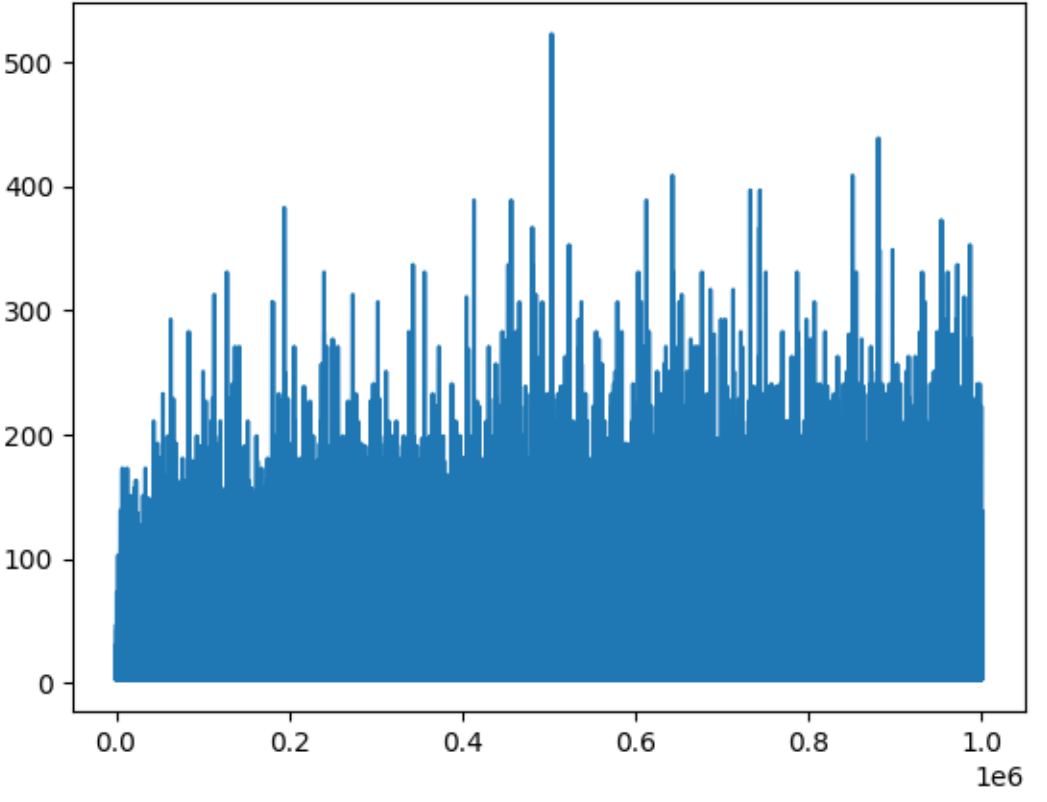


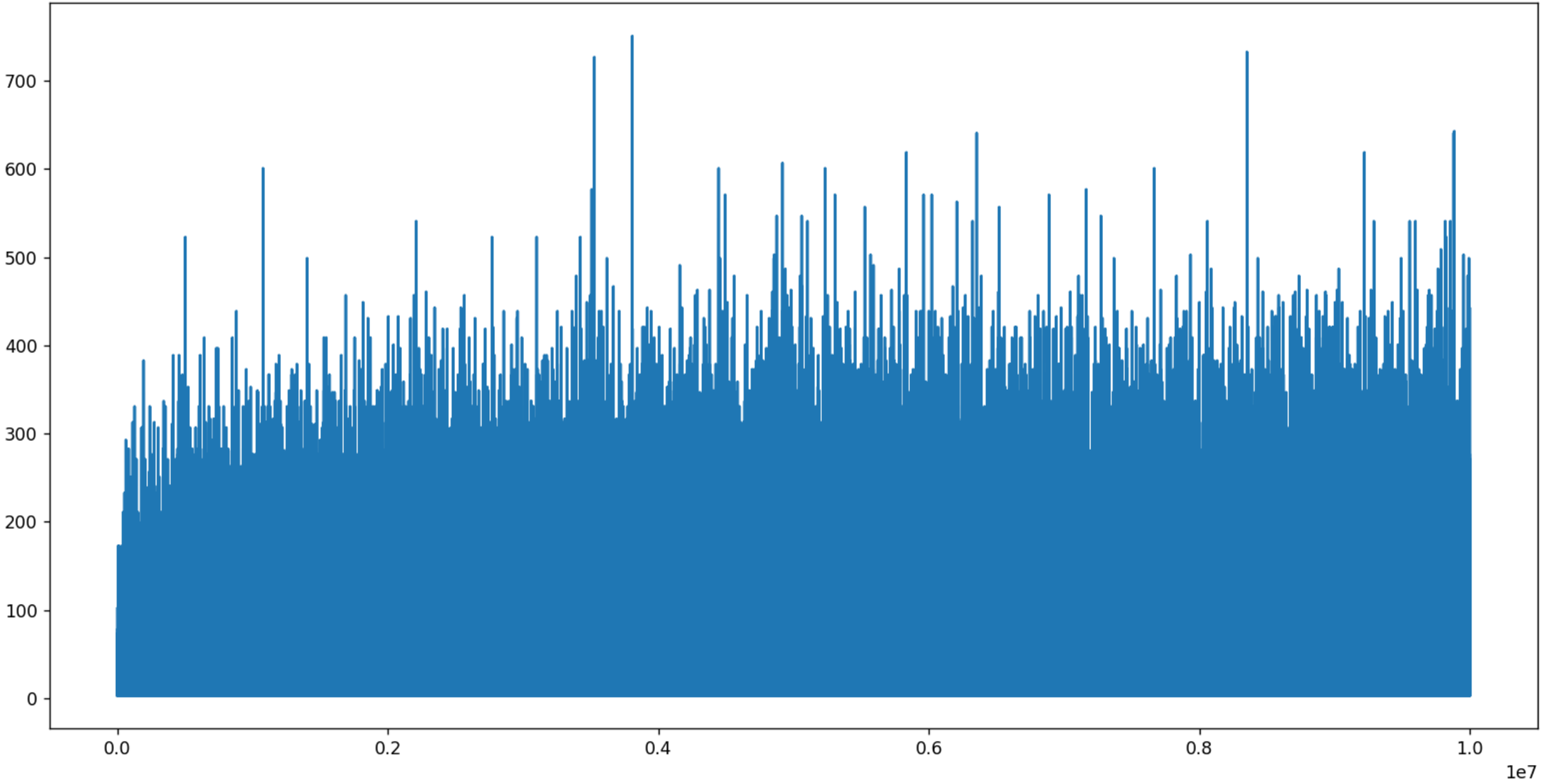
Le problème de la recherche d'un décomposant de Goldbach de n un nombre pair, qui soit supérieur à $\sqrt{n}$ s'est transformé en la recherche d'un point dans la grille de nombres de Minkowski :

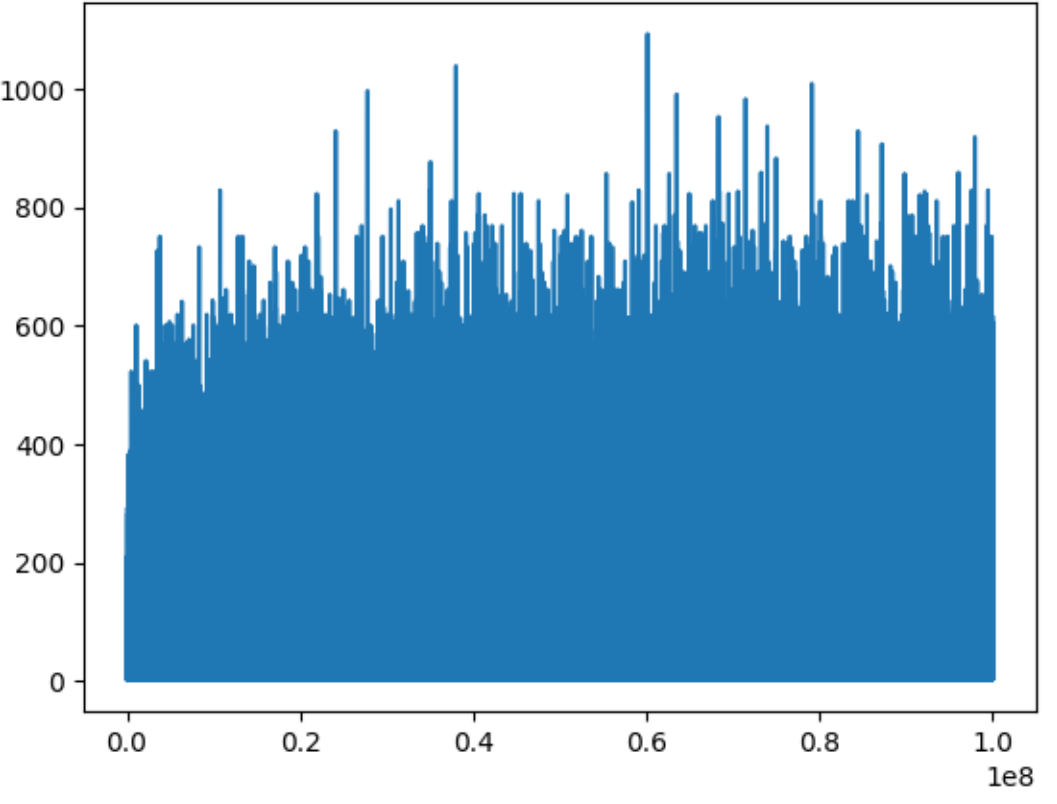
> *n étant associé à un point de la grille des nombres, un décomposant de Goldbach de n, supérieur à $\sqrt{n}$, est un autre point D ($D \neq 1$ et de $D \neq n-1$) de la grille tel que D n'a aucune coordonnée nulle et D et n ont toutes leurs coordonnées différentes 2 à 2.*

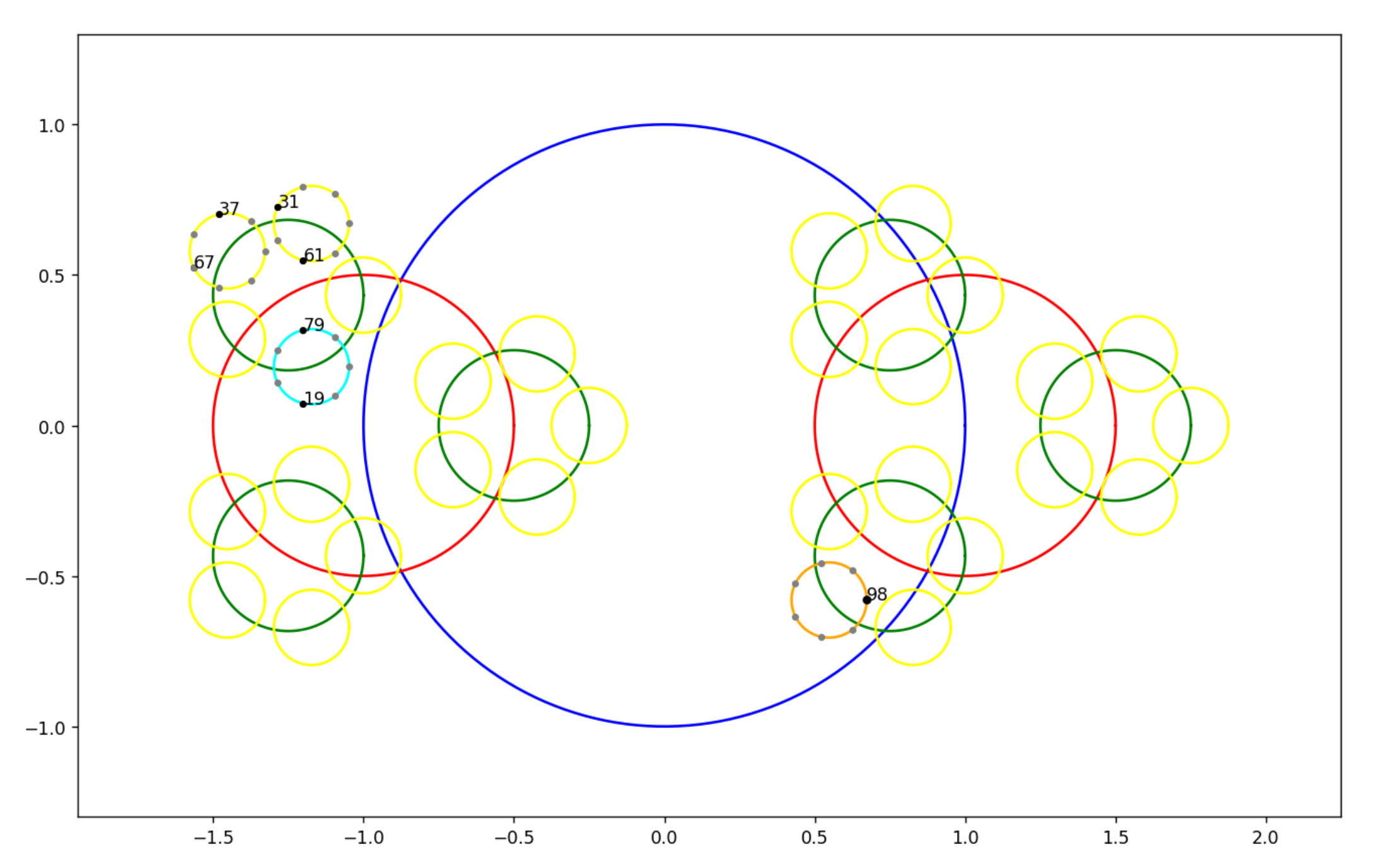

175
150
125
100
75
50
25
0
0
2000
4000
6000
8000
10000

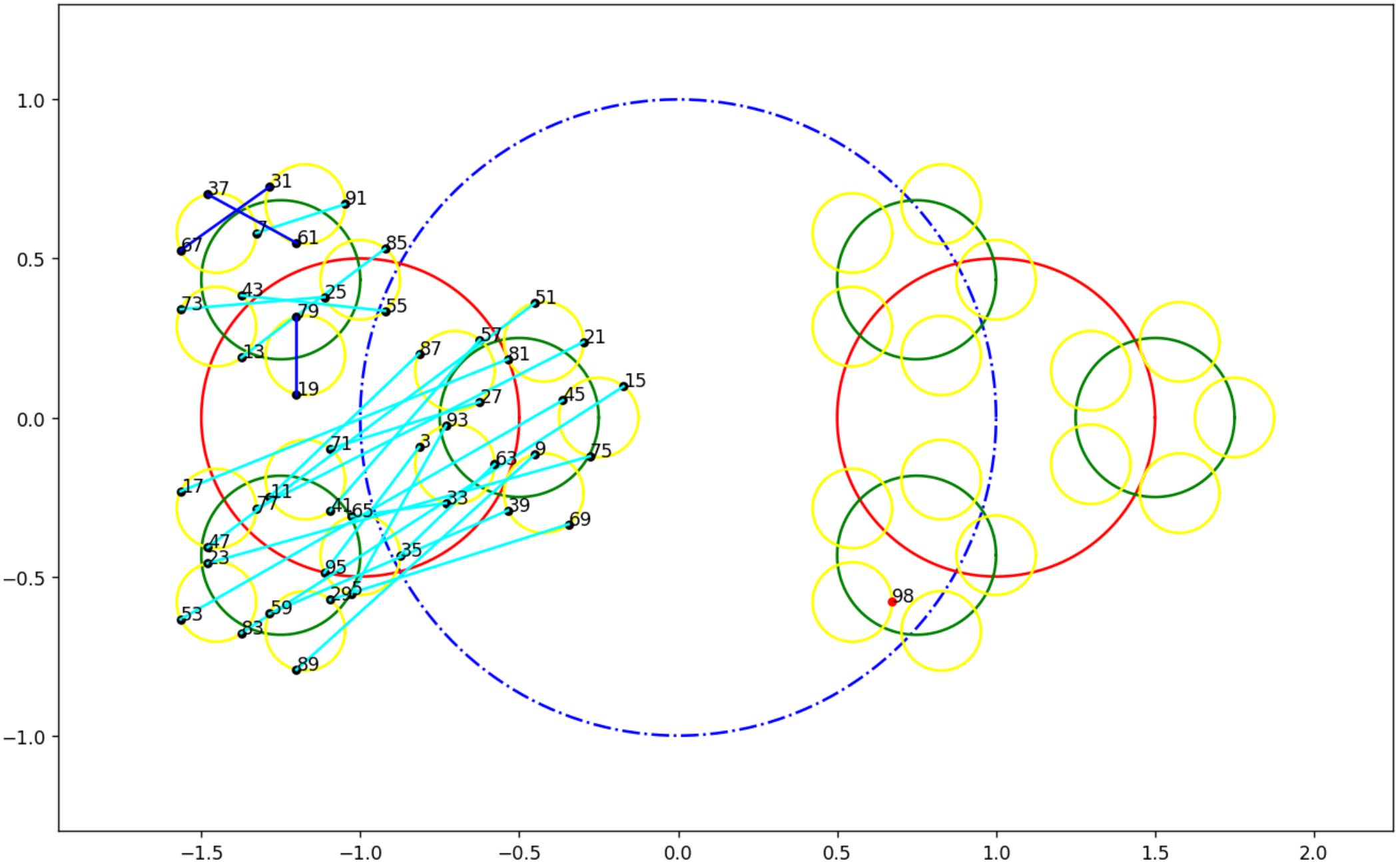

300
250
200
150
100
50
0
0
20000
40000
60000
80000
100000


500
400
300
200
100
0
0.0
0.2
0.4
0.6
0.8
1.0
1e6


700
600
500
400
300
200
100
0
0.0
0.2
0.4
0.6
0.8
1.0
1e7


1000
800
600
400
200
0
0.0
0.2
0.4
0.6
0.8
1.0
1e8


37
31
67
61
79
19
98
1.0
0.5
0.0
−0.5
−1.0
−1.5
−1.0
−0.5
0.0
0.5
1.0
1.5
2.0


1.0
0.5
0.0
−0.5
−1.0
−1.5
−1.0
−0.5
0.0
0.5
1.0
1.5
2.0
37
31
91
7
61
67
85
43
25
73
79
55
51
57
21
87
81
13
19
15
27
45
93
71
3
63
9
75
17
11
77
41
65
33
39
69
47
23
35
95
29
5
59
53
83
89
98

