Courbes fractales selon chaque p et séquences fractales de booléens, février 2006.

Bouts de Frobenius.

Programme de la découverte extraordinaire d'Euler.

Petit baluchon (produits de sinus, CG et jumeaux dans les corps premiers, formule récursive pour la somme des diviseurs d'Euler, addition disjointe et rêves d'un prince), février 2014.

Belles courbes des produits de sinus.

Somme de sommes de cos, juillet 2014.

Opérateur continu.

Malte.

Polygones réguliers sur cercle unité.

Résidus quadratiques.

Partitions par compositions.

Transparents des partitions par compositions.

Programme de ma courbe préférée somme de sommes de cos.

Premier = A la puissance 1 dans la factorisation de sa factorielle.

La part du hasard dans le passage de n à $n+2$.

Toute seule.

Proba disjointes et programme.

Compositions et palindromes.

Spectre de la chaleur.

Points entiers sur spirale logarithmique.

Formule sur pièce de puzzle qui généralise la conjecture des pairs aux impairs.

Nombre de solutions de $x^{10} \equiv 1 \ (mod \ n)$ et belles représentations sur cercles unités.

Fractales, symétrie et conjecture de Goldbach

Denise Vella

Février 2006

1 Introduction

Dans cette note, nous utilisons la théorie fractale de Mandelbrot pour étudier certaines propriétés des nombres entiers naturels. Nous mettons en évidence les symétries que l'on trouve dans certaines séquences fractales d'entiers. Ces symétries ont vraisemblablement pour conséquence que tout entier naturel supérieur à 4 est la moyenne de deux nombres premiers.

2 Séquences fractales de valuations p-adiques

2.1 Définitions

On appelle valuation p-adique (p premier) d'un entier n l'exposant de p dans la factorisation de n. On a l'habitude de noter cette valuation $v_p(n)$.

On peut définir $v_p(n)$ de la façon suivante :

$$v_p(n) = \begin{cases} 0 & \text{si} \quad n \not\equiv 0 \pmod{p} \\ v_p(n/p) + 1 & \text{sinon.} \end{cases}$$

Voici la séquence des valuations 2-adiques des nombres entiers de 1 à 100 :

0 1 0 2 0 1 0 3 0 1 0 2 0 1 0 4
0 1 0 2 0 1 0 3 0 1 0 2 0 1 0 5
0 1 0 2 0 1 0 3 0 1 0 2 0 1 0 4
0 1 0 2 0 1 0 3 0 1 0 2 0 1 0 6
0 1 0 2 0 1 0 3 0 1 0 2 0 1 0 4
0 1 0 2 0 1 0 3 0 1 0 2 0 1 0 5
0 1 0 2 0

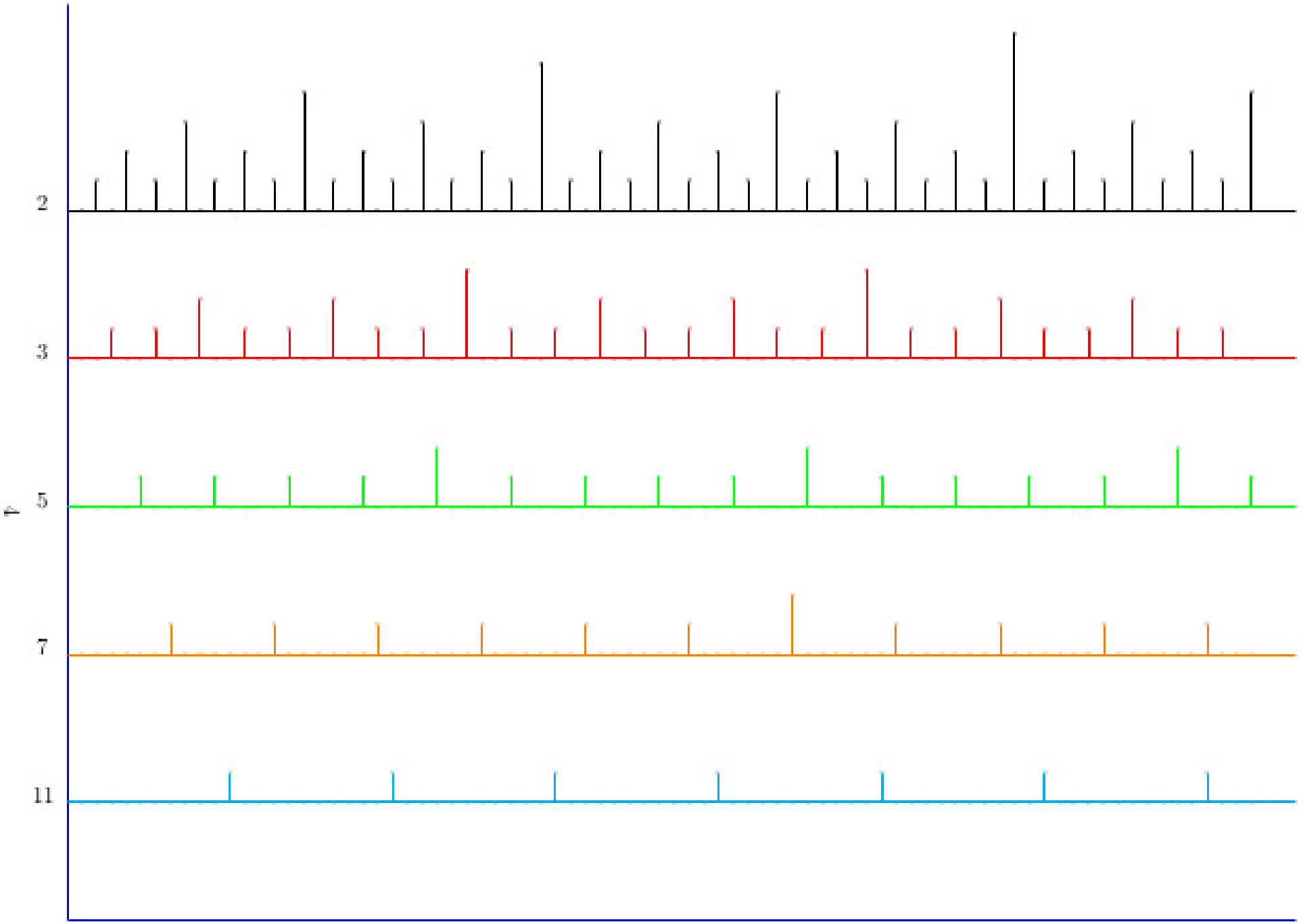


Figure 1 : Séquences fractales de valuations p-adiques

La séquence des valuations 3-adiques des mêmes nombres est [1] :

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
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
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 4
0 0 1 0 0 1 0 0 2
0 0 1 0 0 1 0 0 2
0

On appelle *séquence fractale d'entiers* une séquence d'entiers qui s"'auto-contient". Cette notion a été définie précisément par Mandelbrot [1]. On peut dire que d'un point de vue mathématique, les fractales sont des objets construits par récurrence d'une homothétie interne, ce que l'on appelle l"'auto-similarité". Avant Mandelbrot, Peano, Sierpinski, ou Hilbert avaient inventé des courbes fractales. Chaque partie de ces courbes a une structure identique à la structure du tout.

Cette notion de "fractale" est esthétique par sa "beauté naturelle" au sens où elle permet de représenter des objets naturels tels une courbe littorale accidentée, la structure d'un arbre, etc. Enfin, Kimberling [2] a introduit la notion de "séquence fractale d'entiers" qui sera utilisée ici.

D'abord, il faut constater que les séquences constituées des valuations p-adiques des entiers sont autant de séquences fractales d'entiers : si l'on supprime de l'une de ces séquences tous ses éléments nuls et que l'on retranche 1 aux éléments restant, on obtient la séquence initiale avant transformation.

Considérons maintenant la séquence obtenue en additionnant les éléments de la séquence p-adique et de la séquence q-adique (p et q premiers). On constate que cette séquence est également fractale. Si l'on ne conserve de cette séquence que les éléments d'indices multiples du produit pq et qu'on leur retranche 2, on trouve à nouveau la séquence initiale des sommes.

[1] Il est démontré que $v_p(a+b) \geq v_p(a) + v_p(b)$.

On comprend que les réglettes étant construites à l'avance, et un simple glissement permettant de passer d'un nombre à un autre, les vérifications sont très rapides.

Annexe 3 : L"'empilement" des valuations p-adiques"

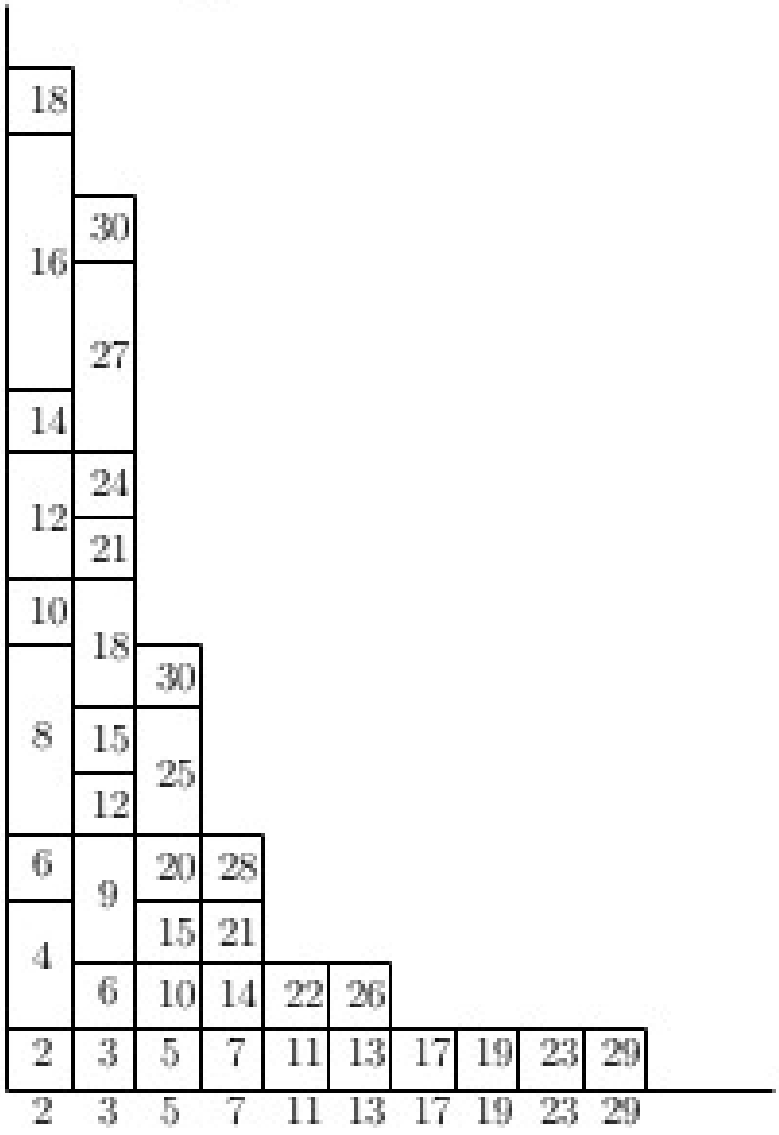
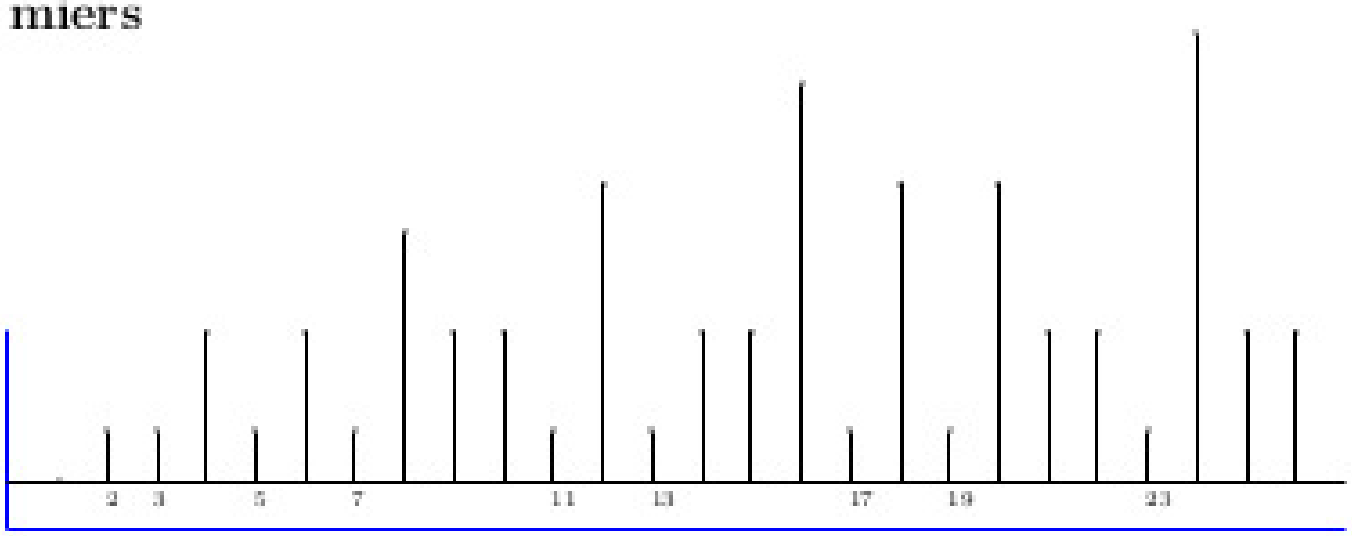


FIG. 4 – Courbe hyperbolique d'équation $xy = nlog(n)$

Annexe 6 : la séquence fractale des nombres premiers



La séquence fractale des nombres premiers (de dimension fonction de la primorielle ?)

C'est insatisfaisant, on poursuit les calculs. Ce sera la somme des puissances 4èmes des racines ajoutée à la somme des carrés des racines qui sera "quasiment" divisible par 98 ($19^4+31^4+37^4+19^2+31^2+37^2 = 2930694$ tandis que $29905 \times 98 = 2930690$).

On essaye ainsi de trouver des polynômes symétriques qui relient *toutes* les solutions ensemble. Les résultats sont présentés dans le tableau ci-dessous.

