Cantique des nombres premiers.

Pollen.

Lien entre les derniers chiffres de la somme et du produit de deux nombres premiers consécutifs.

Esprit de contradiction ?.

Courbe de Hilbert en python-logo.

Pourquoi la moyenne des parties fractionnaires des parties réelles des zéros de ζ semble-t-elle être asymptotiquement égale à 1/2 ?.

Moyenne des parties fractionnaires des parties réelles des zéros de ζ.

Faire le point.

Relation surprenante.

Orthogonalité.

Couleur.

Belle égalité.

Nombre de tours.

Programme de calcul de la formule de Connes-Consani d'une fonction de comptage liée à la fonction zêta de Riemann.

Quel ordre ?.

Chercher des idées.

Je lui ai écrit.

Bonne idée ?.

Montrer ce qu'on a trouvé, même si on ne sait rien démontrer.

Deviendrons-nous tous des produits ?.

Snurpf, exemple.

Tables des dg des nombres de 12 à 104.

L'été, revenir à des calculs simples.

Memo pour les puissances $10^{\text{ièmes}}$.

Hyperboloïde à une nappe.

Conjecture de Goldbach et chip-firing games.

$(x1)!/x \ \in N$?.

Conjecture de Goldbach, chip-firing game, matrices 2×2 et descente infinie.

Décomposants de Goldbach sur planche de Galton.

Quantifier les nombres premiers.

Etirement.

Tendre vers 0.5.

Surface à faire vibrer.

Petit memo.

Compter les nombres premiers.

Compter les nombres composés.

Sommes par lignes d'une matrice et nombres premiers.

Une fonction de comptage des nombres premiers.

Arbres.

Ennuyée.

Danses serpentines.

Arêtes.

Alterner les termes de la somme de cosinus qui s'annule pour les nombres premiers.

Interrupteurs.

Programme en C++ pour les sommes alternées de cosinus (les $4k+3$ ont pour image 0 et les $4k+1$ ont pour image 1).

Décroissances rapides.

Interrupteurs ou bien une somme alternée de cosinus assez surprenante.

Différence de logarithmes intégrals.

Triplets Goldbachiques.

Coder le vrai par -1.

Alignements.

PGCD d'Euclide et matrices.

Essayer de comprendre la formule de Riemann.

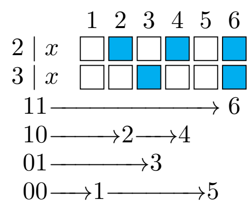
Fonction $\psi(x)$ et $\xi(t)$ de Riemann.

Cantique des nombres premiers (Denise Vella-Chemla, 3/1/2018)

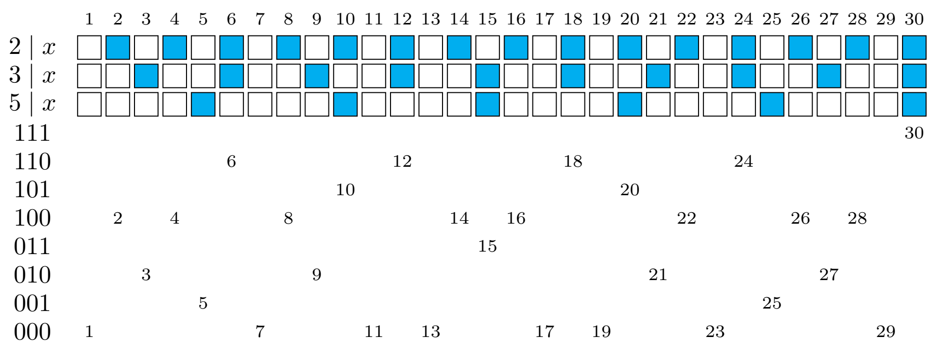
Cette note est l'ébauche d'une tentative d'utiliser le formalisme quantique pour représenter l'espace des nombres premiers.

Commençons par deux images, l'une des nombres de 1 à 6, l'autre des nombres de 1 à 30 et de leurs caractères de divisibilité l'une, par 2 et 3 et l'autre, par 2, 3 et 5.

Divisibilité par 2 ou 3 (ou inclusif) des nombres de 1 à 6



Divisibilité par 2 ou 3 ou 5 des nombres de 1 à 30



On utilise la notation par les kets de Dirac pour représenter les états suivants :

- ⋆ $|\mathbf{0_2}, 1/2\rangle$ représente l'imparité d'un nombre qui a une chance sur deux d'avoir lieu tandis que $|\mathbf{1_2}, 1/2\rangle$ représente la parité d'un nombre qui a aussi une chance sur deux d'avoir lieu ;
- ⋆ $|\mathbf{0_3}, 2/3\rangle$ représente le fait qu'un nombre a deux chances sur 3 de ne pas être divisible par 3 tandis que $|\mathbf{1_3}, 1/3\rangle$ représente le fait qu'un nombre a une chance sur 3 d'être divisible par 3 ;
- ⋆ $|\mathbf{0_5}, 4/5\rangle$ représente le fait qu'un nombre a 4 chances sur 5 de ne pas être divisible par 5 tandis que $|\mathbf{1_5}, 1/5\rangle$ représente le fait qu'un nombre a une chance sur 5 d'être divisible par 5 ;
- ⋆ plus généralement, $|\mathbf{0_p}, (p-1)/p\rangle$ représente le fait qu'un nombre a $p-1$ chances sur p de ne pas être divisible par p tandis que $|\mathbf{1_p}, 1/p\rangle$ représente le fait qu'un nombre a une chance sur p d'être divisible par p.

Faire le produit tensoriel des différents états possibles permet d'obtenir leur probabilité :

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 & b_2 \end{pmatrix} = \begin{pmatrix} a_1b_1 & a_1b_2 \\ a_2b_1 & a_2b_2 \end{pmatrix}$$

$$\begin{pmatrix} a_1b_1 & a_1b_2 \\ a_2b_1 & a_2b_2 \end{pmatrix} \otimes \begin{pmatrix} c_1 & c_2 \end{pmatrix} = \begin{pmatrix} a_1b_1c_1 & a_1b_2c_1 & a_1b_1c_2 & a_1b_2c_2 \\ a_2b_1c_1 & a_2b_2c_1 & a_2b_1c_2 & a_2b_2c_2 \end{pmatrix}$$

Pour l'exemple choisi des nombres premiers 2, 3 et 5, on a :

$$\begin{pmatrix} |\mathbf{0_2}, 1/2\rangle & |\mathbf{1_2}, 1/2\rangle \end{pmatrix} \otimes \begin{pmatrix} |\mathbf{0_3}, 2/3\rangle & |\mathbf{1_3}, 1/3\rangle \end{pmatrix} = \begin{pmatrix} |\mathbf{0_2}, 1/2\rangle\,|\mathbf{0_3}, 2/3\rangle & |\mathbf{0_2}, 1/2\rangle\,|\mathbf{1_3}, 1/3\rangle \\ |\mathbf{1_2}, 1/2\rangle\,|\mathbf{0_3}, 2/3\rangle & |\mathbf{1_2}, 1/2\rangle\,|\mathbf{1_3}, 1/3\rangle \end{pmatrix}$$

On peut “réduire le paquet d’onde” en agrégeant les probabilités mais il faut garder l’état intermédiaire à l’esprit qui seul représente la multiplicité d’états possibles.

$$\begin{pmatrix} |\mathbf{0_2 0_3}, 2/6\rangle & |\mathbf{0_2 1_3}, 1/6\rangle \\ |\mathbf{1_2 0_3}, 2/6\rangle & |\mathbf{1_2 1_3}, 1/6\rangle \end{pmatrix}$$

Réutilisons la matrice de probabilité avant réduction et occupons-nous alors de la divisibilité par 5 en effectuant le produit tensoriel :

$$\begin{pmatrix} |\mathbf{0_2}, 1/2\rangle\, |\mathbf{0_3}, 2/3\rangle & |\mathbf{0_2}, 1/2\rangle\, |\mathbf{1_3}, 1/3\rangle \\ |\mathbf{1_2}, 1/2\rangle\, |\mathbf{0_3}, 2/3\rangle & |\mathbf{1_2}, 1/2\rangle\, |\mathbf{1_3}, 1/3\rangle \end{pmatrix} \otimes \begin{pmatrix} |\mathbf{0_5}, 4/5\rangle & |\mathbf{1_5}, 1/5\rangle \end{pmatrix}$$

$$=$$

$$\begin{pmatrix} |\mathbf{0_2}, 1/2\rangle\, |\mathbf{0_3}, 2/3\rangle\, |\mathbf{0_5}, 4/5\rangle & |\mathbf{0_2}, 1/2\rangle\, |\mathbf{1_3}, 1/3\rangle\, |\mathbf{0_5}, 4/5\rangle & |\mathbf{0_2}, 1/2\rangle\, |\mathbf{0_3}, 2/3\rangle\, |\mathbf{1_5}, 1/5\rangle & |\mathbf{0_2}, 1/2\rangle\, |\mathbf{1_3}, 1/3\rangle\, |\mathbf{1_5}, 1/5\rangle \\ |\mathbf{1_2}, 1/2\rangle\, |\mathbf{0_3}, 2/3\rangle\, |\mathbf{0_5}, 4/5\rangle & |\mathbf{1_2}, 1/2\rangle\, |\mathbf{1_3}, 1/3\rangle\, |\mathbf{0_5}, 4/5\rangle & |\mathbf{1_2}, 1/2\rangle\, |\mathbf{0_3}, 2/3\rangle\, |\mathbf{1_5}, 1/5\rangle & |\mathbf{1_2}, 1/2\rangle\, |\mathbf{1_3}, 1/3\rangle\, |\mathbf{1_5}, 1/5\rangle \end{pmatrix}$$

On multiplie les probabilités de façon à aboutir à la matrice 2×4 suivante :

$$\begin{pmatrix} |\mathbf{0_2 0_3 0_5}, 8/30\rangle & |\mathbf{0_2 0_3 1_5}, 2/30\rangle & |\mathbf{0_2 1_3 0_5}, 4/30\rangle & |\mathbf{0_2 1_3 1_5}, 1/30\rangle \\ |\mathbf{1_2 0_3 0_5}, 8/30\rangle & |\mathbf{1_2 0_3 1_5}, 2/30\rangle & |\mathbf{1_2 1_3 0_5}, 4/30\rangle & |\mathbf{1_2 1_3 1_5}, 1/30\rangle \end{pmatrix}$$

On retrouve les probabilités correspondant aux cardinaux des ensembles de nombres ligne par ligne de la seconde image fournie en introduction[1].

[1] Jusqu’à 5, on avait 1+2+4+8=15 moitié de 30. Avec le nombre premier 7 en plus, la somme de toutes les combinaisons de produits des $p-1$ donne 1+2+4+6+8+12+24+48=105 moitié de 210.

Pollen (Denise Vella-Chemla, 2/1/2018)

Cette note est destinée à garder trace de deux idées qu'on aimerait savoir mettre en oeuvre et qui sont liées à la physique :

- ⋆ la première idée provient du fait qu'on peut utiliser la récurrence suivante :

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

  (et $\sigma(1) = 1$) pour calculer la somme des diviseurs $\sigma(n)$ d'un nombre n. Cette formule de récurrence a été proposée par Dominique Giard dans les formules de calcul de la séquence A000203 de l'OEIS. Celui-ci nous a expliqué qu'elle provenait de l'égalité de Chazy, qui était liée aux équations de Painlevé VI. La compréhension de telles équations différentielles est totalement hors de notre portée. Cependant, on a trouvé un article de référence récent [1] qui fournit une analyse détaillée des équations de Painlevé I à VI et qui explique précisément certains calculs pour les équations de Painlevé II. L'article semble permettre de parvenir du système différentiel Fuchsien à l'opérateur hamiltonien qui décrit l'évolution du système (?). On se demande si la mise en relation de tels éléments pourraient servir à comprendre l'ensemble des nombres premiers : un nombre premier p est caractérisé par le fait que la somme de ses diviseurs $\sigma(p)$ est égale à $p + 1$.

- ⋆ la seconde idée consisterait à suivre l'exemple de ceux qui proposent de voir le chaos de l'ensemble des nombres premiers comme similaire au chaos d'un ensemble de grains de pollen et à utiliser pour le comprendre des résultats de physique statistique (cf. [2]) ; on pourrait peut-être considérer qu'il y a n grains dans une cavité et chercher un opérateur physique qui permettrait que seuls $\pi(n)$ (avec $\pi(n)$ le nombre de nombres premiers inférieurs ou égaux à n) grains passent dans une cavité reliée à la première. Il faudrait réussir à utiliser le fait que les nombres premiers ne font pas partie de la moitié (1/2) de l'ensemble de tous les nombres, i.e. ceux qui sont divisibles par 2, du tiers (1/3) de l'ensemble de tous les nombres, ceux qui sont divisibles par 3, (du 1/4 de l'ensemble des nombres, ceux qui sont divisibles par 4 ?), du 1/5 de l'ensemble des nombres, ceux qui sont divisibles par 5, (du 1/6 de l'ensemble des nombres, ceux qui sont divisibles par 6 ?), etc. Dans [2] p. 26 est fournie une formule pour l'équilibre, quand pile la moitié des grains de pollen passent de la cavité gauche à la cavité droite, i.e. quand un état d'équilibre est atteint.

Références

[1] Noncommutative Painlevé equations and systems of Calogero type, M. Bertola, M. Cafasso, V.Rubstov, 2017, https://arxiv.org/pdf/1710.00736.pdf.

[2] Cours de Physique statistique, Ecole polytechnique, G. Montambaux, 2017 https://www.equipes.lps.u-psud.fr/Montambaux/polytechnique/PHY433/PHY433-2017-amphi1-GM.pdf

Lien entre les derniers chiffres de la somme et du produit de deux nombres premiers consécutifs (Denise Vella-Chemla, 1/1/2018)

On continue de petites expérimentations de programmation autour des nombres premiers. On a l'idée de calculer pour deux nombres premiers consécutifs p_n et p_{n+1} leur produit et leur somme.

Intriguée par le fait que les derniers chiffres du produit et de la somme semblent "aller de pair", on décide de calculer ce que vaut :

$$10 \times ((p_n \times p_{n+1})\ mod\ 10)\ +\ ((p_n + p_{n+1})\ mod\ 10).$$

On est alors surprise de constater que ce nombre ne semble pouvoir prendre que 13 valeurs différentes qui sont :

$$10, 12, 18, 34, 36, 52, 58, 65, 72, 78, 90, 94, 96.$$

Il faut interpréter ces valeurs ainsi :

- ⋆ si le produit de deux nombres premiers consécutifs a pour dernier chiffre 1, alors leur somme ne peut avoir pour dernier chiffre que 0, 2 ou 8 ;
- ⋆ si le produit de deux nombres premiers consécutifs a pour dernier chiffre 3, alors leur somme ne peut avoir pour dernier chiffre que 4 ou 6 ;
- ⋆ si le produit de deux nombres premiers consécutifs a pour dernier chiffre 5 ou 7, alors leur somme ne peut avoir pour dernier chiffre que 2 ou 8 ;
- ⋆ si le produit de deux nombres premiers consécutifs a pour dernier chiffre 6, alors leur somme ne peut avoir pour dernier chiffre que 5 ;
- ⋆ si le produit de deux nombres premiers consécutifs a pour dernier chiffre 9, alors leur somme ne peut avoir pour dernier chiffre que 0, 4 ou 6.

Ce qui surprend le premier de l'an surprend moins le lendemain.

Parmi les 13 valeurs trouvées, on oublie celles commençant ou se terminant par 5 : 65 correspond à $2 \times 3 = 6$ et $2 + 3 = 5$ tandis que 58 est associé aux produit et somme $3 \times 5 = 15, 3 + 5 = 8$ (resp. 52, $5 \times 7 = 35, 5 + 7 = 12$).

On comprend les autres nombres en dressant les tables des derniers chiffres du produit et de la somme pour les nombres premiers autres que 2 ou 5, qui se terminent par 1, 3, 7 ou 9.

×	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

+	1	3	7	9
1	2	4	8	0
3	4	6	0	2
7	8	0	4	6
9	0	2	6	8

On constate une symétrie pour les derniers chiffres de produit 1 ou 9 : la moitié des produits se terminant par 1 (resp. 9) correspondent à une somme de premiers consécutifs qui se termine par 0 tandis qu'un quart des produits correspondent à une somme se terminant par 2 et un quart des produits correspondent à une somme se terminant par 8 (resp. par 4 ou 6).

On constate une autre symétrie pour les derniers chiffres de produit 3 ou 7 : il semblerait qu'il y ait équilibre (50-50) entre ceux dont la somme se termine par 4 et ceux dont la somme se termine par 6 lorsque le produit se termine par 3 et équilibre également entre ceux dont la somme se termine par 2 et ceux dont la somme se termine par 8 lorsque le produit se termine par 7.

```cpp
#include <iostream>
#include <stdio.h>
#include <cmath>

int prime(int atester) {
  bool pastrouve=true;
  unsigned long k = 2;

  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve) {
    if ((k * k) > atester) return 1;
    else if ((atester % k) == 0) {
      return 0 ;
    }
    else k++;
  }
}

int stocke[100] ;

int main (int argc, char* argv[]) {
  long int i, p, q, why, a, b, indice ;

  p = 2 ;
  indice = 1 ;
  for (i = 1 ; i <= 100 ; ++i)
    stocke[i] = 0 ;
  for (i = 3 ; i <= 1000000 ; ++i) {
      q = i ;
      if ((prime(p)) && (prime(q))) {
        std::cout << "\np = " << p ;
        std::cout << " q = " << q ;
        a = (p*q) % 10 ;
        b = (p+q) % 10 ;
        std::cout << "\npq = " << a << " p+q " << b << "\n" ;
        why = 10*a + b ;
        stocke[why] = 1 ;
        indice = indice+1 ;
        p = q ;
      }
  }
  for (i = 1 ; i <= 100 ; ++i)
    if (stocke[i])
     std::cout << i << " " ;
}
```

Fin de l'exécution du programme ci-dessus pour les nombres premiers jusqu'à 10^6

```
p = 999883 q = 999907
pq = 1 p+q 0

p = 999907 q = 999917
pq = 9 p+q 4

p = 999917 q = 999931
pq = 7 p+q 8

p = 999931 q = 999953
pq = 3 p+q 4

p = 999953 q = 999959
pq = 7 p+q 2

p = 999959 q = 999961
pq = 9 p+q 0

p = 999961 q = 999979
pq = 9 p+q 0

p = 999979 q = 999983
pq = 7 p+q 2



10   12   18   34   36   52   58   65   72   78   90   94   96
```

Esprit de contradiction ? (Denise Vella-Chemla, 21.02.2018)

On écrit littéralement la somme $\zeta(s)$ avec $s = a + ib$.

$$\zeta(s) = 1 + \left(\frac{1}{2}\right)^a e^{-ib\ ln\ 2} + \left(\frac{1}{3}\right)^a e^{-ib\ ln\ 3} + \left(\frac{1}{4}\right)^a e^{-ib\ ln\ 4} + \ldots$$

Les zéros de ζ vont par 4, du fait de la symétrie par rapport à la droite critique d'une part, et de la symétrie par rapport à l'axe des abscisses d'autre part.

$$\zeta(s) = \zeta(a + ib) = 0 \iff \zeta(1 - \bar{s}) = \zeta((1 - a) + ib) = 0.$$

$$\zeta(1 - \bar{s}) = 1 + \left(\frac{1}{2}\right)^{1-a} e^{-ib\ ln\ 2} + \left(\frac{1}{3}\right)^{1-a} e^{-ib\ ln\ 3} + \left(\frac{1}{4}\right)^{1-a} e^{-ib\ ln\ 4} + \ldots$$

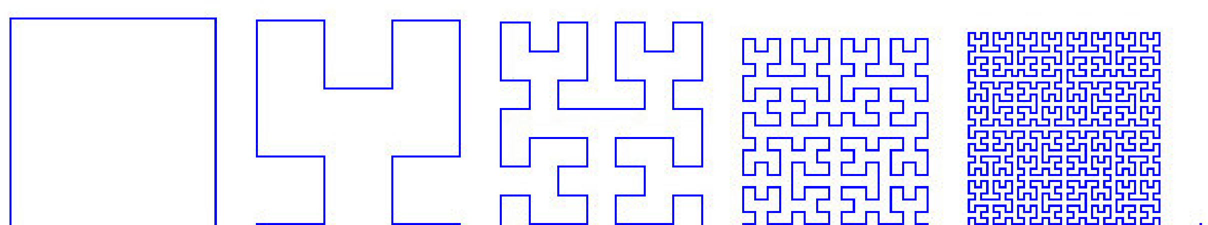
Les deux complexes $\zeta(s)$ et $\zeta(1 - \bar{s})$ peuvent-ils être tous les deux nuls sans que a soit égal à $\frac{1}{2}$, les deux formules de $\zeta(s)$ et de $\zeta(1 - \bar{s})$ n'étant différentes que par les éléments de la forme $\left(\frac{1}{n}\right)^k$, k réel ?