youpi-gamma-python.py - GNU Emacs at DESKTOP-4PROGGL

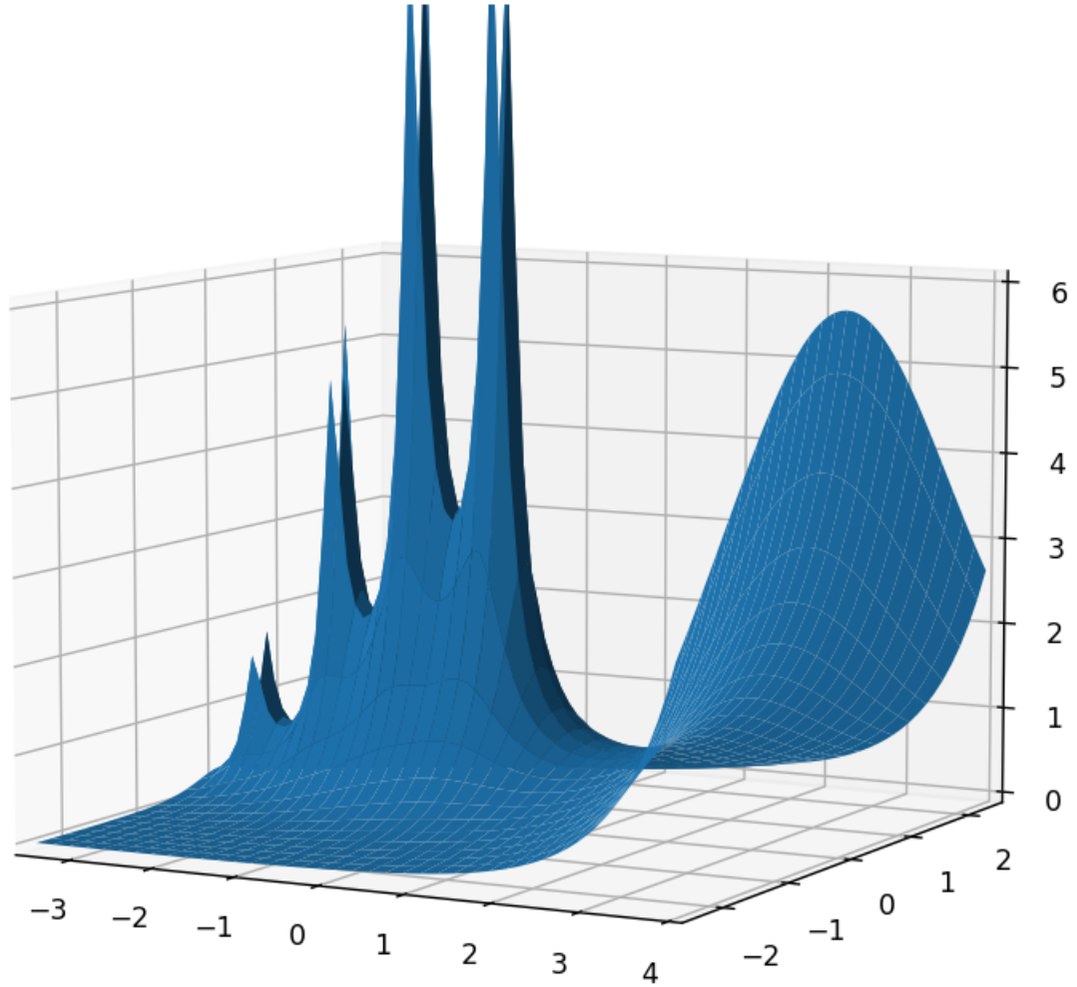
File Edit Options Buffers Tools Python Help

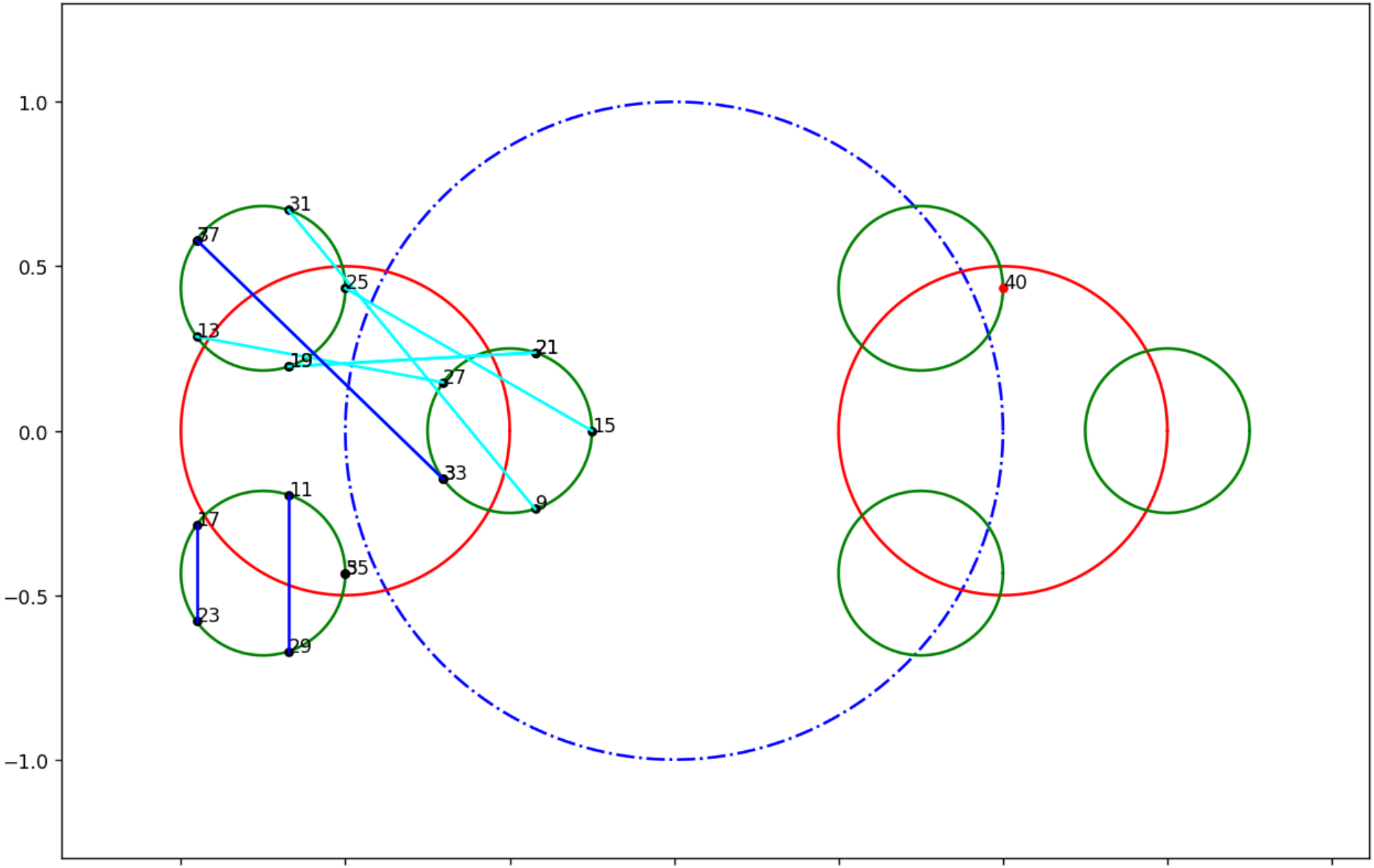
```
from mpl_toolkits.mplot3d import Axes3D
import matplotlib.pyplot as plt
from matplotlib import cm
import numpy as np

fig = plt.figure()
ax = Axes3D(fig)

N=70
theta = -np.pi + (2*np.pi/N) * (0.5 + np.arange(N))
c=-11
r=16
s=0.1
x = np.arange( -3.5, 4+s, s)
y = np.arange(-2.5, 2.5+s, s)
xx, yy = np.meshgrid(x, y)
zz = xx + 1j*yy
gaminv = 0*zz
for k in range(N):
    t = c + r*np.exp(1j*theta[k])
    gaminv += np.exp(t)*(t**(-zz))*(t-c)
gaminv = gaminv/N
gam = 1.0/gaminv
ax = fig.add_subplot(111, projection='3d')
ax.plot_surface(xx,yy, abs(gam))
ax.set_xlim(-3.5,4)
ax.set_ylim(-2.5,2.5)
ax.set_zlim(0,6)
plt.show()
```

-\--- **youpi-gamma-python.py** All L1 (Python El

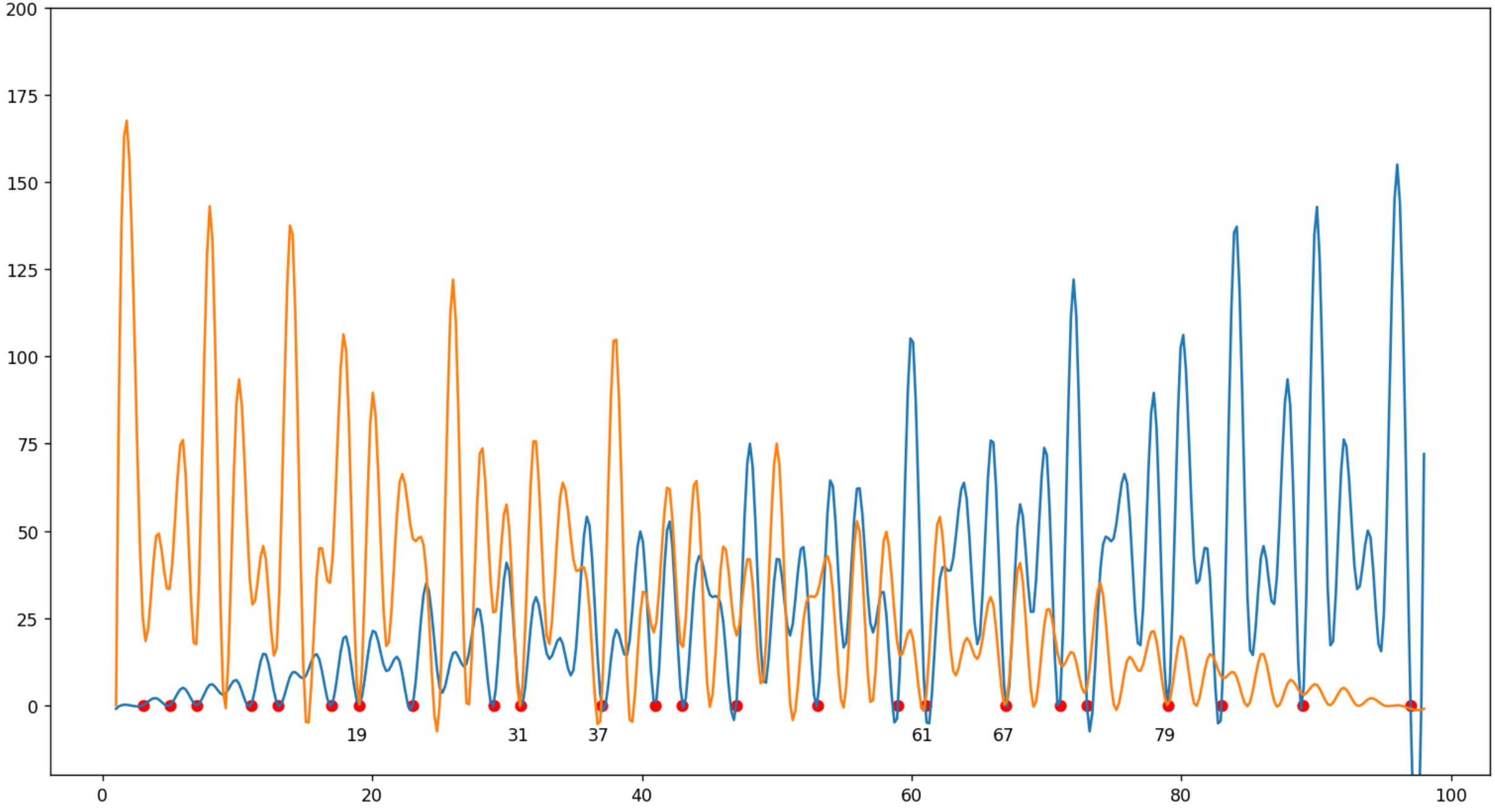
Wrote c:/Users/DENISE 2022/Desktop/youpi-gamma-python

Figure 1




31
37
25
13
19
21
27
15
33
11
9
17
35
23
29
40
1.0
0.5
0.0
−0.5
−1.0
−1.5
−1.0
−0.5
0.0
0.5
1.0
1.5
2.0

```
C:\Users\DENISE_2022\Desktop\conserve-banquet>python3 bodessin26à48.py
3  --> perim =  5.299449151387604 aire =  0.8361734721014444 distmilieu  2.088506694578861 DG.
5  --> perim =  4.358898943540672 aire =  7.177915983922293e-15 distmilieu  2.179449471770332
7  --> perim =  5.299449151387602 aire =  0.8361734721014387 distmilieu  2.0885066945788617
9  --> perim =  4.936769975775583 aire =  0.8978527070498491 distmilieu  1.8107359792910886
11  --> perim =  5.174325755308906 aire =  0.5166010012818898 distmilieu  2.3389792859822323 DG.
13  --> perim =  4.945570679534387 aire =  0.22568376580879224 distmilieu  2.0885066945788617
15  --> perim =  4.18890105931673 aire =  0.4330127018922135 distmilieu  1.6393596310754994
17  --> perim =  5.502637756781938 aire =  0.36034972054872655 distmilieu  2.600682775685266 DG.
19  --> perim =  4.373001009245786 aire =  0.04297380129143002 distmilieu  1.8107359792910895
```