Nombre pair 2a	*Nombres premiers décomposants*	*polynôme divisible(ou"presque") par* 2a
6	3	$\Sigma x + \Sigma x^2$
8	3	$\Sigma x + \Sigma x^2 + \Sigma x^3 + \Sigma x^4$
10	3, 5	$\Sigma x + \Sigma x^3$
12	5	$\Sigma x + \Sigma x^2 + \Sigma x^3 + \Sigma x^4$
14	3, 7	$\Sigma x + \Sigma x^4$
16	3, 5	$\Sigma x + \Sigma x^3$
18	5, 7	Σx^3
20	3, 7	$\Sigma x + \Sigma x^3$
22	3, 5, 11	Σx^2
24	5, 7, 11	$\Sigma x + \Sigma x^2$
26	3, 7, 13	Σx^4
28	5, 11	Σx^3
30	7, 11, 13	Σx^3
32	3, 13	$\Sigma x + \Sigma x^3$
34	3, 5, 11, 17	$\Sigma x^3 + \Sigma x^4$
36	5, 7, 13, 17	$\Sigma x^3 + \Sigma x^4$
38	7, 19	$\Sigma x + \Sigma x^2 + \Sigma x^3$
40	3, 11, 17	$\Sigma x + \Sigma x^2 + \Sigma x^3$
42	5, 11, 13, 19	Σx^2
44	3, 7, 13	$\Sigma x + \Sigma x^2 + \Sigma x^3$
46	3, 5, 17, 23	$\Sigma x^2 + \Sigma x^4$
48	5, 7, 11, 17, 19	$\Sigma x + \Sigma x^3 + \Sigma x^4$
50	3, 7, 13, 19	$\Sigma x^2 + \Sigma x^4$
52	5, 11, 23	Σx^2
54	7, 11, 13, 17, 23	Σx^3
56	3, 13, 19	$\Sigma x + \Sigma x^2 + \Sigma x^3 + \Sigma x^4$
58	5, 11, 17, 29	Σx^2
60	7, 13, 17, 19, 23, 29	$\Sigma x + \Sigma x^2 + \Sigma x^3 + \Sigma x^4$
62	3, 19, 31	$\Sigma x^2 + \Sigma x^3$
64	3, 5, 11, 17, 23	Σx^3
66	5, 7, 13, 19, 23, 29	$\Sigma x + \Sigma x^4$
68	7, 31	$\Sigma x^2 + \Sigma x^3$
70	3, 11, 17, 23, 29	$\Sigma x^3 + \Sigma x^4$
72	5, 11, 13, 19, 29, 31	$\Sigma x + \Sigma x^3$
74	3, 7, 13, 31, 37	Σx^4
76	3, 5, 17, 23, 29	Σx
78	5, 7, 11, 17, 19, 31, 37	$\Sigma x^2 + \Sigma x^3$
80	7, 13, 19, 37	$\Sigma x + \Sigma x^4$
82	3, 11, 23, 29, 41	$\Sigma x^3 + \Sigma x^4$

Nombre pair 2a	*Nombres premiers décomposants*	*polynôme divisible(ou"presque") par* 2a
84	$5, 11, 13, 17, 23, 31, 37, 41$	Σx^3
86	$3, 7, 13, 19, 43$	Σx
88	$5, 17, 29, 41$	$\Sigma x^3 + \Sigma x^4$
90	$7, 11, 17, 19, 23, 29, 31, 37, 43$	$\Sigma x + \Sigma x^2 + \Sigma x^3$
92	$3, 13, 19, 31$	$\Sigma x + \Sigma x^2$
94	$5, 11, 23, 41, 47$	$\Sigma x + \Sigma x^3$
96	$7, 13, 17, 23, 29, 37, 43$	$\Sigma x + \Sigma x^3$
98	$19, 31, 37$	$\Sigma x^2 + \Sigma x^4$
100	$3, 11, 17, 29, 41, 47$	$\Sigma x + \Sigma x^2 + \Sigma x^3$
128	$19, 31, 61$	$\Sigma x^2 + \Sigma x^3$

6 Conclusion

Tous ces résultats sont étranges, même si rien de systématique n'a été trouvé. De plus, Abel a prouvé l'impossibilité de résoudre l'équation générale de degré supérieur à 5 par radicaux. Il est vrai qu'ici, à aucun moment, il n'a été question d'équation générale. Enfin, quand on est seulement amatrice, les cours d'algèbre, de théorie des groupes, de théorie des anneaux sont totalement hermétiques, même si on aimerait beaucoup avoir une explication. A feuilleter ces cours et ces ouvrages, on prend la pleine mesure de notre incompréhension. Finissons cependant humoristiquement avec cette citation de H.Poincaré in "La Science et l'Hypothèse" : *"une accumulation de faits n'est pas plus une science qu'un tas de pierre n'est une maison."*.

Annexe 1 : l'article d'Euler auquel il a été fait référence

L'article d'Euler "Découverte d'une loi toute extraordinaire des nombres par rapport à la somme de leurs diviseurs peut être trouvé au format *pdf* dans la page http://math-doc.ujf-grenoble.fr/OEUVRES/

Annexe 2 : programme de calcul de la somme des diviseurs des entiers successifs par la méthode récurrente d'Euler

```
#include <iostream>
#include <cmath>

const int taille = 100;
int a[taille];
int h[taille];
int euler[taille];

int f(int x) { return (3 * x * x - x) / 2 ; }

int g(int x) { return (3 * x * x + x) / 2 ; }

int fh(){
    int i, y, z;

    for (i = 1 ; i < taille ; i++)
        if (i % 2 == 0) {
```

```
            y = i / 2 ;
            z = f(y) ;
            h[i] = z ; }
        else {
            y = (i-1) / 2 ;
            z = g(y) ;
            h[i] = z ; } }

int fa(){
    int i;

    for (i = 1 ; i < taille ; i++)
        if (i % 4 == 1) a[i] = 1 ;
        else if (i % 4 == 2) a[i] = 1 ;
        else if (i % 4 == 0) a[i] = -1 ;
        else if (i % 4 == 3) a[i] = -1 ; }

int calcule(){
    int x, y, somme;

    euler[0] = 1 ;
    euler[1] = 1 ;
    for (x = 1 ; x < taille ; x++) {
        somme = 0 ;
        y = 1 ;
        while (x - h[y+1] >= 0)
            if (x == h[y+1])
                somme = somme + a[y] * x;
            else
                somme = somme + a[y] * euler[x - h[y+1]];
                y++ ;}
        euler[x] = somme ;}}

int main (int argc, char* argv[]){
    int i, x;

    fa();
    fh();
    calcule();
    for (i = 1 ; i < taille ; i++)
        std::cout << " " << euler[i];}
```

Le petit baluchon

Denise Vella-Chemla

21 février 2014

On voudrait rassembler ici les cailloux trouvés durant la promenade.

1 Sinusoïdes

On s'est intéressé à elles en réalisant que $sin(5\pi x)$ s'annule 4 fois sur l'intervalle $]0,1[$, pour les fractions $\frac{1}{5};\frac{2}{5};\frac{3}{5};\frac{4}{5}$. De même, la sinusoïde $sin(p\pi x)$ s'annule exactement $p-1$ fois sur l'intervalle $]0,1[$ et ce jamais sur un point sur lequel s'annule la sinusoïde d'un nombre premier p' inférieur à $\sqrt{p}$. On saisit ainsi bien l'infinité de l'intervalle $]0,1[$, les sinusoïdes d'une infinité de nombres premiers réussissant à s'intercaler sans les toucher entre toutes les sinusoïdes correspondant à des nombres premiers plus petits et déjà placées sur l'intervalle.

Si on se place sur la droite réelle habituelle au lieu de se focaliser sur l'intervalle $]0,1[$, les décomposants de Goldbach se calculent très simplement ; ce sont les seuls nombres entiers inférieurs à $n/2$ qui n'annulent pas le produit suivant :

$$\prod_{p \text{ un nb 1ers} \leq \sqrt{n}} sin\left(\frac{x\pi}{p}\right).sin\left(\frac{(n-x)\pi}{p}\right)$$

En annexe sont fournis de tels produits de sinusoïdes présentant le fait que 5 est décomposant de Goldbach de 16, que 7, 11, 17 et 19 sont décomposants de Goldbach de 48 ou encore que 19, 31 et 37 sont décomposants de Goldbach de 98.

On est tenté de relier ces interférences entre sinusoïdes à l'expérience de mécanique quantique dite des "fentes de Young".

2 Essayer de suivre les professeurs : rechercher la limpidité et la sincérité

Nathalie Charraud signale le souci du style de présentation des résultats et de la transmission qui motive Cantor. Il insiste en effet sur l' 'effort de présenter le cheminement de pensée aussi clairement que possible" et admire particulièrement les exposés d'Hermite pour leur limpidité : "Le style personnel de Cantor va avec le souci de communiquer de la façon la plus transparente possible le processus et les étapes de sa découverte.".

Ce souci de limpidité se retrouve chez Hilbert, dans un extrait de sa conférence de 1900 : "On peut néanmoins se demander s'il n'existe pas des attributs généraux caractérisant un bon problème de mathématiques. Un mathématicien des temps passés a dit : "une théorie mathématique ne doit être regardée comme parfaite que si elle a été rendue tellement claire qu'on puisse la faire comprendre au premier individu rencontré dans la rue". Cette clarté, cette limpidité si énergiquement exigée ici d'une théorie mathématique, je l'exigerai encore davantage d'un problème mathématique parfait ; ce qui est clair et limpide nous attire en effet, ce qui est embrouillé nous rebute".

L'extrait particulièrement émouvant de Galois : "On doit prévoir que, traitant des sujets aussi nouveaux, hasardé dans une voie aussi insolite, bien souvent des difficultés se sont présentées que je n'ai su vaincre.

Aussi, dans ces deux mémoires et surtout dans le second qui est plus récent, trouvera-t-on souvent la formule : "Je ne sais pas". La classe des lecteurs dont j'ai parlé au commencement ne manquera pas d'y trouver à rire. C'est que malheureusement on ne se doute pas que le livre le plus précieux du plus savant serait celui où il dirait tout ce qu'il ne sait pas, c'est qu'on ne se doute pas qu'un auteur ne nuit jamais tant à ses lecteurs que quand il dissimule une difficulté. Quand la concurrence, c'est à dire l'égoïsme, ne règnera plus dans les sciences, quand on s'associera pour étudier, au lieu d'envoyer aux Académies des paquets cachetés, on s'empressera de publier les moindres observations pour peu qu'elles soient nouvelles, et on ajoutera : Je ne sais pas le reste.".

En cherchant à suivre Galois, on a trouvé que les décomposants de Goldbach de n sont les solutions communes et inférieures à $n/2$ de l'inéquation $x^2 - nx \neq 0$ que l'on doit résoudre simultanément dans tous les corps premiers $\mathbb{Z}/p_i\mathbb{Z}$ avec p_i un nombre premier quelconque inférieur à $\sqrt{n}$.

Traitons l'exemple de la recherche des décompositions de Goldbach de 98.
Le polynôme $x^2 - 98x$ est égal à $x^2 - 2x$ dans $\mathbb{Z}/3\mathbb{Z}$ tandis qu'il est égal à $x^2 - 3x$ dans $\mathbb{Z}/5\mathbb{Z}$, ou encore égal à x^2 tout simplement dans $\mathbb{Z}/7\mathbb{Z}$ puisque 7 divise 98.

Notons dans un tableau pour les nombres premiers supérieurs à $\sqrt{98}$ et inférieurs à 49 la moitié de 98 les valeurs des polynômes en question et voyons ceux qui sont éliminés dans chacun des corps premiers.

	11	13	17	19	23	29	31	37	41	43	47
x^2 (dont on teste la nullité dans $\mathbb{Z}/7\mathbb{Z}$)	121	169	289	361	529	841	961	1369	1681	1849	220
$x^2 - 2x$ (dont on teste la nullité dans $\mathbb{Z}/3\mathbb{Z}$)	~~99~~	143	~~255~~	323	~~483~~	~~783~~	899	1295	~~1599~~	1763	241
$x^2 - 3x$ (dont on teste la nullité dans $\mathbb{Z}/5\mathbb{Z}$)	88	~~130~~	238	304	~~460~~	754	868	1258	1558	~~1720~~	206

On voit que ne sont conservés que les nombres 19, 31 et 37 qui sont comme attendu les décomposants de Goldbach de 98.

3 Somme des diviseurs d'Euler[1], minimiser / maximiser

L'article d'Euler *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs* est magique. On reste subjugué par la manière dont le mathématicien a trouvé la formule récurrente de la somme des diviseurs. Même le fait de la programmer la laisse hermétique. On trouve particulièrement esthétique la manière dont les nombres pentagonaux surgissent de la combinaison par différence de la suite des entiers et de la suite des impairs. Ci-dessous une formule récurrente plus simple que celle d'Euler pour calculer la somme des diviseurs d'un entier $\sigma(n)$.

$$\sigma(n) = \frac{12}{n^2(n-1)} \sum_{k=1}^{k=n-1} (5k(n-k) - n^2)\sigma(k)\sigma(n-k)$$

On peut voir les nombres premiers comme des minima locaux de la fonction somme des diviseurs.

Puisque la somme des diviseurs d'un nombre premier p vaut $p+1$, $p+q$ est une décomposition de Goldbach de n si et seulement si $\sigma(p) + \sigma(q) = n + 2$. Les décomposants de Goldbach minimisent donc la somme de la somme des diviseurs de p et de la somme des diviseurs de q.

L'idée duale consiste à trouver les décomposants de Goldbach en maximisant le produit des indicateurs d'Euler des deux décomposants. Dominique Ceugniet a vérifié cette idée par programme jusqu'à 7.10^6[2].

1. M. Giard, qui fournit cette formule récurrente différente de celle d'Euler sur la toile dans les notes de la séquence A000203 de l'OEIS fournit comme explication que cette formule provient d'un résultat de Chazy mais ceci serait à confirmer par des spécialistes des fonctions modulaires.
2. une cacahuète devant l'infini.

4 Ma conjecture

Tout nombre pair supérieur à 14 partage un décomposant de Goldbach avec $n-6$.