Cela ne semble pas possible lorsqu'on regarde les représentations colorées aux couleurs de l'arc-en-ciel de ζ qu'on trouve sur la toile car on constate que, verticalement, l'ordre des couleurs en se promenant sur la droite critique (dans les dendrites, ces espèces de tentacules qui viennent comme se poser sur la droite critique) est le même dans les deux demi-plans supérieur et inférieur des ordonnées. On a dû mal comprendre la représentation.

Courbe de Hilbert en python-logo (DV, 1.3.2018)

Souvenirs, souvenirs, de la courbe de Hilbert, de Logo, de Minsky et de l'IA à Montpellier.

```
import turtle
from turtle import *
def Hilbert(n,longueur,sens):
    if (n>0):
        right(90*sens)
        Hilbert(n-1,longueur,-sens)
        left(90*sens)
        forward(longueur)
        Hilbert(n-1,longueur,sens)
        right(90*sens)
        forward(longueur)
        left(90*sens)
        Hilbert(n-1,longueur,sens)
        right(180*sens)
        forward(longueur)
        left(180*sens)
        left(90*sens)
        Hilbert(n-1,longueur,-sens)
        right(90*sens)
def Trace_Hilbert(n):
    longueur=100/(2**n-1)
    Hilbert(n,longueur,1)
setup()
speed(0)
setheading(90)
up()
turtle.setposition(-300,0)
down()
for n in range(1,6):
    Trace_Hilbert(n)
    up()
    right(90)
    forward(20)
    left(90)
    down()
exitonclick()
```



Pourquoi la moyenne des parties fractionnaires des parties réelles des zéros de zêta semble-t-elle être asymptotiquement égale à 1/2 ? (Denise Vella-Chemla, 7.3.2018)

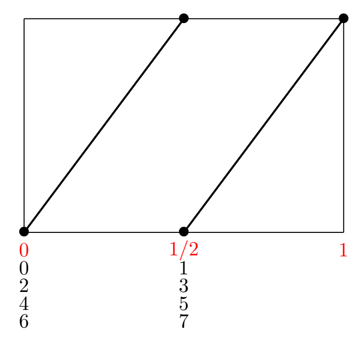
On voudrait fournir ici une explication informelle à une constatation effectuée récemment et qui est que la moyenne des parties fractionnaires des parties réelles des zéros de la fonction zêta semble tendre vers 1/2.

On utilise pour illustrer cette explication la notion de fonction ou signal en dents-de-scie dont on peut trouver une présentation dans les pages wikipedia en français (https://fr.wikipedia.org/wiki/Signal$_{e}n_{d}ents_{d}e_{s}cie$) ou en anglais (https://en.wikipedia.org/wiki/Sawtooth$_{w}ave$).

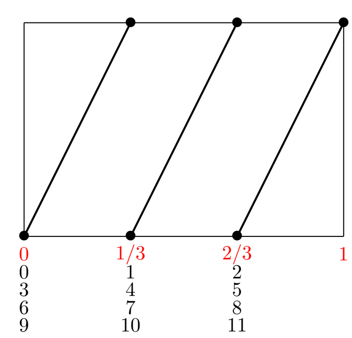
On pense au Snurpf, système de Numération par les Restes (modulaires de Gauss) dans les Parties Finies de $\mathbb{N}$. On conçoit aisément que les restes des divisions euclidiennes des nombres entiers successifs par 2 (en commençant par l'entier 1) sont 1, 0, 1, 0, 1, etc. De même les restes des divisions euclidiennes des entiers successifs par 3 sont 1, 2, 0, 1, 2, 0, 1, 2, 0, etc.

Pour représenter ces *fonctions croissantes "restes de divisions euclidiennes"* ainsi décrites (et qui retombent régulièrement à 0) , on se place sur l'intervalle $[0, 1]$ et on utilise des fonctions en dents-de-scie.

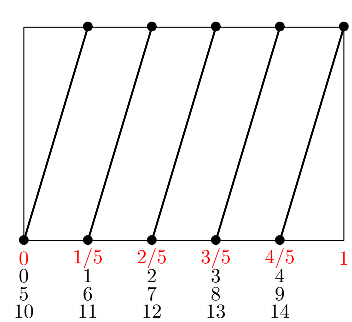
Voici la fonction en dents-de-scie qui permet de visualiser la notion de parité. Les entiers impairs ont pour image le point médian, les pairs ont pour image 0.



Voici la fonction en dents-de-scie qui permet de visualiser la notion de divisibilité par 3. Les entiers qui ont pour reste 1 dans la division euclidienne par 3 ont pour image le point 1/3, ceux qui ont pour reste 2 ont pour image le point 2/3, et les nombres divisibles par 3 ont pour image 0.



Voici la fonction en dents-de-scie qui permet de visualiser la notion de divisibilité par 5. Les nombres qui ont pour reste r dans la division euclidienne par 5 ont pour image $r/5$.



Comme les fonctions en dents-de-scie sont périodiques, il faut les imaginer sur un tore (ou du moins un cylindre). Sur les bords verticaux des représentations planes du cylindre ci-dessus vont se retrouver tous les nombres multiples d'un nombre donné, ainsi que le nombre en question. La périodicité qui fait que la fonction attribue la même image à deux nombres dont la différence vaut 1 s'exprime par la condition $x(t) = t \ (mod\ 1)$.

Il faut imaginer les nombres qui ne sont pas divisibles (par 3 par exemple) comme positionnés sur les lignes verticales de part et d'autre de la droite $x = 1/2$. Les nombres premiers doivent être équitablement répartis entre ces deux ordonnées de localisation (les densités associés à de tels sous-ensembles de nombres dans $\mathbb{N}$ doivent être égales). On imagine qu'on peut trouver une fonction qui envoie les entiers qui ont pour reste 1 dans une division euclidienne par 3 sur le "lieu" $x = 1/3$ et qui envoie les entiers qui ont pour reste 2 dans une division euclidienne par 3 sur le "lieu" $x = 2/3$.

On peut "mélanger" ou "agréger" toutes les fonctions en dents-de-scie en une seule fonction par la fonction inverse de la décomposition en série de Fourier. Du fait de l'équilibre des restes des divisions euclidiennes, les nombres doivent se répartir équitablement de part et d'autre de la droite $x = 1/2$. L'article wikipedia en anglais fournit comme renseignement supplémentaire : *"a sawtooth wave's sound is harsh and clear and its spectrum contains both even and odd harmonics of the fundamental frequency. Because it contains all the integer harmonics, it is one of the best waveforms to use for subtractive synthesis of musical sounds, particularly bowed string instruments like violins and cellos, since the slip-stick behavior of the bow drives the strings with a sawtooth-like motion."*.

Moyenne des parties fractionnaires des parties réelles des zéros de zêta (Denise Vella-Chemla, 4.3.2018)

On calcule par le programme python suivant les moyennes des parties fractionnaires des parties réelles des zéros de zêta qui sont fournies par Odlyzko ici http://www.dtc.umn.edu/ odlyzko/zeta$_t$*ables/index.html*.

```
import math
from math import *

zeros=[]
with open(’leszerosdezeta’, ’r’) as f:
    for p in f.readlines():
        z = float(p.split()[1])
        zeros.append(z)
f.close()
print(’’)
somme=0.0
for i in range(0,100000):
    res = zeros[i]-floor(zeros[i])
    somme=somme+res
    print(res)
print(’moyenne’)
print(somme/i)
```

Pour le fichier contenant 100000 zéros, la moyenne obtenue est : 0.499356115471.

Pour le fichier des zéros autour de 10^{12}, la moyenne obtenue est : 0.499758301944.

Pour le fichier des zéros autour de 10^{21}, la moyenne obtenue est : 0.496515278444.

Pour le fichier des zéros autour de 10^{22}, la moyenne obtenue est : 0.4983445377.

Pour le très gros fichier fourni par Odlyzko et contenant 2001053 zéros de zêta, la moyenne obtenue est : 0.500277516477.

On refait quelques tests, en les complétant de tests sur un fichier de nombres aléatoires de l'intervalle $[0, 1]$.

On obtient pour le fichier contenant les 2001053 zéros fournis par Odlyzko :
- moyenne = 0.50027726647,
- médiane = 0.499993778489,
- écart-type = 0.288607100069.

On obtient pour le fichier contenant des nombres aléatoires :
- moyenne = 0.500009450015,
- médiane = 0.499661660179,
- écart-type = 0.28860413121.

```
import math
from math import *
import numpy
from numpy import *
import numpy.random

tabzeros=fromfile('leszerostresgrosfichier',dtype=float,count=-1,sep=' ')
tab2=numpy.random.random(tabzeros.size)
print('')
print(tabzeros.ndim)
print(tabzeros.size)
for i in range(tabzeros.size):
    tabzeros[i]=tabzeros[i]-floor(tabzeros[i])
print('tab1')
print(mean(tabzeros))
print(median(tabzeros))
print(std(tabzeros))
print('tab2')
print(mean(tab2))
print(median(tab2))
print(std(tab2))
```

Faire le point (Denise Vella-Chemla, 25.02.2018)

Cette note est destinée à conserver la trace de réflexions éparses, une manière de faire le point.

1) Ensembles de Cantor, nombres réels, nombres premiers

Ci-dessous, un extrait du premier magazine Accromaths “Les Fractales”, téléchargeable ici :
http://accromath.uqam.ca/2006/07/les-fractales/
au sujet de l’ensemble de Cantor.

“En 1883, Cantor publie son fameux ensemble triadique (ou poussières de Cantor). Pour construire l’ensemble, il prend l’intervalle [0,1] et retire le tiers central en conservant les extrémités. Ensuite, il enlève le tiers central de chacun des nouveaux segments et ce, indéfiniment. Le résultat trouble à l’époque puisqu’il s’agit d’un exemple d’ensemble qui contient une quantité non-dénombrable de points mais dont la mesure est nulle.”

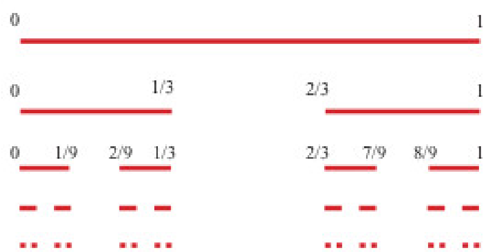


Figure 1 : L’ensemble de Cantor

Dans la mesure où les nombres premiers ne sont ni divisibles par 2, ni par 3, ni par 5, etc., il semblerait naturel de représenter leur ensemble par l’ensemble de Cantor suivant (on n’arrive cependant pas trop à savoir comment gérer le fait qu’un nombre premier est divisible par lui-même) :

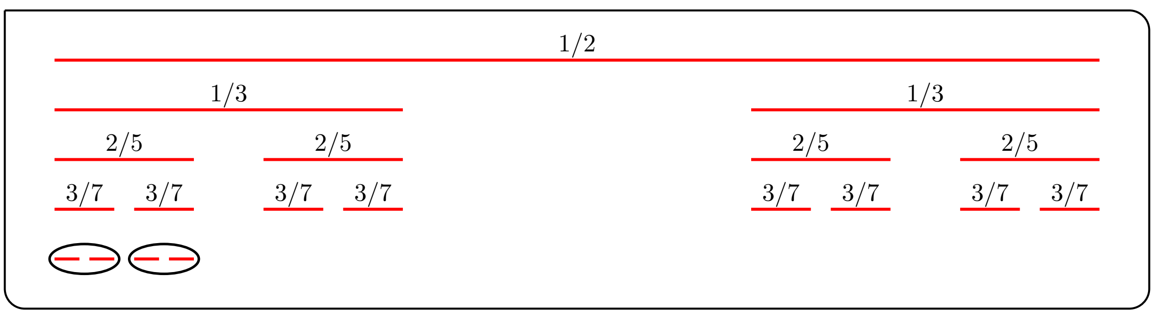


Figure 2 : L’ensemble de Cantor dédié aux nombres premiers

avec comme zoom sur les parties encerclées :

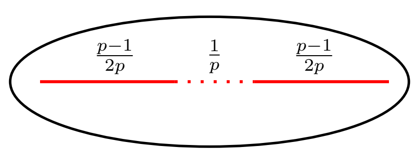


Figure 3 : Zoom sur les parties encerclées de la figure 2

Pour mieux cerner, si c’était possible, les points d’un tel espace, on revient au Snurpf, le Système de NUmération par les Restes dans les Parties Finies de $\mathbb{N}$. On associe à chaque entier n un réel compris entre 0 et 1 dans la partie décimale duquel sont codés les restes des divisions euclidiennes de n par l’infinité des nombres premiers. On normalise les tranches de décimales pour que les décimales correspondant aux restes des différents entiers selon un même nombre premier “tombent bien en face” : si on note $nbdigits(p)$ le nombre de chiffres de p, on réserve $nbdigits(p)$ décimales du réel pour coder le reste de la division euclidienne de n par p.

Le chiffre des dixièmes code le reste de la division euclidienne de n par 2, celui des centièmes code le reste de la division euclidienne de n par 3, les deux chiffres des 100000-èmes et millionièmes codent le reste de la division euclidienne de n par 11. Fournir les réels associés aux nombres de 1 à 16 pour des décimales associées aux nombres premiers de 2 à 13 sera plus explicite :

$$\begin{array}{rl}
1 \rightarrow & 0,1\ 1\ 1\ 1\ 01\ 01\ \ldots \\
2 \rightarrow & 0,0\ 2\ 2\ 2\ 02\ 02\ \ldots \\
3 \rightarrow & 0,1\ 0\ 3\ 3\ 03\ 03\ \ldots \\
4 \rightarrow & 0,0\ 1\ 4\ 4\ 04\ 04\ \ldots \\
5 \rightarrow & 0,1\ 2\ 0\ 5\ 05\ 05\ \ldots \\
6 \rightarrow & 0,0\ 0\ 1\ 6\ 06\ 06\ \ldots \\
7 \rightarrow & 0,1\ 1\ 2\ 0\ 07\ 07\ \ldots \\
8 \rightarrow & 0,0\ 2\ 3\ 1\ 08\ 08\ \ldots \\
9 \rightarrow & 0,1\ 0\ 4\ 2\ 09\ 09\ \ldots \\
10 \rightarrow & 0,0\ 1\ 0\ 3\ 10\ 10\ \ldots \\
11 \rightarrow & 0,1\ 2\ 1\ 4\ 00\ 11\ \ldots \\
12 \rightarrow & 0,0\ 0\ 2\ 5\ 01\ 12\ \ldots \\
13 \rightarrow & 0,1\ 1\ 3\ 6\ 02\ 00\ \ldots \\
14 \rightarrow & 0,0\ 2\ 4\ 0\ 03\ 01\ \ldots \\
15 \rightarrow & 0,1\ 0\ 0\ 1\ 04\ 02\ \ldots \\
16 \rightarrow & 0,0\ 1\ 1\ 2\ 05\ 03\ \ldots
\end{array}$$

Le réel associé à un nombre premier p est à une distance maximale du réel associé à $p-1$, si on choisit comme distance la somme des différences des décimales “associées” (i.e. celles correspondant à la division par un même nombre premier). On n’arrive pas à voir comment il faut procéder pour ordonner correctement les éléments de l’ensemble de réels obtenu par cette représentation.

On trouve dans la littérature qu’on peut également considérer chaque entier n comme une fonction qui associe à tout nombre premier p le reste de la division euclidienne de n par p.

2) Coïncidences numériques

Après avoir constaté que $e^{2\pi} = 535.492$ ressemble à une fréquence de note de la gamme [1] et lu que “Logarithmiquement, la racine, c’est la moitié” [2], on a l’idée de calculer les valeurs de la fonction f définie sur les réels par :

$$f(x) = \frac{\left(zerozeta[x]^2 - zerozeta[1]^2\right)}{e^{2\pi}}$$

avec $zerozeta(x)$ la partie réelle du x-ème zéro de zêta [3].

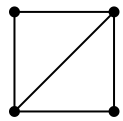
Les valeurs obtenues sont étonnantes :

$zerozeta(i)$	$(zerozeta(i))^2$	$f(zerozeta(i))$	$zerozeta(i)$	$(zerozeta(i))^2$	$f(zerozeta(i))$
14.1347	199.79	0.373097	60.8318	3700.51	6.91048
21.022	441.926	0.825272	65.1125	4239.64	7.91729
25.0109	625.543	1.16817	67.0798	4499.7	8.40293
30.4249	925.673	1.72864	69.5464	4836.7	9.03226
32.9351	1084.72	2.02565	72.0672	5193.68	9.69889
37.5862	1412.72	2.63818	75.7047	5731.2	10.7027
40.9187	1674.34	3.12674	77.1448	5951.33	11.1138
43.3271	1877.24	3.50563	79.3374	6294.42	11.7545
48.0052	2304.49	4.30351	82.9104	6874.13	12.837
49.7738	2477.43	4.62647	84.7355	7180.1	13.4084
52.9703	2805.85	5.23977	87.4253	7643.18	14.2732
56.4462	3186.18	5.95001	88.8091	7887.06	14.7286
59.347	3522.07	6.57727			

1. cf http://denise.vella.chemla.free.fr/gammes.pdf.
2. Pour passer de la fréquence d’un *do* à la fréquence d’un $fa\#$, la note située à 6 demi-tons de *do* quand l’octave contient 12 demi-tons, i.e. la note “au milieu d’une gamme”, on multiplie cette fréquence par $\sqrt{2}$ (il faut la multiplier par 2 pour obtenir la fréquence d’une note à l’octave).
3. Les parties réelles des zéros de zêta sont fournies par Odlyzko ici http://www.dtc.umn.edu/ odlyzko/zeta$_tables/index.html$.

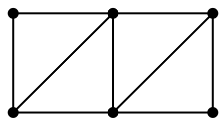
3) Triangulation du tore et formule d'Euler

On veut se rappeler ici qu'on a lu que la formule invariante d'Euler s'applique sur un tore triangulé de la façon suivante : $S-A+T=0$ avec S le nombre de sommets, A le nombre d'arêtes et T le nombre de triangles de la triangulation. Voyons l'application sur 3 exemples, on note à droite des dessins les nombres de sommets du carré initial, puis les 2 soustractions à effectuer du fait du repli horizontal puis vertical pour obtenir un tore :



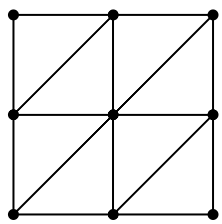
$S=4-2-1=1,\ A=5-1-1=3,\ T=2$

$S-A+T=0$



$S=6-3-1=2, A=9-2-1=6, T=4$

$S-A+T=0$



$S=9-3-2=4, A=16-2-2=12, T=8$

$S-A+T=0$

Figure 4 : Formule de Descartes-Euler sur le tore triangulé

4) Ordre dans lequel doivent être effectués les calculs dans l'article de Riemann

La dernière phrase de l'extrait de la note de Riemann ci-dessous explique l'importance d'effectuer certains calculs faisant intervenir les zéros de ζ (ou de ξ qui leur sont égaux sur l'axe réel) en les considérant dans l'ordre dans lequel ils apparaissent sur la droite critique en s'écartant progressivement de 0 (i.e. dans l'ordre $1/2+14,...i$ puis $1/2-14,...i$ puis $1/2+21,...i$ puis $1/2-21,...i$, etc.).