200
175
150
125
100
75
50
25
0
19
31
37
61
67
79
0
20
40
60
80
100

Invite de commandes

```
C:\Users\DENISE_2022\Desktop>
C:\Users\DENISE_2022\Desktop>python3 primes-et-Li.py
50847534  : pi( 1000000000 ) calcul par pgm.
50847517  : pi( 1000000000 ) calcul par formule de Riemann :
                        li(x)-li(2)-0.5*(li(isqrt(x))-li(2)).
erreur entre valeur reelle et valeur par li : -3.2415816729509853e-07
resultat obtenu en  12.327210903167725  s.

C:\Users\DENISE_2022\Desktop>python3 primes-et-Li.py
455052511  : pi( 10000000000 ) calcul par pgm.
455050799  : pi( 10000000000 ) calcul par formule de Riemann :
                        li(x)-li(2)-0.5*(li(isqrt(x))-li(2)).
erreur entre valeur reelle et valeur par li : -3.7618525728499203e-06
resultat obtenu en  166.38413405418396  s.

C:\Users\DENISE_2022\Desktop>
C:\Users\DENISE_2022\Desktop>
```

primes-et-Li.py - GNU Emacs at DESKTOP-4PROGGL

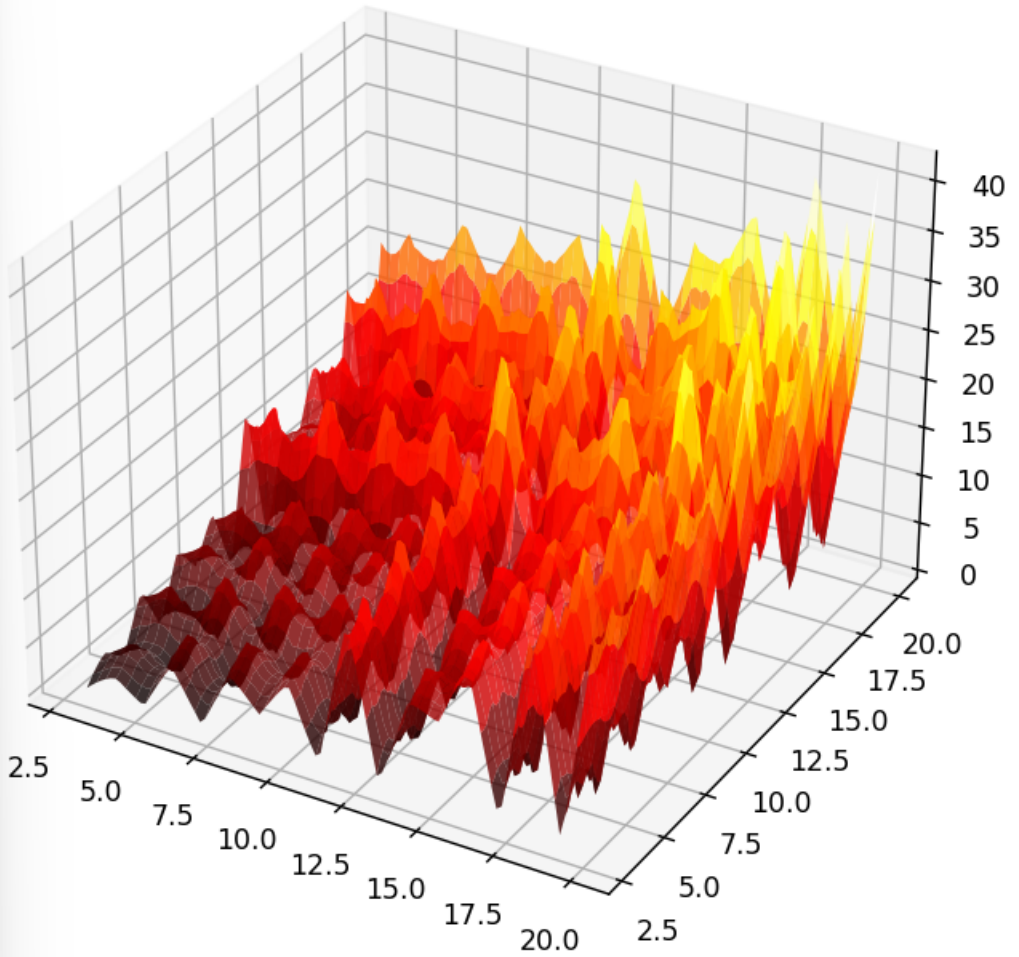
File Edit Options Buffers Tools Python Help

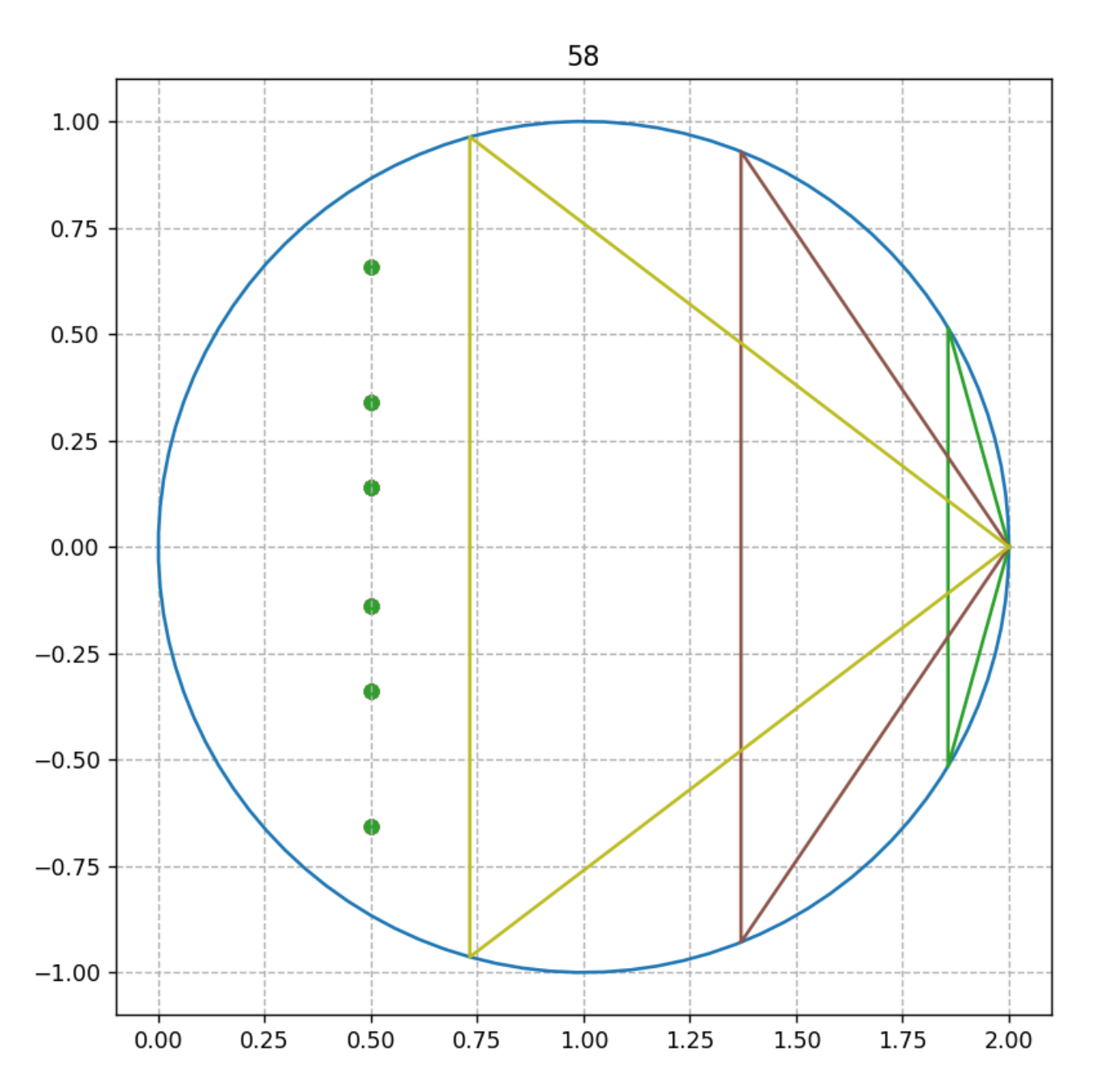
```
import time
import math
from math import isqrt
import numpy as np
import mpmath
from mpmath import *

class Primes():
    def __init__(self, n):
        is_prime = np.full(n, True)
        is_prime[:2] = False
        for p in range(2, math.isqrt(n) + 1):
            if is_prime[p]:
                is_prime[p*p::p] = False
        self.__primes = np.nonzero(is_prime)[0]
    def count(self, x):
        return np.searchsorted(self.__primes, x, side='right')

tic = time.time()
P = Primes(10000000001)
x = 10000000000
res = li(x)-li(2)
a = P.count([x])
print(int(a), ' : pi(',x,') calcul par pgm.')
b = li(isqrt(x))-li(2)
res = res-(1.0/2.0)*b
print(int(res),' : pi(',x,') calcul par formule de Riemann :\n
x)-li(2)-0.5*(li(isqrt(x))-li(2)).')
erreur = float((res-a)/a)
print('erreur entre valeur reelle et valeur par li :', erreur)
tac = time.time()
print('resultat obtenu en ',tac-tic, ' s.')
```

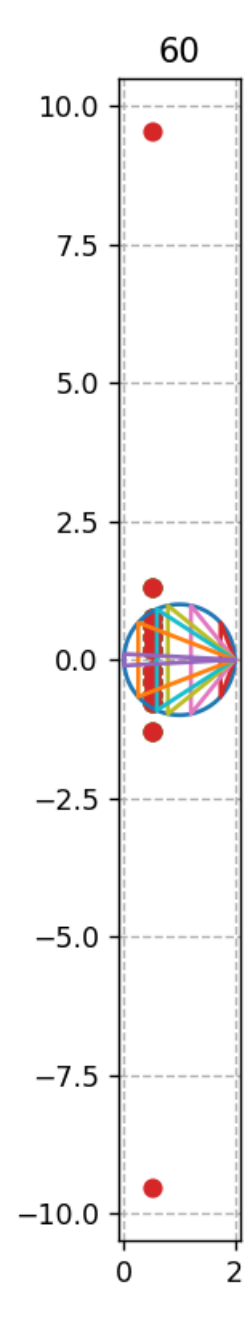
Jacques-interpole-ma-surface.py - GNU Emacs at DESKTOP-4PROGGL

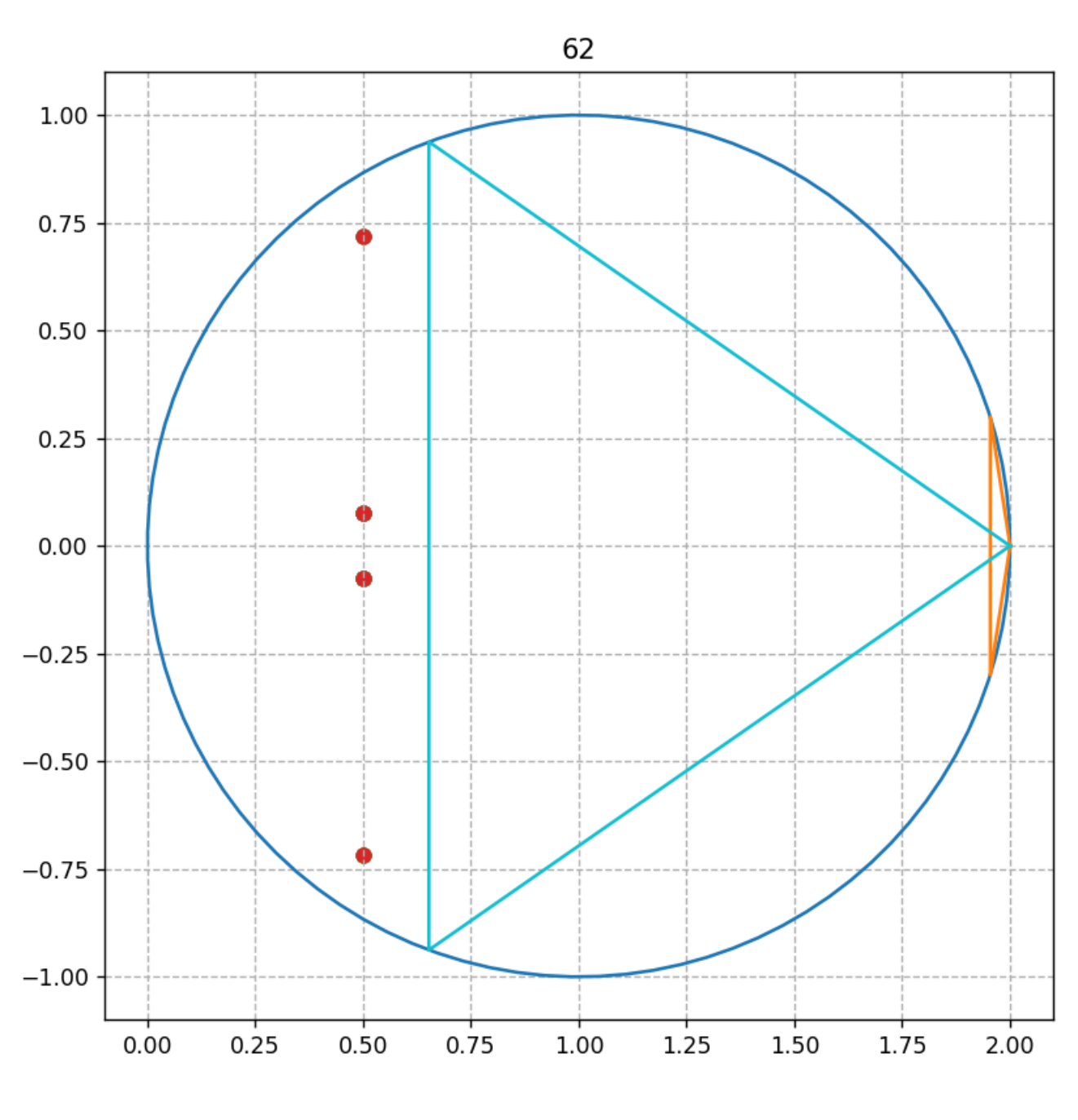
File Edit Options Buffers Tools Python Help

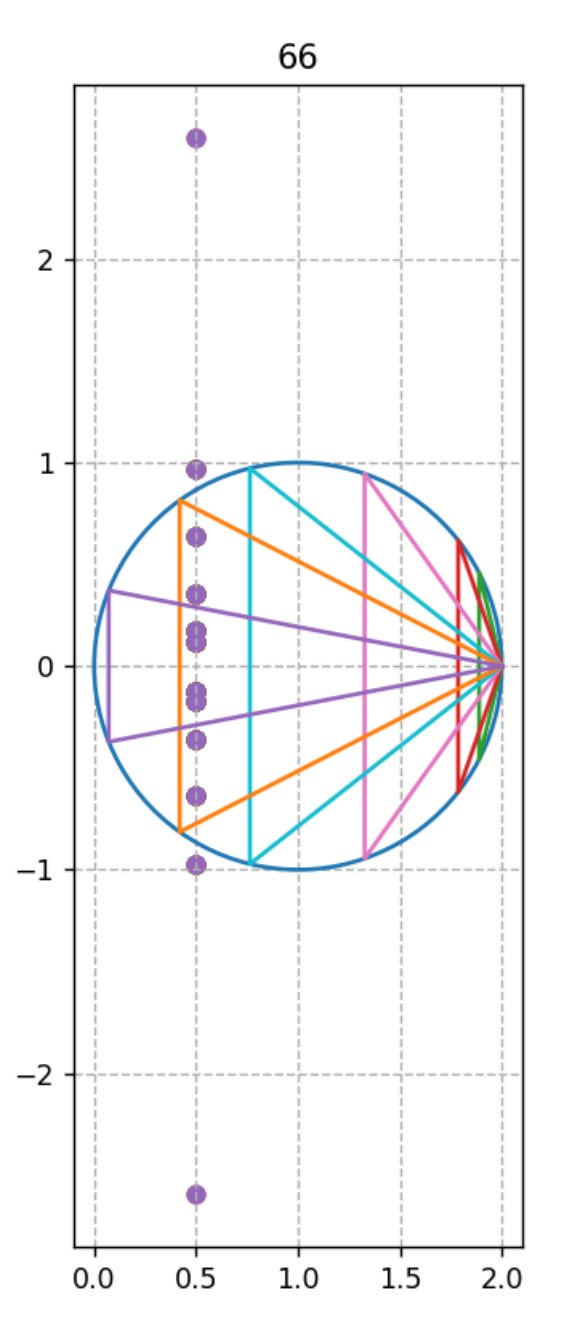
```
from mpl_toolkits.mplot3d import Axes3D
import matplotlib.pyplot as plt
import math
import numpy as np
from scipy.interpolate import RBFInterpolator

fig = plt.figure()
ax = Axes3D(fig)

def sd(n):
  return(np.sum([np.sum([np.cos(2*np.pi*n*l/k) for l in range(1,k+1)]) for k in range(1,n+1)]))
print(sd(100))

n = 20  # taille de la grille d'entiers
m = 5*n  # taille de sa discretisation

XY = np.array([[i, j] for j in range(3, n+1) for i in range(3, n+1)])
Z = np.array([sd(i) + sd(j)-i-j-2 for j in range(3, n+1) for i in range(3, n+1)])
print(Z)

Xd = Yd = np.linspace(3, n, num=m)
Xgrid, Ygrid = np.meshgrid(Xd, Yd)
XYd = np.array(list(zip(Xgrid.flat, Ygrid.flat)))
#print(f'\nXgrid =\n{Xgrid}\nYgrid =\n{Ygrid}\nXYd =\n{XYd}')

Zd = RBFInterpolator(XY, Z, kernel='linear', epsilon=7, neighbors=8)(XYd)
Zgrid = Zd.reshape(m, m)
#print(f'\nZd =\n{Zd}\nZgrid =\n{Zgrid}')

ax = fig.add_subplot(111, projection='3d')
ax.plot_surface(Xgrid, Ygrid, Zgrid, cmap=plt.cm.hot, linewidth=0,antialiased=True,alpha=0.8)
#ax.plot_wireframe(Xgrid, Ygrid, Zgrid, alpha=0.3)
#ax = fig.add_subplot(111)
#CS = ax.contour(Xgrid, Ygrid, Zgrid)
#ax.clabel(CS, inline=True, fontsize=10)
plt.show()
```