5 Addition disjointe

La définition récursive $x \oplus y = x + y - xy$ simplifie considérablement les calculs provenant de l'application du principe d'inclusion-exclusion.

Par exemple,

$$\begin{aligned}((a \oplus b) \oplus c) \oplus d &= ((a+b-ab) \oplus c) \oplus d \\ &= ((a+b-ab)+c-(a+b-ab)c) \oplus d \\ &= (a+b-ab+c-ac-bc+abc) \oplus d \\ &= a+b+c+d-ab-ac-ad-bc-bd-cd+abc+abd+acd+bcd-abcd\end{aligned}$$

6 Rêves d'un prince

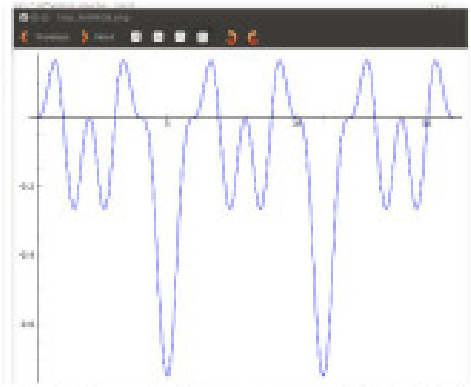
On peut trouver sur la toile le journal mathématique de Gauss. On y lit que Gauss a étudié la conjecture de Goldbach le 14 mai 1796 à Göttingen. On peut imaginer que les deux premières lettres mystérieuses du mot GEGAN qui apparaît dans la citation "Vicimus GEGAN" du 11 octobre 1796 sont les initiales respectives de Goldbach et Euler...

Ci-dessous l'extrait de la lettre qu'il a adressée à Sophie Germain, qui s'était fait passer pour un homme M. Leblanc, pour lui envoyer les résultats de ses travaux en théorie des nombres.

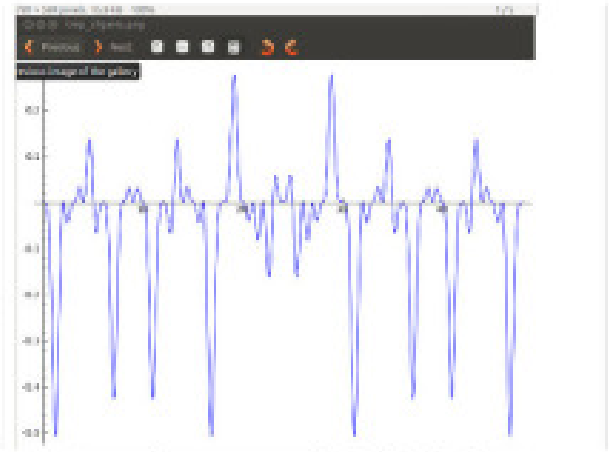
"Le goût pour les sciences abstraites en général et surtout pour les mystères des nombres est fort rare : on ne s'en étonne pas ; les charmes enchanteurs de cette sublime science ne se dévèlent dans toute leur beauté qu'à ceux qui ont le courage de les approfondir. Mais lorsqu'une personne de ce sexe, qui, par nos moeurs et par nos préjugés, doit rencontrer infiniment plus d'obstacles et de difficultés que les hommes à se familiariser avec ces recherches épineuses, sait néanmoins franchir ces entraves et pénétrer ce qu'elles ont de plus caché, il faut sans doute qu'elle ait le plus noble courage, des talents tout à fait extraordinaires, le génie supérieur. En effet, rien ne pourrait me prouver d'une manière plus flatteuse et moins équivoque, que les attraits de cette science, qui ont embelli ma vie de tant de jouissances, ne sont pas chimériques, que la prédilection dont vous l'avez honorée."

Annexe : 3 exemples de calculs de produits de sinusoïdes pour trouver les décomposants de Goldbach des nombres pairs 16, 48 et 98

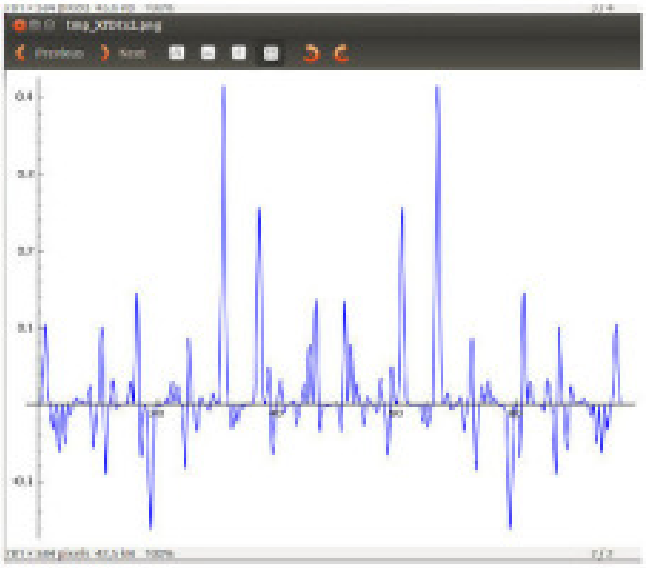
5 est décomposant de Goldbach de 16.



7, 11, 17 et 19 sont décomposants de Goldbach de 48.



19, 31 et 37 sont décomposants de Goldbach de 98.



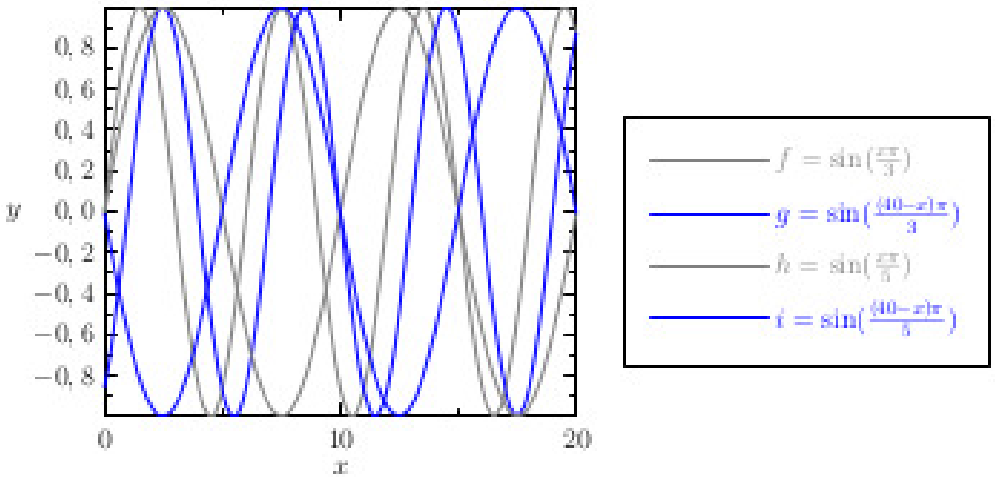
On ne réexplique pas ici la représentation par les grilles de divisibilité qui nous a permis de mieux comprendre la conjecture de Goldbach et dont l'exemple du nombre pair 40 est représenté ci-dessus. 11 et 17, qui ne sont divisibles ni par 3 ni par 5 et qui ne partagent avec 40 aucun de leur reste dans des divisions euclidiennes par 3 ou 5 (i.e. dont la colonne ne contient pas de case colorée) sont des décomposants de Goldbach de 40.

On a proposé à partir de ces grilles la possibilité de trouver les décomposants de Goldbach en calculant des produits de sinusoïdes.

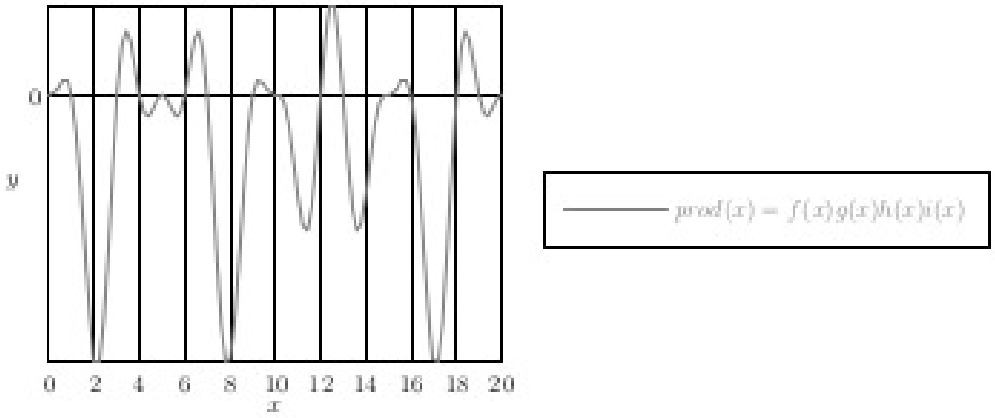
Les décomposants de Goldbach de n sont en effet les seuls nombres entiers impairs inférieurs à $n/2$ qui n'annulent pas le produit suivant :

$$\prod_{3 \leqslant p \text{ et } p \text{ premier} \leqslant \sqrt{n}} \sin\left(\frac{x\pi}{p}\right).\sin\left(\frac{(n-x)\pi}{p}\right)$$

Les sinusoïdes correspondant au cas du nombre pair 40 (se reporter à la grille de divisibilité ci-dessus) sont :



Leur produit ne s'annule effectivement pas pour les nombres entiers impairs 11 et 17.



On peut établir une analogie entre ces sinusoïdes et les fonctions d'onde de la mécanique quantique. En poussant l'analogie, on peut imaginer qu'on puisse établir une probabilité qu'un nombre pair ait un décomposant de Goldbach sans pouvoir établir sa valeur, selon une sorte de principe d'incertitude.

Enfin, si on souhaite établir une analogie avec la propriété d'*intrication quantique* : on associe à chaque case de la grille de divisibilité ci-dessus un q-bit qui est simultanément dans les états 0 et 1. On peut imaginer cette grille comme de taille infinie si on considère tous les nombres pairs d'un même coup. Le fait de fixer

Primalité et zéros de sommes de cosinus

Denise Vella-Chemla

10/7/14

L'article d'Euler *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs* est magique. On reste subjugué par la manière dont le mathématicien a trouvé la formule récurrente de la somme des diviseurs.

On peut trouver sur un forum de mathématiques à l'adresse *http://www.les-mathematiques.net/phorum/read.php?5,892412,892599* une autre formule :

$$\sigma(n) = \sum_{k=1}^{n} \sum_{l=1}^{k} cos\left(\frac{2\pi nl}{k}\right)$$

Les cosinus se comportent ici comme des booléens qui comptent pour chaque diviseur sa valeur comme une somme de 1, de façon analogue à la fonction $Succ$ de l'arithmétique de Peano.

Du coup, on en déduit une manière rigolote de trouver les nombres premiers : ce sont les zéros de la fonction *sumsumcos* ci-dessous :

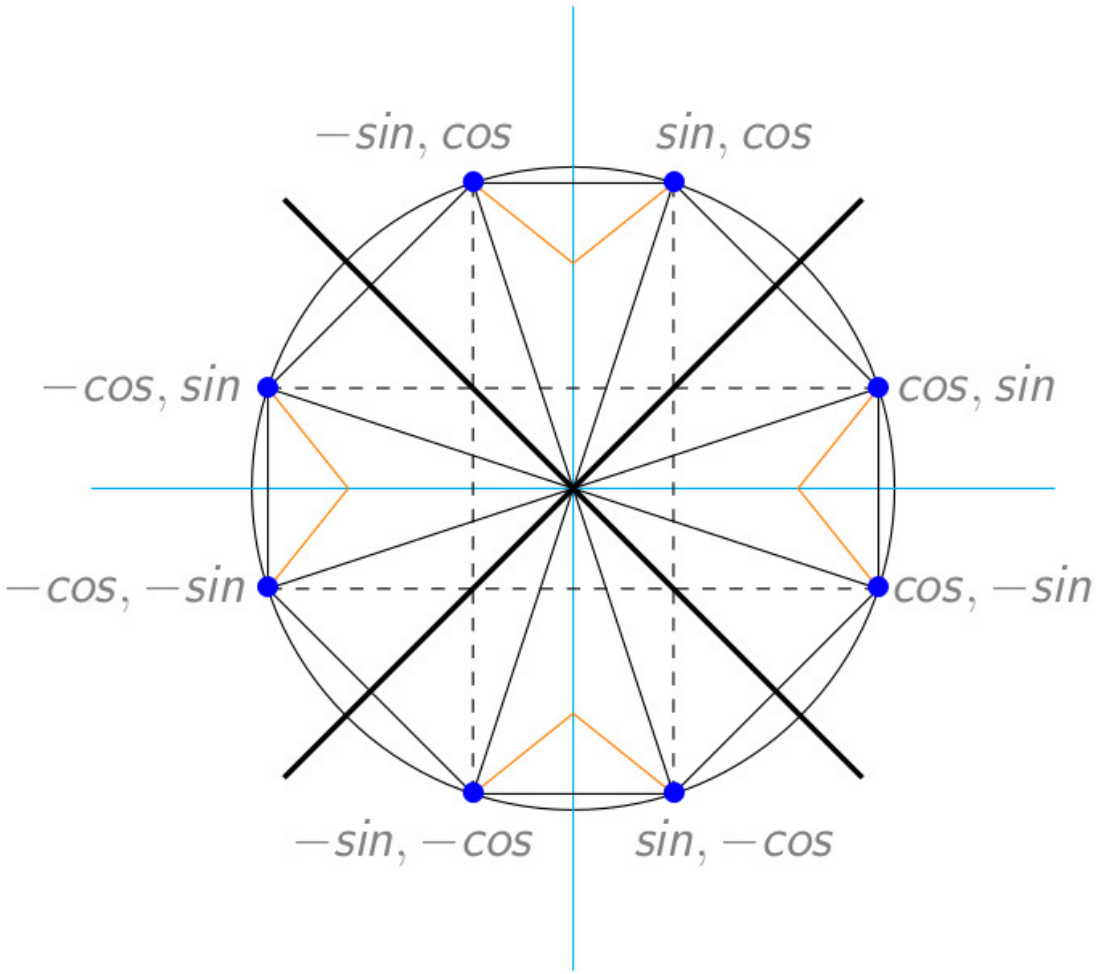
$$sumsumcos(n) = \sum_{k=2}^{n-1} \sum_{l=1}^{k} cos\left(\frac{2\pi nl}{k}\right)$$

For me, that's F_{un} !