"En portant ces valeurs dans l'expression de $f(x)$ on obtient

$$f(x)=Li(x)-\sum_{\alpha}\left[Li\left(x^{\frac{1}{2}+\alpha i}\right)+Li\left(x^{\frac{1}{2}-\alpha i}\right)\right]$$

$$+\int_x^{\infty}\frac{1}{x^2-1}\frac{dx}{x\log x}+\log\xi(0),$$

où, dans la série $\sum\limits_{\alpha}$ on donnera à α pour valeurs toutes les racines positives (ou à parties réelles positives) de l'équation $\xi(\alpha)=0$ en les rangeant par ordre de grandeur. On peut alors, après une discussion plus approfondie de la fonction ξ, démontrer aisément que lorsque les termes sont rangés, comme il est prescrit ci-dessus, dans la série

$$\sum\left[Li\left(x^{\frac{1}{2}+\alpha i}\right)+Li\left(x^{\frac{1}{2}-\alpha i}\right)\right],$$

celle-ci converge vers la même limite que l'expression

$$\frac{1}{2\pi i}\int\limits_{a-bi}^{a+bi}\frac{d\frac{1}{s}\sum\log\left[1+\frac{\left(s-\frac{1}{2}\right)^2}{\alpha^2}\right]}{ds}x^s ds,$$

lorsque la grandeur b croît sans limites. Mais, si l'on changeait cet ordre des termes de la série, on pourrait obtenir pour résultat n'importe quelle valeur réelle."

La note [7] de la traduction en français de l'article de Riemann explique qu'une erreur typographique doit faire lire *log* $\zeta(0)$ à la place de *log* $\xi(0)$.

[7]. Note HME 1974, p. 31. Riemann écrit log $\xi(0)$ à la place de $-log\ 2$, mais puisqu'il utilise ξ pour noter une fonction différente à savoir la fonction $\xi(\frac{1}{2}+it)$, son $\xi(0)$ dénote $\xi(\frac{1}{2}) \neq \frac{1}{2}$. Cette erreur a été détectée du vivant de Riemann par Angelo Genocchi (1817-1889), Formole per determinare quanti siano i numeri primi fino ad un dato limite, in Annali di Matematica Pura ed Applicata 3 (1860), p. 52-59.

On a :

$$log\ \xi(0) = log\ \frac{-1}{2} = -log\ 2 + \pi i.$$

Dans l'article d'Alain Connes extrait du livre Open Problems in Mathematics de J.F. Nash et M.T. Rassias [4] (téléchargeable à l'adresse https://arxiv.org/pdf/1509.05576.pdf), le $+\pi i$ est omis.

On a souhaité ici programmer en python la fonction $f(x)$ de l'article de Riemann pour calculer $\pi(x)$, i.e. le nombre de nombres premiers inférieurs à x.

Cette formule est :

$$f(x) = Li(x) - \sum_{\rho}(Li(x^{\rho}) + Li(x^{\overline{\rho}})) + \int_{x}^{\infty} \frac{du}{u(u^2-1)ln\ u} - ln\ 2$$

avec $\rho = \frac{1}{2} + \alpha\ i$ et $\overline{\rho} = \frac{1}{2} - \alpha\ i$

Le programme python ci-dessous code la formule.

4. paru chez Springer eds. en 2016.

```
import math
from math import *
import cmath
from cmath import *
import mpmath
from mpmath import *
import scipy
from scipy import integrate
import numpy
from numpy import *

"""zeros=[0.5+ 14.134725141734693790457251983562476 6j,
      0.5- 14.134725141734693790457251983562476 6j,
      0.5+ 21.022039638771554992628479593896916 2j,
      0.5- 21.022039638771554992628479593896916 2j,..."""
zeros=[]
with open(’leszerosb’, ’r’) as f:
   for p in f.readlines():
      z = float(p.split()[1])
      zeros.append(0.5+z*j)
      zeros.append(0.5-z*j)
f.close()
print(’’)
print(’les zeros’)
for z in zeros:
    print(z)
print(’’)
print(’la fonction’)
Li = lambda z : li(z)-li(2)
f = lambda x : 1/((x**2-1)*x*log(x))
for x in range(2,101):
    print(’’)
    print(x)
    somme = 0
    for z in zeros:
        somme = somme + Li(x**z)
    pi_x = Li(x)
    pi_x = pi_x - somme
    pi_x = pi_x + integrate.quad(f, x, numpy.inf)[0]
    pi_x = pi_x - ln(2)
    print(pi_x)
```

Voici les images des entiers de 2 à 100 par la fonction f, obtenus par exécution du programme en utilisant 3 zéros seulement.

	21 → -2.516313	41 → 11.261739	61 → 11.058728	81 → 16.721597
2 → 2.552851	22 → 2.557449	42 → 12.607959	62 → 12.812713	82 → 14.054151
3 → 3.972725	23 → 9.106070	43 → 11.429642	63 → 14.580415	83 → 11.007882
4 → 3.614547	24 → 5.206529	44 → 10.311043	64 → 13.855415	84 → 8.073442
5 → 4.933246	25 → 0.744832	45 → 8.467303	65 → 12.832935	85 → 5.380225
6 → -0.919238	26 → -0.787661	46 → 7.490361	66 → 12.002598	86 → 3.049299
7 → 5.151988	27 → 1.357078	47 → 7.300341	67 → 11.500934	87 → 1.187144
8 → 1.059366	28 → 6.597947	48 → 7.691295	68 → 11.441763	88 → -0.119387
9 → 1.132025	29 → 10.833081	49 → 8.422025	69 → 10.757353	89 → -0.806673
10 → 0.058194	30 → 13.213916	50 → 6.393970	70 → 10.299160	90 → -0.836393
11 → 0.058194	31 → 11.090516	51 → 4.382955	71 → 10.429712	91 → -0.196099
12 → 3.115234	32 → 5.106740	52 → 2.950471	72 → 11.115368	92 → 1.101528
13 → 3.055617	33 → -0.282600	53 → 2.274725	73 → 12.286638	93 → 3.020415
14 → 2.371227	34 → -3.544514	54 → 2.451181	74 → 13.846118	94 → 5.503451
15 → -2.651217	35 → -4.140278	55 → 3.482370	75 → 15.675854	95 → 8.475321
16 → -0.335024	36 → -2.154444	56 → 5.290759	76 → 17.645653	96 → 11.845845
17 → 8.242808	37 → 1.752106	57 → 6.589052	77 → 18.044536	97 → 15.513863
18 → 11.807454	38 → 6.666511	58 → 7.081729	78 → 17.894065	98 → 19.371596
19 → 3.188116	39 → 8.664084	59 → 8.064510	79 → 17.640197	99 → 23.309205
20 → -2.493924	40 → 9.914963	60 → 9.432731	80 → 17.253096	100 → 27.219271

Voici le résultat de son exécution avec 10 zéros.

	21 → -26.072	41 → -0.241	61 → 4.187	81 → -6.321
2 → 10.674	22 → -5.023	42 → 4.618	62 → -1.964	82 → -8.865
3 → 9.542	23 → -2.423	43 → -3.293	63 → -15.050	83 → -10.236
4 → 6.853	24 → -11.188	44 → -17.094	64 → -28.435	84 → -12.589
5 → 7.611	25 → -9.944	45 → -20.940	65 → -34.846	85 → -17.877
6 → 0.116	26 → -15.700	46 → -14.401	66 → -32.481	86 → -22.608
7 → 7.025	27 → -16.521	47 → -6.018	67 → -22.161	87 → -24.474
8 → 0.796	28 → -5.549	48 → -10.002	68 → -6.519	88 → -23.729
9 → -0.835	29 → -7.428	49 → -14.445	69 → 4.418	89 → -25.175
10 → -10.869	30 → -3.326	50 → -15.840	70 → 7.105	90 → -27.780
11 → 6.216	31 → -0.722	51 → -19.421	71 → 5.515	91 → -28.381
12 → -13.693	32 → -4.902	52 → -20.634	72 → -2.141	92 → -29.371
13 → 4.956	33 → -25.194	53 → -16.271	73 → -12.332	93 → -30.857
14 → -14.961	34 → -31.762	54 → -13.963	74 → -22.201	94 → -32.370
15 → -9.961	35 → -22.449	55 → -21.963	75 → -27.307	95 → -30.936
16 → -9.687	36 → -6.973	56 → -25.894	76 → -26.613	96 → -26.490
17 → 4.893	37 → -2.515	57 → -26.241	77 → -22.294	97 → -21.625
18 → -11.774	38 → -18.933	58 → -19.629	78 → -15.262	98 → -15.597
19 → 0.888	39 → -26.168	59 → -8.854	79 → -10.220	99 → -7.517
20 → -9.249	40 → -16.603	60 → 2.435	80 → -5.757	100 → -0.451

Avec 1000 zéros, le temps d'exécution est trop important pour qu'on ait le courage de patienter.

Les résultats en calculant $f(x)$ avec 3 zéros seulement semblant pertinents, on relance l'exécution jusqu'à 1000, le dernier résultat trouvé est $f(1000) = 173$ (alors que $\pi(1000) = 168$).

Jusqu'à 10000, après avoir écrit le sympathique message *"lib/python2.7/site-packages/scipy/integrate/quadpack.py :364 : IntegrationWarning : The integral is probably divergent, or slowly convergent.*
warnings.warn(msg, IntegrationWarning)", $f(10000) = 1192$ alors que $\pi(x) = 1229$.
$f(100000) = 9500$ alors que $\pi(x) = 9629$.
$f(1000000) = 77811$ alors que $\pi(x) = 78498$ (temps d'exécution : 30 minutes).

Tout ça n'est pas probant ; il faudrait réessayer en utilisant plutôt la fonction $\xi(t)$, dont Riemann écrit *"Cette fonction est finie pour toutes les valeurs finies de t et peut être développée suivant les puissances de t^2 en une série qui converge très rapidement."*. Les définitions à utiliser sont fournies plus haut dans la note de Riemann :

$$\sum_1^\infty e^{-n^2\pi x} = \psi(x)$$

et

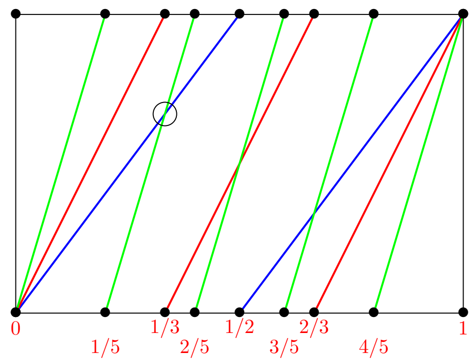
$$\xi(t) = \frac{1}{2} - \left(t^2 + \frac{1}{4}\right) \int_1^\infty \psi(x) x^{-\frac{3}{4}} cos\left(\frac{1}{2} t \; log \; x\right) dx,$$

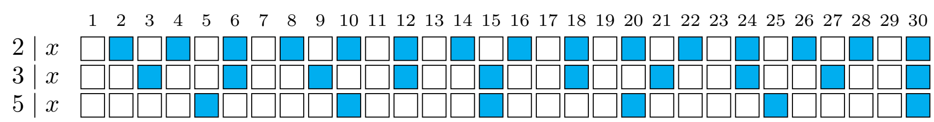
ou encore

$$\xi(t) = 4 \int_1^\infty \frac{d\left[x^{\frac{3}{2}} \psi'(x)\right]}{dx} x^{-\frac{1}{4}} cos\left(\frac{1}{2} t \; log \; x\right) dx.$$

Relation surprenante (Denise Vella-Chemla, 17.3.2018)

On cherchait à mettre en relation deux représentations auxquelles on s'était intéressé. On ne comprenait pas pourquoi le nombre d'intersections sur le tore (représentation du haut) ne permettait pas de compter les cardinaux des ensembles de nombres de mêmes caractères de divisibilité (représentation du bas). L'intersection entourée représente les nombres qui sont à la fois des $2x + a\ (mod\ 1)$ et des $5x + b\ (mod\ 1)$ avec $0 \leqslant a, b \leqslant 1$ et de fil en aiguille, ces réflexions nous ont amené à la définition et à la conjecture présentées après les représentations à mettre en regard.





111	30
110	6 12 18 24
101	10 20
100	2 4 8 14 16 22 26 28
011	15
010	3 9 21 27
001	5 25
000	1 7 11 13 17 19 23 29

Définition : on appelle *nombres orthogonaux* des nombres qui voient leurs caractères de divisibilité par tous les nombres premiers inférieurs ou égaux à la racine du plus grand d'entre eux être opposés. Sur la seconde représentation ci-dessus, les nombres de l'ensemble $\{6, 12, 18, 24\}$ (représentés par les 3 booléens 110) sont orthogonaux un à un aux nombres de l'ensemble $\{5, 25\}$ (représentés par les 3 booléens 001).

Comme autre exemple, 963 et 1000 sont *des nombres orthogonaux* car pour tous les nombres premiers inférieurs ou égaux à $\sqrt{1000}$ ($=\ 31, ...$), les relations entre les nombres premiers en question et chacun des 2 nombres 963 et 1000 sont opposées : 2 ne divise pas 963 tandis qu'il divise 1000 ; il en est de même pour tous les nombres premiers compris entre 5 et 31. Inversement, 3 divise 963 et ne divise pas 1000.

On doit noter qu'*orthogonaux* ne signifie pas *premiers entre eux* : $992 = 2^5.31$ et $995 = 5.199$ sont *premiers entre eux* mais ne sont pas *orthogonaux* car 3 ne les divise ni l'un ni l'autre.

On conjecture et on vérifie par programme que la différence de deux nombres *orthogonaux* est soit 1 soit un nombre premier.

Je n'ai pas suffisamment lu le récent livre de Laurent Lafforgue *Géométrie plane et algèbre* aux éditions Hermann mais le parcourir m'a sûrement donné une petite impulsion, à la recherche de ces liens entre nombres et géométrie.

Orthogonalité (Denise Vella-Chemla, 18.3.2018)

On associe à chaque nombre entier naturel x une chaîne infinie m de sous-chaînes de caractères (chaque sous-chaîne est indicée par un nombre premier parmi l'infinité des nombres premiers). La i-ème sous-chaîne de m est égale au reste de la division euclidienne de x par le i-ème nombre premier.

Voici les premières lettres des chaînes de caractères associées aux nombres de 1 à 100 (ε est le mot vide). Il faut avoir à l'esprit qu'il faudra 2 caractères (non présents ci-dessous) pour représenter les restes des divisions euclidiennes par les nombres premiers de 11 à 97, qu'il faudra 3 caractères pour coder les restes selon les nombres premiers compris entre 101 et 997, puis 4 caractères pour coder les restes selon les nombres premiers compris entre 1009 et 9973, etc.

$m_1 = \varepsilon$	$m_{21} = 10\ldots$	$m_{41} = 121\ldots$	$m_{61} = 1115\ldots$	$m_{81} = 1014\ldots$
$m_2 = 0\ldots$	$m_{22} = 01\ldots$	$m_{42} = 002\ldots$	$m_{62} = 0226\ldots$	$m_{82} = 0125\ldots$
$m_3 = 1\ldots$	$m_{23} = 12\ldots$	$m_{43} = 113\ldots$	$m_{63} = 1030\ldots$	$m_{83} = 1236\ldots$
$m_4 = 0\ldots$	$m_{24} = 00\ldots$	$m_{44} = 024\ldots$	$m_{64} = 0141\ldots$	$m_{84} = 0040\ldots$
$m_5 = 1\ldots$	$m_{25} = 110\ldots$	$m_{45} = 100\ldots$	$m_{65} = 1202\ldots$	$m_{85} = 1101\ldots$
$m_6 = 0\ldots$	$m_{26} = 021\ldots$	$m_{46} = 011\ldots$	$m_{66} = 0013\ldots$	$m_{86} = 0212\ldots$
$m_7 = 1\ldots$	$m_{27} = 102\ldots$	$m_{47} = 122\ldots$	$m_{67} = 1124\ldots$	$m_{87} = 1023\ldots$
$m_8 = 0\ldots$	$m_{28} = 013\ldots$	$m_{48} = 003\ldots$	$m_{68} = 0235\ldots$	$m_{88} = 0134\ldots$
$m_9 = 10\ldots$	$m_{29} = 124\ldots$	$m_{49} = 1140\ldots$	$m_{69} = 1046\ldots$	$m_{89} = 1245\ldots$
$m_{10} = 01\ldots$	$m_{30} = 000\ldots$	$m_{50} = 0201\ldots$	$m_{70} = 0100\ldots$	$m_{90} = 0006\ldots$
$m_{11} = 12\ldots$	$m_{31} = 111\ldots$	$m_{51} = 1012\ldots$	$m_{71} = 1211\ldots$	$m_{91} = 1110\ldots$
$m_{12} = 00\ldots$	$m_{32} = 022\ldots$	$m_{52} = 0123\ldots$	$m_{72} = 0022\ldots$	$m_{92} = 0221\ldots$
$m_{13} = 11\ldots$	$m_{33} = 103\ldots$	$m_{53} = 1234\ldots$	$m_{73} = 1133\ldots$	$m_{93} = 1032\ldots$
$m_{14} = 02\ldots$	$m_{34} = 014\ldots$	$m_{54} = 0045\ldots$	$m_{74} = 0244\ldots$	$m_{94} = 0143\ldots$
$m_{15} = 10\ldots$	$m_{35} = 120\ldots$	$m_{55} = 1106\ldots$	$m_{75} = 1005\ldots$	$m_{95} = 1204\ldots$
$m_{16} = 01\ldots$	$m_{36} = 001\ldots$	$m_{56} = 0210\ldots$	$m_{76} = 0116\ldots$	$m_{96} = 0015\ldots$
$m_{17} = 12\ldots$	$m_{37} = 112\ldots$	$m_{57} = 1021\ldots$	$m_{77} = 1220\ldots$	$m_{97} = 1126\ldots$
$m_{18} = 00\ldots$	$m_{38} = 023\ldots$	$m_{58} = 0132\ldots$	$m_{78} = 0031\ldots$	$m_{98} = 0230\ldots$
$m_{19} = 11\ldots$	$m_{39} = 104\ldots$	$m_{59} = 1243\ldots$	$m_{79} = 1142\ldots$	$m_{99} = 1041\ldots$
$m_{20} = 02\ldots$	$m_{40} = 010\ldots$	$m_{60} = 0004\ldots$	$m_{80} = 0203\ldots$	$m_{100} = 0102\ldots$

On appelle *nombres orthogonaux* des nombres x et y dont les mots associés voient toutes leurs lettres de même position différentes jusqu'à la position $i = \lfloor \sqrt{max(x,y)} \rfloor$. Par exemple, (93 de début de mot associé 1032) est orthogonal à 10 (de début de mot associé 0103). On a étudié la différence de 4 lettres car $\pi(\lfloor \sqrt{93} \rfloor) = \pi(9) = 4$.

Deux nombres pairs ne peuvent être orthogonaux ainsi que deux nombres impairs.