58
1.00
0.75
0.50
0.25
0.00
−0.25
−0.50
−0.75
−1.00
0.00
0.25
0.50
0.75
1.00
1.25
1.50
1.75
2.00


60
10.0
7.5
5.0
2.5
0.0
−2.5
−5.0
−7.5
−10.0
0
2


62
1.00
0.75
0.50
0.25
0.00
−0.25
−0.50
−0.75
−1.00
0.00
0.25
0.50
0.75
1.00
1.25
1.50
1.75
2.00


66
2
1
0
−1
−2
0.0
0.5
1.0
1.5
2.0

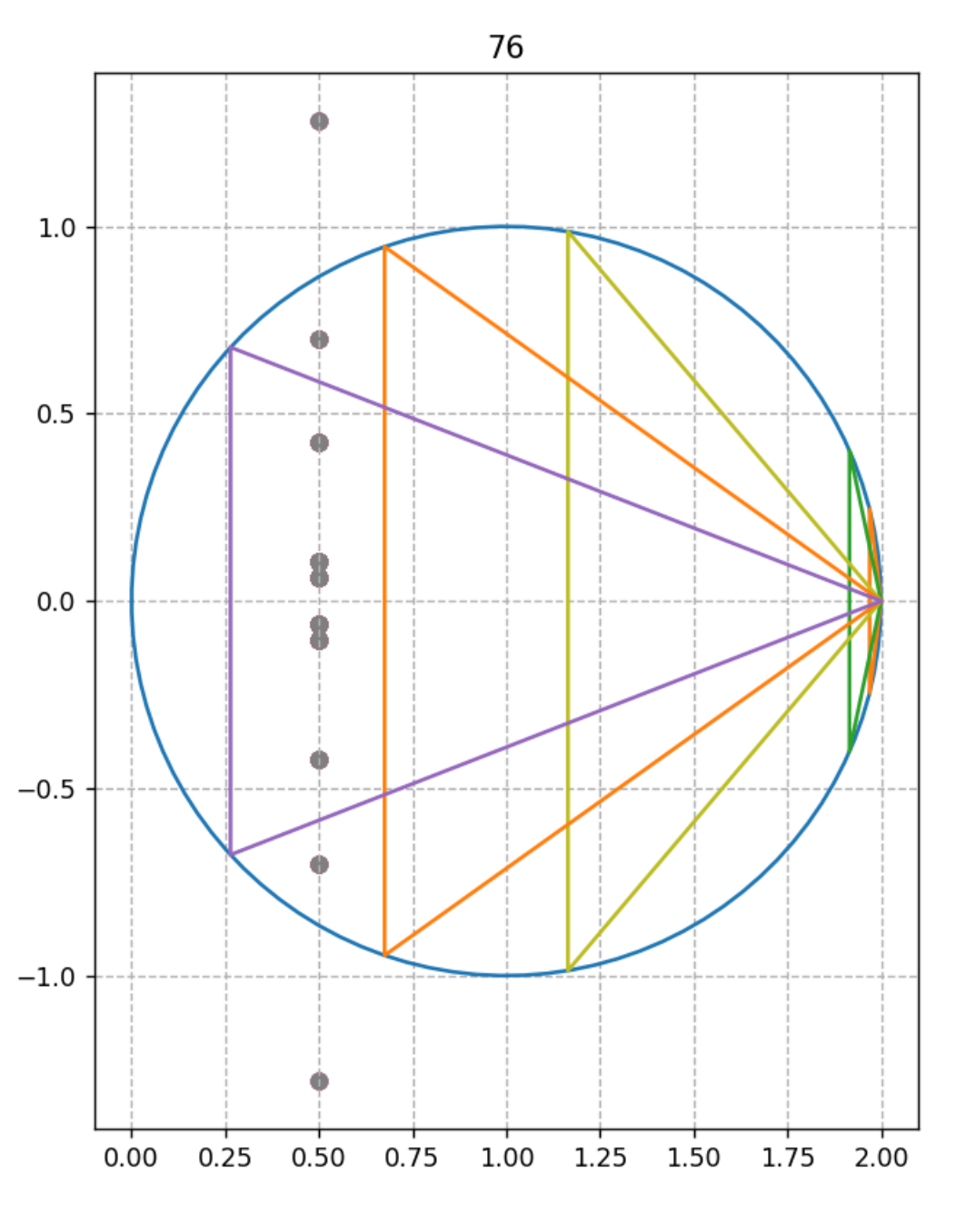

76
1.0
0.5
0.0
−0.5
−1.0
0.00
0.25
0.50
0.75
1.00
1.25
1.50
1.75
2.00

Figure 1

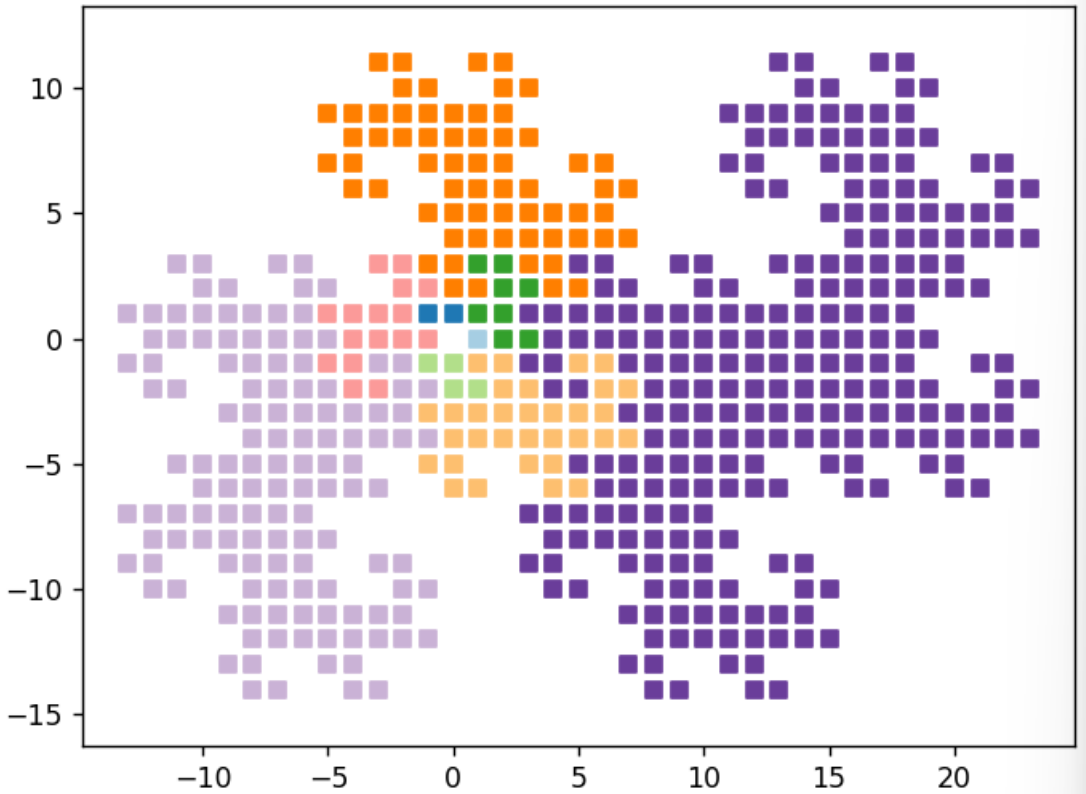


fig-entiers-de-Gauss.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos
cmap = plt.colormaps['Paired']

n = 2
X = -1+1j
lesmu = [1]
polynomes = [0]

degre = 9
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        facecolor=cmap(k/(degre+1)), marker='s')
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```

Figure 1

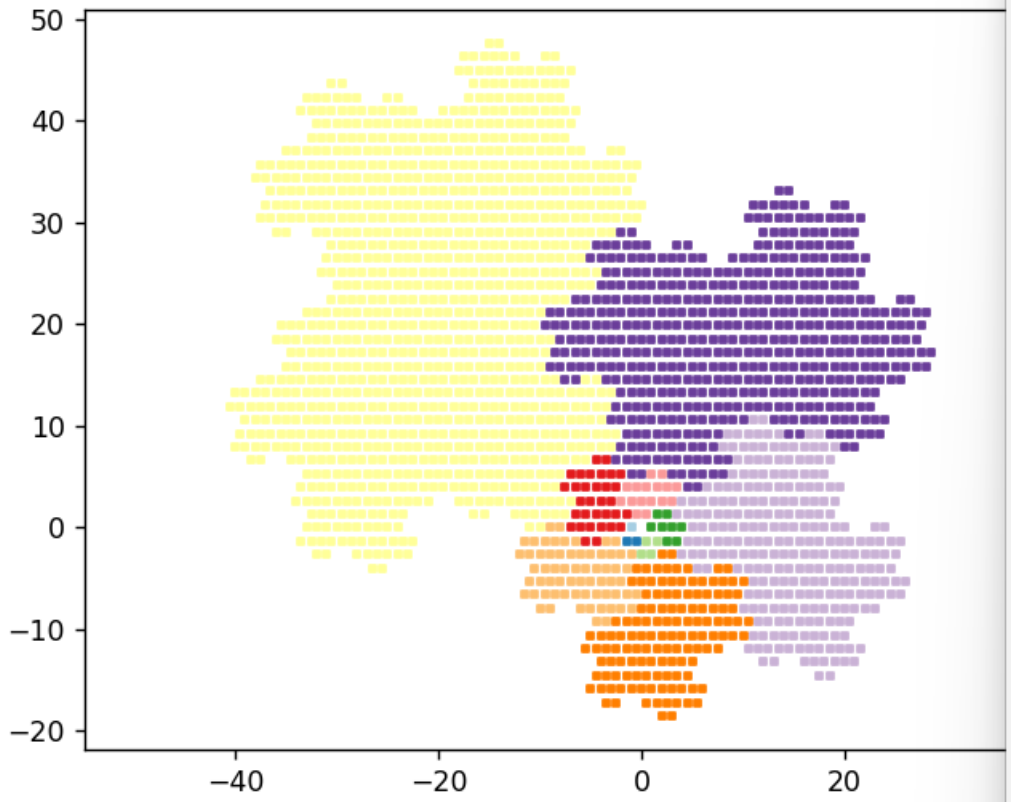


fig614.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos, sqrt
cmap = plt.colormaps['Paired']

X = 0.5*(1+1j*sqrt(7))
lesmu = [-1]
polynomes = [0]

degre = 11
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        facecolor=cmap(k/(degre+1)), marker='s', s=5)
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```

Figure 1

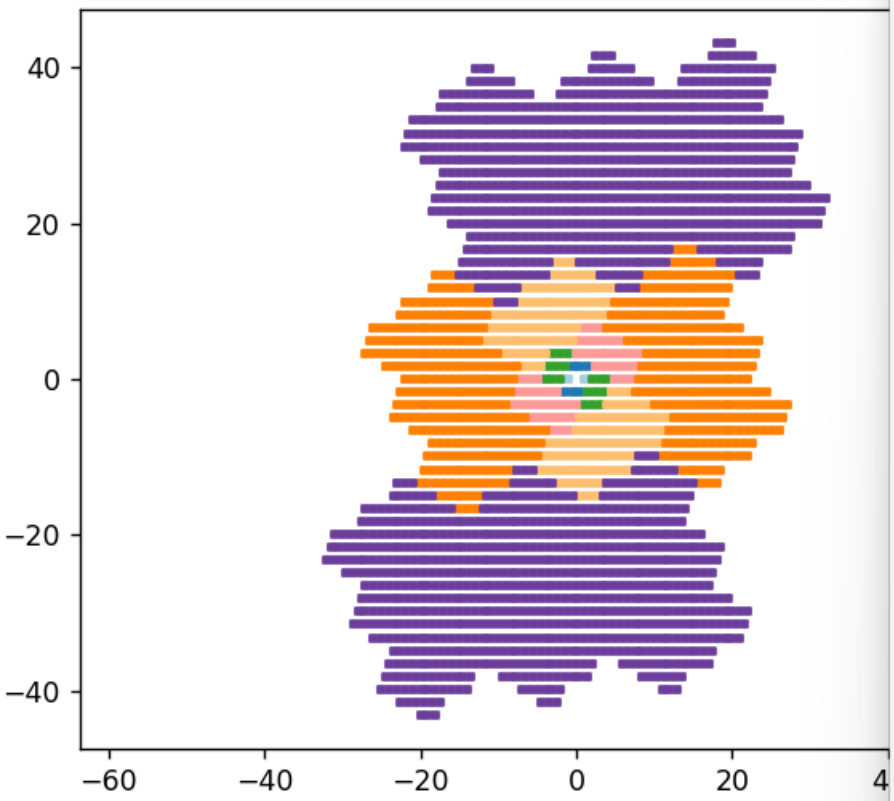


fig7.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos, sqrt
cmap = plt.colormaps['Paired']

n = 3
X = 0.5*(1+1j*sqrt(11))
lesmu = [-1,1]
polynomes = [0]

degre = 7
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        facecolor=cmap(k/(degre+1)), marker='s', s=5)
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```

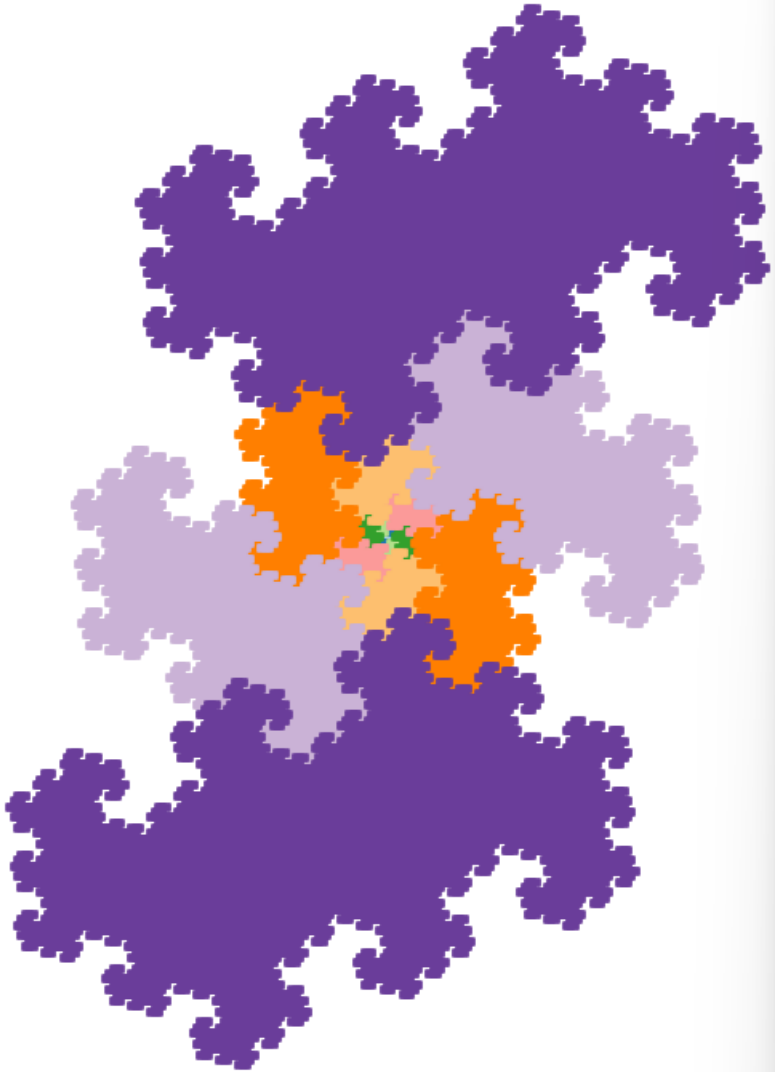


fig8.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos, sqrt
cmap = plt.colormaps['Paired']

X = 1+1j*sqrt(2)
lesmu = [-1,1]
polynomes = [0]

degre = 9
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        facecolor=cmap(k/(degre+1)), marker='s', s=5
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```

triflake.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```python
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos
cmap = plt.colormaps['Paired']

n = 3
X = -2
lesmu = [exp(1j*2*pi*k/n) for k in range(n)]
polynomes = [0]

degre = 7
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        color='red', marker='s', s=2)
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```