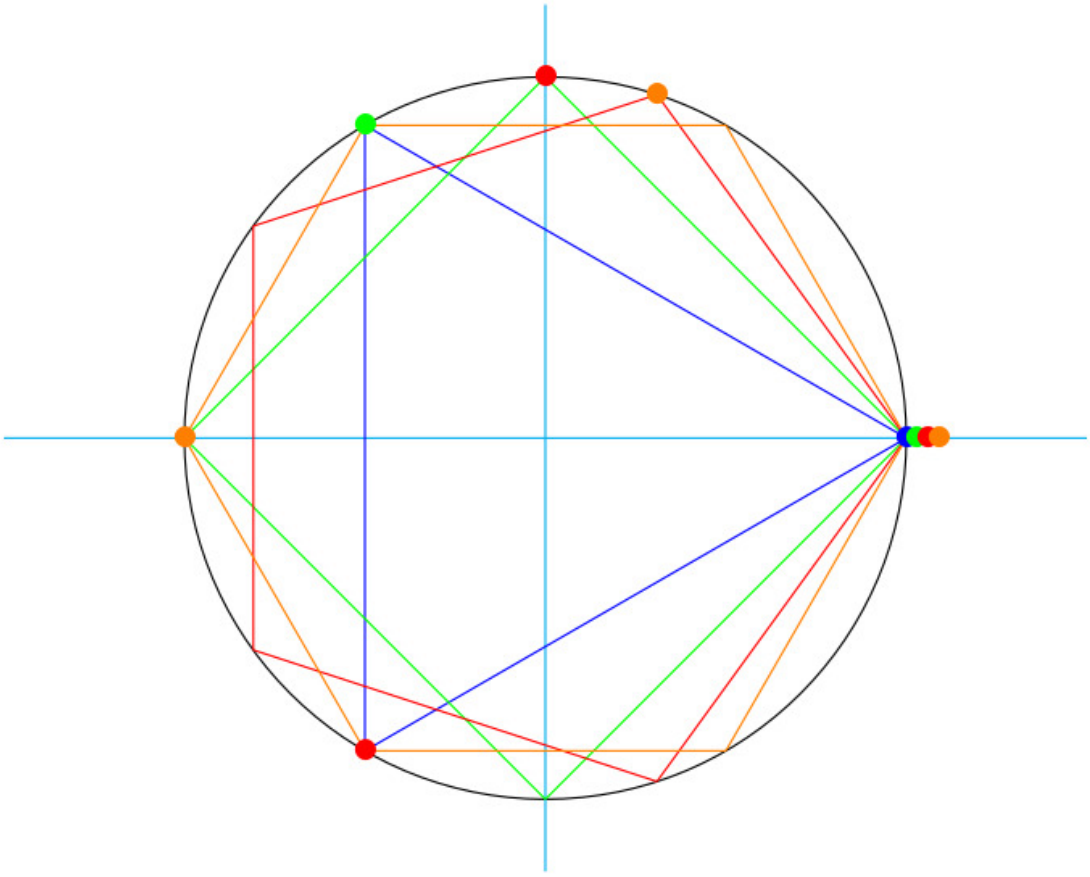
L'opérateur Snur∞

$$PlusUn = \begin{pmatrix} exp\left(\frac{2i\pi}{2}\right) & 0 & 0 & 0 & 0 & \dots \\ 0 & exp\left(\frac{2i\pi}{3}\right) & 0 & 0 & 0 & \dots \\ 0 & 0 & exp\left(\frac{2i\pi}{5}\right) & 0 & 0 & \dots \\ 0 & 0 & 0 & exp\left(\frac{2i\pi}{7}\right) & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

Malte



Polygones sur lesquels cyclent les restes modulaires



Tables de résidus quadratiques des modules 3 à 51 (Denise Vella-Chemla, 16.8.16)

Voici les tables qui permettent d'induire, de visu, mais cela ne reste qu'une hypothèse :

- que les nombres premiers de la forme $4k+3$ ont strictement plus de $n/4$ résidus quadratiques inférieurs ou égaux à leur moitié ;
- que les nombres premiers de la forme $4k+1$ ont $(n-1)/4$ résidus quadratiques inférieurs ou égaux à leur moitié ;
- que les nombres composés ont moins de $n/4$ résidus quadratiques inférieurs ou égaux à leur moitié.

On commence par calculer les carrés modulo le nombre n considéré et les noter dans la troisième ligne, sous la barre. Puis on colorie leur occurrence dans les deux premières lignes. Enfin, on compte les petits résidus quadratiques (notés *prq*, i.e. ceux qui sont inférieurs à $n/2$, et qui apparaissent dans la seconde ligne).

Module $n = 3$ (1 prq $> 3/4$)

2
1
1

Module $n = 5$ (1 prq)

4	3
1	2
1	4

Module $n = 7$ (2 prq $> 7/4$)

6	5	4
1	2	3
1	4	2

Module $n = 9$ (2 prq $< 9/4$)

8	7	6	5
1	2	3	4
1	4	0	7

Module $n = 11$ (4 prq $> 11/4$)

10	9	8	7	6
1	2	3	4	5
1	4	9	5	3

Module $n = 13$ (3 prq $= 13/4$)

12	11	10	9	8	7
1	2	3	4	5	6
1	4	9	3	12	10

Module $n = 15$ (3 prq $< 15/4$)

14	13	12	11	10	9	8
1	2	3	4	5	6	7
14	9	1	10	6	4	

Module $n = 17$ (4 proj $= 17/4$)

16	15	14	13	12	11	10	9
1	2	3	4	5	6	7	8
1	4	9	16	8	2	15	13

Module $n = 19$ (6 proj $> 19/4$)

18	17	16	15	14	13	12	11	10
1	2	3	4	5	6	7	8	9
1	4	9	16	6	17	11	7	5

Module $n = 21$ (4 proj $< 21/4$)

20	19	18	17	16	15	14	13	12	11
1	2	3	4	5	6	7	8	9	10
1	4	9	16	4	15	7	1	18	16

Module $n = 23$ (7 proj $> 23/4$)

22	21	20	19	18	17	16	15	14	13	12
1	2	3	4	5	6	7	8	9	10	11
1	4	9	16	2	13	3	18	12	8	6

Module $n = 25$ (5 proj $< 25/4$)

24	23	22	21	20	19	18	17	16	15	14	13
1	2	3	4	5	6	7	8	9	10	11	12
1	4	9	16	0	11	24	14	6	0	21	19

Module $n = 27$ (6 proj $< 27/4$)

26	25	24	23	22	21	20	19	18	17	16	15	14
1	2	3	4	5	6	7	8	9	10	11	12	13
1	4	9	16	25	9	22	10	0	19	13	9	7

Module $n = 29$ (7 proj $> 29/4$)

28	27	26	25	24	23	22	21	20	19	18	17	16	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	4	9	16	25	7	20	6	23	13	5	28	24	22

Module $n = 31$ (9 proj $> 31/4$)

30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	4	9	16	25	5	18	2	19	7	28	20	14	10	8

Module $n = 33$ (7 proj $< 33/4$)

32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	4	9	16	25	3	16	31	15	1	22	12	4	31	27	25

Module $n = 35$ (7 proj $< 35/4$)

34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	4	9	16	25	1	14	29	11	30	16	4	29	21	15	11	9

Module $n = 37$ (9 prq $> 37/4$)

36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	4	9	16	25	36	12	27	7	26	10	33	21	11	3	34	30	28

Module $n = 39$ (8 prq $< 39/4$)

38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	4	9	16	25	36	10	25	3	22	4	27	13	1	30	22	16	12	10

Module $n = 41$ (10 prq $> 41/4$)

40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	4	9	16	25	36	8	23	40	18	39	21	5	32	20	10	2	37	33	31

Module $n = 43$ (12 prq $> 43/4$)

42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	4	9	16	25	36	6	21	38	14	35	15	40	24	10	41	31	23	17	13	11

Module $n = 45$ (6 prq $< 45/4$)

44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	4	9	16	25	36	4	19	36	10	31	9	34	16	0	31	19	9	1	40	36	34

Module $n = 47$ (14 prq $> 47/4$)

46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	4	9	16	25	36	2	17	34	6	27	3	28	8	37	21	7	42	32	24	18	14	12

Module $n = 49$ (11 prq $< 49/4$)

48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	4	9	16	25	36	0	15	32	2	23	46	22	0	29	11	44	30	18	8	0	43	39	37

Module $n = 51$ (10 prq $< 51/4$)

50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26
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
1	4	9	16	25	36	49	13	30	49	19	42	16	43	21	1	34	18	4	43	33	25	19	15	13

On remarque enfin un élément qu'il est peut-être intéressant de souligner : selon le module $p = 23$ par exemple, les carrés s'obtenant par additions d'impairs successifs à partir de 0, on a la succession de restes modulaires suivante :

$$0 \xrightarrow{+1} 1 \xrightarrow{+3} 4 \xrightarrow{+5} 9 \xrightarrow{+7} 16 \xrightarrow{+9} 2$$

$$\xrightarrow{+11} 13 \xrightarrow{+13} 3 \xrightarrow{+15} 18 \xrightarrow{+17} 12 \xrightarrow{+19} 8 \xrightarrow{+21} 6$$

dans laquelle on compte 7 restes quadratiques inférieurs ou égaux à $11 = \dfrac{23-1}{2}$.

Approche purement syntaxique (Denise Vella-Chemla, 12.1.2017)

1) Modéliser

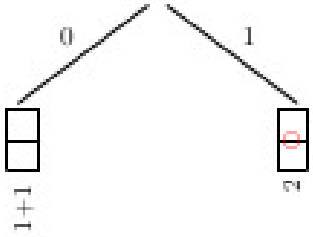
On cherche ce que les nombres premiers symétrisent.

On sait par exemple qu'un nombre premier p a exactement $\frac{p-1}{2}$ résidus quadratiques, tandis que ce n'est pas le cas d'un nombre composé. Si on considère x et $p-x$ inférieurs à p, soit tous 2 sont résidus quadratiques de p simultanément, soit si l'un l'est, l'autre ne l'est pas et inversement. On peut voir dans ces faits une forme de symétrie.

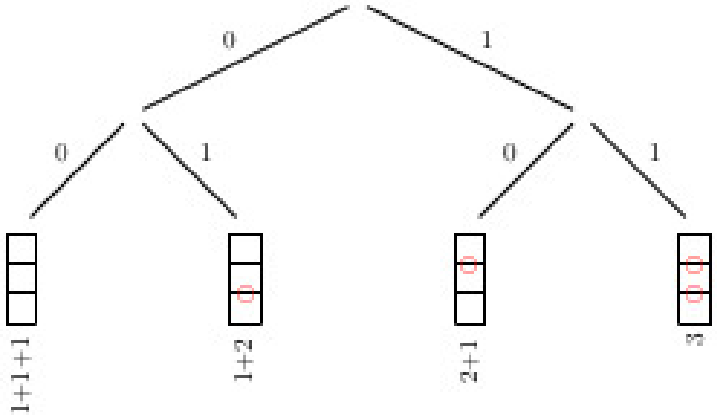
Cherchons d'autres formes de symétrie en étudiant les compositions des nombres. On prend comme référence l'article de wikipedia https://fr.wikipedia.org/wiki/Composition_(*combinatoire*).

Un nombre n a 2^{n-1} compositions différentes. On peut voir les compositions de n comme feuilles d'un arbre binaire de hauteur $n-1$. On voit que l'ordre des sommants importe, 1+1+2+2 et 1+2+1+2 sont des compositions différentes de 6 (alors qu'elles correspondent à la même partition). Il y a une correspondance bijective entre les mots booléens de $n-1$ caractères et les compositions de n. Par exemple, le mot de 5 lettres 10010 correspond à la décomposition $2+1+2+1$ de 6.

Arbre binaire des compositions de 2



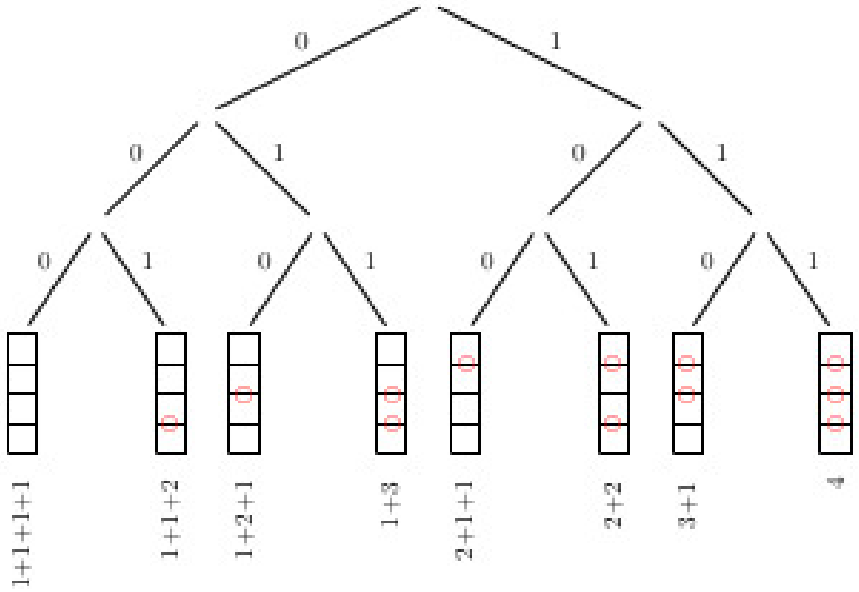
Arbre binaire des compositions de 3 (lire les dessins de haut en bas)



Pour obtenir une composition de $n+1$ à partir d'une composition de n, il suffit soit d'ajouter un sommant 1+ au début de la composition de n, soit de remplacer le premier sommant de la composition de n par son successeur, en obtenant à partir de la composition $n = s_0 + A$ la composition $n+1 = (1+s_0) + A$, le calcul entre parenthèses devant être effectivement effectué.