La différence de deux nombres orthogonaux x et y est égale soit à 1 soit à un nombre premier : en effet,

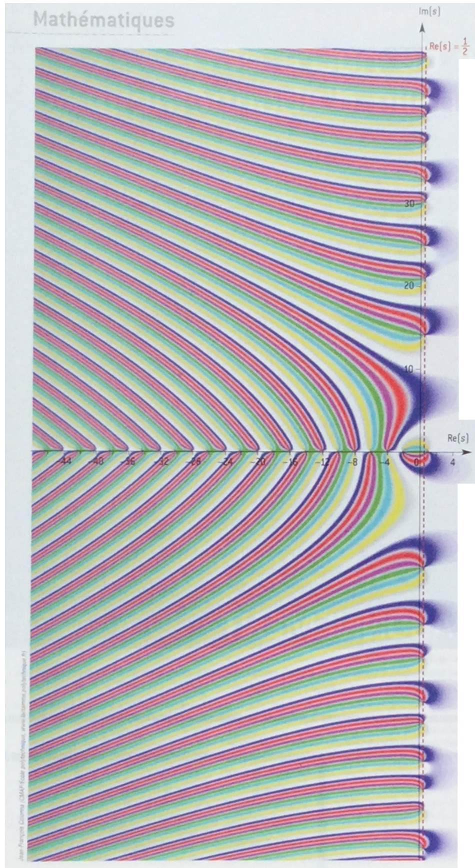
$$\begin{array}{llll} \text{si } x \perp y \text{ alors} & \forall k \leqslant \sqrt{max(x,y)}, & m_x[k] \neq m_y[k] & \\ & \iff & x \not\equiv y \ (mod\ p_k) & \\ & \iff & x - y \not\equiv 0 \ (mod\ p_k) & \\ & \iff & (x - y = 1) \vee & (x - y \text{ est un nombre premier puisqu'il n'est divisible} \\ & & & \text{par aucun nombre premier inférieur à sa racine).} \end{array}$$

Ainsi 93-10=83 est premier tandis que 93-16=77 ne l'est pas (les mots associés à 93 et 16 ont pour même quatrième lettre la lettre 2 car $93 \equiv 16 \equiv 2 \ (mod\ 7)$).

On peut aussi imaginer projeter les nombres sur l'intervalle $[0,1[$ selon un nombre premier p de la façon suivante : un nombre dont le reste de la division euclidienne par le nombre premier p est égal à i se projette sur le rationnel $\dfrac{i}{p}$. Par exemple, les nombres $3x+1$ ont pour projeté $\dfrac{1}{3}$, les $3x+2$ ont pour projeté $\dfrac{2}{3}$ et les $3x$ se projettent en 0. A chaque nombre peuvent ainsi être associés une infinité de rationnels de l'intervalle $[0,1[$ selon l'infinité des nombres premiers. Selon chaque premier, la densité de l'ensemble des nombres qui se projettent en le rationnel $\dfrac{i}{p}$ vaut $\dfrac{1}{p}$ et autant de nombres se projettent sur les rationnels de l'intervalle $\left[0, \dfrac{1}{2}\right[$ que sur les rationnels de l'intervalle $\left[\dfrac{1}{2}, 1\right[$.

Couleur (Denise Vella-Chemla, 30.3.2018)

On observe la représentation colorée de la fonction zêta qu'on trouve dans certains articles de vulgarisation [1]. On lit que la couleur correspond à l'argument (l'angle) du complexe image tandis que l'intensité correspond à son module (sa longueur). On discerne les regroupements de 7 couleurs qui aboutissent chacun à un zéro (et qu'on appelle les dendrites).



On a envie d'associer certaines couleurs : le bleu foncé avec le violet, séparés par le rouge, ce groupe de 3 couleurs étant séparé par le vert du groupe des deux couleurs cyan et jaune. On trouve cette séparation par la couleur verte plus pertinente qu'une autre possibilité envisagée initialement [2] parce que la couleur verte "traverse" l'axe des abscisses au niveau des zéros triviaux, alors que les autres couleurs ne "traversent" pas cet axe (on voit au niveau des zéros triviaux deux sous-dendrites par dendrite (l'une regroupant (bleu, rouge, violet) et l'autre regroupant (cyan, jaune)).

Ce qui est intrigant, côté droite critique, c'est qu'on se serait attendu à une symétrie des couleurs : puisque le bleu foncé est en haut des dendrites et le jaune en bas dans le demi-plan supérieur, le bleu foncé devrait se retrouver en bas et le jaune en haut des dendrites dans le demi-plan inférieur. Or les dendrites ont les couleurs dans le même ordre dans les demi-plans inférieur et supérieur pour deux zéros non triviaux conjugués. On peut exprimer cela par cette formule qui semble s'appliquer sur la droite critique :

$$\zeta(a - i(b + k)) = \zeta(a + i(b - k))$$

On a pour objectif de trouver une transformation (un opérateur) qui aurait, comme axes invariants (i.e. un point de ces axes a son image sur ces axes), l'axe des abscisses (qui contient les zéros triviaux) et son orthogonal la droite critique (qui contient les zéros non-triviaux). On se dit que cet opérateur devrait peut-être inverser les couleurs par symétrie dans chaque dendrite de chaque demi-plan puis réaliser une symétrie des couleurs par conjugaison complexe habituelle (telle que si $\zeta(a + ib) = c + id = \rho e^{i\theta}$ alors $\zeta(a - ib) = c - id = \rho e^{-i\theta}$) pour obtenir cette propriété d'ordre des couleurs de l'arc-en-ciel identique dans les deux demi-plans supérieur et inférieur, peut-être.

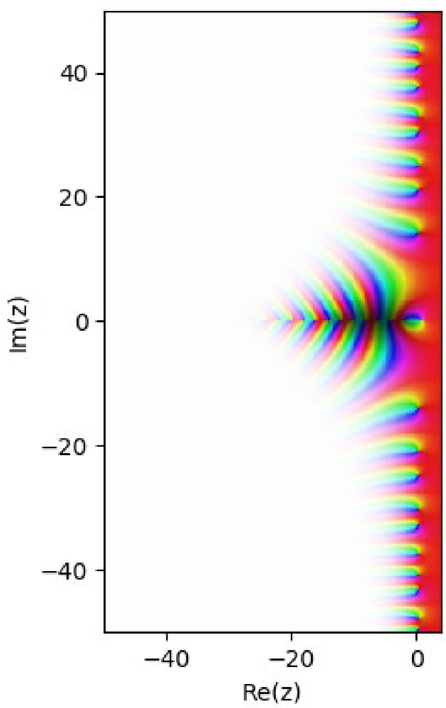
1. image extraite de l'article de Peter Meier et Jörn Steuding du magazine Pour la Science n°377, mars 2009.
2. qui reliait bleu à jaune, rouge à cyan et violet à vert.

On expérimente des petits essais en python, en vue de trouver cet opérateur qui permettrait de réobtenir les couleurs de zêta par un procédé qu'on maîtriserait un peu.

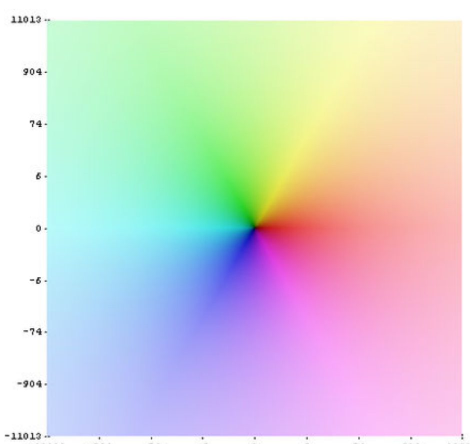
Par les instructions python,

```
import mpmath
from mpmath import zeta

mpmath.cplot(zeta,[-50,4],[-50,50],points=100000)
```

on obtient :

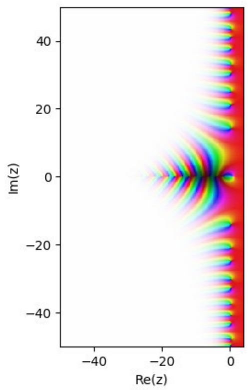


Les couleurs utilisées par python proviennent de la palette :



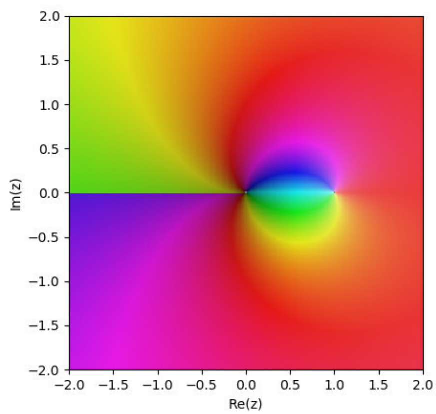
Ce sont les couleurs cyan et rouge qui traverse l'axe des abscisses dans la représentation colorée de zêta par programme python et les arguments (angles) des complexes bleu et vert d'une part, jaune et rose d'autre part, sont opposés.

On se trompait en croyant que les couleurs dans les dendrites devaient être symétriques les unes des autres du demi-plan supérieur au demi-plan inférieur : les couleurs sont dans le même ordre dans les deux demi-plans à cause de la conjugaison des complexes ; on a $\zeta(z) = \overline{\zeta(\overline{z})}$. On vérifie qu'on retrouve ζ par :

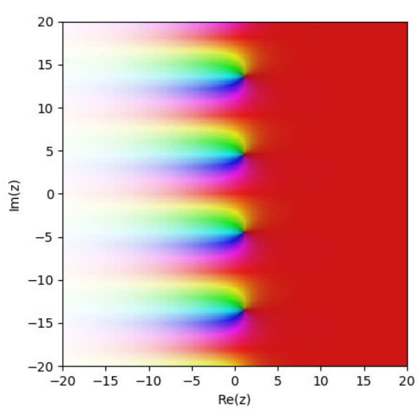



```python
import mpmath
from mpmath import zeta

mpmath.cplot(lambda z:(zeta(z.conjugate())).conjugate(),[-50,4],[-50,50], points = 100000)
```

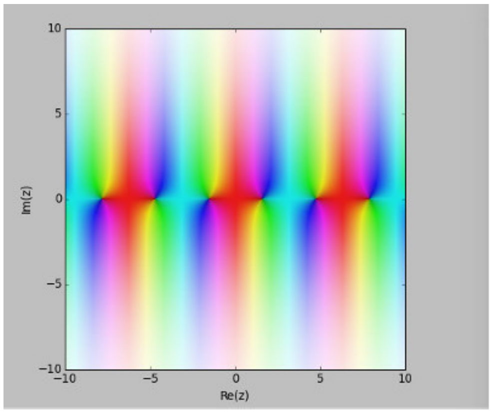
Zêta semble être un mélange d'éléments similaires à ceux qu'on retrouve en faisant calculer les fonctions suivantes : $f_1(z) = z/ln\ z$ pour ce qui se passe aux alentours de 0 et 1, $f_2(z) = 2^{-z} + 0.5$ pour ce qui se passe aux alentours de chaque zéro non trivial (aux extrémités des dendrites) et $f_3(z) = cos\ z$ pour la vue qu'on a au niveau de l'axe des abscisses, sur lequel se trouvent les zéros triviaux, si ce n'est que les dendrites de zêta semblent toutes orientées asymptotiquement en $-\infty$ vers $+\infty$ dans le demi-plan supérieur et vers $-\infty$ dans le demi-plan inférieur.




```python
import mpmath
from mpmath import ln

mpmath.cplot(lambda z:z/ln(z),[-2,2],[-2,2], points = 100000)
```



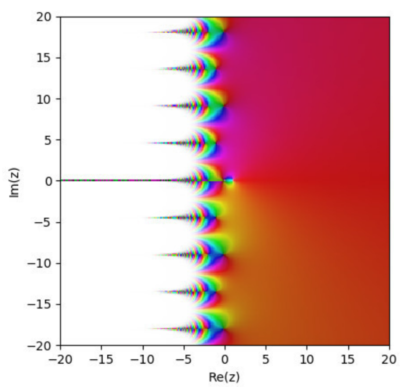

```python
import mpmath
from mpmath import ln

eee=2.71828
mpmath.cplot(lambda z:2**(-z)+0.5,[-20,20],[-20,20], points = 100000)
```




```
import mpmath
from mpmath import *

mpmath.cplot(lambda z:cos(z),[-10,10],[-10,10], points =1000000)
```

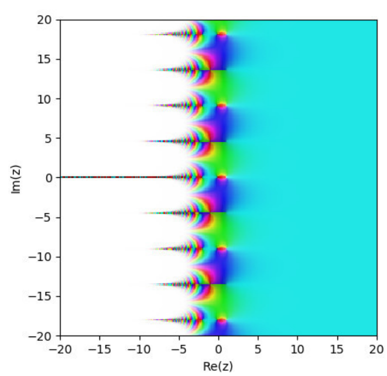
Par curiosité, on combine ces 3 fonctions des 6 manières possibles ($f_1 \circ f_2 \circ f_3$, $f_1 \circ f_3 \circ f_2$, $f_2 \circ f_1 \circ f_3$, ...). Les résultats sont hasardeux.

Graphique associé à $f_2 \circ f_3 \circ f_1(z) = cos(2^{-z} + 0.5)/ln(cos(2^{-z} + 0.5))$



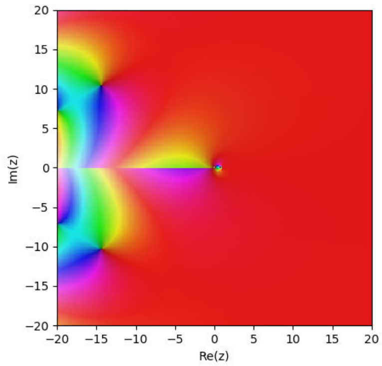

```
import mpmath
from mpmath import cos
from mpmath import ln

mpmath.cplot(lambda z:cos(2**(-z)+0.5)/ln(z),[-20,20],[-20,20], points = 100000)
```

Graphique associé à $f_2 \circ f_1 \circ f_3(z) = cos(2^{-z} + 0.5/ln(2^{-z} + 0.5))$



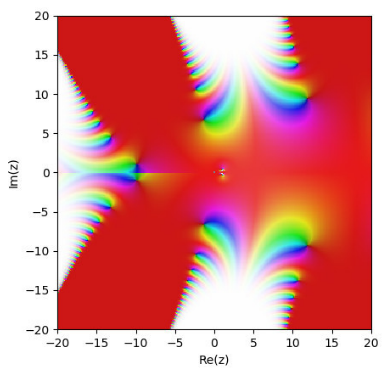

```
import mpmath
from mpmath import cos
from mpmath import ln

mpmath.cplot(lambda z:cos(2**(-z)+0.5)/ln(2**(-z)+0.5),[-20,20],[-20,20], points
 = 100000)
```

Graphique associé à $f_1 \circ f_2 \circ f_3(z) = cos(2^{-z/ln(z)} + 0.5)$



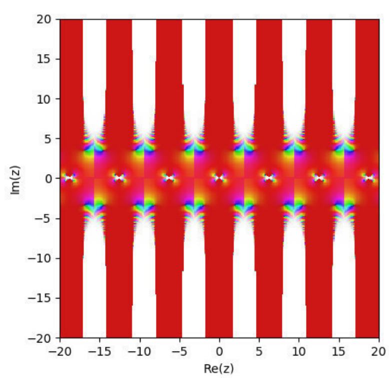

```
import mpmath
from mpmath import cos
from mpmath import ln

mpmath.cplot(lambda z:cos(2**(-z/ln(z))+0.5),[-20,20],[-20,20], points = 100000)
```

Graphique associé à $f_1 \circ f_3 \circ f_2(z) = 2^{-(cos(z/ln(z))} + 0.5$



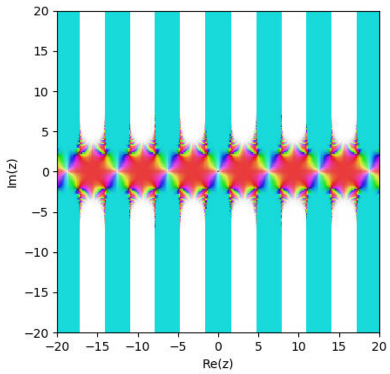

```
import mpmath
from mpmath import cos
from mpmath import ln

mpmath.cplot(lambda z:2**(-1*(cos(z/ln(z))))+0.5,[-20,20],[-20,20], points = 100
000)
```

Graphique associé à $f_3 \circ f_1 \circ f_2(z) = 2^{-cos(z)/ln(cos(z))} + 0.5$



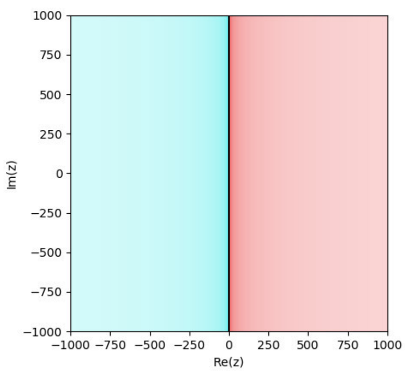

```
import mpmath
from mpmath import cos
from mpmath import ln

eee=2.71828
mpmath.cplot(lambda z:2**(-1*(cos(z)/ln(cos(z))))+0.5,[-20,20],[-20,20], points
= 100000)
```

Graphique associé à $f_3 \circ f_2 \circ f_1(z) = (2^{-cos(z)} + 0.5)/ln(2^{-cos(z)} + 0.5)$




```
import mpmath
from mpmath import cos
from mpmath import ln

mpmath.cplot(lambda z:(2**((-1)*cos(z))+0.5)/ln(2**((-1)*cos(z))+0.5),[-20,20],[
-20,20], points = 100000)
```

On a trouvé par hasard une manière d'implémenter la fonction layette $z \mapsto z + \overline{z}$.




```
import mpmath

mpmath.cplot(lambda z:z+z.conjugate(),[-1000,1000],[-1000,1000], points=100000)
```

Belle égalité (Denise Vella-Chemla, 2.4.2018)

$$\boxed{e^{\frac{-ln\ 3}{2}} \simeq \gamma}$$

avec γ la constante d'Euler-Mascheroni.

$\gamma = 0.5772156649015328606...$
$e^{\frac{-ln\ 3}{2}} = 0.57735026919...$

Autre chose : $2^{-z} + \frac{\sqrt{2}}{2}$ aussi a tous ses zéros sur la droite de partie réelle $\frac{1}{2}$, et on n'en parle pas...

Nombre de tours (Denise Vella-Chemla, 7.4.2018)

On continue de tester par programme des éléments de la note de Riemann au sujet du nombre de nombres premiers inférieurs à une valeur donnée.

On note dans le tableau ci-dessous le nombre de zéros de zêta inférieurs à une valeur donnée x (qu'on note $nbzeros(x)$) en regard de la valeur de la formule apparaissant dans l'article $nbtours(x) = \frac{T}{2\pi} log\left(\frac{T}{2\pi}\right) - \frac{T}{2\pi}$ (programme de calcul ci-après).