Figure 1

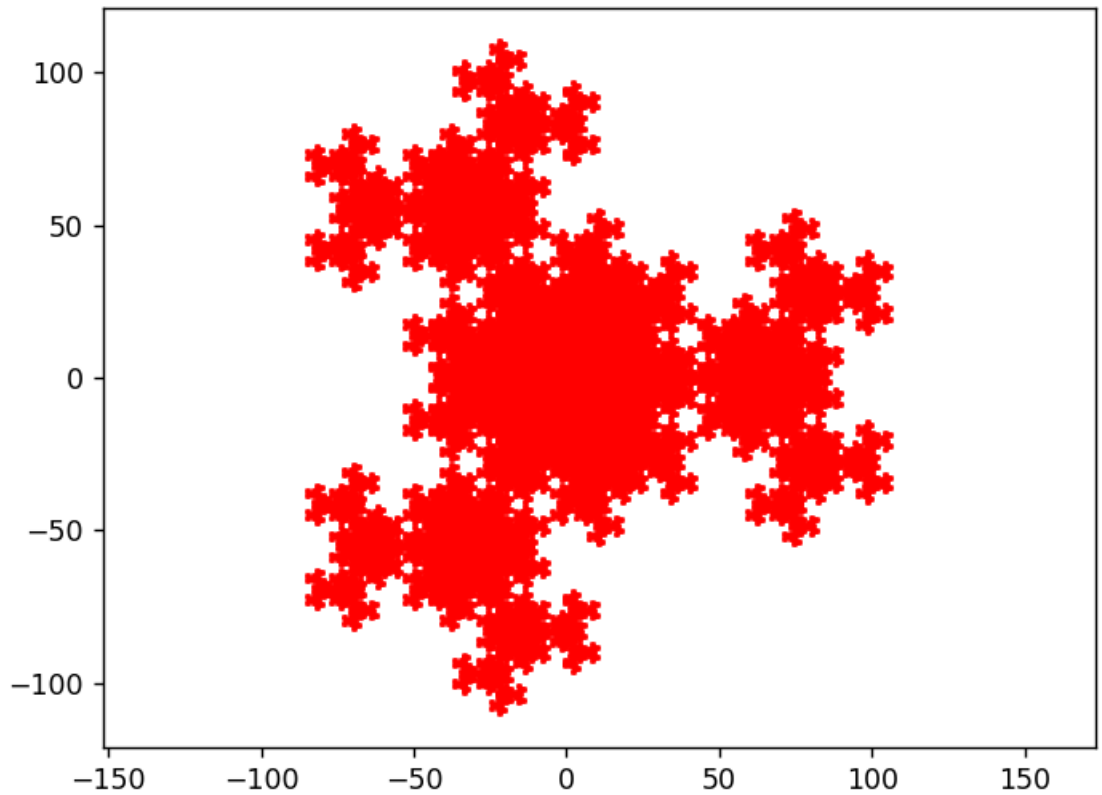
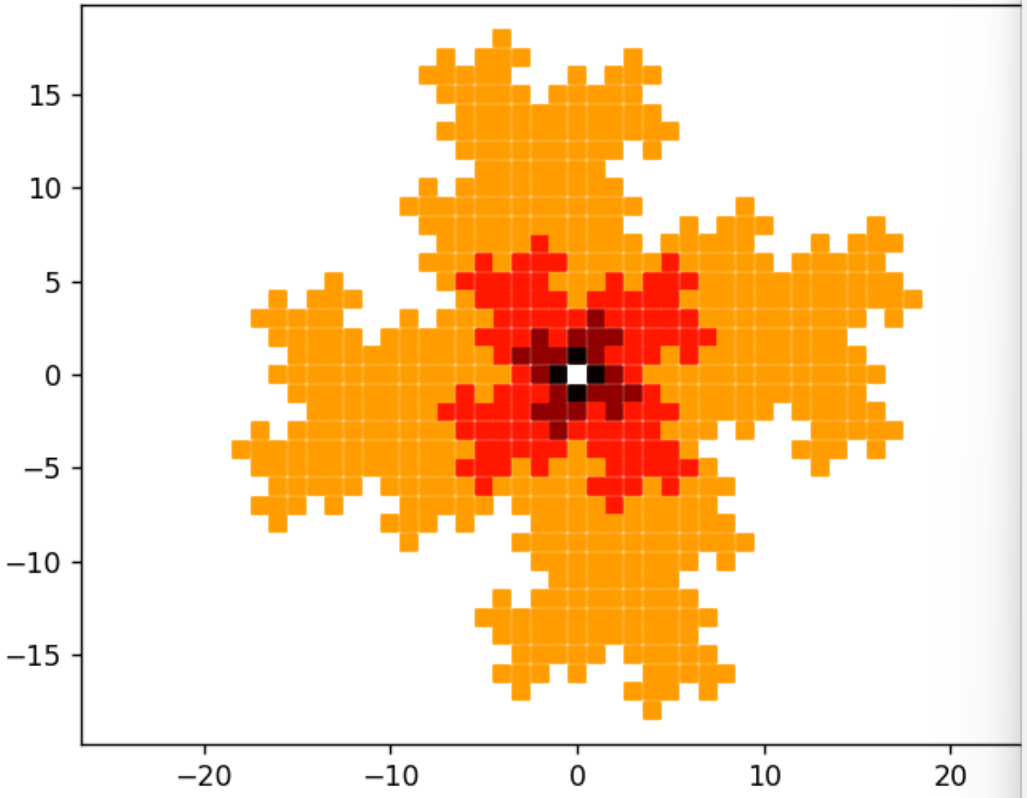


Figure 1



unfractaldes.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

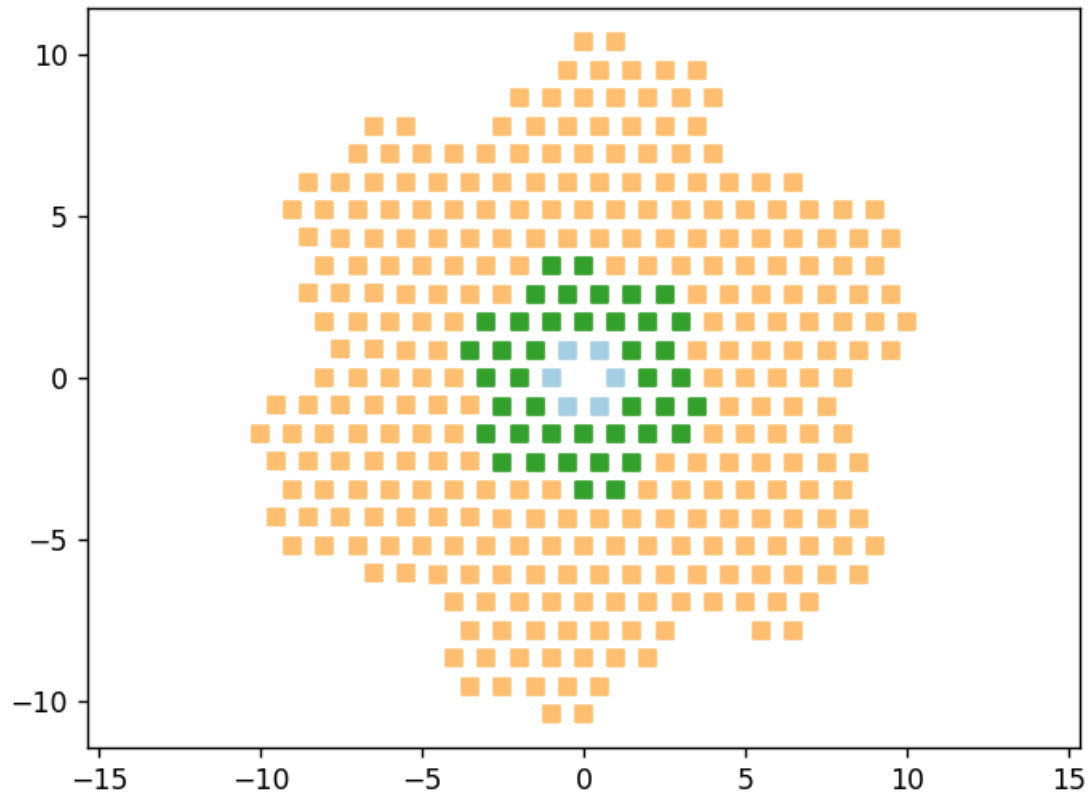
```
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos
cmap = plt.colormaps['hot']

n = 4
X = 1+2j
lesmu = [exp(1j*2*pi*k/n) for k in range(n)]
polynomes = [0]

degre = 4
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        facecolor=cmap(k/(degre+1)), marker='s')
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```

hexabis.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```python
import matplotlib.pyplot as plt
import numpy as np
from numpy import exp, pi, sin, cos, sqrt
cmap = plt.colormaps['Paired']

n = 6
X = 0.5*(5-sqrt(3)*1j)
lesmu = [exp(1j*2*pi*k/n) for k in range(n)]
polynomes = [0]

degre = 3
for k in range(degre):
    polynomesk = []
    for a in lesmu:
        for p in polynomes:
            res = a*X**k + p
            polynomesk.append(res)
            plt.scatter(res.real, res.imag,
                        facecolor=cmap(k/(degre+1)), marker='s')
    for pc in polynomesk:
        polynomes.append(pc)
plt.axis('equal')
plt.show()
```

Figure 1



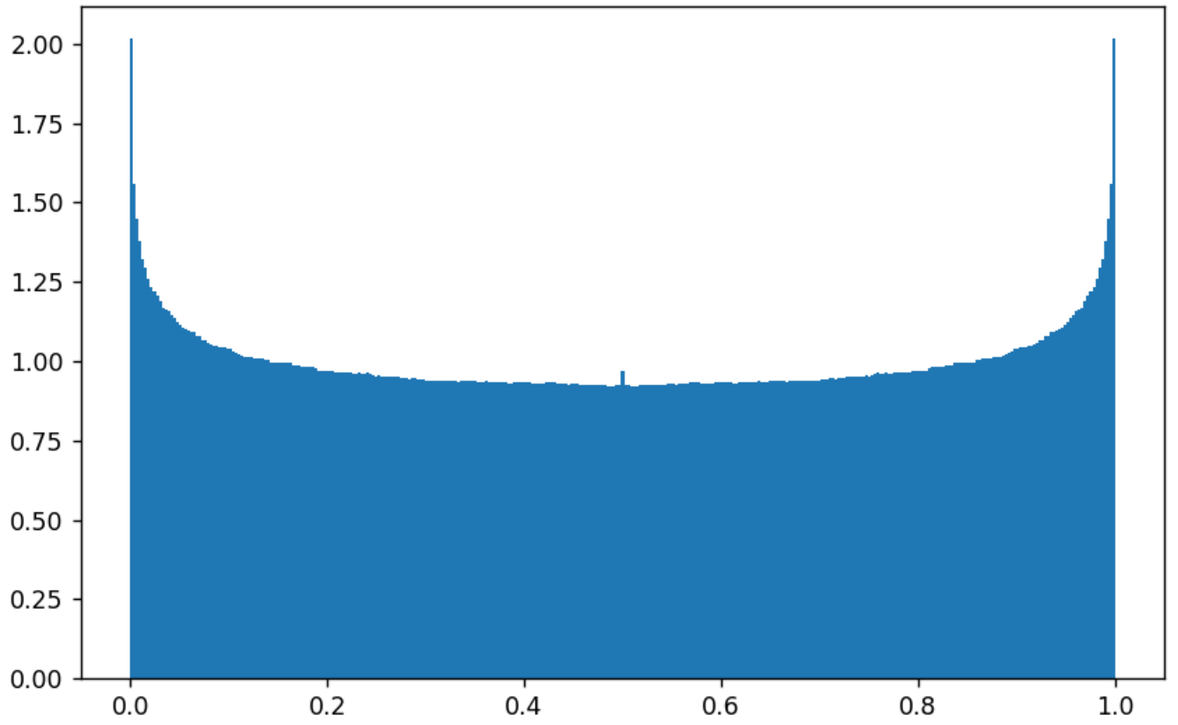
```
Invite de commandes - pytho
Microsoft Windows [version 10.0.22621.1413]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\DENISE_2022>cd Desktop

C:\Users\DENISE_2022\Desktop>python3 histoprimes.py
[gb_density: 472.37 s, hist:  4.58 s]
```

histoprimes.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
    def factors(self, n):
        if n in self:
            return np.array([n])
        else:
            P = self.range(2, n//2 + 1)
            return P[n % P == 0]

def gb_density(N):
    P = Primes(N)
    #print(P)
    D = []
    for n in range(6,N+1,2):
        #print(n)
        for p in P.range(3, n//2+1):
            if n-p in P:
                #print(p,'+',n-p)
                D.append(p/n)
                D.append((n-p)/n)
    return D

import math, matplotlib.pyplot as plt, numpy as np, time

fig, ax = plt.subplots(figsize=(8, 5))
N = 100000
t0 = time.perf_counter()
D = gb_density(N)
#print(len(D))
#print(D)
t1 = time.perf_counter()
counts, bins = np.histogram(D, bins='auto', range=(0,1), density=True)
plt.hist(bins[:-1], bins, weights=counts)
t2 = time.perf_counter()
print(f"[gb_density: {t1-t0:5.2f} s, hist: {t2-t1:5.2f} s]")
plt.show()
```

Figure 1



Invite de commandes

```
C:\Users\DENISE_2022\Desktop>
C:\Users\DENISE_2022\Desktop>
C:\Users\DENISE_2022\Desktop>python3 jolies-minutes.py
jolie minute :  308  =  5 h 8 min. et  5 , 8 , 3  et  8  sont tous les 4 premiers.
  On a deux decompositions de Goldbach pour le prix  d une a cette belle heure (!) de la journee.
jolie minute :  310  =  5 h 10 min.
jolie minute :  316  =  5 h 16 min.
jolie minute :  322  =  5 h 22 min.
jolie minute :  334  =  5 h 34 min.
jolie minute :  346  =  5 h 46 min.
jolie minute :  718  =  11 h 58 min.
jolie minute :  786  =  13 h 6 min.
jolie minute :  790  =  13 h 10 min.
jolie minute :  796  =  13 h 16 min.
jolie minute :  1142  =  19 h 2 min.
jolie minute :  1148  =  19 h 8 min.
jolie minute :  1152  =  19 h 12 min.
jolie minute :  1154  =  19 h 14 min.
jolie minute :  1158  =  19 h 18 min.
jolie minute :  1164  =  19 h 24 min.
jolie minute :  1170  =  19 h 30 min.
jolie minute :  1172  =  19 h 32 min.
jolie minute :  1178  =  19 h 38 min.
jolie minute :  1182  =  19 h 42 min.
jolie minute :  1190  =  19 h 50 min.
jolie minute :  1384  =  23 h 4 min.
jolie minute :  1386  =  23 h 6 min.
jolie minute :  1392  =  23 h 12 min.
jolie minute :  1396  =  23 h 16 min.
25 jolies minutes par jour,
ca fait  0.017361111111111112 % de jolies minutes par jour sur 1440, c est peu.