Voyons cela pour le passage des compositions de 3 à celles de 4 : de l'ensemble $\{1+1+1, 1+2, 2+1, 3\}$ des compositions de 3, on peut concaténer 1+ au début de chaque somme, ce qui permet d'obtenir l'ensemble de compositions de 4 $\{1+1+1+1, 1+1+2, 1+2+1, 1+3\}$; ou bien dans chaque composition de 3, on remplace le premier sommant par son successeur, ce qui permet d'obtenir l'ensemble de compositions de 4 $\{2+1+1, 2+2, 3+1, 4\}$. On réitère le processus pour passer de l'ensemble des compositions de 4 $\{1+1+1+1, 1+1+2, 1+2+1, 1+3, 2+1+1, 2+2, 3+1, 4\}$ à l'ensemble de compositions de 5 constitué de l'union des deux ensembles $\{1+1+1+1+1, 1+1+1+2, 1+1+2+1, 1+1+3, 1+2+1+1, 1+2+2, 1+3+1, 1+4\}$ et $\{2+1+1+1, 2+1+2, 2+2+1, 2+3, 3+1+1, 3+2, 4+1, 5\}$.

Arbre binaire des compositions de 4



On appelle compositions triviales les deux compositions constituées l'une uniquement de n caractères 1 séparés par des signes "+", de la forme $1+1+\ldots+1$, et l'autre de n seul. Un nombre composé est notamment caractérisé par le fait que l'une de ses compositions au moins, différente des deux compositions triviales, est telle que quelle que soit la permutation qu'on pourrait effectuer entre 2 de ses sommants, cette composition reste identique à elle-même. Il en est ainsi de la composition 2+2+2 de 6, ou 5+5+5+5+5 de 25. Un nombre premier n'a aucune de ses compositions qui est ainsi invariante par toute permutation de ses sommants. Cette caractérisation de la primalité est exclusivement syntaxique.

2) Essayer de formaliser

A chaque entier est associé un ensemble de parties de $\mathbb{N}$. Chaque partie de $\mathbb{N}$ est une application de $\mathbb{N}$ dans $\{0,1\}$ et on code par un booléen le fait qu'une partie soit image d'un entier ou pas.

Une partie de $\mathbb{N}$ étant codée par un mot infini, on complète chaque mot booléen de la section précédente par une infinité de 0 ; cette infinité de zéros à droite n'ajoute pas de sommant à l'écriture additive.

$$\begin{aligned}&\mathbb{N} \longrightarrow \{0,1\}^{\{0,1\}^n}\\ &n \longmapsto \left\{s \in \{0,1\}^{\mathbb{N}} / \forall i \geqslant n, s[i]=0\right\} \subset \mathcal{P}(\mathbb{N})\end{aligned}$$

Voyons en quoi consiste le passage d'un entier au suivant selon cette formalisation (informatiquement, c'est trivial, ça consiste à concaténer une lettre 0 ou 1 à gauche des mots de n).

On a le diagramme suivant :

$$\begin{array}{ccc}\mathbb{N} & \xrightarrow{d_n} & \{0,1\}^{\{0,1\}^n}\\ \downarrow{\scriptstyle +1} & & \downarrow{\scriptstyle d_{n+1}}\\ \mathbb{N} & \xrightarrow{d_n} & \{0,1\}^{\{0,1\}^n}\end{array}$$

avec $d_n : \mathbb{N} \longrightarrow \{0,1\}$ et

$$\begin{array}{rccl} d_{n+1} : & k & \longmapsto & d_n(k-1), \forall k \geqslant 1\\ & 0 & \longmapsto & 0\\ & & \longmapsto & 1\end{array}$$

La condition correspondant au fait d'être composé pour un nombre entier qui consiste à avoir une composition (différente des deux compositions triviales) de la forme $x+x+\ldots+x+x$ se traduit très simplement sur les mots booléens : elle consiste en l'apparition dans le mot d'une puissance au moins carrée d'un sous-mot non-nul (le sous-mot en question est appelé période en théorie des langages rationnels) ; par

exemple, la composition $2+2+2$ de 6, codée par le mot $1010100000\ldots$ contient le sous-mot 10 répété trois fois, elle s'écrit $(10)^3 0^\infty$.

Annexe 1 : les 32 compositions de 6 et leur mot booléen correspondant

$1+1+1+1+1+1$ (00000)	$2+1+1+1+1$ (10000)
$1+1+1+1+2$ (00001)	$2+1+1+2$ (10001)
$1+1+1+2+1$ (00010)	$2+1+2+1$ (10010)
$1+1+1+3$ (00011)	$2+1+3$ (10011)
$1+1+2+1+1$ (00100)	$2+2+1+1$ (10100)
$1+1+2+2$ (00101)	$2+2+2$ (10101)
$1+1+3+1$ (00110)	$2+3+1$ (10110)
$1+1+4$ (00111)	$2+4$ (10111)
$1+2+1+1+1$ (01000)	$3+1+1+1$ (11000)
$1+2+1+2$ (01001)	$3+1+2$ (11001)
$1+2+2+1$ (01010)	$3+2+1$ (11010)
$1+2+3$ (01011)	$3+3$ (11011)
$1+3+1+1$ (01100)	$4+1+1$ (11100)
$1+3+2$ (01101)	$4+2$ (11101)
$1+4+1$ (01110)	$5+1$ (11110)
$1+5$ (01111)	6 (11111)

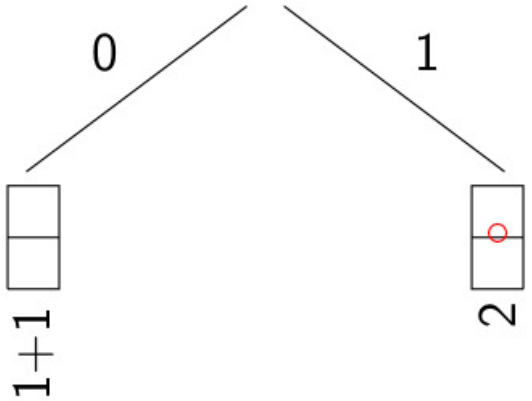
Annexe 2 : Programme de passage des mots booléens aux compositions

```
#include <cstdlib>
#include <iostream>
#include <vector>

using std::cout;
using std::endl;
using std::atoi;

typedef std::vector<bool> bitset;

void print_bits(bitset &bits) {
    for (int i = 0; i < bits.size(); ++i)
        cout << (int) bits[i];
}

void print_deco(bitset &bits) {
    int s = 1;
    for (int i = 0; i < bits.size(); ++i) {
        if (bits[i]) {
            ++s;
        } else {
            cout << s << "+";
            s = 1;
        }
    }
    cout << s;
}
```

```
void generate(int n, bitset &bits) {
    if (n-- > 0) {
        bits[n] = 0; generate(n, bits);
        bits[n] = 1; generate(n, bits);
    } else {
        print_bits(bits);
        cout << " : ";
        print_deco(bits);
        cout << endl;
    }
}

int main(int argc, char* argv[]) {
    int n_max = 0;
    if (argc > 1) n_max = atoi(argv[1]);
    for (int n = 0; n < n_max; ++n) {
        cout << "n = " << n + 1 << " :" << endl;
        bitset bits(n);
        generate(n, bits);
        cout << endl;
    }
}
```

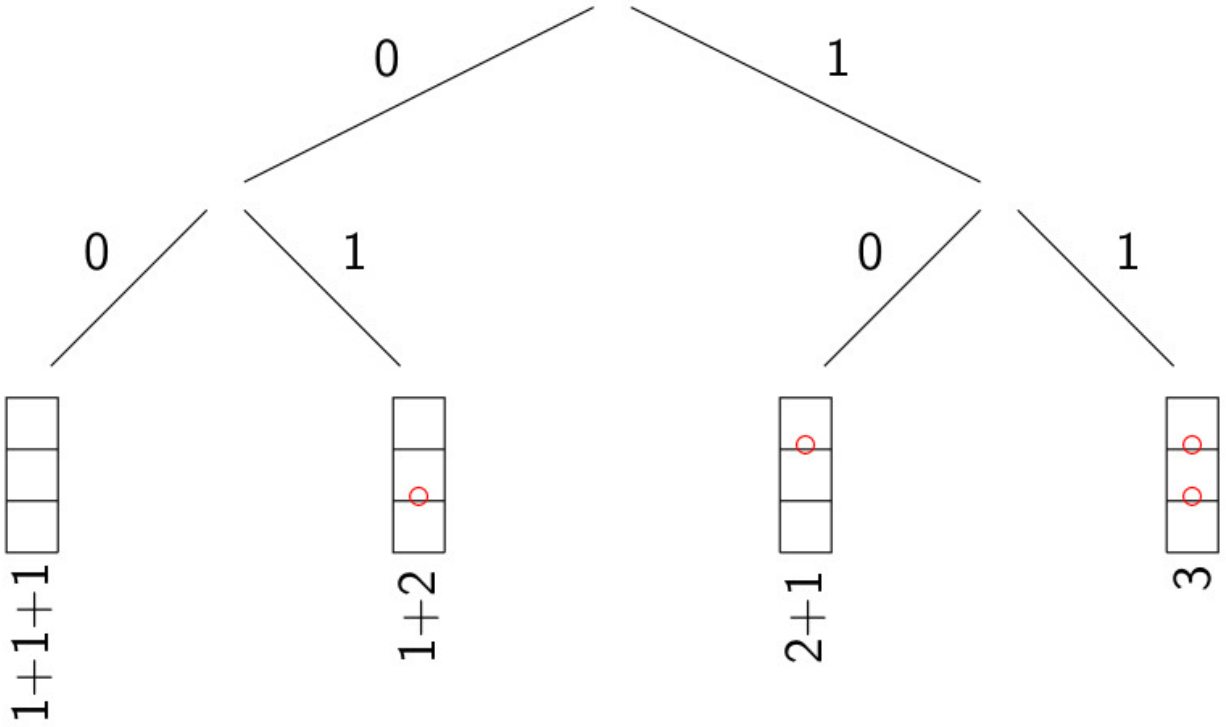
Compositions et mots booléens

- A chaque entier n, on associe ses 2^{n-1} compositions additives.
- *exemple* : arbre binaire des compositions de 2



Exemple

- *exemple* : arbre binaire des compositions de 3



- Noter que la composition $1 + 2$ est différente de la composition $2 + 1$.

Obtention des compositions de $n+1$ à partir de celles de n

- On concatène 0 ou 1 au début de chaque mot booléen de n.
- Cela correspond à deux actions syntaxiques : concaténer "1+" en début de composition ou bien remplacer le premier sommant par son successeur.

Nombre composé / nombre premier

- On appelle compositions triviales la composition correspondant au mot booléen ne contenant que des 0 (composition de la forme $1 + 1 + \ldots + 1$) ou bien la composition correspondant au mot booléen contenant $n - 1$ lettres 1 (composition de la forme n).

- Un nombre composé admet au moins une décomposition non triviale de la forme $x + x + x + \ldots + x$ contenant 2 occurrences de x au moins.

- A chaque entier est associé un ensemble de mots booléens, i.e. un ensemble de parties de $\mathbb{N}$.

$$\mathbb{N} \longrightarrow \{0,1\}^{\{0,1\}^{\mathbb{N}}}$$
$$n \longmapsto \{s \in \{0,1\}^{\mathbb{N}} / \forall i \geqslant n, s[i] = 0\} \subset \mathcal{P}(\mathbb{N})$$

Formalisation

- Le passage de n à $n+1$ est codé par le diagramme suivant :

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{d_n} & \{0,1\}^{\{0,1\}^{\mathbb{N}}} \\ {\scriptstyle +1}\downarrow & & \downarrow{\scriptstyle d_{n+1}} \\ \mathbb{N} & \xrightarrow[d_n]{} & \{0,1\}^{\{0,1\}^{\mathbb{N}}} \end{array}$$

avec $\quad d_n : \mathbb{N} \longrightarrow \{0,1\}$

et

$$d_{n+1} : \begin{array}{ccc} k & \longmapsto & d_n(k-1), \forall k \geqslant 1 \\ 0 & \longmapsto & 0 \end{array}$$

- faire l'union de cet ensemble de fonctions avec l'ensemble des fonctions d_{n+1} qui associent l'image 1 (plutôt que 0) à 0.

Nombre composé / nombre premier

- Un nombre est composé n si l'un de ces mots non triviaux (dont on considère les $n-1$ premières lettres, i.e. la partie des mots avant l'infinité de zéros) admet une période (c'est un motif qui se répète, en théorie des langages).

- Un nombre est premier si tous ses mots sont apériodiques.