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

int main (int argc, char* argv[])
{ double ppii = 3.14159265359 ;
  double T, elle ;

  for (T = 100 ; T <= 700000 ; T=T+100)
    {
      elle = T/(2*ppii) ;
      std::cout << T << " -> " << elle*log(elle)-elle << "\n" ;
    }
}
```

x	$nbzeros(x)$	$nbtours(x)$	x	$nbzeros(x)$	$nbtours(x)$	x	$nbzeros(x)$	$nbtours(x)$
100	29	28	900	569	567	8000	7830	7829
200	79	78	1000	649	647	9000	8978	8976
300	138	136	2000	1517	1516	10000	10142	10142
400	202	200	3000	2469	2467	20000	22491	22490
500	269	268	4000	3474	3473	30000	35673	35671
600	341	339	5000	4520	4519	40000	49395	49393
700	414	413	6000	5598	5597	50000	63519	63518
800	491	489	7000	6703	6702	60000	77963	77962

Programme de calcul de la formule de Connes-Consani d'une fonction de comptage liée à la fonction zêta de Riemann (Denise Vella-Chemla, 22.4.2018)

On fournit ici le programme de calcul de la fonction de comptage fournie dans le cours d'Alain Connes au Collège de France de l'année 2008-2009 "Le monoïde des classes d'Adèles", consultable ici : https://www.college-de-france.fr/media/alain-connes/UPL59830$_{c}onnes_{r}es0809.pdf$.

Cette fonction de comptage $N(q)$ vaut, pour $q \in [1, \infty)$ et Z l'ensemble des zéros non-triviaux de la fonction zêta de Riemann :

$$N(q) = q - \sum_{\rho \in Z} order(\rho) q^{\rho} + 1$$

```
import math
from math import *
import cmath
from cmath import *
import mpmath
from mpmath import *
import scipy
from scipy import integrate
import numpy
from numpy 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

"""for x in range(1,1000000):
    if prime(x):
        print(x)"""

"""zeros=[0.5+ 14.1347251417346937904572519835624766j,
   0.5- 14.1347251417346937904572519835624766j,
   0.5+ 21.0220396387715549926284795938969162j,
   0.5- 21.0220396387715549926284795938969162j,..."""
```

```
zeros=[]
with open('leszerosdezeta', 'r') as f:
   for p in f.readlines():
      z = float(p.split()[1])
      zeros.append(0.5+z*j)
      zeros.append(0.5-z*j)
f.close()
"""
print('')
print('les zeros')
for z in zeros:
   print(z)
"""
print('')
print('la fonction')
for p in range(2,12):
  if (prime(p)):
    for l in range(1,12):
       x = p**l
       s=''
       s+='{0:d}^{1:d}={2:d}'.format(p,l,x)
       print('')
       print(s)
       somme = x+1
       for z in zeros:
          """print(z.imag)"""
          somme = somme - x**z
       print(somme)
```

On note dans les tableaux ci-dessous les résultats du calcul de $N(q)$ avec $q = p^l$ pour p nombre premier inférieur à 48 et l compris entre 1 et 12, avec Z l'ensemble des 200000 premiers zéros non-triviaux de zêta (100000 de parties imaginaires positives et leur conjugué) fournis sur la toile par Odlyzko. On voit clairement la formule être “de plus en plus” juste, plus la taille des nombres augmente.

p^l	q	$N(q)$	p^l	q	$N(q)$	p^l	q	$N(q)$
2^1	2	16526.022751118	3^1	3	26202.3597929168	5^1	5	38379.993254418
2^2	4	16526.8723080138	3^2	9	26193.5141189349	5^2	25	38376.4744394744
2^3	8	16541.8346696773	3^3	27	26215.9897049863	5^3	125	38497.7951430358
2^4	16	16529.9378096922	3^4	81	26215.0292622448	5^4	625	38212.7669195398
2^5	32	16517.1894144178	3^5	243	26234.1241967476	5^5	3125	39692.8475347931
2^6	64	16541.3837311068	3^6	729	25557.1812357914	5^6	15625	38978.1712748674
2^7	128	16596.457314137	3^7	2187	25139.34262301	5^7	78125	−21909.0320787703
2^8	256	16530.1027525653	3^8	6561	22813.9543148104	5^8	390625	34087.6262616789
2^9	512	16677.4128374294	3^9	19683	60904.2606401426	5^9	1953125	1822603.05018823
2^{10}	1024	16924.5256439669	3^{10}	59049	19819.9498798134	5^{10}	9765625	8812263.10212509
2^{11}	2048	16487.7126061848	3^{11}	177147	128839.908639892	5^{11}	48828125	53338264.3395279

p^l	q	$N(q)$	p^l	q	$N(q)$
7^1	7	46404.9338047014	11^1	11	57188.4645348426
7^2	49	46376.3368749039	11^2	121	57156.8354495423
7^3	343	46397.6984599656	11^3	1331	56511.0593488764
7^4	2401	42855.8567832658	11^4	14641	36201.8474304666
7^5	16807	40850.3069858886	11^5	161051	433036.226139666
7^6	117649	92518.822968482	11^6	1771561	1037835.49029106
7^7	823543	943094.788109194	11^7	19487171	19883161.943641
7^8	5764801	5592070.70530986	11^8	214358881	222968138.395264
7^9	40353607	40259900.2377517	11^9	2357947691	2375040033.44047
7^{10}	282475249	275547273.890145	11^{10}	25937424601	25929023679.1753
7^{11}	1977326743	2013531665.95512	11^{11}	285311670611	285325042242.14

p^l	q	$N(q)$	p^l	q	$N(q)$
13^1	13	61173.455982275	17^1	17	67570.864210361
13^2	169	61152.1842074158	17^2	289	67488.2796872391
13^3	2197	61595.0817517291	17^3	4913	64494.4571301473
13^4	28561	35119.101318525	17^4	83521	95126.1413652707
13^5	371293	842806.502153679	17^5	1419857	1527796.0967923
13^6	4826809	4844105.03767551	17^6	24137569	26266974.9339189
13^7	62748517	66948670.668413	17^7	410338673	405312134.16939
13^8	815730721	804835326.305623	17^8	6975757441	6972350256.91798
13^9	10604499373	10625393957.1387	17^9	118587876497	118773726755.062
13^{10}	137858491849	137927288531.251	17^{10}	2015993900449	2016130632947.47
13^{11}	1792160394037	1792181268163.27	17^{11}	34271896307633	34271018666148.3

p^l	q	$N(q)$	p^l	q	$N(q)$
19^1	19	70244.6576283392	23^1	23	74795.6836331307
19^2	361	70626.4147101706	23^2	529	74556.3563989949
19^3	6859	71558.4933286857	23^3	12167	61902.2398292989
19^4	130321	120687.966682127	23^4	279841	90297.7769623467
19^5	2476099	3108778.96872056	23^5	6436343	5808412.75514133
19^6	47045881	41647361.006971	23^6	148035889	145563305.665317
19^7	893871739	888579108.932336	23^7	3404825447	3382857937.92773
19^8	16983563041	17062763333.8805	23^8	78310985281	78448993931.1218
19^9	322687697779	322562612953.024	23^9	1801152661463	1801519334170.95
19^{10}	6131066257801	6129947084940.08	23^{10}	41426511213649	41426393227455.9
19^{11}	116490258898219	116488446544531.0	23^{11}	952809757913927	952800960795587.0

p^l	q	$N(q)$	p^l	q	$N(q)$
29^1	29	80323.6441199599	31^1	31	81900.3203876187
29^2	841	80751.8276029748	31^2	961	81705.2330983772
29^3	24389	51337.2372113353	31^3	29791	33791.6242719332
29^4	707281	890987.725034893	31^4	923521	982442.746257106
29^5	20511149	17317106.4403853	31^5	28629151	27728902.3587587
29^6	594823321	605265022.769502	31^6	887503681	896751867.654895
29^7	17249876309	17185843641.7054	31^7	27512614111	27517818436.106
29^8	500246412961	500492898863.202	31^8	852891037441	853222584696.395
29^9	14507145975869	14510068897520.6	31^9	26439622160671	26437295777642.8
29^{10}	420707233300201	420710600489541.0	31^{10}	819628286980801	819638888298087.0
29^{11}	12200509765705829	$1.22006051245098e+16$	31^{11}	25408476896404831	$2.5408429837307e+16$

p^l	q	$N(q)$	p^l	q	$N(q)$
37^1	37	86115.7665596133	41^1	41	88557.9701305219
37^2	1369	85426.9937307177	41^2	1681	89285.021388377
37^3	50653	118992.562151978	41^3	68921	67825.0760413148
37^4	1874161	1924935.75138671	41^4	2825761	3290709.52789768
37^5	69343957	67824350.7908732	41^5	115856201	112903420.619561
37^6	2565726409	2610041137.45719	41^6	4750104241	4739603369.24744
37^7	94931877133	95041507191.6032	41^7	194754273881	194660225230.829
37^8	3512479453921	3512577903295.74	41^8	7984925229121	7986619198004.87
37^9	129961739795077	129952955798711.0	41^9	327381934393961	327384739370054.0
37^{10}	4808584372417849	$4.8085634376082e+15$	41^{10}	13422659310152401	$1.34226913543118e+16$
37^{11}	177917621779460413	$1.7791766795618e+17$	41^{11}	550329031716248441	$5.50329233007557e+17$

p^l	q	$N(q)$	p^l	q	$N(q)$
43^1	43	89681.4528919395	47^1	47	91791.6074703618
43^2	1849	88460.612053587	47^2	2209	88865.4662431519
43^3	79507	108705.324306434	47^3	103823	174505.824660669
43^4	3418801	4147830.65155219	47^4	4879681	6082031.07152182
43^5	147008443	144403785.698815	47^5	229345007	237611519.978432
43^6	6321363049	6349617605.81833	47^6	10779215329	10716283351.5966
43^7	271818611107	272082250666.8	47^7	506623120463	506835012007.946
43^8	11688200277601	11687472448563.0	47^8	23811286661761	23810227304479.1
43^9	502592611936843	502593505096544.0	47^9	1119130473102767	$1.11911124064231e+15$
43^{10}	21611482313284249	$2.16114155590442e+16$	47^{10}	52599132235830049	$5.25990765071702e+16$
43^{11}	929293739471222707	$9.29293155038425e+17$	47^{11}	2472159215084012303	$2.47215916414308e+18$

Quel ordre ? (Denise Vella-Chemla, 22.4.2018)

En programmant la fonction de comptage fournie dans le cours d'Alain Connes au Collège de France de l'année 2008-2009 "Le monoïde des classes d'Adèles", consultable ici :
https://www.college-de-france.fr/media/alain-connes/UPL59830$_c onnes_r es0809.pdf$,
on s'interrogeait sur la fonction $ordre(\rho)$ intervenant dans la formule [1] :

$$N(q) = q - \sum_{\rho \in Z} ordre(\rho) q^{\rho} + 1$$

Comme on n'avait pas trop idée de ce que pouvait valoir cette fonction *ordre*, on a choisi une fonction $ordre2(\rho)$ un peu bizarre, qui fait que les calculs donnent des résultats surprenants qu'on voudrait fournir ici.

On définit $ordre2(\rho) = signe(\Im(\rho)) \times rang(\rho)$ [2].
Le zéro de zêta de partie imaginaire 14 (on omet de noter les chiffres des parties décimales des parties imaginaires des zéros de zêta) a pour rang 1 et son conjugué -1, le zéro de partie imaginaire 21 a pour rang 2 et son conjugué -2, le zéro de partie imaginaire 25 a pour rang 3 et son conjugué -3, etc.

$rang(\rho) = \#\{\rho' \in Z \ tel \ que \ 0 < Im(\rho') < |Im(\rho)|\} + 1$. La fonction $D(x)$ vaut, pour $x \in [1, \infty)$ et Z l'ensemble des zéros non-triviaux de la fonction zêta de Riemann :

$$D(x) = x - \sum_{\rho \in Z} ordre2(\rho) x^{\rho}$$

Le résultat de l'exécution de ce programme peut être trouvé ici :
http://denisevellachemla.eu/quelordrepourchaquezero.pdf.
On constate et ça nous surprend que $\Re(x - \sum_{\rho \in Z} ordre2(\rho) x^{\rho}) = x$. Si on commence à développer la formule avec les 3 premiers zéros, on obtient :

$$\begin{aligned}
&1 \times x^{1/2+14i} - 1 \times x^{1/2-14i} \\
&+2 \times x^{1/2+21i} - 2 \times x^{1/2-21i} \\
&+3 \times x^{1/2+21i} - 3 \times x^{1/2-21i} \dots \\
&= \textstyle\sum_{\rho \in Z, |\Im(\rho)|>0} rang(\rho) \sqrt{x} \, (e^{\Im(\rho) ln \ x \ i} - e^{-\Im(\rho) ln \ x \ i}) \\
&= \sum_{\rho \in Z, |\Im(\rho)|>0} 2 \ i \ rang(\rho) \sqrt{x} \, (sin(\Im(\rho) \ ln \ x)
\end{aligned}$$

Le fait qu'on retrouve x en partie réelle du résultat provient de ce que $\sum_{\rho \in Z, |\Im(\rho)|>0} 2 \ i \ rang(\rho) \sqrt{x} \, (sin(\Im(\rho) \ ln \ x)$ est de partie réelle toujours nulle (ou imaginaire pur).

Pour résumer, en affectant comme coefficients aux zéros successifs, ordonnés selon les valeurs absolues de leur partie imaginaire, les valeurs 1, -1, 2, -2, 3, -3, etc., on obtient comme résultat du calcul

$$x - \sum 2 \ i \ rang(\rho) \sqrt{x} \ sin(\Im(\rho) \ ln \ x)$$

qui est un imaginaire pur, tandis qu'en affectant 1 comme coefficient à tous les zéros, la formule qui vaut alors

$$x + 1 - \sum 2 \sqrt{x} \ cos(\Im(\rho) \ ln \ x)$$

est égale à x', qui est un réel pur asymptotiquement de plus en plus proche de x.

1. Alain Connes nous a indiqué plus tard qu'elle valait 1 pour tous les zéros et on a finalement trouvé dans un cours que l'ordre d'un zéro est le nombre de fois qu'apparaissent les couleurs de la palette des arguments quand on tourne autour de lui et on voit sur la représentation graphique de zêta que les couleurs n'apparaissent effectivement qu'une fois chacune autour des zéros non-triviaux.

2. On a $signe(x) = \dfrac{x}{|x|}$.

```
import math
from math import *
import cmath
from cmath import *
import mpmath
from mpmath import *
import scipy
from scipy import integrate
import numpy
from numpy 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

"""for x in range(1,1000000):
    if prime(x):
        print(x)"""

"""zeros=[0.5+ 14.1347251417346937904572519835624766j,
   0.5- 14.1347251417346937904572519835624766j,
   0.5+ 21.0220396387715549926284795938969162j,
   0.5- 21.0220396387715549926284795938969162j,..."""