C:\Users\DENISE_2022\Desktop>
```

jolies-minutes.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
def premier(atester):
    k = 2
    if atester in [0, 1]: return False
    if atester in [2, 3, 5, 7]: return True
    while True:
        if k * k > atester: return True
        else:
            if atester % k == 0: return False
            else: k = k + 1

compteles = 0
premiere = True
for x in [2,3,5,7,11,13,17,19,23]:
    for y in range(1,59):
        if premier(x) and premier(y-x) and premier((x*60+y)//100) and premier(((x*60+y)%100) - ((x*60+y)//100)) and ((x*60+y)%100) - ((x*60+y)//100) > (x*60+y)/100:
            if premiere:
                print('jolie minute : ',
                  x*60+y, ' = ', x, 'h', y,
                  'min. et ', x, ',', y, ',', (x*60+y)//100, ' et ',
                  (x*60+y)%100, ' sont tous les 4 premiers.\n ',
                  'On a deux decompositions de Goldbach pour le prix ',
                  'd une a cette belle heure (!) de la journee.')
                premiere = False
            else:
                print('jolie minute : ',x*60+y, ' = ', x, 'h', y,'min.')
            compteles = compteles+1
print(compteles, 'jolies minutes par jour,')
print('ca fait ', float(compteles/1440), '% de jolies minutes par jour sur 1440,
 c est peu.')
```

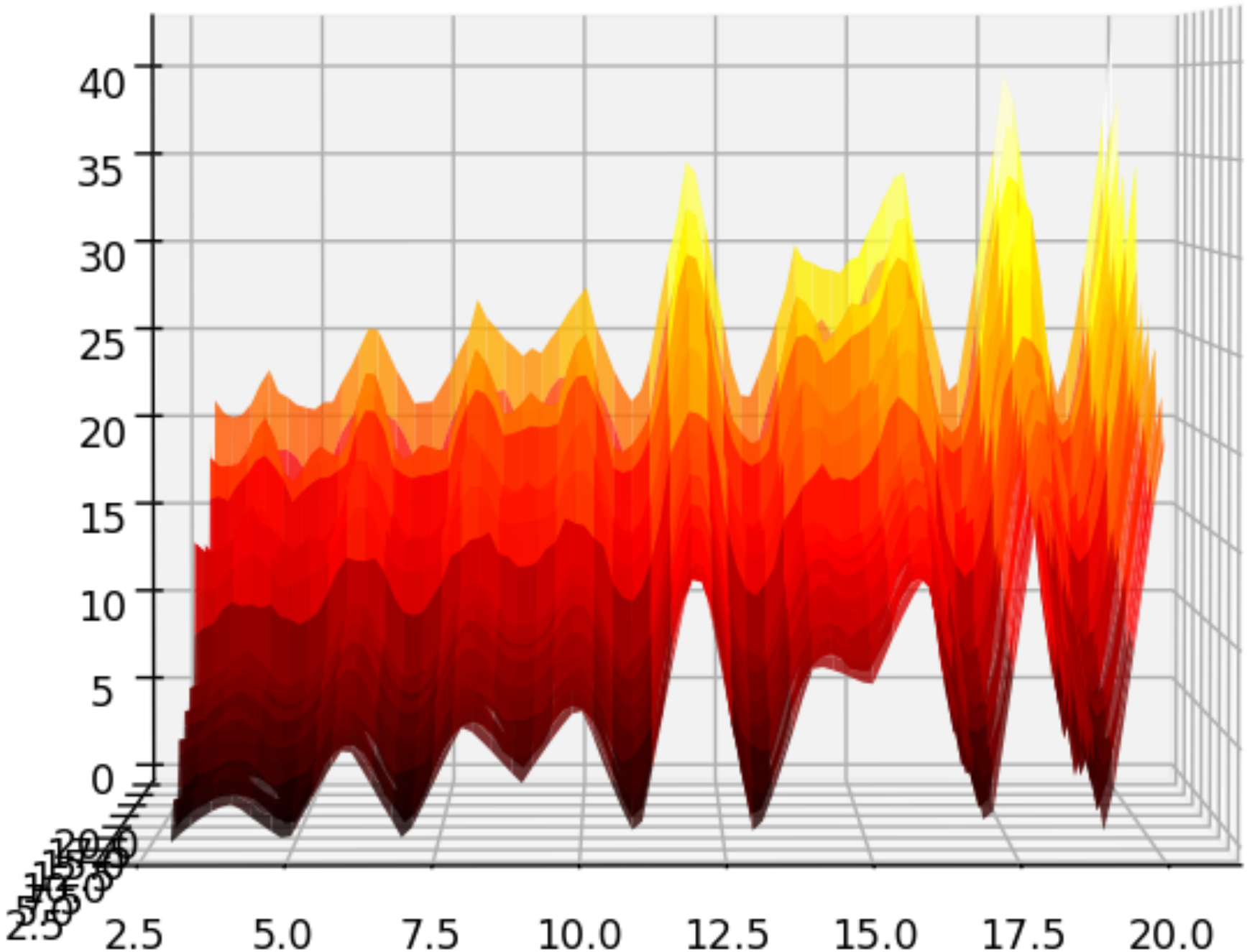
-\--- **jolies-minutes.py** All L11 (Python ElDoc)

```
C:\Users\DENISE_2022\Desktop\conserve-banquet>python3 bodessin50à120.py
3  --> perim =  3.847435987423748 aire =  0.3659990614777857 distmilieu  1.661986965969646
5  --> perim =  3.8170474067801807 aire =  0.45421096531501076 distmilieu  1.578551152375549
7  --> perim =  4.732977894233356 aire =  0.25292128870398106 distmilieu  2.2166026443472537
9  --> perim =  4.110920070470572 aire =  0.5541187174548746 distmilieu  1.5035691982829507
11  --> perim =  4.3175490668800185 aire =  0.5189700472266332 distmilieu  1.8103018041344512
13  --> perim =  4.6972136735633985 aire =  0.5241942714043881 distmilieu  2.0490163078592216
15  --> perim =  4.563054513291625 aire =  0.7349163945668143 distmilieu  1.474727402584816
17  --> perim =  4.8038231555828865 aire =  0.6439091005962185 distmilieu  1.8103018041344487
19  --> perim =  4.304722555442971 aire =  0.22829236393513905 distmilieu  2.0273688601322295 DG.
21  --> perim =  4.445655519213422 aire =  0.6751129958320433 distmilieu  1.585836481861092
23  --> perim =  4.459831057640576 aire =  0.4351742754005213 distmilieu  1.57855115237555
25  --> perim =  4.899858452924814 aire =  0.25114260371506086 distmilieu  2.2200823393022096
27  --> perim =  3.7666636961374698 aire =  0.24317470673992084 distmilieu  1.6299984322491068
29  --> perim =  3.6008008929396746 aire =  0.2125373176080315 distmilieu  1.398215937876957
31  --> perim =  5.192288882003902 aire =  0.37749019342592083 distmilieu  2.4194748168030134 DG.
33  --> perim =  3.459323320571371 aire =  0.0760149816063239 distmilieu  1.5785511523755484
35  --> perim =  3.2904815799185494 aire =  0.243255339158611 83 distmilieu  1.4286124166959466
37  --> perim =  5.011263297809169 aire =  0.014536802621137362 distmilieu  2.3463220337758925 DG.
39  --> perim =  4.017618159207392 aire =  0.3040262828095534 distmilieu  1.5880941873437056
41  --> perim =  4.042155567464725 aire =  0.5426766638520251 distmilieu  1.6299984322491152
43  --> perim =  4.556207164120552 aire =  0.16827787117487994 distmilieu  2.0490163078592207
45  --> perim =  4.8378458566454885 aire =  0.7376202830851503 distmilieu  1.6619869659696487
47  --> perim =  4.908287631296902 aire =  0.9147615144817 56 distmilieu  1.7297877941811706
49  --> perim =  3.7741424538073134 aire =  0.0 distmilieu  1.8870712269036567
```

miroir-interpol.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
from mpl_toolkits.mplot3d import Axes3D
import matplotlib.pyplot as plt
import math
import numpy as np
from scipy.interpolate import interp1d

fig, ax = plt.subplots(figsize=(15, 10))

def sd(n):
    # somme des diviseurs de n >= 1
    return sum([sum([math.cos(2*math.pi*n*l/k) for l in range(1, k+1)]) for k in range(1, n+1)])
#for n in 1, 2, 3, 4, 5, 6, 12, 100: print(f'sd({n:3}) = {sd(n):6.2f}')

n = 98  # taille de la grille d'entiers
m = 5*n  # taille de sa discretisation

X = np.array([i for i in range(1, n+1)])
Z = np.array([sd(i) - i - 1 for i in range(1, n+1)])
#print(f'\nX =\n{X}\nZ =\n{Z}')
Zp = np.array([sd(n-i) - n + i - 1 for i in range(1, n+1)])

Xd = np.linspace(1, n, num=m)
#print(f'\nXd =\n{Xd}')

Zd = interp1d(X, Z, kind='cubic')(Xd)
Zdp = interp1d(X, Zp, kind='cubic')(Xd)
#print(f'\nZd =\n{Zd}')

ax.plot(Xd, Zd)
ax.plot(Xd, Zdp)
ax.set_ylim(-20,200)
#ax.scatter(X, Z, c='r', marker='o')
ax.scatter([3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97], [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0], c='r', marker='o')
plt.text(18,-10,'19')
plt.text(30,-10,'31')
plt.text(36,-10,'37')
plt.text(78,-10,'79')
plt.text(66,-10,'67')
plt.text(60,-10,'61')
plt.show()
```


40
35
30
25
20
15
10
5
0
2.5
2.5
5.0
7.5
10.0
12.5
15.0
17.5
20.0

```
import matplotlib.pyplot as plt
import numpy as np
from numpy import pi, sin, cos
import math
from math import sqrt

def prime(atester):
    pastrouve = True ; k = 2 ;
    if (atester in [0,1]): return False ;
    if (atester in [2,3,5,7]): return True ;
    while (pastrouve):
        if ((k * k) > atester): return True
        else:
            if ((atester % k) == 0): return False
            else: k=k+1

def cercle(rayon, xcentre, ycentre, c, s):
    theta = np.linspace(0,2*pi,360)
    x = xcentre + rayon * cos(theta)
    y = ycentre + rayon * sin(theta)
    plt.plot(x,y, color=c, ls = s)

def trouvexy(n, c):
    x = r2* cos(2*pi*n/2) + r3* cos(2*pi*n/3) + r5* cos(2*pi*n/5)+r7* cos(2*pi*n
s/7)
    y = r2* sin(2*pi*n/2) + r3* sin(2*pi*n/3) + r5* sin(2*pi*n/5)+r7* sin(2*pi*n
s/7)
    plt.plot(x, y, c, marker='o', markersize=4)
    plt.annotate(str(n),xy=(x, y))
    return x,y

fig = plt.figure(figsize=(15,15))
ax = fig.gca()
ax.set_aspect('equal')
r2 = 1 ; r3 = 1/2 ; r5 = 1/4 ; r7 = 1/8
cercle(r2,0,0,'blue', '-.')
c3d = 1 ; c3g = c3d-2 ; c3y = 0
c5dx = 1 ; c5gx = c5dx-2 ; c5y = 0
c7dx = 1 ; c7gx = c7dx-2 ; c7y = 0
cercle(r3, c3d, c3y, 'red', '-')
cercle(r3, c3g, c3y, 'red', '-')
for m in range(3):
    cercle(r5, c5dx + r3* cos(m*2*pi/3), c5y + r3* sin(m*2*pi/3), 'green', '-')
```

```
for m in range(3):
    cercle(r5, c5dx + r3* cos(m*2*pi/3), c5y + r3* sin(m*2*pi/3),'green', '-')
    cercle(r5, c5gx + r3* cos(m*2*pi/3), c5y + r3* sin(m*2*pi/3),'green', '-')
    for n in range(5):
        cercle(r7, c7dx + r3* cos(m*2*pi/3) + r5* cos(n*2*pi/5), c7y + r3* sin(m*2*pi/3) + r5* sin(n*2*pi/5),'yellow', '-')
        cercle(r7, c7gx + r3* cos(m*2*pi/3) + r5* cos(n*2*pi/5), c7y + r3* sin(m*2*pi/3) + r5* sin(n*2*pi/5),'yellow', '-')
xprec,yprec = 0, 0
n = 98
for n in range(n,n+2,2):
    xn, yn = trouvexy(n, 'red')
    for d in range(3, n//2, 2):
        print(d, ' --> ', end='')
        xd, yd = trouvexy(d, 'black')
        xcompl, ycompl = trouvexy(n-d, 'black')
        c1 = sqrt((xcompl-xd)**2+(ycompl-yd)**2)
        c2 = sqrt((xcompl-xn)**2+(ycompl-yn)**2)
        c3 = sqrt((xd-xn)**2+(yd-yn)**2)
        xmilieu=0.5*(xd+xcompl)
        ymilieu=0.5*(yd+ycompl)
        distmilieu = sqrt((xmilieu-xn)**2+(ymilieu-yn)**2)
        psur2 = 0.5*(c1+c2+c3)
        aireheron = sqrt(psur2*(psur2-c1)*(psur2-c2)*(psur2-c3))
        print('perim = ', c1+c2+c3, 'aire = ',aireheron,'distmilieu ', distmilieu,end='')
        if prime(d) and prime(n-d):
            plt.plot([xd,xcompl],[yd,ycompl],'blue')
            print(' DG.')
        else:
            plt.plot([xd,xcompl],[yd,ycompl],'cyan')
            print('')
#for n in range(1,210+2):
#    if prime(n):
#        xn, yn = trouvexy(n, 'cyan')
#    else:
#        xn, yn = trouvexy(n, 'black')

xmin, xmax, ymin, ymax = ax.axis()
ax.set_xlim(xmin-0.2, xmax+0.2) ;
ax.set_ylim(ymin-0.2, ymax+0.2)
plt.show()
```

banquet-de-Jacques.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt, numpy as np
from matplotlib.patches import Circle
from itertools import product
from numpy import exp, pi

def primes(n):        # np.array of all primes < n
    is_prime = np.full(n, True)
    is_prime[:2] = False
    for p in range(2, int(round(np.sqrt(n))) + 1):
        if is_prime[p]:
            is_prime[p*p::p] = False
    return np.nonzero(is_prime)[0]

ax = plt.figure(figsize=(16, 16)).subplots(1, 1)
ax.set_aspect('equal')
cmap = plt.colormaps['hsv']
r = 1
p = primes(10)
k = np.arange(len(p))
for n in range(np.prod(p)):
    z = np.sum(r/(2**k)*exp(2j*pi*(n % p)/p))
    plt.plot(z.real, z.imag, 'o', alpha=0.8, markersize=2**2)
    plt.annotate(f'{n}', xy=(z.real, z.imag), textcoords='offset points', xytext
=(2, 2), fontsize=8)
c = [0]
for i in range(len(p)):
    for z in c:
        ax.add_patch(Circle((z.real, z.imag), r/(2**i), fill=False, ec=cmap(i/le
n(p))))
    c = [z + r/(2**i)*exp(2j*pi*j/p[i]) for z in c for j in range(p[i])]
xmin, xmax, ymin, ymax = (1.1*x for x in (-1.6, 1.9, -1.0, 1.0))
ax.set(xlim=(xmin, xmax), ylim=(ymin, ymax))
plt.show()
```

-\--- **banquet-de-Jacques.py** All L25 (Python ElDoc)

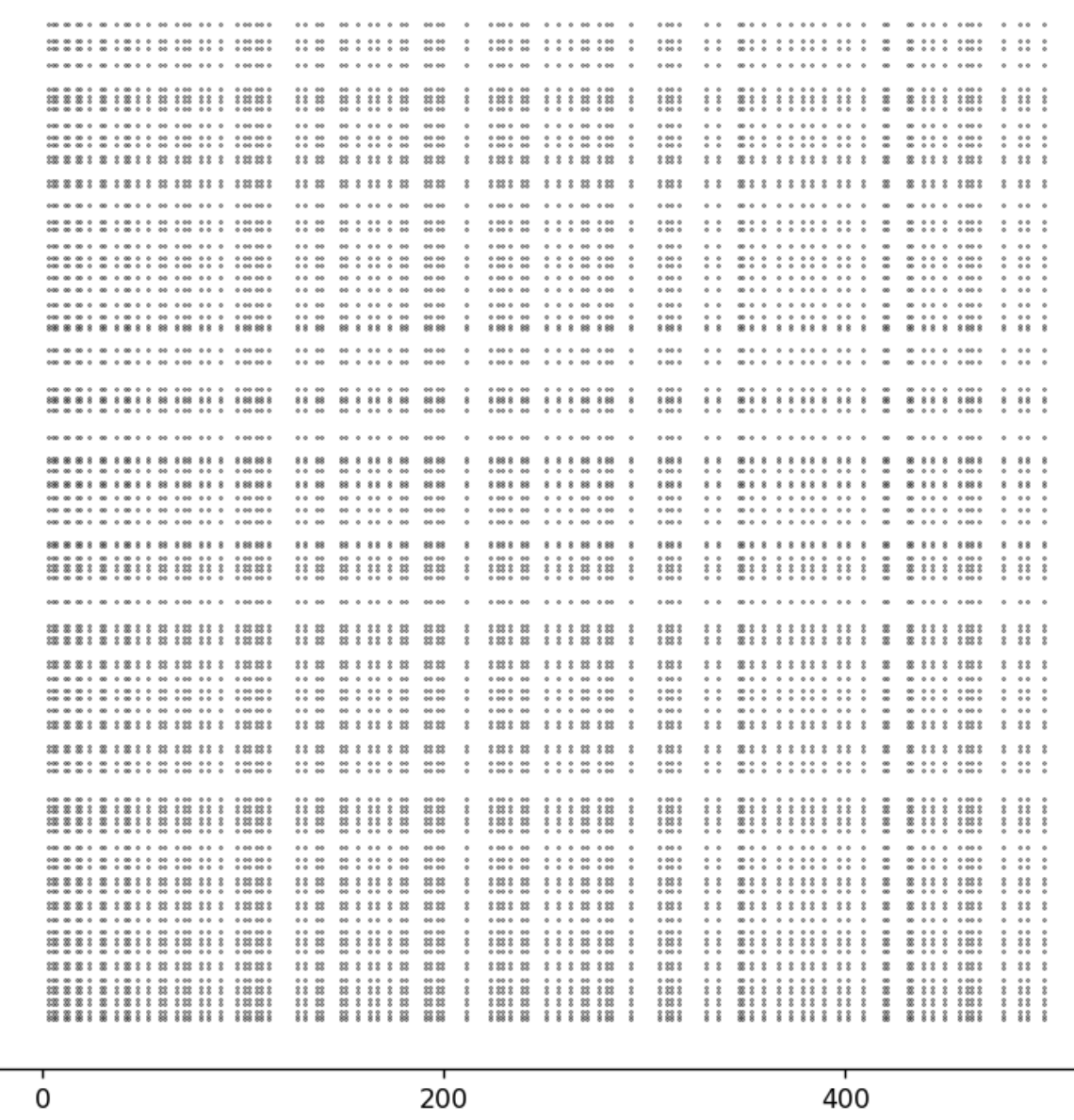
Wrote c:/Users/DENISE 2022/Desktop/conserve-banquet/banquet-de-Jacques.py