Figure 1

emacs24@vella-VGN-FW51MF-H

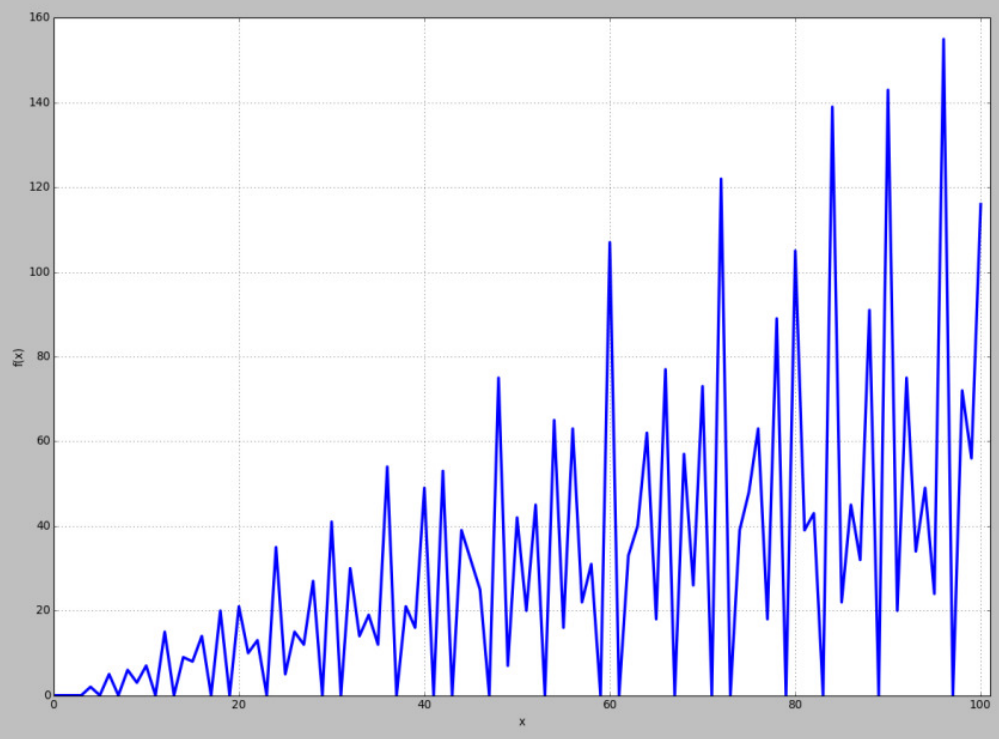
File Edit Options Buffers Tools Python Help

Save Undo

```
import mpmath
from mpmath import *

def mafct(n):
  PI = 3.14159265359
  liste=[]
  for b in range(2,n):
    for o in range(1,b+1):
      liste.append(cos(2.0*PI*n*o/b))
  return sum(liste)

for x in range(101):
  print mafct(x)

mpmath.plot(mafct,[0,101],points=101)
```

-:--- trescontente-mafct-mercredi20170712.py

Figure 1



• S'octroyer le droit de conjecturer aussi. Conjecturons, conjecturons donc : je crois que du fait que ζ s'appuie sur Γ, il faut chercher pour comprendre ζ du côté de la divisibilité des factorielles (Γ est l'extension de la factorielle au plan complexe). J'ai lu dans la Théorie des nombres de Lucas un théorème intéressant sur la divisibilité des factorielles. Pour trouver l'exposant de 7 dans la factorielle de 10000, il divise itérativement 10000 par 7 et il ajoute les quotients. Cela a comme conséquence qu'un nombre premier est le seul nombre dont on soit sûr qu'il apparaît à puissance de 1 dans la factorisation de sa factorielle, les premiers plus petits que lui peuvent apparaître à puissance plus grande (par exemple dans la factorisation de 7!, 3 est dans 3 mais aussi caché dans 6). Peut-être que cette propriété mise au jour par Lucas permettrait de plaquer un ordre total sur les nombres, ce que ne permet pas la divisibilité qui plaque un ordre partiel sur eux. C'est peut-être aussi cette propriété qui aurait pour conséquence l'alignement des zéros...

90
92
3 87 89
5 85 87
7 83 85
11 79 81
13 77 79
17 73 75
19 71 73
23 67 69
29 61 63
31 59 61
37 53 55
41 49 51
43 47 49
89 91
87 89
85 87
81 83
79 81
77
73 75
69 71
63 65
61 63
55 57
51 53
49 51

« Mon intérêt passionné pour la justice sociale et la responsabilité sociale s'opposa toujours curieusement à mon inaptitude marquée pour tout désir d'association directe avec les hommes et les femmes. Je suis un cheval pour le harnais individuel, nullement taillé pour le tandem ou l'attelage. Je n'ai jamais appartenu de tout cœur à aucun pays ni à aucun Etat, ni à mes amis, ni même à ma propre famille. Ces liens s'accompagnent toujours d'un vague éloignement, et l'envie de me retirer en moi-même s'est accrue avec les années. Un tel isolement est parfois amer, mais je ne regrette pas d'y être coupé de la compréhension ou de la sympathie des autres. J'y perds quelque chose à coup sûr, mais en revanche je me libère des coutumes, des opinions ou des préjugés d'autrui et ne suis point tenté de fonder ma sérénité d'esprit sur de si mouvantes assises ».

Probabilités disjointes ou application du crible de Poincaré quand on élimine au maximum 2 classes de congruence sur p selon tout p premier (Denise Vella-Chemla, 26.1.2019)

Il s'agit ici d'écrire correctement un calcul[1] qui utilise la formule du crible de Poincaré.

On a vu dans d'autres notes que trouver les décomposants de Goldbach d'un nombre pair n supérieurs à $\sqrt{n}$ consiste à cribler les nombres qui n'ont aucun reste de division nul dans des divisions euclidiennes par les nombres premiers inférieurs à la racine carrée de n et qui, de plus, ne partagent aucun reste de division avec n. C'est ce que l'on note "application du crible de Poincaré quand on élimine au maximum 2 classes de congruence sur p (pour tout p premier inférieur à $\sqrt{n}$)". On élimine *au maximum* 2 classes de congruence car selon tout diviseur p' de n (p' premier), seuls les nombres de la classe $\hat{0}$ sont éliminés.

Un nombre a une chance sur deux d'être divisible par 2, une chance sur 3 d'être divisible par 3, une chance sur n d'être divisible par n.

Combien de chances un nombre a-t-il d'être divisible soit par 2 soit par 3 ?

Les probabilités concernant la divisibilité par 2 ou par 3 sont indépendantes l'une de l'autre. On appellera "addition disjointe" l'opération définie par $x \oplus y = x + y - xy$ qui va nous permettre de calculer la possibilité pour un nombre d'être divisible soit par 2 soit par 3.

$$\frac{1}{2} \oplus \frac{1}{3} = \frac{1}{2} + \frac{1}{3} - \frac{1}{6} = \frac{4}{6}$$

Effectivement, de 1 à 6, il y a 4 nombres divisibles par 2 ou par 3 (2, 4 et 6 le sont par 2 et 3 et 6 le sont par 3).

L'intérêt de cette "addition disjointe" est qu'elle permet d'obtenir directement les résultats de fastidieux calculs faisant appel à la combinatoire (produit de 2 nombres parmi n, de 3 nombres parmi n, etc) à cause de la propriété d'associativité.

$$\begin{aligned}((a \oplus b) \oplus c) \oplus d &= ((a+b-ab) \oplus c) \oplus d \\ &= ((a+b-ab) + c - (a+b-ab)c) \oplus d \\ &= (a+b-ab+c-ac-bc+abc) \oplus d \\ &= a+b+c+d-ab-ac-ad-bc-bd-cd+abc+abd+acd+bcd-abcd\end{aligned}$$

1. du 9 janvier 2019.

Le programme ci-dessous calcule le résultat obtenu en appliquant la formule de Poincaré aux nombres premiers compris entre 3 et 100.

```
from math import *

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

        mult = 0.0
for n in range(13,101,2):
  if prime(n):
    mult=mult+(float(n)-2)/float(n)-((float(n)-2)/n)*mult
    print(str(n)+"  -->"+str(mult))
```

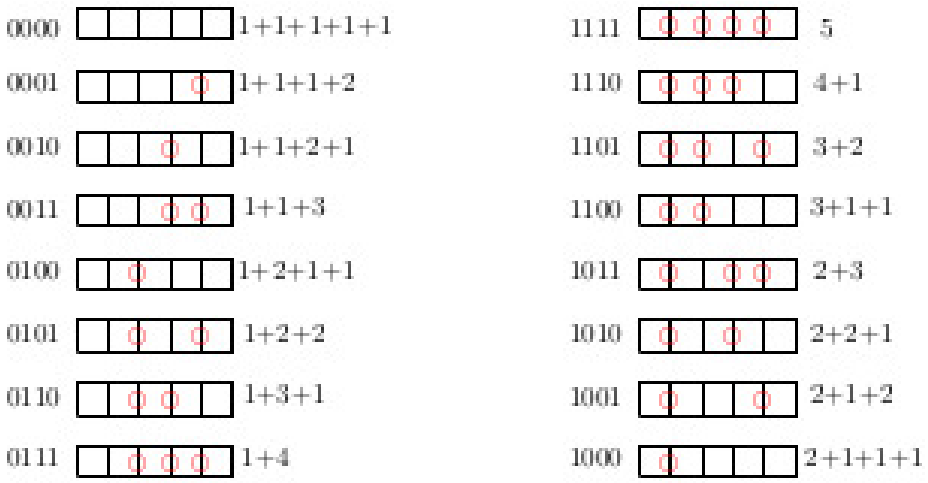
Voici le résultat de l'application du programme pour les nombres premiers compris entre 3 et 100. L'application de la formule lorsque $p = 2$ donne un résultat nul.

```
3 .........0.333333333333
5 .........0.733333333333
7 .........0.92380952381
11 ........0.986147186147
13 ........0.997868797869
17 ........0.999749270338
19 ........0.999973607404
23 ........0.999997704992
29 ........0.999999841724
31 ........0.999999989789
37 ........0.999999999448
41 ........0.999999999973
43 ........0.999999999999
47 ........1.0
53 ........1.0
59 ........1.0
61 ........1.0
67 ........1.0
71 ........1.0
73 ........1.0
79 ........1.0
83 ........1.0
89 ........1.0
97 ........1.0
```

Compositions palindromiques (Denise Vella-Chemla, 29.4.2019)

Il s'agit ici de revenir à une modélisation plaisante[1] qui considère les mots palindromiques associés aux nombres entiers et qui permet de caractériser la primalité en théorie des mots.

On rappelle les mots booléens, les représentations imagées par des coupures ou au contraire accolements entre cases et les compositions additives associées au nombre 5.



Un nombre n a 2^{n-1} compositions additives (chaque séparation entre 2 cases de la représentation imagée, ou chaque booléen du mot à gauche peut prendre la valeur 0 ou 1).

On ne va s'intéresser parmi ces compositions qu'aux mots palindromiques, en quantité $2^{\lfloor \frac{n}{2} \rfloor}$.

Un mot palindromique peut être lu dans les deux sens, il est égal à son image-miroir (par exemple, radar ou rotor sont palindromiques). Le nombre de mots palindromiques ($2^{\lfloor \frac{n}{2} \rfloor}$) se justifie par le fait qu'il y en a autant que de mots de longueur moitié moindre, et la moitié droite du mot est alors totalement déterminée par sa moitié gauche, puisqu'elle doit en être l'image-miroir.

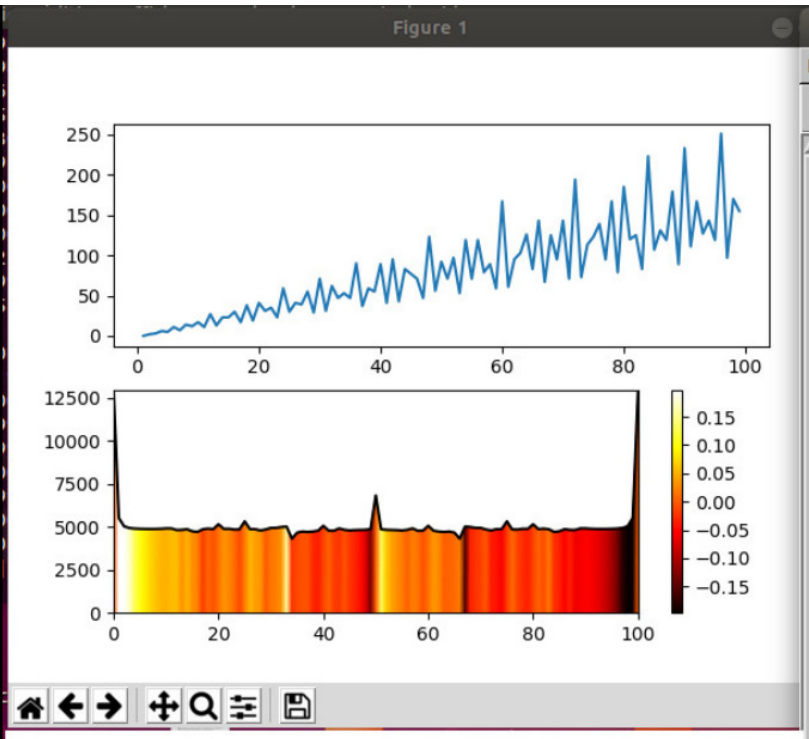
Voici les mots palindromiques pour l'entier 7, au nombre de 8 : les deux mots triviaux 000000 (correspondant à 1+1+1+1+1+1+1) et 111111 (correspondant à 7) ; et les moins triviaux, 001100 (correspondant à 1+1+3+1+1), 010010 (resp. 1+2+1+2+1), 011110 (ou 1+5+1), 101101 (ou 2+3+2), 110011 (ou 3+1+3) et 100001 (ou 2+1+1+1+2). Un moyen sûr d'allonger un mot palindromique en conservant sa palindromie est de le faire par les extrémités du mot, soit en ajoutant deux lettres 0, soit en ajoutant deux lettres 1 à ses extrémités.

Un nombre n est alors composé si l'un de ses mots (non triviaux) associés m_k, auquel on concatène un 0 (noté en rouge pour le distinguer du mot initial) est une puissance au moins carrée de l'un des sous-mots propres de m_k. Inversement, un nombre n est premier si aucun de ses mots associés m_k ne vérifie cette propriété.