zeros=[]
with open('leszerosdezeta', 'r') as f:
   for p in f.readlines():
      z = float(p.split()[1])
      zeros.append(0.5+z*j)
      zeros.append(0.5-z*j)
f.close()
print('')
print('les zeros')
"""for z in zeros:
   print(z)"""
print('')
print('la fonction')
for p in range(2,48):
  if (prime(p)):
    for l in range(1,12):
      x = p**l
      print('')
      print(x)
      somme = x
      order=1
      for z in zeros:
        """print(z.imag)"""
        somme = somme - order*(x**z)
        if (order%2 == 1):
          order=(-1)*order
        else:
          order=(-1)*order+1
      print(somme)
```

Chercher des idées (Denise Vella-Chemla, 31.5.2018)

On propose ici l'ébauche d'une façon de voir les nombres premiers comme annulant certains polynômes sur le disque-unité.

On a proposé la caractérisation suivante des nombres premiers (motivée par le fait que si p est un nombre premier, $\sigma(p) = p + 1$) :

$$n \text{ est premier} \iff \sum_{b=2}^{n-1} \sum_{o=1}^{b} cos \frac{2\pi no}{b} = 0$$

Victor Varin, du Keldysh Institute de Moscou, nous a fourni une démonstration de cette assertion, que l'on peut consulter ici : http://denise.vella.chemla.free.fr/VictorVarinKeldyshSumsumcos.pdf.

On peut utiliser les polynômes de Tchebychev, pour calculer chacun des cosinus.

On trouve les propriétés de ces polynômes dans la page wikipedia *Polynômes de Tchebychev*.

Utiliser le résultat $\forall \theta \in \mathbb{R}, \cos(x\theta) = T_x(\cos\theta)$ (n *entier*) du paragraphe *Définition trigonométrique* permet de remplacer dans la somme de sommes de cosinus chacun des cosinus par un polynôme.

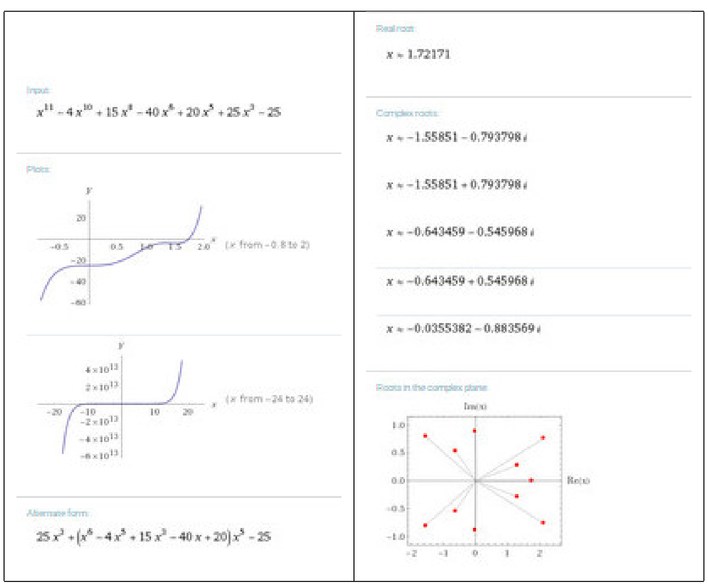
Cependant le remplacement de chaque cosinus en appliquant la formule polynomiale nécessite que celui-ci ait pour argument un multiple entier de θ ; problème : comme les dénominateurs des arguments des cosinus sont les entiers successifs, pour éliminer ces dénominateurs de manière à obtenir des multiples entiers de θ comme arguments des cosinus, il nous faudrait multiplier chaque argument de cosinus par $n!$ pour obtenir le caractère entier de l'argument. Mais alors une autre conséquence de cette multiplication des arguments par $n!$ est de permettre l'obtention d'un polynôme en une seule et même variable $X = cos\ \theta$ avec $\theta = 2\pi n^2$ qui est la partie commune des arguments de tous les cosinus à sommer. Et alors tous les cosinus étant d'argument pair valent 1. Non seulement ce qu'on a fait perd tout intérêt mais en plus, on ne sait pas revenir en arrière pour éliminer les opérations effectuées.

On imagine cependant qu'on aurait ainsi obtenu de manière théorique un polynôme dont les zéros seraient les nombres premiers.

Ce polynôme se serait annulé sur le disque unité, comme le fait par exemple le polynome :

$$P(x) = x^{11} - 4 * x^{10} + 15 * x^8 - 40 * x^6 + 20 * x^5 + 25 * x^3 - 25.$$

Visualisons les racines de l'équation polynomiale $P(x) = 0$ sur le disque-unité complexe en utilisant la version en ligne du logiciel Wolfram-Mathematica.



Certaines solutions sont dans le disque-unité du plan complexe.

On aurait alors peut-être pu utiliser la formule de Jensen qui décrit le comportement d'une fonction analytique f sur un cercle selon les modules des zéros de cette fonction. La formule de Jensen fournit des résultats sur certaines intégrales logarithmiques dans lesquelles interviennent les zéros de f.

Je lui ai écrit (Denise Vella-Chemla, 28.5.2018)

— j'ai parlé de palindromie et de non-commutativité de la concaténation des lettres dans les monoïdes dans le premier mail que je lui ai envoyé et que j'ai retrouvé (3.5.9) ;

— la non-commutativité des lettres permet le langage ; cette non-commutativité de la concaténation dans les monoïdes est enseignée dans tout cursus informatique en cours de théorie des langages formels (née à peu près en même temps que l'informatique elle-même) (12.6.13) ;

— je lui ai dit quelle avait été mon éducation mathématique (mes expériences initiatiques (la petite maison géométrique, le puzzle de Notre-Dame), mon cursus élémentaire intégralement “Maths modernes” (et qui m'a ravie), mes prises de parole pour polémiquer en cours de maths contre $\sqrt{2}$, puis contre $\sqrt{-1}$, ou bien le principe d'incertitude d'Heisenberg en Terminale, ou encore l'ensemble qui se contient lui-même en fac, j'ai “vécu” toute seule des petits morceaux de l'Histoire des mathématiques) ; puis le *I don't like machine learning* en DEA parce que les “serrages de boulons” pour que les coefficients dans les matrices fournissent bien la sortie escomptée m'ont toujours semblé être du bidouillage (15.6.13) ; je lui ai raconté le projet européen Equator sur le qualitative temporal reasoning avec Marek Sergot, Bob Kowalski et Murray Shanahan de l'Imperial College of London, le projet européen Tao pour Therapy Advisor in Oncology qui devait mettre en place un traitement du langage naturel sur des lettres de suivi de patients pour en extraire des éléments de leur dossier médical, patients que l'on souhaitait être de plus en plus éclairés (22.6.13) ;

— le simple engendre le complexe (22.6.13) ;

— mon *Snurpf* (Système de NUmération par les Restes dans les Parties Finies de $\mathbb{N}$) est non-positionnel et mes lettres commutent (23.6.13) ;

— tout est donné d'emblée, il n'y a pas de dynamisme tel que celui que l'on ressent dans le raisonnement par récurrence, “les invariants sont éternels !”, et il n'y a pas de temps qui joue pour tout raisonnement sur les entiers (23.6.13) ;

— *puce dans le cerveau : de toute façon, ce qui fait surtout la différence, pour un outil, que ce soit un ordinateur, un marteau, ou un théorème mathématique (ou encore le bâton à fourmis du grand singe chimpanzé), c'est l'intelligence de la personne (sic pour le chimpanzé) qui l'utilise* (17.9.13) ;

— *l'écriture d'un programme nécessite de comprendre très finement ce qui est à l'oeuvre dans un processus* (12.10.13) ;

— *lorsque plusieurs causes différentes produisent un même effet, on ne peut remonter de l'effet à sa cause ; c'est ce qui se produit dans le cas de mes 16 règles de réécriture : plusieurs règles ont pour partie droite la même lettre résultante ;* (28.10.13)

— je voyais la symétrie du clavier du piano autour de Ré ou Sol# ; je ne voyais pas l'assymétrie engendrée par le fait que le clavier contienne des paquets de 2 ou 3 touches noires, ce qui constitue une brisure de symétrie. *J'ai compris cet après-midi que de même que le groupe de Galois caractérise la symétrie d'une équation, l'indicateur d'Euler, maximum pour les premiers, caractérise le fait que ceux-ci (les nombres premiers) sont très symétriques, contrairement aux composés, dans la mesure où chaque non-divisibilité d'un composé par un premier particulier “brise” sa symétrie (en colorant et des cases bleues et des cases grises dans mes grilles), alors que la divisibilité par un premier favorise la symétrie puisque cases bleues et grises sont alors confondues* (10.11.13) ;

— danger du profilage : Unetelle travaille sur la toile internet et étudie la notion de famille d'“internautes semblables”, dans le but d'accélérer les recherches d'information. Les usages potentiels de son travail peuvent être merveilleux ou bien “craindre un max”, c'est au choix de l'utilisateur, suivant sa bienveillance ou malveillance... (10.11.13) ;

— *Ce qui crée l'intelligence, et la créativité mathématique, c'est l'importance du ressenti des événements, d'imprégnabilité à toute perception, quelque chose qu'on n'est pas près de pouvoir simuler par n'importe quelle machine que ce soit. Je peux vous assurer que les informaticiens ne s'y trompent pas et qu'ils sont malheureux que des personnes pas sérieuses, des imposteurs intellectuels, pré-*

tendent que l'IA va faire monts et merveilles et ainsi abîment l'image de l'informatique qui doit être au service de l'humain, le blason redoré par internet, pourrait se dédorer très vite si la toile ne devient qu'une vulgaire boîte à pub (10.11.13) ;

— tout est relation : pourquoi les tiroirs ont-ils des tables ? écrivain pour enfants Gianni Rodari, très apprécié de Carlo Rovelli (23.11.13) ;

— *Mon grand désir, en année de maîtrise, était de modéliser toute la connaissance humaine en machine et j'imaginais des taxonomies* (9.2.14) ; finalement trouvé sur la toile : projet CyC de Douglas Lenat ;

— éthique des hackers, vive le logiciel libre, aucune idée de propriété (des idées, des programmes, des articles,...) (9.2.14) citoyenne du monde, je me sens plus proche d'un intelligent inuit que d'un idiot européen, je ne suis donc pas en opposition avec le mondialisme provoqué de fait par la technologie (mais j'aimerais que gros moteur arrête de manipuler les résultats qui me maintiennent en bas de la matrice : de temps en temps, mon image descend brutalement de la page 7 à la page 12 sans raison apparente ; pourquoi ?) (24.8.14) ;

— *"J'ajoute plus d'erreurs que j'en enlève, forcément, ça diverge"* (6.4.14) ;

— *Ce qui est extraordinaire, c'est le fait d'avoir trouvé ces règles de réécriture, non-commutatives, et qui en simplifiant la vision que l'on peut avoir des décompositions, permettent de mettre au jour des régularités impossibles à voir sans cela* (6.4.14) ;

— *vu le morceau sur lequel je suis en ce moment* (7.4.14), a posteriori un machin qui tient finalement en 10 lignes et 2 pages au lieu des 23 que j'avais écrites et qui n'est peut-être toujours pas juste, je ne sais pas (21.5.18) ;

— *Cela me procurerait une joie incommensurable si ça s'avérait juste* (25.4.14) ;

— *J'essaye de rester dans le domaine discret. Je n'ai aucune maîtrise des réels ou du réel. Je me cache dans le virtuel, tout y est si net : 1, 0, vrai, faux, juste, buggé, y a pas plus fiable et loyal, la machine me déçoit rarement* (11.10.14) ;

— Untel a dit hier dans une émission de radio qu'avoir bossé comme un malade 10 années durant sur un problème et n'avoir pas avancé, c'est comme ne rien avoir fait du tout. Pour la société sûrement, mais pour la personne qui cherche, sûrement pas (13.10.14) ;

— *Je reste contente d'avoir fait tout ça : je ne peux m'empêcher de relier ces dernières idées à la théorie de l'ambiguité de Galois : on a des décompositions (0,0), des (1,0), des (0,1) et des (1,1), on peut faire quelques liens entre elles (lorsqu'elles partagent une coordonnée), mais on ne sait pas "qui devient qui" lors du passage de n à $n+2$, combien de décompositions passent "de tel sac à tel sac" et du coup, même s'il y a un "équilibre global des sacs", on ne peut être assuré qu'à un moment le sac qui nous intéresse (celui contenant les décompositions (0,0)) ne va pas être vide. Ca fait aussi un peu penser aux bits quantiques d'Alice et Bob et aux inéquations de Bell (21.10.14) ;*

— dernière cartouche (22.10.14) ;

— pagerank ou le privilège de l'ancienneté : plus ça fait longtemps que tu es sur la toile, plus tu grimpes, plus tu es félicité, ça fait penser aux César et Oscar d'honneur, quand t'es trop haut, t'es plus très loin de la fin (7.11.14) et mon père disait "à partir de maintenant, faut qu'on s'accroche aux branches" quand chaque année, un nouveau manquait à l'appel (7.11.14) ;

— mon cerveau en mouvement (19.2.15) et dessin de Sylvia "Come here, right now" et le cerveau qui court et qui répond "Never" ;

— texte superbe de l'Ecclésiaste sur la vanité trouvé dans le cv de Michel Chein :
Fumée de fumées, dit Qohélet ; fumée de fumées, tout est fumée.
Quel avantage pour l'humain en tout son labeur, dont il a labeur sous le soleil ?
Un cycle va, un cycle vient ; en pérennité la terre se dresse.
Le soleil brille, le soleil décline ; à son lieu il aspire et brille là.
Il va au midi, il tourne au septentrion, il tourne, tourne et va, le souffle, et retourne sur ses tours, le souffle.
Tous les torrents vont à la mer et la mer n'est pas pleine.
Au lieu où tous les torrents vont, là, ils retournent pour aller.
Toutes les paroles lassent, l'homme ne peut pas en parler.
L'œil ne se rassasie pas de voir, l'oreille ne se remplit pas d'entendre.
Ce qui a été sera, ce qui s'est fait se fera ; il n'est rien de tout neuf sous le soleil.
Il est une parole qui dit : "Vois cela, c'est neuf !"
C'était déjà dans les pérennités, c'était avant nous.
Pas de souvenirs des premiers, ni même des derniers qui seront, pas de souvenirs d'eux, ni de ceux qui seront en dernier (23.2.15) ;

— *Le gigantisme des données noie l'information, il faudrait inventer le métier d'archiviste du net, je ne crois pas que ça existe encore, et une sorte de fleur Dewey, un principe de classification, comme pour les livres en bibliothèque, on est loin d'être au point là-dessus* (18.7.15) → Stéphane Mallat ;

— ia et perception : *Mais comment feraient-ils pour me dire table ou plus difficile démocratie, si nous ne sommes pas en présence les uns des autres et qu'ils ne peuvent me montrer la table du doigt ou faire des gestes pour tenter de m'expliquer la démocratie. Je ne peux l'imaginer, je ne peux imaginer communiquer avec des lointains sans une perception commune minimale du monde extérieur* (30.9.15 et 23.11.15) ;

— pérennité de l'information : *Je m'interrogeais ce matin dans la voiture : avec internet, on externalise toute la mémoire (Michel Serres dit qu'on va enfin avoir la possibilité de devenir intelligents puisque le cerveau ne perdra plus son temps à une telle tâche subalterne de mémorisation). Avec l'imprimerie, on l'avait fait également (externaliser la mémoire du corps), mais un livre a une très très longue durée de vie, du moins un livre en bibliothèque. Un élément mémorisé digitalement, informatiquement, a une durée de vie bien moindre (je n'ai plus de magnétophone pour écouter les cassettes que j'écoutais quand j'avais 20 ans, ni d'électrophone pour écouter de vieux vinyles, et question information digitalisée, j'ai jeté toutes les petites disquettes souples, puis 3 pouces et demi, parce que je n'avais plus d'ordin ayant un périphérique me permettant de les interpréter, je n'utilise même plus de CD-Rom ou DVD-Rom que j'utilisais il y a 4-5 ans). Que deviendra une société sans mémoire ? A cause de la profusion d'informations actuelle, et aussi par inconscience du fait informatique, les webmasters pour créer de nouveaux sites tendance, n'hésitent pas à "paumer" toute une partie de l'information du site qu'ils doivent "rendre plus fun"* (14.10.15) ;

— propriété des informations personnelles : *je dois vous dire que je n'ai plus jamais eu le courage de lire ma note de tout ce temps et qu'elle s'évanouit depuis un an dans les limbes de ma mémoire défaillante.*
Sinon, j'ai la preuve que moteur préféré fait ce qu'il veut : j'ai changé la photo de la page de garde mais je lui ai conservé le nom de l'ancienne photo, pour voir ce qui se produirait et l'ancienne

photo est réapparue dans les images, alors qu'elle n'est plus dans les fichiers du site, cela signifie que moteur a gardé copie de ma photo et ne s'est pas rendu compte de la différence des contenus (j'espère que ce que j'écris est compréhensible) ; je trouve ça gênant, ça veut dire que je ne suis plus propriétaire de ce que je veux faire apparaître de ma personne alors que je suis pourtant ma propre webmaster et que j'ai modifié les fichiers comme je le souhaitais + possibilité de modifier tous les adressages (23.10.15) ;

— explicativité des réseaux de neurones : *Ce qui m'a toujours ennuyée dans les réseaux neuronaux, c'est qu'une fois le résultat trouvé, on ne peut dire précisément quels ajustements des paramètres d'apprentissage ont été effectués et du coup, on obtient un truc qui réussit mais dont on ne sait pas tout à fait précisément pourquoi il réussit (et je me dis qu'il pourrait de la même façon rater sans qu'on puisse trop l'expliquer non plus, mais on peut dire qu'il y a le même risque avec un humain)* (31.1.16) ;

— somme de trois triangles programmée le 10.7.2016 et Gauss en a parlé dans son journal le 10.7.1796 ; dans son journal, Gauss fait référence à la conjecture de Goldbach le 14 mai 1796 (19.7.13) ;

— preuve non constructive (8.2.17) ;