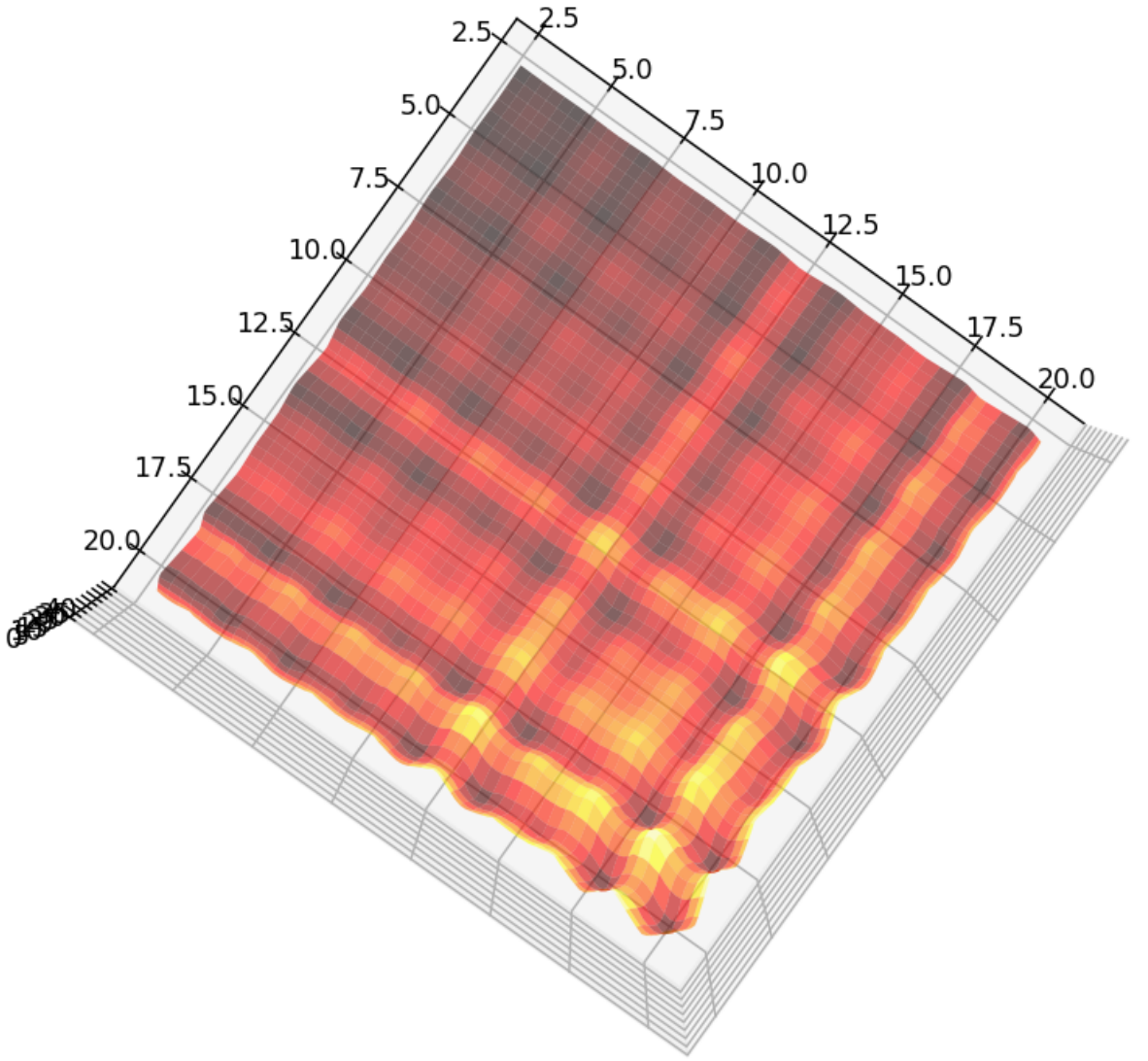
courbe-croix-grecque-2.py - GNU Emacs at DESKTOP-4PROGGL

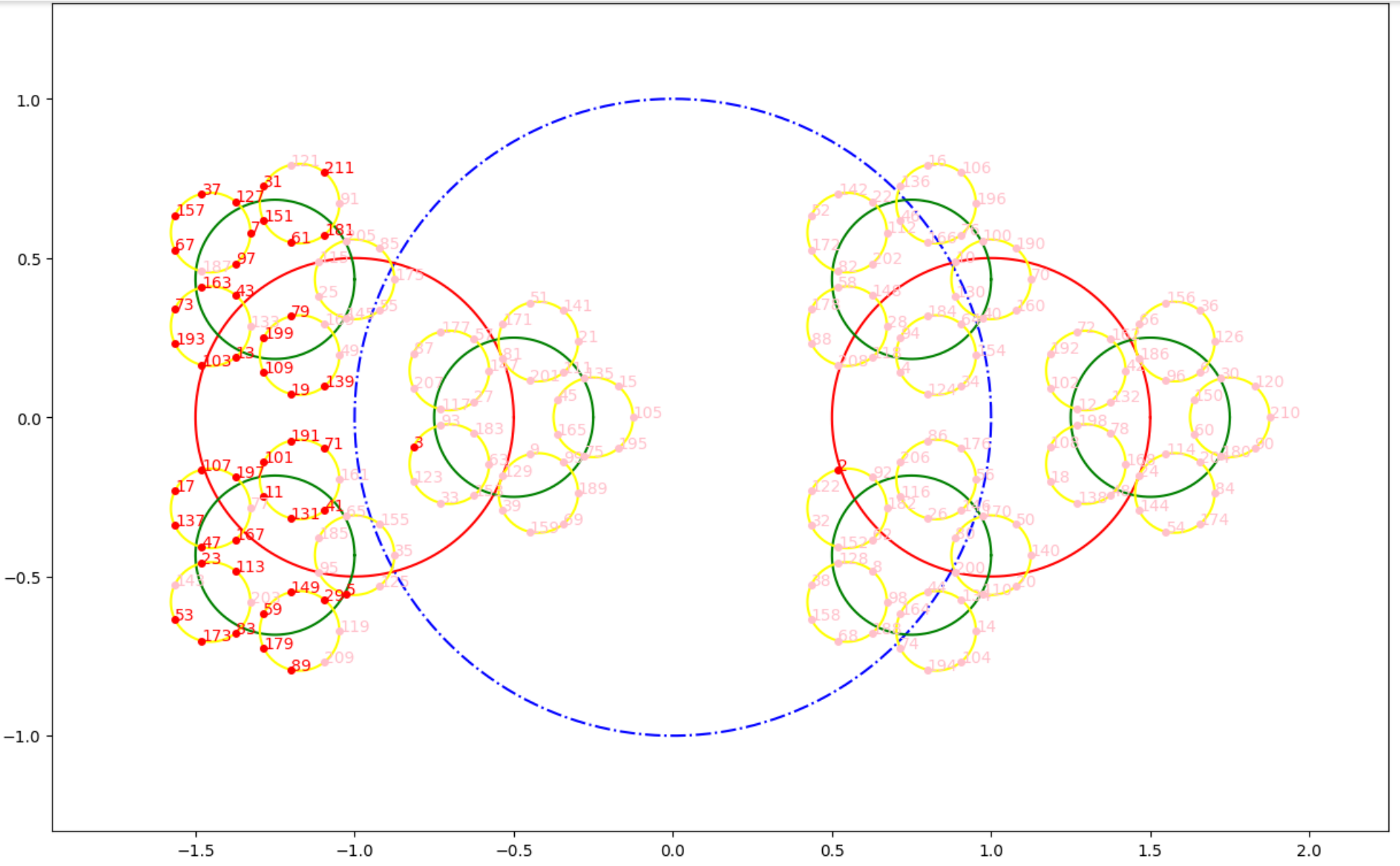
File Edit Options Buffers Tools Python Help

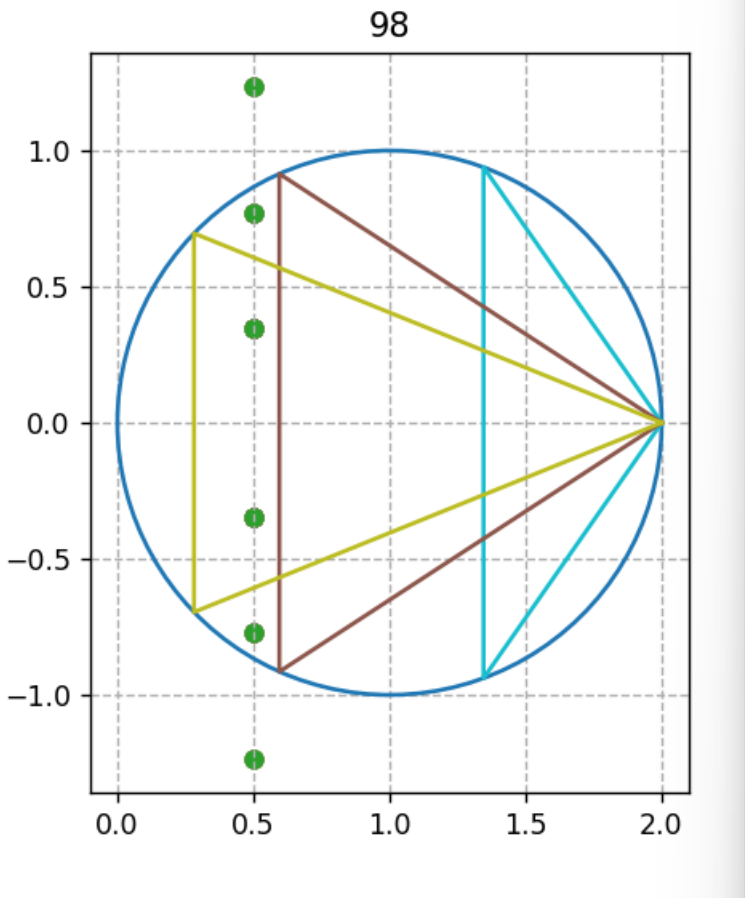
```
str2='AGADADAGAGADAGADAD'
longueur = 25
setheading(90)
up()
x = x+taille
turtle.setposition(x,y)
down()
dessine(str2)

str3='AGADADAGAGADAGADADAGADADAGAGADAGAGADAGADADAGAGADAGADAD'
setheading(90)
up()
longueur = 12
x = x+taille
turtle.setposition(x,y)
down()
dessine(str3)

str4 = str3+str3
str4b = str4[0:2*len(str3)-1]
str4b += 'G'+str3
setheading(0)
up()
longueur = 6
x = x+1.3*taille
y = y+taille
turtle.setposition(x,y)
down()
dessine(str4b)

str5 = str4b+str4b
str5b = str5[0:2*len(str4b)-1]
str5b += 'G'+str4b
setheading(90)
up()
longueur = 3
x = x+1.2*taille
y = y-0.6*taille
turtle.setposition(x,y)
down()
dessine(str5b)
exitonclick()
```

-\--- **courbe-croix-grecque-2.py** Bot L42 (Python ElDoc)


0
200
400


2.5
5.0
7.5
10.0
12.5
15.0
17.5
20.0


1.0
0.5
0.0
−0.5
−1.0
−1.5
−1.0
−0.5
0.0
0.5
1.0
1.5
2.0

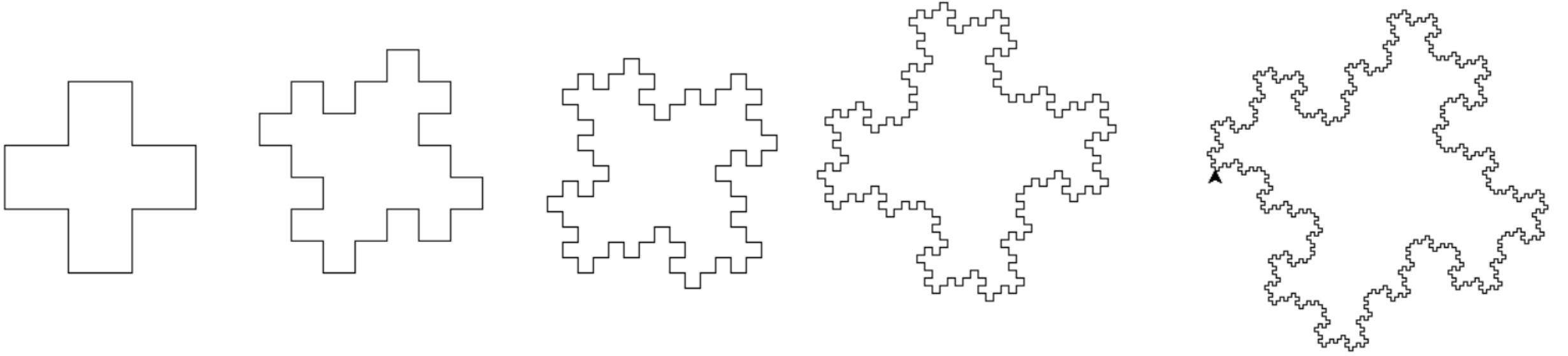


invcos.py - GNU Emacs at DESKTOP-4PROGGL

File Edit Options Buffers Tools Python Help

```
    ax.plot(x, y)
    ax.set_aspect(1)
    #plt.xlim(-0.25,2.25)
    #plt.ylim(-1.25,1.25)
    plt.grid(linestyle='--')
    lesinvx = []
    lesinvy = []
    for x in range(3, int(n//2), 2):
        lescos = [2] ; lessin = [0]
        if x in P and n-x in P:
            #print('x =',x, ' --> ',end='')
            p1x = cos(2*pi*x/n)+1
            p1y = sin(2*pi*x/n)
            z1 = p1x+1j*p1y
            z1p = 1/z1
            lesinvx.append(z1p.real)
            lesinvy.append(z1p.imag)
            p2x = cos(2*pi*(n-x)/n)+1
            p2y = sin(2*pi*(n-x)/n)
            z2 = p2x+1j*p2y
            z2p = 1/z2
            lesinvx.append(z2p.real)
            lesinvy.append(z2p.imag)
            #print('2cos ', 2*cos(2*pi*x/n))
            #print('2sin ', 2*sin(2*pi*x/n))
            lescos.append(p1x) ; lescos.append(p2x)
            lessin.append(p1y) ; lessin.append(p2y)
            lescos.append(2) ; lessin.append(0)
        plt.plot(lescos, lessin)
        plt.scatter(lesinvx, lesinvy)
    plt.title(str(n))
plt.show()
```

-\--- **invcos.py** Bot L35 (Python ElDoc)