Par exemple, aucun des mots palindromiques associés à 7 et auxquels on concatène un 0 n'est puissance de l'un de ses sous-mots propres : $0011000, 0100100, 0111100, 1000010, 1100110, 1011010$.
9 est composé : son mot associé 11011011 auquel on concatène 0 est puissance cubique de 110.

$$11011011\textcolor{red}{0} = (110)^3$$

1. étudiée un peu en janvier 2017, voir http://denisevellachemla.eu/compo-sans-pgm.pdf



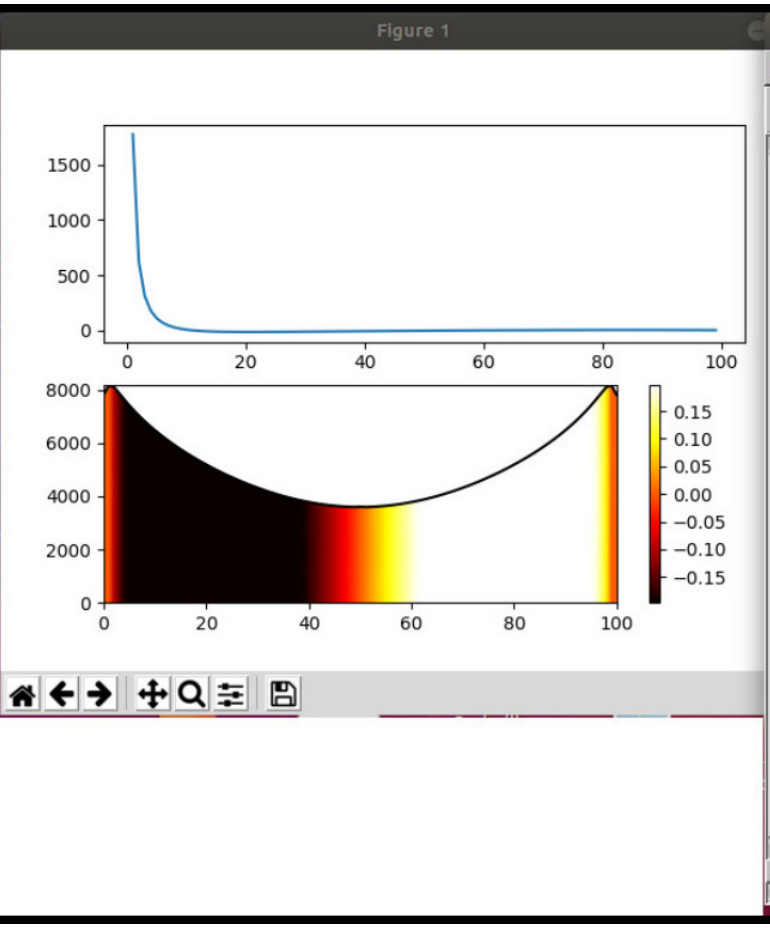
emacs25@vellachemla-X510UA

File Edit Options Buffers Tools Python Help

```
import numpy as np
import matplotlib.pyplot as plt

dt = 0.1
autren = 100
t = range(1,autren)
signal = [np.sum([sum([np.cos(2*np.pi*n*o/b) if (n != 0) else 1 for o in r
ange(1,b+1)]) for b in range(2,100)]) for n in range(100)]
print(signal)
plt.subplot(211)
plt.plot(t,signal[1:])

fourier = np.fft.fft(signal)
freq = np.fft.fftfreq(autren, d=dt)
plt.subplot(212)
k = np.arange(autren)
x = np.append(k, k[-1]+k[1]-k[0]) # calcul d'une valeur supplementaire
z = np.append(fourier, fourier[0])
X = np.array([x,x])
y0 = np.zeros(len(x))
y = np.abs(z)
Y = np.array([y0,y])
Z = np.array([z,z])
C = np.angle(Z)

plt.plot(x,y,'k')

plt.pcolormesh(X, Y, C, cmap='hot',shading="gouraud",vmin=-np.pi/16.0, vma
x=np.pi/16.0)
plt.colorbar()
plt.show()
```

-:--- **flute3.py** All L7 (Python)

Wrote /home/vella-chemla/Desktop/flute3.py



emacs25@vellachemla-X510UA

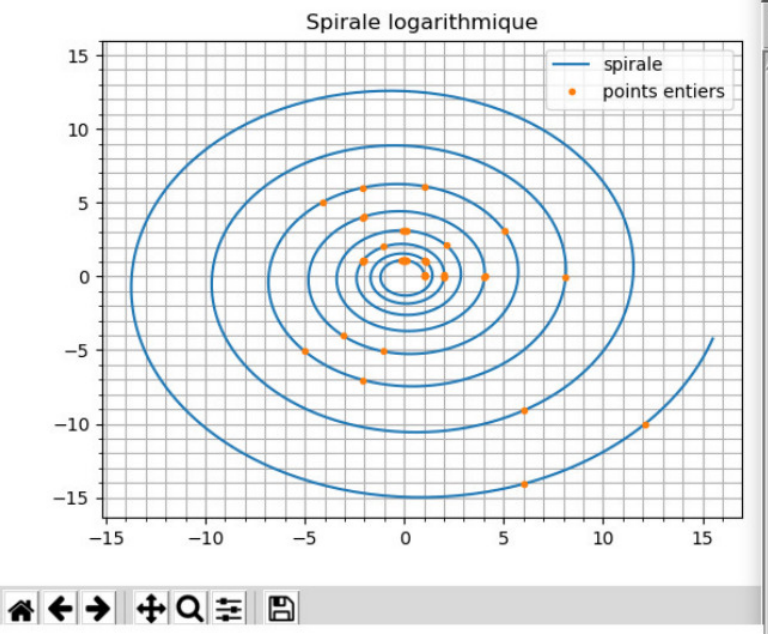
File Edit Options Buffers Tools Python Help

```
import numpy as np
import matplotlib.pyplot as plt

dt = 0.1
autren = 100
t = range(1,autren)
signal = [np.sum([sum([np.cos(2*np.pi*n*o/b)/(2*np.pi*n*o/b) if (n != 0) else 1 f
or o in range(1,b+1)]) for b in range(2,100)]) for n in range(100)]
print(signal)
plt.subplot(211)
plt.plot(t,signal[1:])

fourier = np.fft.fft(signal)
freq = np.fft.fftfreq(autren, d=dt)
plt.subplot(212)
k = np.arange(autren)
x = np.append(k, k[-1]+k[1]-k[0]) # calcul d'une valeur supplementaire
z = np.append(fourier, fourier[0])
X = np.array([x,x])
y0 = np.zeros(len(x))
y = np.abs(z)
Y = np.array([y0,y])
Z = np.array([z,z])
C = np.angle(Z)

plt.plot(x,y,'k')

plt.pcolormesh(X, Y, C, cmap='hot',shading="gouraud",vmin=-np.pi/16.0, vmax=np.p
i/16.0)
plt.colorbar()
plt.show()
```

-:--- **flute3.py** All L27 (Python)

Wrote /home/vella-chemla/Desktop/flute3.py

Figure 1



emacs25@vellachemla-X510UA

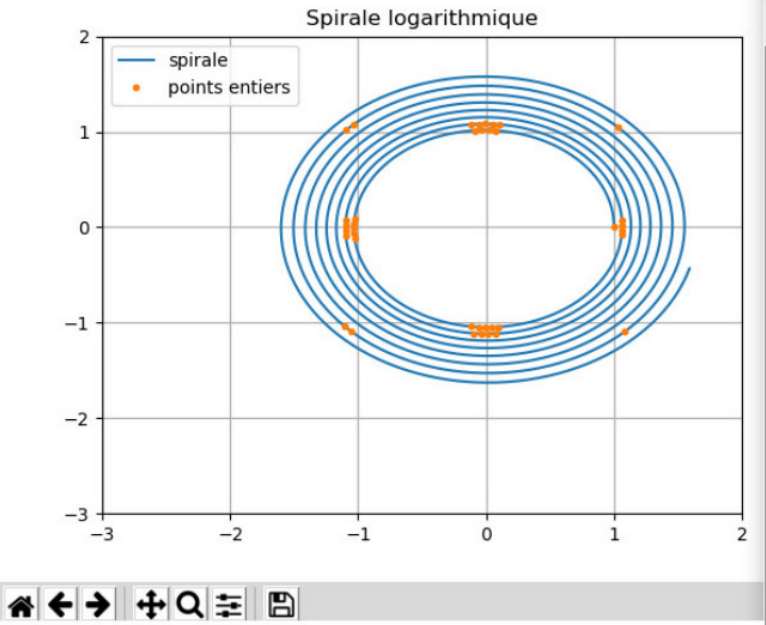
File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np

a, b = 1.0, 0.05555

t = np.linspace(0, 50, 2000)
x = a*np.exp(b*t)*np.cos(t)
y = a*np.exp(b*t)*np.sin(t)

err = 0.12
p = [(i, u, v) for i, (u, v) in enumerate(zip(x, y)) if abs(u-int(u)) < err and
abs(v-int(v)) < err]
u = [c[1] for c in p]
v = [c[2] for c in p]
w = [t[c[0]] for c in p]
for i in range(len(w)):
    print('{}: {}, {}'.format(w[i], u[i], v[i]))

plt.plot(x, y, '-', label='spirale')
plt.plot(u, v, '.', label='points entiers')
plt.title("Spirale logarithmique")
plt.legend()
xmin, xmax = int(np.min(x))-2, int(np.max(x))+2
ymin, ymax = int(np.min(y))-2, int(np.max(y))+2
minor_ticks = np.arange(xmin, xmax, 1)
axes = plt.gca()
axes.set_xticks(minor_ticks, minor=True)
axes.set_yticks(minor_ticks, minor=True)
plt.grid(b=True, which='both', axis='both')

plt.show()
```

-(DOS)--- **spirale.py** All L4 (Python)

Wrote /home/vella-chemla/Desktop/spirale.py

Figure 1



emacs25@vellachemla-X510UA

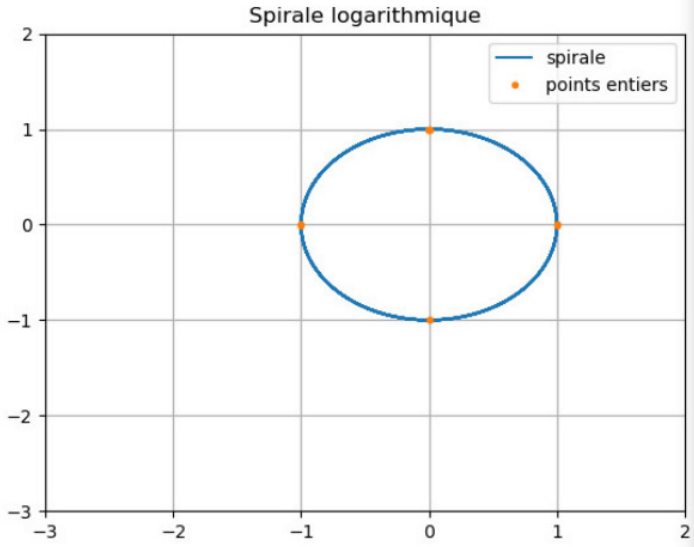
File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np

a, b = 1.0, 0.01

t = np.linspace(0, 50, 1000)
x = a*np.exp(b*t)*np.cos(t)
y = a*np.exp(b*t)*np.sin(t)

err = 0.12
p = [(i, u, v) for i, (u, v) in enumerate(zip(x, y)) if abs(u-int(u)) < err and
abs(v-int(v)) < err]
u = [c[1] for c in p]
v = [c[2] for c in p]
w = [t[c[0]] for c in p]
for i in range(len(w)):
    print('{}: {}, {}'.format(w[i], u[i], v[i]))

plt.plot(x, y, '-', label='spirale')
plt.plot(u, v, '.', label='points entiers')
plt.title("Spirale logarithmique")
plt.legend()
xmin, xmax = int(np.min(x))-2, int(np.max(x))+2
ymin, ymax = int(np.min(y))-2, int(np.max(y))+2
minor_ticks = np.arange(xmin, xmax, 1)
axes = plt.gca()
axes.set_xticks(minor_ticks, minor=True)
axes.set_yticks(minor_ticks, minor=True)
plt.grid(b=True, which='both', axis='both')

plt.show()
```

-(DOS)--- **spirale.py** All L4 (Python)

Wrote /home/vella-chemla/Desktop/spirale.py

Figure 1



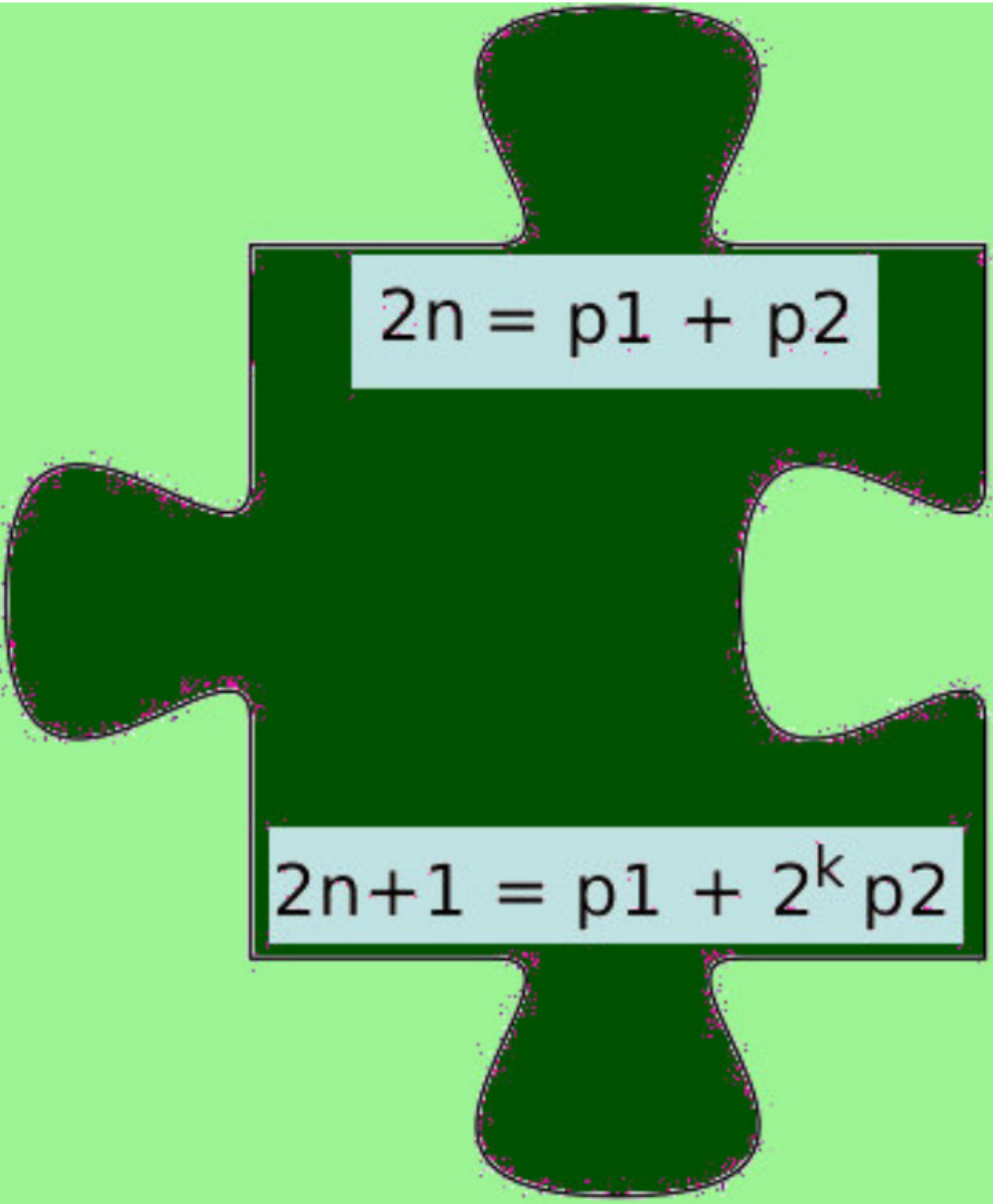
emacs25@vellachemla-X510UA

File Edit Options Buffers Tools Python Help

```
import matplotlib.pyplot as plt
import numpy as np

a, b = 1.0, 0.000001

t = np.linspace(0, 50, 1000)
x = a*np.exp(b*t)*np.cos(t)
y = a*np.exp(b*t)*np.sin(t)

err = 0.12
p = [(i, u, v) for i, (u, v) in enumerate(zip(x, y)) if abs(u-int(u)) < err and
abs(v-int(v)) < err]
u = [c[1] for c in p]
v = [c[2] for c in p]
w = [t[c[0]] for c in p]
for i in range(len(w)):
    print('{}: {}, {}'.format(w[i], u[i], v[i]))

plt.plot(x, y, '-', label='spirale')
plt.plot(u, v, '.', label='points entiers')
plt.title("Spirale logarithmique")
plt.legend()
xmin, xmax = int(np.min(x))-2, int(np.max(x))+2
ymin, ymax = int(np.min(y))-2, int(np.max(y))+2
minor_ticks = np.arange(xmin, xmax, 1)
axes = plt.gca()
axes.set_xticks(minor_ticks, minor=True)
axes.set_yticks(minor_ticks, minor=True)
plt.grid(b=True, which='both', axis='both')

plt.show()
```