— dénigrement de l'informatique par les mathématiciens : *"la démonstration n'a rien d'informatique, aucune informatique, je vous rassure, uniquement du conceptuel"* (15.2.17) ne pas s'étonner qu'alors les étudiants fuient ;

— test de Turing : *quand sait-on que quelqu'un a compris ? (20.4.17) Je m'interroge sur le fait que les aliens puissent être considérés de façon sûre comme intelligents sous prétexte qu'ils auront trouvé le code de 131, sous-entendu "plus la réponse à trouver est compliquée, plus cela garantit de leur compréhension" mais c'est sans compter sur les probas et sur le fait qu'ils puissent expliquer comment ils ont trouvé. Quand votre prof de 6ème vous a hypnotisé, vous dites vous-même que vous ne savez pas comment vous aviez trouvé votre réponse, pensez-vous vraiment que vous aviez "effectivement compris" la réponse que vous avez fournie. J'ai déjà parlé un peu de ça à un internaute Anlois Cenna sur le forum des mathématiques, j'avais Aline Delves comme pseudo* ;

— Humanité : une seule personne visite le site mais c'est très bien : même un seul humain, c'est mieux que des milliers de robots (20.4.17)

— "Ce ne sont pas des fréquences mais ce sont des temps" : remarque de l'informaticienne : ce sont des nombres et les nombres, je les ai vus comme des lettres ; ce ne sont que des symboles, sans aucune accroche dans le monde réel ailleurs que dans nos cerveaux (27.5.2018) ;

— logarithmiquement, la racine c'est le milieu (22.2.18) ;

— l'or du ruisseau, les doreurs en bijouterie, l'ouvrier galvanoplaste, la source (7.11.14, 18.8.14) ;

— si les zéros de zêta qui correspondent en quelque sorte aux nombres premiers sont sur la droite critique, où tombent par zêta les images des nombres composés ?

— ce que je pense des non-informaticiens qui s'auto-décrètent spécialistes de l'IA : *Si des gens qui s'écoutent parler et qui font partie de ce qu'on appelle les "milieux autorisés" (sous prétexte qu'ils ont un salaire conséquent, un certain pouvoir, ou qu'ils font partie d'un certain Landerneau) veulent amuser le chaland en disant n'importe quoi, cela ne me regarde pas. Qu'ils programment quelques lignes pour essayer de réfléchir à la manière dont ce qu'ils envisagent pourrait être effectué, qu'ils étudient un peu sérieusement le sujet, et j'aurai alors envie de les écouter. En ce moment, ça fait vendre* (6.10.17) ; le livre qui pousse la réflexion le plus loin en terme d'étude de l'IA et que j'ai lu jusque-là est celui de Murray (Shanahan) : La singularité technologique (30.5.2018) ;

— *quand on a appris par le stylo écrivant, on ne peut comprendre que par le stylo écrivant. Je ne sais pas si ceux qui apprendront en tapant au clavier ne comprendront également qu'ainsi* (4.12.17) ;

— $e^{\frac{-ln\ 3}{2}} \simeq \gamma$, avec γ la constante d'Euler-Mascheroni,
$\gamma = 0.5772156649015328606...$ et $e^{\frac{-ln\ 3}{2}} = 0.57735026919...$ (2.4.2018) ;

— *Je voudrais trouver un opérateur qui me permettrait de descendre le long de "chemins vers zéro" que je vois comme des rigoles dans lesquelles descendraient des billes avec les zéros points fixes d'altitude min à atteindre et dont on ne sort pas une fois atteints ; j'ai besoin d'aide pour écrire l'opérateur dont voici les spec : c'est un opérateur du plan complexe (en fait de R4) qui permet de passer d'un point à un point de même couleur "pas loin à sa droite", pour essayer de descendre le long des dendrites jusqu'aux zéros, dendrite par dendrite, il s'agit de faire baisser la distance à la droite critique au fur et à mesure (ce serait bête de partir de l'autre côté, vers l'infini où j'ai pas pied !). Mon but est de faire descendre mes billes le long des lignes de zêta de même couleur, en les faisant s'approcher petit à petit de la droite critique (le long de sortes de géodésiques, les couleurs des dendrites). J'essaierai que ce soit une matrice qui fasse se déplacer de point en point jusqu'aux zéros* (9.4.2018) ;

— *Du coup, j'ai pensé que peut-être les parties imaginaires des zéros de zêta avaient simplement pour propriété d'annuler les sinus, en les faisant être des multiples de $\pi/2$ ou bien pour votre formule à vous, d'annuler les cosinus, en les faisant être des multiples de π, par multiplication par ce qu'il y a comme multiplicande dans les sin ou cos (23.4.18)* ;

— je ne sais pas si on peut dire que c'est la non-commutativité qui est à l'œuvre dans le fait qu'une combinaison *premier* + *compos*é n'est pas confondable avec une décomposition *compos*é + *premier* dans la mesure où j'oblige le petit sommant à être inférieur à $n/2$ et le grand sommant à être supérieur à $n/2$ (7.5.18) ;

— je ne sais pas si la théorie de Galois peut être vue comme à l'oeuvre dans le fait qu'on échange les décompositions de manière à mettre toutes les décompositions de la même forme (en terme de la qualité 0 ou 1 de leurs deux sommants) pour pouvoir les compter par contiguité (ou bien s'il s'agit d'un bazooka pour tuer une mouche), i.e. (mieux dit) ou bien si la théorie des ensembles est suffisante pour le raisonnement (7.5.18) ;

— quantique : *on a beau savoir qu'il y aura toujours au moins une décomposition premier + premier, on ne peut absolument pas savoir où elle est passée (ce qui correspond à cette idée du non-constructif qui déplaît à certains, et vraiment qui rapproche du quantique dans le sens où une décomposition premier + premier peut surgir n'importe où, comme un photon)* (8.5.18) ;

— *Ce qui est intéressant dans les règles de passage, c'est le fait que les deux a, c, d bleus dans le dessin du triangle page 2 du joint correspondent aux résultats des mêmes règles appliquées sur les nombres juste avant et sont identifiables, même s'ils ne correspondent pas du tout à des décompositions identiques (écrasement de l'information, 2 classes d'équivalence premier et composé et tout nombre projeté sur l'une de ces deux classes) (8.5.18) ;*

— *On comprend ce que j'écrivais du caractère "quantique" des X_a : on ne sait pas d'où $X_a(2n)$ provient dans la mesure où il peut provenir des éléments haut et bas constitutifs des $X_a(n)$, ou bien des nombres premiers qui interviennent en haut des $X_b(n)$ ou en bas des $X_c(n)$. La quantisation comme vous l'appelez est quant à elle associée au fait qu'on ne peut fournir les invariants que sur $X_c(2n) = 2X_a(n) + X_b(n) + X_c(n)$ ou sur $X_b(2n) = X_b(n) + X_c(n) + 2X_d(n)$ (voire sur $X_c(kn)$ ou $X_b(kn)$ en remplaçant les 2 dans les membres droits des égalités par des 4, des 6, etc) mais qu'on ne peut rien dire en utilisant $X_a(n)$, $X_b(n)$, $X_c(n)$ et $X_d(n)$ sur un truc comme $X_a(n+k)$, il faut mettre $2n$, $3n$, $4n$, etc., dans la parenthèse, i.e. un multiple entier de n, comme pour les quanta* (18.5.18) ;

— *Cette idée de nombre entier de nombres composés et nombre non-entier de nombres premiers fait penser aux quanta, non ?* (23.5.2018) ;

Bonne idée ? (Denise Vella-Chemla, 28.7.18)

La conjecture de Goldbach forte stipule que tout nombre pair supérieur à 6 est la somme de deux nombres premiers.

Ajouté le 29.7.2018
Il faut démontrer que pour tout n supérieur à 300, $\exists p, q$ premiers avec $p^2 + q = kn$ tels que $n - p$ premier.

Voici les quadruplets (n, p, q, k) pour n compris entre 16 et 100 (sauf pour $n = 44$), n non de forme triviale $2p$ avec p premier.

(16,5,7,2)	(50,3,41,1)	(78,7,29,1)
(18,7,5,3)	(52,23,43,11)	(80,13,71,3)
(20,3,11,1)	(54,7,5,1)	(84,5,59,1)
(24,7,23,3)	(56,3,47,1)	(88,41,79,20)
(28,5,3,1)	(60,7,11,1)	(90,7,41,1)
(30,7,11,2)	(64,11,7,2)	(92,3,83,1)
(32,3,23,1)	(66,7,17,1)	(96,7,47,1)
(36,7,23,2)	(68,31,59,15)	(98,19,31,4)
(40,3,31,1)	(70,3,61,1)	(100,11,79,2)
(42,5,17,1)	(72,5,47,1)	
(48,7,47,2)	(76,23,3,7)	

Ici est fourni le résultat d'un programme qui calcule les quadruplets jusqu'à 10^6 :

$$http://denise.vella.chemla.free.fr/quadruplets.html.$$

On peut résumer cette découverte ainsi : pour tout nombre pair n supérieur à 300, il semblerait qu'existe toujours un nombre premier p qui est un décomposant de Goldbach de n et qui est tel que $\sqrt{-p^2}\ (mod\ n)$ est un nombre premier.

Découvert le 28.7.2018
A la recherche d'une caractérisation des décomposants de Goldbach d'un nombre pair, on a découvert une propriété qui est vérifiée par l'un des décomposants de Goldbach au moins de tout nombre pair compris entre 300 et 10^6 et qui serait peut-être utilisable pour démontrer que tout nombre pair vérifie la conjecture de Goldbach.

On choisit un nombre premier p (parmi ceux qui ne sont pas des décomposants de Goldbach de n). On trouve la classe de congruence selon le module $n + 2$ de l'opposé du carré de p ($\equiv -p^2\ (mod\ n + 2)$, i.e. le nombre q compris entre 0 et $n + 2$ tel que $q - k(n + 2) = -p^2$).

Parfois, on a à la fois que p est un nombre premier, que q est également premier, et que p est un décomposant de Goldbach de $n + 2$.

Il faudrait être capable de démontrer (peut-être en utilisant la loi de réciprocité quadratique) qu'un tel nombre premier, dont l'opposé du carré est également premier, existe toujours (pour $n \geq 300$), et n'est jamais congru à $n + 2$, selon tout module premier inférieur à $\sqrt{n+2}$ (cette incongruence entre p et $n + 2$ selon tout module inférieur à $\sqrt{n+2}$ caractérise un décomposant de Goldbach de $n + 2$).

Ici est fourni le résultat d'un programme qui teste cette nouvelle idée :

$$http://denise.vella.chemla.free.fr/nouvellidee2871828.html.$$

Pour les seuls nombres inférieurs à 10^6 que sont $8, 12, 44, 104, 128, 152, 170, 212, 248$ et 296, on trouve bien un certain nombre de décomposants de Goldbach de $n + 2$ congrus à l'opposé du carré de p, mais aucun d'entre eux n'est premier.

Montrer ce qu'on a trouvé, même si on ne sait rien démontrer (Denise Vella-Chemla, 1.8.18)

A la recherche d'une inatteignable démonstration de la conjecture de Goldbach *, voici ce qu'on a trouvé récemment : on sait qu'un décomposant de Goldbach d'un nombre n est premier à n (puisqu'il est premier tout court). Quand on calcule les restes des divisions de $p(n-p) = -p^2$ par n, on réalise que l'un des décomposants de Goldbach de $n^{\dagger}$ a systématiquement le reste de la division de l'opposé de son carré par n qui est premier.

Ci-dessous, les tables de multiplication modulaire selon n jusqu'à 60 dans lesquelles on ne note que les restes des divisions par n qui sont premiers. Les décompositions de Goldbach de n sont colorées en bleu sur la diagonale ascendante. On peut noter le rétrécissement des tables pour les pairs multiples de 3. Dans chaque ligne et chaque colonne apparaissent tous les nombres premiers inférieurs à n qui ne divisent pas n une fois et une seule chacun. Chaque table a $\varphi(n)$ lignes et $\varphi(n)$ colonnes.

$n = 8$

	1	3	5	7
1		+	+	+
3	+		⊕	+
5	+	⊕		+
7	+	+	+	

$n = 12$

	1	5	7	11
1		+	+	+
5	+		⊕	+
7	+	⊕		+
11	+	+	+	

$n = 16$

	1	3	5	7	9	11	13	15
1		+	+	+		+	+	
3	+			+	+		⊕	+
5	+			+	+	⊕		+
7	+	+	+			+	+	
9		+	+			+	+	+
11	+		⊕	+	+			+
13	+	⊕		+	+			+
15		+	+		+	+	+	

$n = 18$

	1	5	7	11	13	17
1		+	+	+	+	+
5	+	+	+		⊕	+
7	+	+	+	⊕		+
11	+		⊕	+	+	+
13	+	⊕		+	+	+
17	+	+	+	+	+	

$n = 20$

	1	3	7	9	11	13	17	19
1		+	+		+	+	+	+
3	+			+	+	+	⊕	+
7	+			+	+	⊕	+	+
9		+	+		+	+	+	+
11	+	+	+	+		+	+	
13	+	+	⊕	+	+			+
17	+	⊕	+	+	+			+
19	+	+	+	+		+	+	

$n = 24$

	1	5	7	11	13	17	19	23
1		+	+	+	+	+	+	+
5	+		+	+	+	+	⊕	+
7	+	+		+	+	⊕	+	+
11	+	+	+		⊕	+	+	+
13	+	+	+	⊕		+	+	+
17	+	+	⊕	+	+		+	+
19	+	⊕	+	+	+	+		+
23	+	+	+	+	+	+	+	

$*$. On ne peut s'empêcher de penser à un mirage, une chimère...

$\dagger$. ceci pour tout $n \geq 300$ et $n < 10^6$ car en deça de 300, il y a quelques exceptions, les nombres 8, 12, 44, 104, 128, 152, 170, 212, 248 et 296.

$n = 28$

	1	3	5	9	11	13	15	17	19	23	25	27
1		+	+		+	+		+	+	+		
3	+				+	+	+	+		+	+	
5	+			+			+		+	⊕	+	+
9			+			+	+	+	+	+		+
11	+	+				+		⊕	+		+	+
13	+	+		+	+				+	+	+	
15		+	+	+				+	+		+	+
17	+	+		+	⊕		+				+	+
19	+		+	+	+	+	+			+		
23	+	+	⊕	+		+			+			+
25		+	+		+	+	+	+				+
27			+	+	+		+	+		+	+	

$n = 30$

	1	7	11	13	17	19	23	29
1		+	+	+	+	+	+	+
7	+	+	+		+	+	⊕	+
11	+	+		+	+	⊕	+	+
13	+		+	+	⊕	+	+	+
17	+	+	+	⊕	+	+		+
19	+	+	⊕	+	+		+	+
23	+	⊕	+	+		+	+	+
29	+	+	+	+	+	+	+	

$n = 32$

	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
1		+	+	+		+	+		+	+		+			+	+
3	+						+	+	+		+	+	+	+	⊕	+
5	+			+	+	+		+		+		+	+	+	+	
7	+		+	+	+	+			+	+	+			+	+	
9			+	+	+	+		+		+	+			+	+	+
11	+		+	+	+			+		+	+	+	+		+	
13	+	+						+	+	⊕	+	+	+	+		+
15		+	+		+	+	+		+	+			+		+	+
17	+	+		+			+	+		+	+	+		+	+	
19	+		+	+	+	+	⊕	+	+						+	+
21		+		+	+	+	+		+			+	+	+		+
23	+	+	+			+	+		+		+	+	+	+		
25		+	+			+	+	+			+	+	+	+		+
27		+	+	+	+		+		+		+	+	+			+
29	+	⊕	+	+	+	+		+	+	+						+
31	+	+			+		+	+		+	+		+	+	+	

$n = 36$

	1	5	7	11	13	17	19	23	25	29	31	35
1		+	+	+	+	+	+	+		+	+	
5	+			+	+	+	+	+	+		⊕	+
7	+		+	+	+	+		+	+	⊕		+
11	+	+	+	+		+	+		+	+	+	
13	+	+	+			+	+	⊕		+	+	+
17	+	+	+	+	+			+	+		+	+
19	+	+		+	+			+	+	+	+	+
23	+	+	+		⊕	+	+			+	+	+
25		+	+	+		+	+		+	+	+	+
29	+		⊕	+	+		+	+	+	+		+
31	+	⊕		+	+	+	+	+	+			+
35		+	+		+	+	+	+	+	+	+	

$n = 40$

	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39
1		+	+		+	+	+	+		+		+	+		+	
3	+						+	+	+	+		+	+	+	⊕	+
7	+			+	+	+		+			+	+	+	+	+	
9			+		+	+		+	+	+	+			+	+	+
11	+		+	+		+			+	+	+			+	+	+
13	+		+	+	+			+		+	+	+	+	+		
17	+	+						+	+	⊕	+	+	+		+	+
19	+	+	+	+		+	+			+		+	+		+	
21		+		+	+		+			+	+		+	+	+	+
23	+	+		+	+	+	⊕	+	+						+	+
27			+	+	+	+	+		+			+	+	+		+
29	+	+	+			+	+	+			+		+	+		+
31	+	+	+			+	+	+	+		+	+		+		
33		+	+	+	+	+			+		+	+	+			+
37	+	⊕	+	+	+		+	+	+	+						+
39		+		+	+		+		+	+	+	+		+	+	

$n = 42$

	1	5	11	13	17	19	23	25	29	31	37	41
1		+	+	+	+	+	+		+	+	+	+
5	+		+	+		+	+	+	+	+	⊕	+
11	+	+	+	+	+	+		+		⊕	+	+
13	+	+	+		+	+	+	+	⊕		+	+
17	+		+	+	+	+	+	+	+	+	+	
19	+	+	+	+	+		⊕	+	+		+	+
23	+	+		+	+	⊕		+	+	+	+	+
25		+	+	+	+	+	+	+	+	+		+
29	+	+		⊕	+	+	+	+		+	+	+
31	+	+	⊕		+		+	+	+	+	+	+
37	+	⊕	+	+	+	+	+		+	+		+
41	+	+	+	+		+	+	+	+	+	+	

$n = 44$

	1	3	5	7	9	13	15	17	19	21	23	25	27	29	31	35	37	39	41	43
1		+	+	+		+		+	+		+			+	+		+		+	+
3	+							+	+	+		+	+	+	+	+	+	+		+
5	+						+	+	+	+		+	+	+	+	+		+	+	
7	+			+	+	+	+	+			+	+	+		+				+	+
9				+	+	+	+			+	+	+	+	+		+		+	+	
13	+			+	+	+	+					+	+		⊕		+	+	+	+
15			+	+	+	+	+			+	+	+				+		+	+	+
17	+	+	+	+						+		+	+		+	+	+	+	+	
19	+	+	+							+	+		+	+	+	+	+	+	+	
21		+	+		+		+	+	+		+	+		+		+	+			+
23	+			+	+		+		+	+		+	+	+		+		+	+	
25		+	+	+	+	+	+	+		+	+							+	+	+
27		+	+	+	+	+		+	+		+						+	+	+	+
29	+	+	+		+				+	+	+			+	+	+	+	+		
31	+	+	+	+		⊕		+	+					+	+	+	+			+
35		+	+		+		+	+	+	+	+			+	+	+	+			
37	+	+				+		+	+	+			+	+	+	+	+			+
39		+	+		+	+	+	+	+		+	+	+	+						+
41	+		+	+	+	+	+	+	+		+	+	+							+
43	+	+		+		+	+			+		+	+		+		+	+	+	

$n = 48$

	1	5	7	11	13	17	19	23	25	29	31	35	37	41	43	47
1		+	+	+	+	+	+	+		+	+		+	+	+	+
5	+			+	+	+	+	+	+		+	+	+	+	⊕	+
7	+			+	+	+	+	+	+	+		+	+	⊕	+	+
11	+	+	+		+	+	+	+		+	+		⊕	+	+	+
13	+	+	+	+		+	+	+	+	+	+	+		+	+	
17	+	+	+	+	+			+	+	+	⊕	+	+		+	+
19	+	+	+	+	+			+	+	⊕	+	+	+	+		+
23	+	+	+	+	+	+	+		+	+	+	+		+	+	
25		+	+		+	+	+	+		+	+	+	+	+	+	+
29	+		+	+	+	+	⊕	+	+			+	+	+	+	+
31	+	+		+	+	⊕	+	+	+			+	+	+	+	+
35		+	+		+	+	+	+	+	+	+		+	+	+	+
37	+	+	+	⊕		+	+		+	+	+	+		+	+	+
41	+	+	⊕	+	+		+	+	+	+	+	+	+			+
43	+	⊕	+	+	+	+		+	+	+	+	+	+			+
47	+	+	+	+		+	+		+	+	+	+	+	+	+	

$n = 50$

	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39	41	43	47	49
1		+	+		+	+	+	+		+		+	+		+		+	+	+	
3	+							+	+	+	+	+	+		+	+	+	+	⊕	+
7	+			+		+	+		+	+		+	+	+		+	+		+	+
9			+	+		+	+			+	+	+	+	+			+	+	+	+
11	+					+	+		+	+	+	+	+	+	+	+		+	+	
13	+		+	+	+	+		+	+				+	+	⊕	+			+	+
17	+		+	+	+			+	+	+		+		+	+	+	+	+		
19	+	+				+	+	+		+	+				+	+	+	+	+	+
21		+	+		+	+	+		+		+			+		+	+	+	+	+
23	+	+	+	+	+		+	+		+		+	+			+	+		+	
27		+		+	+			+	+		+		+	+		+	+	+	+	+
29	+	+	+	+	+		+			+		+		+	+	+		+	+	
31	+	+	+	+	+	+				+	+		+	+	+				+	+
33			+	+	+	+	+		+		+	+	+			+	+	+		+
37	+	+			+	⊕	+	+				+	+		+	+	+	+		+
39		+	+		+	+	+	+	+	+	+	+		+	+					+
41	+	+	+	+			+	+	+	+	+			+	+		+	+		
43	+	+		+	+		+	+	+		+	+		+	+		+			+
47	+	⊕	+	+	+	+		+	+	+	+	+	+							+
49		+	+	+		+		+	+		+		+	+	+	+		+	+	

$n = 52$

	1	3	5	7	9	11	15	17	19	21	23	25	27	29	31	33	35	37	41	43	45	47	49	51
1		+	+	+		+		+	+		+			+	+			+	+	+		+		
3	+								+	+	+	+	+		+	+		+	+		+	+	+	
5	+					+	+		+		+		+	+			+	+		+	+		+	+
7	+				+				+	+	+	+		+		+	+			+	+	+	+	