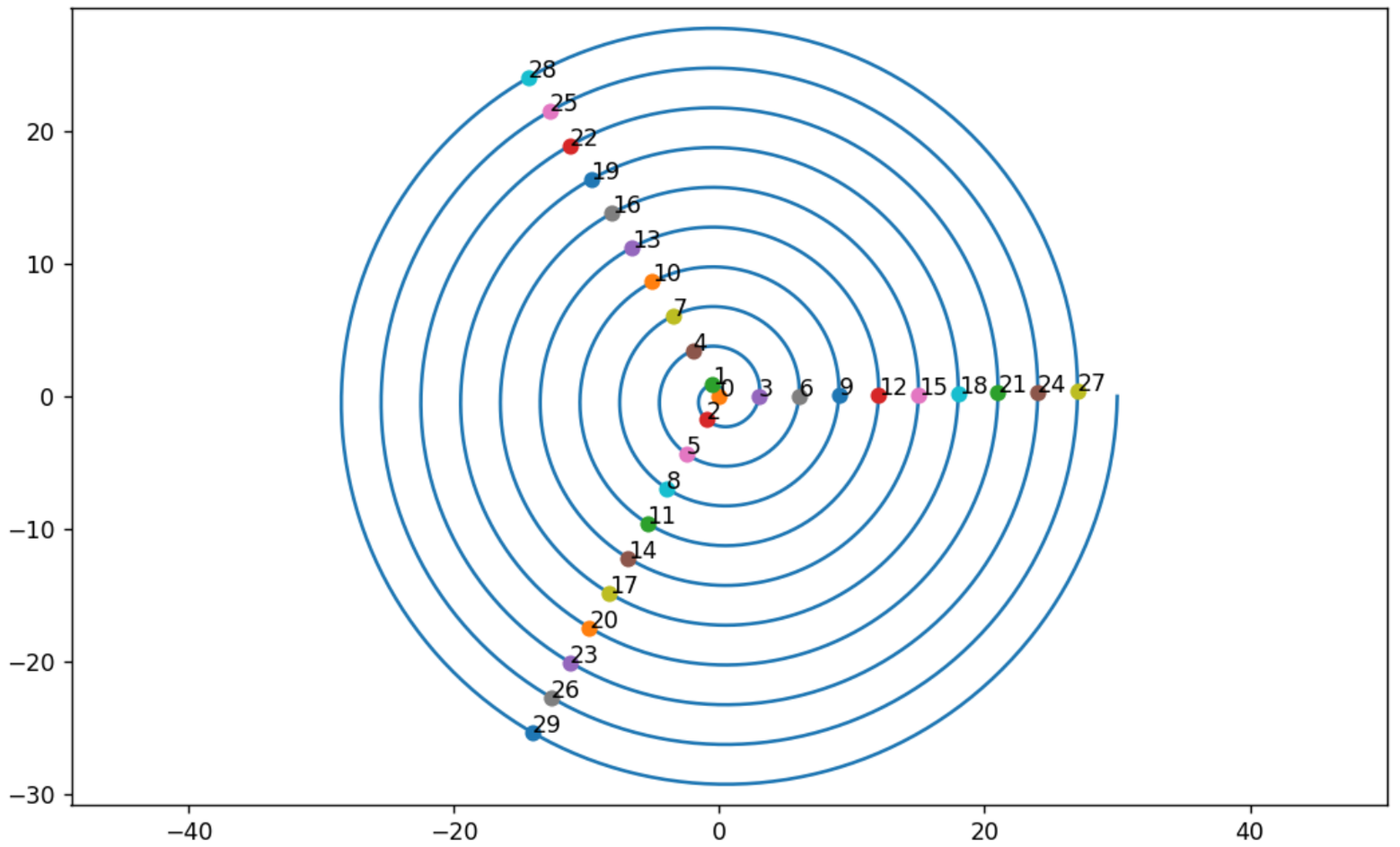
pc2.py - GNU Emacs at DESKTOP-4PROGGL

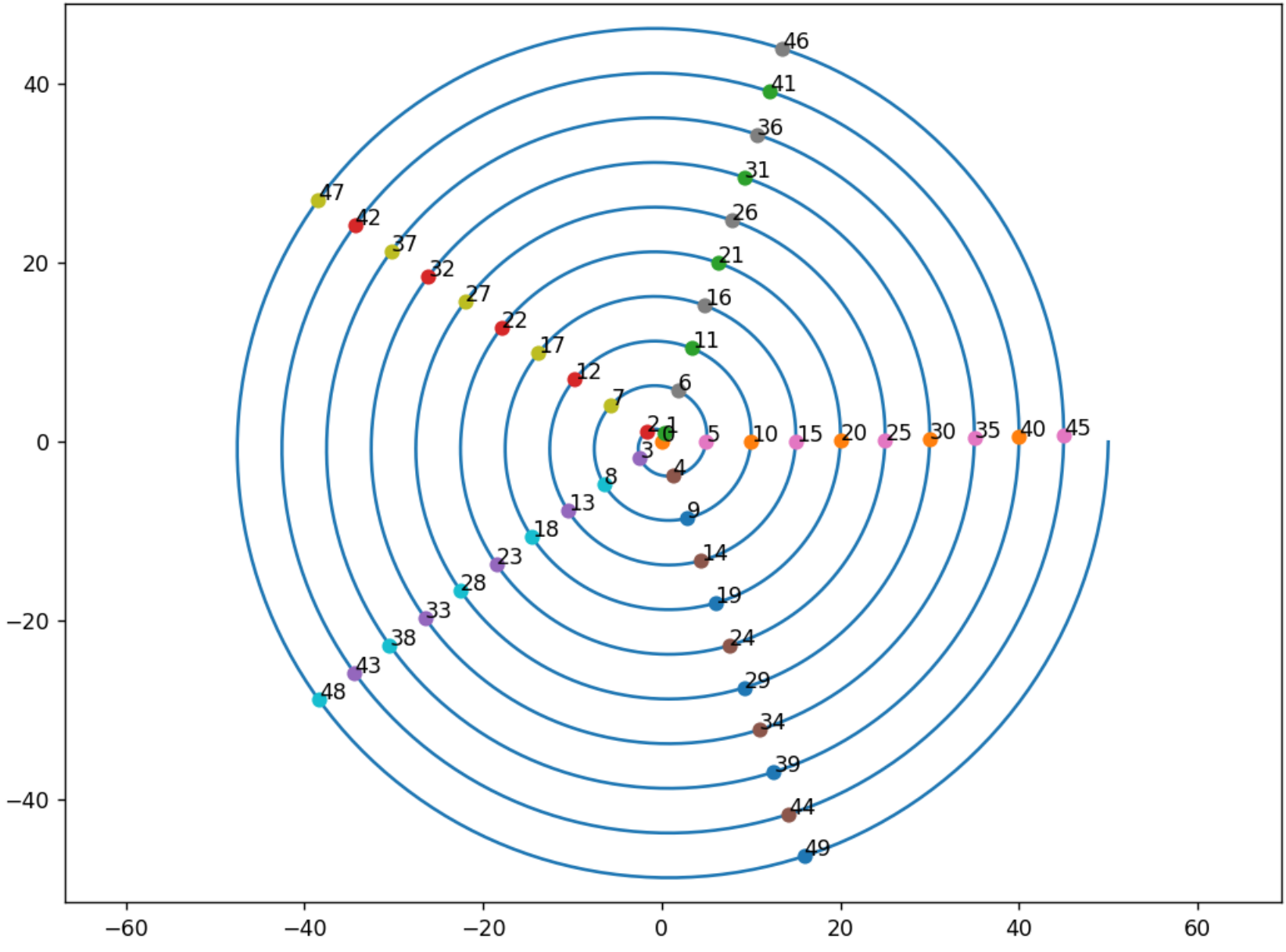
File Edit Options Buffers Tools Python Help

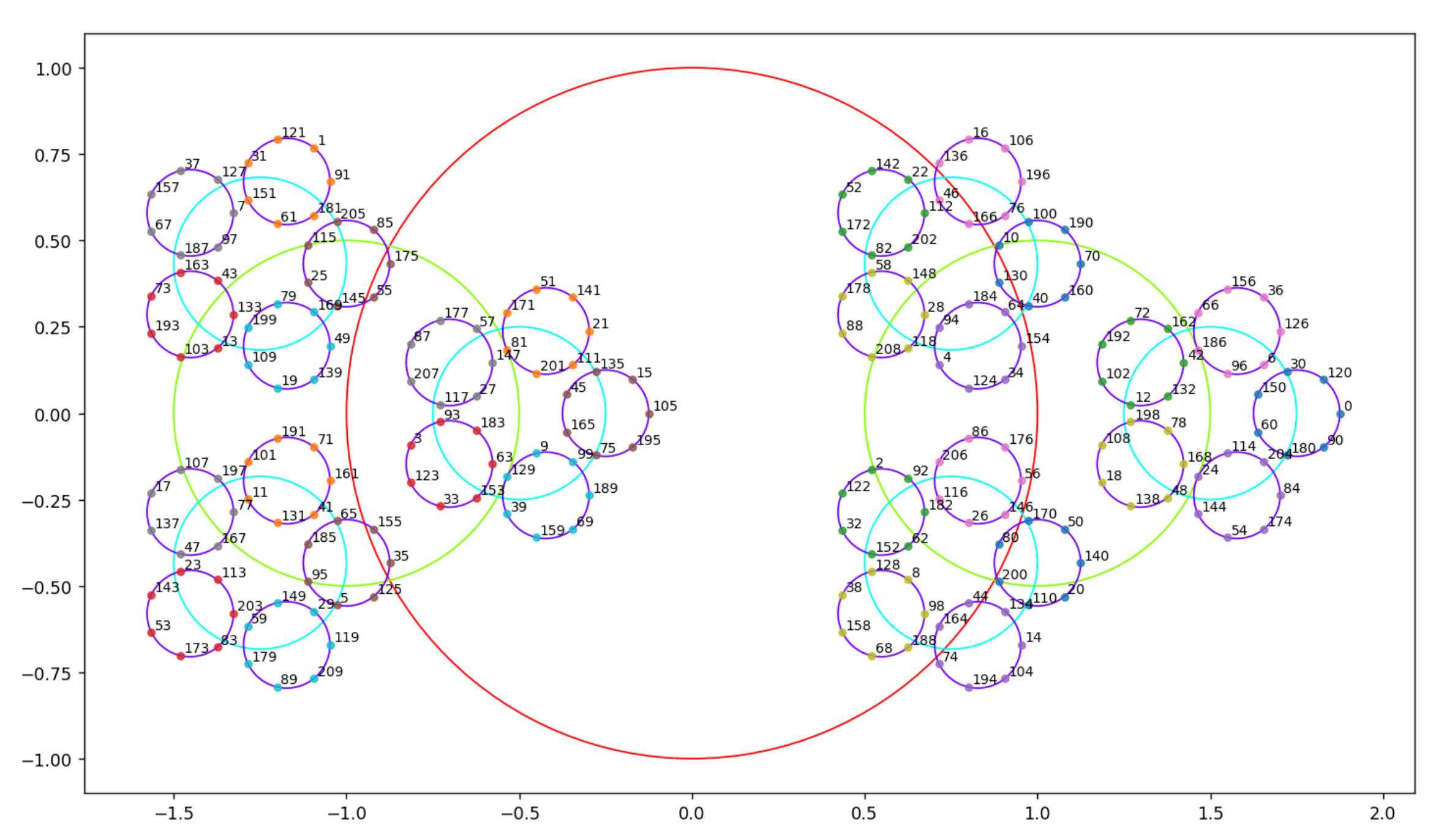
```python
import matplotlib.pyplot as plt
import numpy as np
from numpy import pi, sin, cos

a = 3/(2*pi)
nbtours = 10
print(np.pi)
theta = np.linspace(0, nbtours*2*pi, nbtours*360)
rho = a*theta
x = rho*cos(theta)
y = rho*sin(theta)
plt.plot(x,y)
for nb in range(10):
    ici = nb*360
    icix = rho[ici]*cos(theta[ici])
    iciy = rho[ici]*sin(theta[ici])
    plt.plot([icix],[iciy], 'o')
    plt.annotate(3*nb,xy=(icix,iciy))
    ici = ici+120
    icix = rho[ici]*cos(theta[ici])
    iciy = rho[ici]*sin(theta[ici])
    plt.plot([icix],[iciy], 'o')
    plt.annotate(3*nb+1,xy=(icix,iciy))
    ici = ici+120
    icix = rho[ici]*cos(theta[ici])
    iciy = rho[ici]*sin(theta[ici])
    plt.plot([icix],[iciy], 'o')
    plt.annotate(3*nb+2,xy=(icix,iciy))
plt.axis('equal')
plt.show()
```

-\--- **pc2.py** All L1 (Python ElDoc)

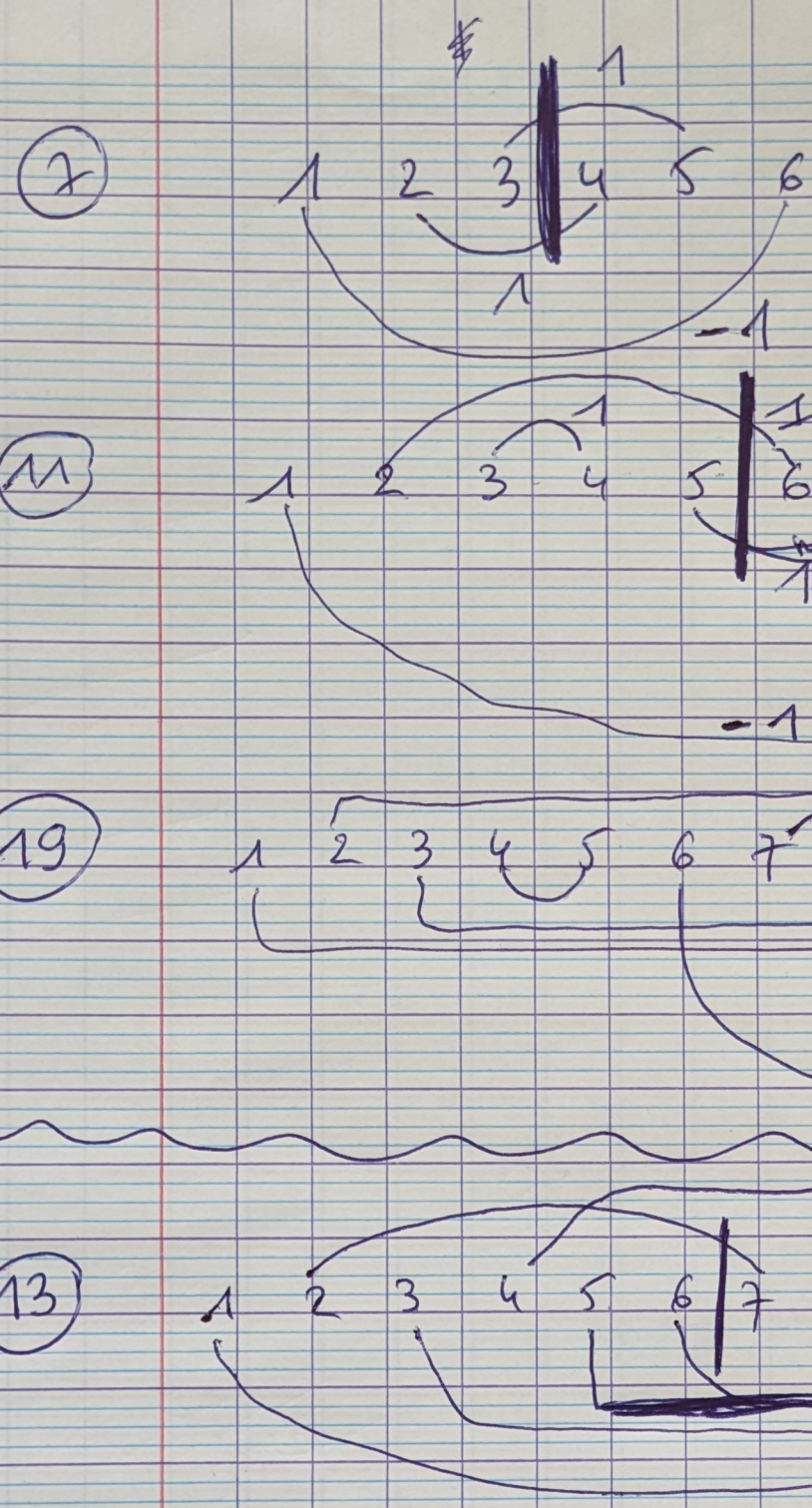
Figure 1




40
20
0
−20
−40
−60
−40
−20
0
20
40
60
46
41
36
31
26
21
16
11
6
7
12
17
22
27
32
37
42
47
2
1
0
5
10
15
20
25
30
35
40
45
3
4
8
13
18
23
28
33
38
43
48
9
14
19
24
29
34
39
44
49


1.00
0.75
0.50
0.25
0.00
−0.25
−0.50
−0.75
−1.00
−1.5
−1.0
−0.5
0.0
0.5
1.0
1.5
2.0

0.5 1.5 2.5 3.5



19
38
57
76
95
114
133
152
171
190
209

115 | 19
16

153 | 3
51

51 | 3
21 17

16
8
128

6
84

15
6
90

16
6
96

8 96
12
14
15
70
14
210

13
5

$$x \times y \equiv 1 \ (p)$$

$$\Leftrightarrow (p-x)(p-y) \equiv 1 \ (p)$$

$$p^2 - (x+y)p + xy \equiv 1 \ (p)$$

$$\left(\frac{p}{2} - \frac{1}{2}(2k+1)\right) \times \left(\frac{p}{2} + \frac{1}{2}(2k+1)\right)$$

on voit les nombres comme à gauche ou à dte de la moitié du module

p 1er $\Leftrightarrow p! \equiv -1 \pmod p$ (ou) Le miroir du Théorème de WILSON pour les 1ers

$$3 \times 5 \equiv 1 \ (7)$$

$$\left(\frac{7}{2} - \frac{1}{2} \times (2 \times 0 + 1)\right) \times \left(\frac{7}{2} + \frac{1}{2}(2 \times 1 + 1)\right) \equiv 1 \ (7)$$

$$\frac{49}{4} - \frac{7}{4}(2 \times 0 + 1) + \frac{7}{4}(2 \times 1 + 1) - \frac{1}{4}(1 \times 3)$$

$$\frac{49}{4} - \frac{7}{4} \times (1 + 3) - \frac{3}{4}$$

$$\frac{49}{4} - 7 - \frac{3}{4}$$

$$\frac{46}{4} - \frac{28}{4} = \frac{18}{4} \equiv 1 \ (7)$$

$$\Leftrightarrow \boxed{18 \equiv 4 \ (7)}$$