-(DOS)--- **spirale.py** All L4 (Python)

Wrote /home/vella-chemla/Desktop/spirale.py


2n = p1 + p2
2n+1 = p1 + 2^k p2

Nombre de solutions de l'équation $x^{10} \equiv 1\ (mod\ n)$ en fonction du dernier chiffre de n (Denise Vella-Chemla, 22.12.2017)

Par programme, on a constaté les faits suivants que l'on énonce comme des conjectures :

- un nombre n qui se termine par 1 est un nombre premier ou une puissance d'un nombre premier se terminant par un 1 si et seulement si l'équation modulaire $x^{10} \equiv 1\ (mod\ n)$ a exactement 10 solutions ;
- un nombre n qui se termine par 3, 7 ou 9 est un nombre premier ou une puissance d'un nombre premier (se terminant par 3, 7, ou 9) si et seulement si l'équation modulaire $x^{10} \equiv 1\ (mod\ n)$ a exactement 2 solutions ;
- un nombre n qui se termine par 1 est une puissance d'un nombre premier se terminant par 3, 7, ou 9 si et seulement si l'équation modulaire $x^{10} \equiv 1\ (mod\ n)$ a exactement 2 solutions.

On a $x^{10} \equiv 1\ (mod\ n) \iff x^{10} - 1 \equiv 0\ (mod\ n)$.

Or $x^{10} - 1 = (x-1)(x+1)(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)$.

On oublie les solutions triviales 1 et $n-1$ qui annulent, l'une, le monôme $x-1$, et l'autre, le monôme $x+1$. On oublie également le polynôme alterné $x^4 - x^3 + x^2 - x + 1$ car il s'annule pour $n - x$ lorsque le polynôme $x^4 + x^3 + x^2 + x + 1$ s'annule pour x et on se concentre donc sur l'annulation de ce polynôme simple symétrique $x^4 + x^3 + x^2 + x + 1$. On cherche pourquoi il s'annule 4 fois pour un nombre premier p se terminant par 1 ou une puissance de nombre premier p^k se terminant par 1 alors qu'il ne s'annule jamais pour un nombre premier p se terminant par $3, 7$ ou 9 ou une puissance de nombre premier p^k se terminant par $3, 7$ ou 9. On ne réfléchit pas pour l'instant au fait que modulo un nombre composé n, l'équation modulaire $x^{10} \equiv 1\ (mod\ n)$ n'admet jamais 2 ou 10 solutions.

On résoud $x^4 + x^3 + x^2 + x + 1 = 0$ ainsi : on divise le polynôme par x^2. On obtient :

$$x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = 0$$

qu'on réécrit en :

$$\left(x^2 + \frac{1}{x^2}\right) + \left(x + \frac{1}{x}\right) + 1 = 0$$

(en mettant ensemble les premier et cinquième termes, ainsi que les second et quatrième termes).

On pose $X = x + \frac{1}{x}$.

L'équation se réécrit $X^2 + X - 1 = 0$. Le discriminant Δ_1 de cette nouvelle équation est égal à 5.

On a abouti aux 2 solutions suivantes pour X :

$$x + \frac{1}{x} = \frac{-1 \pm \sqrt{5}}{2}.$$

On multiplie les deux membres de l'égalité par x et on a à résoudre une autre équation du second degré :

$$x^2 + \frac{1 \pm \sqrt{5}}{2}x + 1 = 0$$

Le discriminant Δ_2 de cette seconde équation du second degré est égal à :

$$\Delta_2 = \frac{(1 \pm \sqrt{5})^2}{4} - 4 = \frac{1 \pm 2\sqrt{5} + 5 - 16}{4} = \frac{-5 \pm \sqrt{5}}{2}$$

Les deux solutions de cette seconde équation du second degré sont :

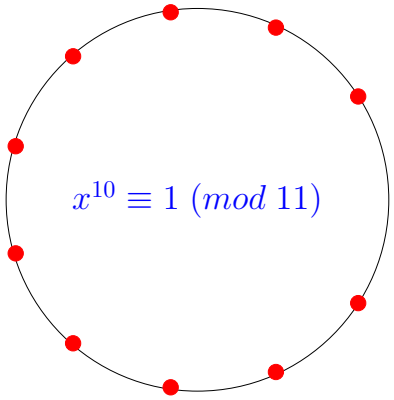
$$X = \frac{\frac{-1 \pm \sqrt{5}}{2} \pm \sqrt{\frac{-5 \pm \sqrt{5}}{2}}}{2}$$

Il n'y a aucune solution pour les nombres n de dernier chiffre 3 et 7 car modulo de tels nombres n, 5 n'est jamais un carré (i.e. n'a pas de racine carrée modulaire) dans $\mathbb{Z}/n\mathbb{Z}$.

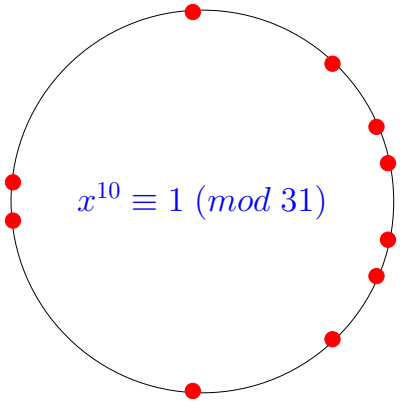
Mais pour les nombres n de dernier chiffre 1 ou 9, 5 admet toujours deux racines carrées (cf. annexe 2), il reste à comprendre pourquoi selon un module n de dernier chiffre 9, bien que 5 admette deux racines carrées modulaires, le polynôme $x^4 + x^3 + x^2 + x + 1$ ne peut cependant jamais être nul. Il faut aussi compléter le raisonnement pour les puissances d'un nombre premier plutôt que pour les nombres premiers simples.

Annexe 1 : Positionnement des solutions de l'équation $x^{10} \equiv 1 \ (mod\ p)$ *sur cercles modulaires pour* $p = 11, 31, 41, 61, 71$

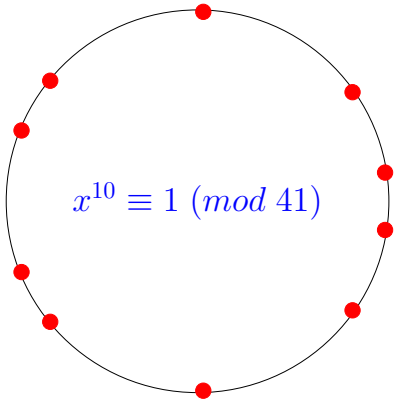
Solutions de $x^{10} \equiv 1 \ (mod\ 11)$: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. 11 est premier. Il y a 10 solutions.



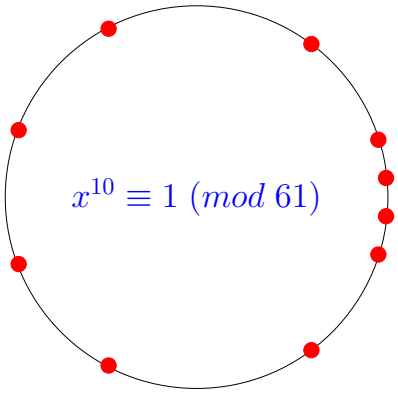
Solutions de $x^{10} \equiv 1 \ (mod\ 31)$: 1, 2, 4, 8, 15, 16, 23, 27, 29, 30. 31 est premier. Il y a 10 solutions.



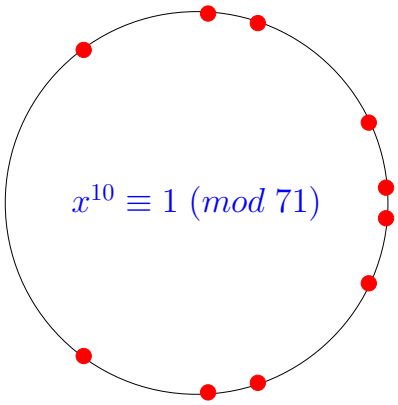
Solutions de $x^{10} \equiv 1 \ (mod\ 41)$: 1, 4, 10, 16, 18, 23, 25, 31, 37, 40. 41 est premier. Il y a 10 solutions.



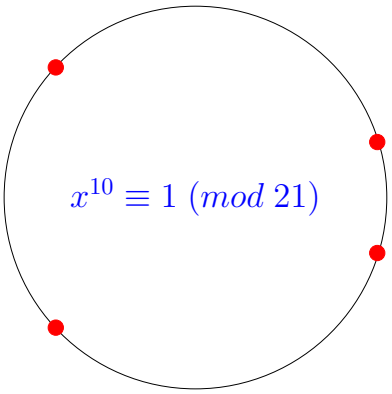
Solutions de $x^{10} \equiv 1 \ (mod\ 61)$: 1, 3, 9, 20, 27, 34, 41, 52, 58, 60. 61 est premier. Il y a 10 solutions.



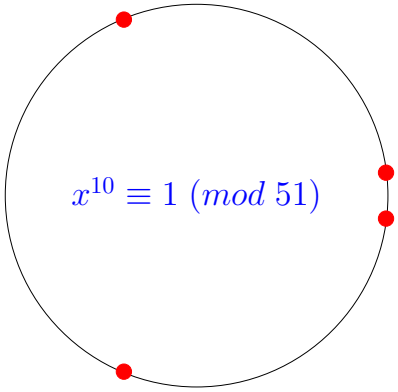
Solutions de $x^{10} \equiv 1 \ (mod\ 71)$: 1, 5, 14, 17, 25, 46, 54, 57, 66, 70. 71 est premier. Il y a 10 solutions.



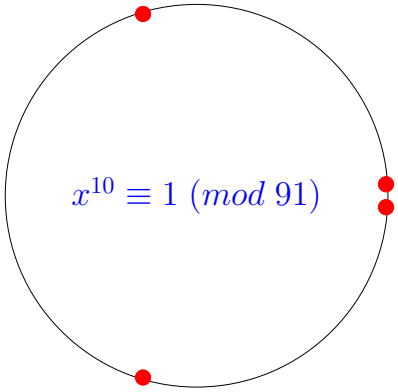
Solutions de $x^{10} \equiv 1 \ (mod\ 21)$: 1, 8, 13, 20. 21 est composé. Il y a 4 solutions.



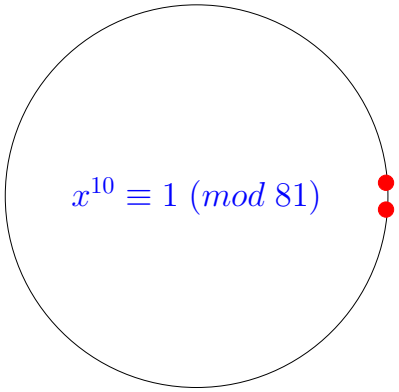
Solutions de $x^{10} \equiv 1 \ (mod\ 51)$: 1, 16, 35, 50. 51 est composé. Il y a 4 solutions.



Solutions de $x^{10} \equiv 1 \ (mod\ 91)$: 1, 27, 64, 90. 91 est composé. Il y a 4 solutions.



Solutions de $x^{10} \equiv 1\ (mod\ 81)$: 1, 80. 81 est composé, c'est une puissance d'un nombre premier se terminant par 3, l'équation n'a que deux solutions, les solutions triviales (de même par exemple, que l'équation $x^{10} \equiv 1\ (mod\ 49)$ (49 étant une puissance de 7), n'a que les deux solutions triviales 1 et 48).



Annexe 2 : Rappel des racines carrées modulaires de 5 pour les nombres n de dernier chiffre 1 ou 9 (obtenues par programme)

4 racine carrée de 5 (mod 11).
7 racine carrée de 5 (mod 11).

9 racine carrée de 5 (mod 19).
10 racine carrée de 5 (mod 19).

11 racine carrée de 5 (mod 29).
18 racine carrée de 5 (mod 29).

6 racine carrée de 5 (mod 31).
25 racine carrée de 5 (mod 31).

13 racine carrée de 5 (mod 41).
28 racine carrée de 5 (mod 41).

8 racine carrée de 5 (mod 59).
51 racine carrée de 5 (mod 59).

26 racine carrée de 5 (mod 61).
35 racine carrée de 5 (mod 61).

17 racine carrée de 5 (mod 71).
54 racine carrée de 5 (mod 71).

20 racine carrée de 5 (mod 79).
59 racine carrée de 5 (mod 79).

19 racine carrée de 5 (mod 89).
70 racine carrée de 5 (mod 89).