9				+	+	+	+					+			+	+	+		+	+	+	+		+
11	+		+		+	+		+		+			+	+	+			+		+			+	+
15			+		+		+	+		+		+	+	+			+		+			+	+	+
17	+					+	+	+	+				+		+	+	+	+		+	+	+		
19	+	+	+	+				+				+		+	+	+	+			+	+		+	
21		+		+		+	+					+	+	+		+	+		+	+			+	+
23	+	+	+	+								+		$\oplus$	+	+		+	+		+	+		+
25		+		+	+		+		+	+	+				+		+	+	+			+	+	
27		+	+			+	+	+		+				+	+	+		+		+	+		+	
29	+		+	+		+	+		+	+	$\oplus$		+								+	+	+	+
31	+	+			+	+		+	+		+	+	+					+	+		+		+	
33		+		+	+			+	+	+	+		+				+				+	+	+	+
35			+	+	+		+	+	+	+		+				+	+	+	+					+
37	+	+	+			+		+			+	+	+		+		+	+		+		+		
41	+	+			+		+			+	+	+			+		+		+	+		+		+
43	+		+	+	+	+		+	+	+			+					+	+	+	+			
45		+	+	+	+			+	+		+		+	+	+	+				+				+
47	+	+		+	+		+	+			+	+		+		+		+	+					+
49		+	+	+		+	+		+	+		+	+	+	+	+								+
51			+		+	+	+			+	+			+		+	+		+		+	+	+	

$n = 54$

	1	5	7	11	13	17	19	23	25	29	31	35	37	41	43	47	49	53
1		+	+	+	+	+	+	+		+	+		+	+	+	+		+
5	+				+	+	+	+	+	+	+	+	+	+	+	+	+	
7	+			+	+	+		+	+	+		+	+	+	+	$\oplus$	+	+
11	+		+	+			+	+	+		+	+	+	+	$\oplus$	+	+	+
13	+	+	+		+	+	+	+		+		+		$\oplus$	+	+	+	+
17	+	+	+		+	+	+	+	+	+	+				+	+	+	+
19	+	+		+	+	+	+	+	+	+		+		+	+	+	+	
23	+	+	+	+	+	+	+	+		+	$\oplus$		+		+		+	+
25		+	+	+		+	+		+	+	+	+	+	+		+	+	+
29	+	+	+		+	+	+	+	+	+		+	+		+	+	+	
31	+	+		+		+		$\oplus$	+		+	+	+	+	+	+	+	+
35		+	+	+	+		+		+	+	+	+	+	+	+		+	+
37	+	+	+	+				+	+	+	+	+	+	+		+	+	+
41	+	+	+	+	$\oplus$		+		+		+	+	+	+		+	+	+
43	+	+	+	$\oplus$	+	+	+	+		+	+	+			+	+		+
47	+	+	$\oplus$	+	+	+	+		+	+	+		+	+	+			+
49		+	+	+	+	+	+	+	+	+	+	+	+	+				+
53	+		+	+	+	+		+	+		+	+	+	+	+	+	+	

$n = 56$

	1	3	5	9	11	13	15	17	19	23	25	27	29	31	33	37	39	41	43	45	47	51	53	55
1		+	+		+	+		+	+	+			+	+		+		+	+		+		+	
3	+									+	+		+	+	+		+	+	+	+	+	+	$\oplus$	+
5	+						+	+		+	+	+		+	+	+		+	+		+	+	+	
9					+	+	+	+	+			+	+		+	+				+	+	+	+	+
11	+			+		+	+	+	+	+		+		+			+	+		+	+		+	
13	+			+	+			+	+	+			+	+	+		+	+				+	+	+
15			+	+	+			+	+			+	+	+	+				+	+		+	+	+
17	+		+	+	+	+	+		+			+		+		+	+		+	+			+	
19	+			+	+	+	+	+					+	+	+	$\oplus$	+				+	+		+
23	+	+	+		+	+						+		+	+	+		+	+		+	+	+	
25		+	+									+	+	+	+	+	+	+	+	+		+	+	+
27			+	+	+		+	+		+	+			+		+		+	+		+		+	+
29	+	+		+		+	+		+		+			+	+		+	+		+	+	+		
31	+	+	+		+	+	+	+	+	+	+	+	+									+	+	
33		+	+	+		+	+		+	+	+		+						+	+		+	+	+
37	+		+	+				+	$\oplus$	+	+	+					+	+	+	+	+			+
39		+			+	+		+	+		+		+			+		+	+	+	+	+		+
41	+	+	+		+	+				+	+	+	+			+	+			+	+	+		
43	+	+	+				+	+		+	+	+			+	+	+			+	+			+
45		+		+	+		+	+			+		+		+	+	+	+	+		+			+
47	+	+	+	+	+				+	+		+	+			+	+	+	+	+				
51		+	+	+		+	+		+	+	+		+	+	+		+	+						+
53	+	$\oplus$	+	+	+	+	+	+		+	+	+		+	+									+
55		+		+		+	+		+		+	+			+	+	+		+	+		+	+	

$n = 60$

	1	7	11	13	17	19	23	29	31	37	41	43	47	49	53	59
1		+	+	+	+	+	+	+	+	+	+	+	+		+	+
7	+		+	+	+	+	+	+	+	+	+		+	+	$\oplus$	+
11	+	+		+	+	+	+	+	+	+	+	+	+	+	+	
13	+	+	+		+	+	+	+	+		+	+	$\oplus$	+	+	+
17	+	+	+	+		+	+	+	+	+	+	$\oplus$	+	+		+
19	+	+	+	+	+		+	+		+	$\oplus$	+	+	+	+	+
23	+	+	+	+	+	+		+	+	$\oplus$	+	+		+	+	+
29	+	+	+	+	+	+	+		$\oplus$	+		+	+	+	+	+
31	+	+	+	+	+		+	$\oplus$		+	+	+	+	+	+	+
37	+	+	+		+	+	$\oplus$	+	+		+	+	+	+	+	+
41	+	+	+	+	+	$\oplus$	+		+	+		+	+	+	+	+
43	+		+	+	$\oplus$	+	+	+	+	+	+		+	+	+	+
47	+	+	+	$\oplus$	+	+		+	+	+	+	+		+	+	+
49		+	+	+	+	+	+	+	+	+	+	+	+		+	+
53	+	$\oplus$	+	+		+	+	+	+	+	+	+	+	+		+
59	+	+		+	+	+	+	+	+	+	+	+	+	+	+	

On dispose des connaissances éparses suivantes qui pourraient être utiles :

- → pour tous p, q, nombres premiers à n, on a $p^{(q-1)/2} \equiv \pm 1 \ (mod\ q)$ selon que p est (+1) ou n'est pas (-1) résidu quadratique de q ;
- → pour tout p premier à n, $p^{\varphi(n)} \equiv 1 \ (mod\ n)$;
- → si n est de la forme $4k+2$ (n double d'impair) alors pour $m \leq n/4$, $\left(\frac{x}{n}\right) = \left(\frac{x+m}{n}\right)$;
- → article 78 des Recherches arithmétiques : le produit des unités (des nombres premiers à n) est congru à -1 $(mod\ n)$ pour n double d'une puissance de nombre premier différent de 2 (ainsi que pour $n = 4$ ou $n = p^m$) ; il est congru à 1 pour les autres nombres pairs ;
- → -1 est résidu quadratique des nombres premiers de la forme $4k+1$ ou bien des nombres composés de la forme $4k+1$ qui ne contiennent aucun premier $4k+3$ dans leur factorisation ;
- → -1 est non résidu quadratique des nombres pairs de la forme $4k$; il est résidu quadratique des nombres pairs de la forme $4k+2$ sauf s'ils contiennent un $4k+3$ dans leur factorisation et -1 est non-résidu quadratique de tous les autres nombres pairs qui ne contiennent aucun $4k+3$ dans leur factorisation.

Montrer ce qu'on a trouvé, même si on ne sait rien démontrer (Denise Vella-Chemla, 1.8.18)

A la recherche d'une inatteignable démonstration de la conjecture de Goldbach [*], voici ce qu'on a trouvé récemment : on sait qu'un décomposant de Goldbach d'un nombre n est premier à n (puisqu'il est premier tout court). Quand on calcule les restes des divisions de $p(n-p) = -p^2$ par n, on réalise que l'un des décomposants de Goldbach de n a systématiquement le reste de la division de l'opposé de son carré par n qui est premier.

Ci-dessous, les tables de multiplication modulaire selon n jusqu'à 60 dans lesquelles on ne note que les restes des divisions par n qui sont premiers. Les décompositions de Goldbach de n sont colorées en bleu sur la diagonale ascendante. On peut noter le rétrécissement des tables pour les pairs multiples de 3. Dans chaque ligne et chaque colonne apparaissent tous les nombres premiers inférieurs à n qui ne divisent pas n une fois et une seule chacun. Chaque table a $\varphi(n)$ lignes et $\varphi(n)$ colonnes.

$n = 6$ $(2p)$

	1	5
1		5
5	5	

$n = 8$

	1	3	5	7
1		3	5	7
3	3		7	5
5	5	7		3
7	7	5	3	

$n = 10$ $(2p)$

	1	3	7	9
1		3	7	
3	3			7
7	7			3
9		7	3	

$n = 12$

	1	5	7	11
1		5	7	11
5	5		11	7
7	7	11		5
11	11	7	5	

$n = 14$ $(2p)$

	1	3	5	9	11	13
1		3	5		11	13
3	3			13	5	11
5	5		11	3	13	
9		13	3	11		5
11	11	5	13			3
13	13	11		5	3	

$n = 16$

	1	3	5	7	9	11	13	15
1		3	5	7		11	13	
3	3			5	11		7	13
5	5			3	13	7		11
7	7	5	3			13	11	
9		11	13			3	5	7
11	11		7	13	3			5
13	13	7		11	5			3
15		13	11		7	5	3	

$n = 18$

	1	5	7	11	13	17
1		5	7	11	13	17
5	5	7	17		11	13
7	7	17	13	5		11
11	11		5	13	17	7
13	13	11		17	7	5
17	17	13	11	7	5	

$n = 20$

	1	3	7	9	11	13	17	19
1		3	7		11	13	17	19
3	3			7	13	19	11	17
7	7			3	17	11	19	13
9		7	3		19	17	13	11
11	11	13	17	19		3	7	
13	13	19	11	17	3			7
17	17	11	19	13	7			3
19	19	17	13	11		7	3	

[*]. On ne peut s'empêcher de penser à un mirage, une chimère...

$n = 22$ $(2p)$

	1	3	5	7	9	13	15	17	19	21
1		3	5	7		13		17	19	
3	3				5	17		7	13	19
5	5		3	13				19	7	17
7	7		13	5	19	3	17			
9		5		19		7	3		17	13
13	13	17		3	7		19		5	
15				17	3	19	5	13		7
17	17	7	19				13	3		5
19	19	13	7		17	5				3
21		19	17		13		7	5	3	

$n = 24$

	1	5	7	11	13	17	19	23
1		5	7	11	13	17	19	23
5	5		11	7	17	13	23	19
7	7	11		5	19	23	13	17
11	11	7	5		23	19	17	13
13	13	17	19	23		5	7	11
17	17	13	23	19	5		11	7
19	19	23	13	17	7	11		5
23	23	19	17	13	11	7	5	

$n = 26$ $(2p)$

	1	3	5	7	9	11	15	17	19	21	23	25
1		3	5	7		11		17	19		23	
3	3					7	19		5	11	17	23
5	5				19	3	23	7	17		11	
7	7			23	11				3	17	5	19
9			19	11	3		5	23		7		17
11	11	7	3			17		5		23	19	
15		19	23		5		17			3	7	11
17	17		7		23	5		3	11	19		
19	19	5	17	3				11	23			7
21			11		17	7	23	3	19			5
23	23	17	11	5		19	7					3
25		23		19	17		11		7	5	3	

$n = 28$

	1	3	5	9	11	13	15	17	19	23	25	27
1		3	5		11	13		17	19	23		
3	3				5	11	17	23		13	19	
5	5			17			19		11	3	13	23
9			17			5	23	13	3	11		19
11	11	5				3		19	13		23	17
13	13	11		5	3				23	19	17	
15		17	19	23				3	5		11	13
17	17	23		13	19		3				5	11
19	19		11	3	13	23	5			17		
23	23	13	3	11		19			17			5
25		19	13		23	17	11	5				3
27			23	19	17		13	11		5	3	

$n = 30$

	1	7	11	13	17	19	23	29
1		7	11	13	17	19	23	29
7	7	19	17		29	13	11	23
11	11	17		23	7	29	13	19
13	13		23	19	11	7	29	17
17	17	29	7	11	19	23		13
19	19	13	29	7	23		17	11
23	23	11	13	29		17	19	7
29	29	23	19	17	13	11	7	

$n = 32$

	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
1		3	5	7		11	13		17	19		23			29	31
3	3						7	13	19		31	5	11	17	23	29
5	5			3	13	23		11		31		19	29	7	17	
7	7		3	17	31	13			23	5	19			29	11	
9			13	31	17	3		7		11	29			19	5	23
11	11		23	13	3			5		17	7	29	19		31	
13	13	7						3	29	23	17	11	5	31		19
15		13	11		7	5	3		31	29			23		19	17
17	17	19		23			29	31		3	5	7		11	13	
19	19		31	5	11	17	23	29	3						7	13
21		31		19	29	7	17		5			3	13	23		11
23	23	5	19			29	11		7		3	17	31	13		
25		11	29			19	5	23			13	31	17	3		7
27		17	7	29	19		31		11		23	13	3			5
29	29	23	17	11	5	31		19	13	7						3
31	31	29			23		19	17		13	11		7	5	3	

$n = 34$ $(2p)$

	1	3	5	7	9	11	13	15	19	21	23	25	27	29	31	33
1		3	5	7		11	13		19		23			29	31	
3	3						5	11	23	29		7	13	19		31
5	5				11		31	7		3	13	23			19	29
7	7				29		23	3	31	11		5	19		13	
9			11	29	13	31				19	3		5	23	7	
11	11				31	19	7	29	5			3		13		23
13	13	5	31	23		7						19	11	3	29	
15		11	7	3		29			13		5		31		23	19
19	19	23		31		5		13			29		3	7	11	
21		29	3	11	19						7		23	31	5	13
23	23		13		3			5	29	7	19	31				11
25		7	23	5		3	19				31	13	29	11		
27		13		19	5		11	31	3	23		29				7
29	29	19			23	13	3		7	31		11				5
31	31		19	13	7		29	23	11	5						3
33		31	29			23		19		13	11		7	5	3	

$n = 36$

	1	5	7	11	13	17	19	23	25	29	31	35
1		5	7	11	13	17	19	23		29	31	
5	5			19	29	13	23	7	17		11	31
7	7		13	5	19	11		17	31	23		29
11	11	19	5	13		7	29		23	31	17	
13	13	29	19			5	31	11		17	7	23
17	17	13	11	7	5			31	29		23	19
19	19	23		29	31			5	7	11	13	17
23	23	7	17		11	31	5			19	29	13
25		17	31	23		29	7		13	5	19	11
29	29		23	31	17		11	19	5	13		7
31	31	11		17	7	23	13	29	19			5
35		31	29		23	19	17	13	11	7	5	

$n = 38$ $(2p)$

	1	3	5	7	9	11	13	15	17	21	23	25	27	29	31	33	35	37
1		3	5	7		11	13		17		23			29	31			37
3	3							7	13		31	37	5	11	17	23	29	
5	5				7	17		37		29		11		31	3	13	23	
7	7			11				29	5			23	37	13		3	17	31
9			7		5	23	3			37	17				13	31	11	29
11	11		17		23	7	29	13		3			31		37		5	
13	13				3	29	17	5	31	7					23	11	37	
15		7	37	29		13	5			11	3			17			31	23
17	17	13		5			31		23		11	7	3	37		29		
21			29		37	3	7	11		23		31			5		13	17
23	23	31			17			3	11			5	13		29	37	7	
25		37	11	23					7	31	5	17	29	3				13
27		5		37		31			3		13	29	7	23		17		11
29	29	11	31	13				17	37			3	23	5		7		
31	31	17	3		13	37	23			5	29				11			7
33		23	13	3	31		11		29		37		17	7				5
35		29	23	17	11	5	37	31		13	7							3
37	37			31	29			23		17		13	11		7	5	3	

$n = 40$

	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39
1		3	7		11	13	17	19		23		29	31		37	
3	3						11	17	23	29		7	13	19	31	37
7	7			23	37	11		13			29	3	17	31	19	
9			23		19	37		11	29	7	3			17	13	31
11	11		37	19		23			31	13	17			3	7	29
13	13		11	37	23			7		19	31	17	3	29		
17	17	11						3	37	31	19	13	7		29	23
19	19	17	13	11		7	3			37		31	29		23	
21		23		29	31		37			3	7		11	13	17	19
23	23	29		7	13	19	31	37	3						11	17
27			29	3	17	31	19		7			23	37	11		13
29	29	7	3			17	13	31			23		19	37		11
31	31	13	17			3	7	29	11		37	19		23		
33		19	31	17	3	29			13		11	37	23			7
37	37	31	19	13	7		29	23	17	11						3
39		37		31	29		23		19	17	13	11		7	3	

$n = 42$

	1	5	11	13	17	19	23	25	29	31	37	41
1		5	11	13	17	19	23		29	31	37	41
5	5		13	23		11	31	41	19	29	17	37
11	11	13	37	17	19	41		23		5	29	31
13	13	23	17		11	37	5	31	41		19	29
17	17		19	11	37	29	13	5	31	23	41	
19	19	11	41	37	29		17	13	5		31	23
23	23	31		5	13	17		29	37	41	11	19
25		41	23	31	5	13	29	37	11	19		17
29	29	19		41	31	5	37	11		17	23	13
31	31	29	5		23		41	19	17	37	13	11
37	37	17	29	19	41	31	11		23	13		5
41	41	37	31	29		23	19	17	13	11	5	

$n = 44$

	1	3	5	7	9	13	15	17	19	21	23	25	27	29	31	35	37	39	41	43
1		3	5	7		13		17	19		23			29	31		37		41	43
3	3							7	13	19		31	37	43	5	17	23	29		41
5	5						31	41	7	17		37	3	13	23	43		19	29	
7	7			5	19	3	17	31			29	43	13		41				23	37
9				19	37	29	3			13	31	5	23	41		7		43	17	
13	13			3	29	37	19					17	43		7		41	23	5	31
15			31	17	3	19	5			7	37	23				41		13	43	29
17	17	7	41	31						5		29	19		43	23	13	3	37	
19	19	13	7							3	41		29	23	17	5	43	37	31	
21		19	17		13		7	5	3		43	41		37		31	29			23
23	23			29	31		37		41	43		3	5	7		13		17	19	
25		31	37	43	5	17	23	29		41	3							7	13	19
27		37	3	13	23	43		19	29		5						31	41	7	17
29	29	43	13		41				23	37	7			5	19	3	17	31		
31	31	5	23	41		7		43	17					19	37	29	3			13
35		17	43		7		41	23	5	31	13			3	29	37	19			
37	37	23				41		13	43	29			31	17	3	19	5			7
39		29	19		43	23	13	3	37		17	7	41	31						5
41	41		29	23	17	5	43	37	31		19	13	7							3
43	43	41		37		31	29			23		19	17		13		7	5	3	

$n = 46$ $(2p)$

	1	3	5	7	9	11	13	15	17	19	21	25	27	29	31	33	35	37	39	41	43	45
1		3	5	7		11	13		17	19				29	31			37		41	43	
3	3								5	11	17	29		41		7	13	19		31	37	43
5	5						19	29		3	13		43	7	17		37		11		31	41
7	7			3	17	31		13		41		37	5	19				29	43	11		
9				17		7		43			5	41	13	31	3			11	29		19	37
11	11			31	7	29	5		3					43	19	41	17			37	13	
13	13		19			5	31	11	37	17	43	3	29				41				7	
15			29	13	43		11	41				7	37		5		19	3		17		31
17	17	5				3	37		13			11					43	31	19	7	41	29
19	19	11	3	41			17				31		7		37	29		13	5	43		
21		17	13		5		43			31		19		11	7	3		41	37		29	
25		29		37	41		3	7	11		19		31			43		5		13	17	
27			43	5	13		29	37		7		31				17			41	3	11	19
29	29	41	7	19	31	43					11			13		37	3				5	17
31	31		17		3	19		5		37	7				41	11		43	13	29		
33		7				41				29	3	43	17	37	11	31	5			19		13
35		13	37			17	41	19	43					3		5	29	7	31			11
37	37	19		29	11			3	31	13	41	5			43		7		17			
39			11	43	29				19	5	37		41		13		31	17	3			7
41	41	31		11		37		17	7	43		13	3		29	19						5
43	43	37	31		19	13	7		41		29	17	11	5								3
45		43	41		37			31	29				19	17		13	11		7	5	3	

$n = 48$

	1	5	7	11	13	17	19	23	25	29	31	35	37	41	43	47
1		5	7	11	13	17	19	23		29	31		37	41	43	47
5	5			7	17	37	47	19	29		11	31	41	13	23	43
7	7			29	43	23	37	17	31	11		5	19	47	13	41
11	11	7	29		47	43	17	13		31	5		23	19	41	37
13	13	17	43	47		29	7	11	37	41	19	23		5	31	
17	17	37	23	43	29			7	41	13	47	19	5		11	31
19	19	47	37	17	7			5	43	23	13	41	31	11		29
23	23	19	17	13	11	7	5		47	43	41	37		31	29	
25		29	31		37	41	43	47		5	7	11	13	17	19	23
29	29		11	31	41	13	23	43	5			7	17	37	47	19
31	31	11		5	19	47	13	41	7			29	43	23	37	17
35		31	5		23	19	41	37	11	7	29		47	43	17	13
37	37	41	19	23		5	31		13	17	43	47		29	7	11
41	41	13	47	19	5		11	31	17	37	23	43	29			7
43	43	23	13	41	31	11		29	19	47	37	17	7			5
47	47	43	41	37		31	29		23	19	17	13	11	7	5	

$n = 50$

	1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39	41	43	47	49
1		3	7		11	13	17	19		23		29	31		37		41	43	47	
3	3							7	13	19	31	37	43		11	17	23	29	41	47
7	7			13		41	19		47	11		3	17	31		23	37		29	43
9			13	31		17	3			7	43	11	29	47			19	37	23	41
11	11					43	37		31	3	47	19	41	13	7	29		23	17	
13	13		41	17	43	19		47	23				3	29	31	7			11	37
17	17		19	3	37			23	7	41		43		11	29	13	47	31		
19	19	7				47	23	11		37	13				3	41	29	17	43	31
21		13	47		31	23	7		41		17			43		19	11	3	37	29
23	23	19	11	7	3		41	37		29		17	13			47	43		31	
27		31		43	47			13	17		29		37	41		3	7	11	19	23
29	29	37	3	11	19		43			17		41		7	23	31		47	13	
31	31	43	17	29	41	3				13	37		11	23	47				7	19
33			31	47	13	29	11		43		41	7	23			37	3	19		17
37	37	11			7	31	29	3				23	47		19	43	17	41		13
39		17	23		29	7	13	41	19	47	3	31		37	43					11
41	41	23	37	19			47	29	11	43	7			3	17		31	13		
43	43	29		37	23		31	17	3		11	47		19	41		13			7
47	47	41	29	23	17	11		43	37	31	19	13	7							3
49		47	43	41		37		31	29		23		19	17	13	11		7	3	

$n = 52$

	1	3	5	7	9	11	15	17	19	21	23	25	27	29	31	33	35	37	41	43	45	47	49	51
1		3	5	7		11		17	19		23			29	31			37	41	43		47		
3	3								5	11	17	23	29		41	47		7	19		31	37	43	
5	5					3	23		43		11		31	41			19	29		7	17		37	47
7	7				11				29	43	5	19		47		23	37			41	3	17	31	
9				11	29	47	31					17			19	37	3		5	23	41	7		43
11	11		3		47	17		31		23			37	7	29			43		5			19	41
15			23		31		17	47		3		11	41	19			5		43			29	7	37
17	17					31	47	29	11				43		7	41	23	5		3	37	19		
19	19	5	43	29				11				7		31	17	3	41			37	23		47	
21		11		43		23	3					5	47	37		17	7		29	19			41	31
23	23	17	11	5								3		43	37	31		19	7		47	41		29
25		23		19	17		11		7	5	3				47		43	41	37			31	29	
27		29	31			37	41	43		47				3	5	7		11		17	19		23	
29	29		41	47		7	19		31	37	43		3								5	11	17	23
31	31	41			19	29		7	17		37	47	5					3	23		43		11	
33		47		23	37			41	3	17	31		7				11				29	43	5	19
35			19	37	3		5	23	41	7		43				11	29	47	31					17
37	37	7	29			43		5			19	41	11		3		47	17		31		23		
41	41	19			5		43			29	7	37			23		31		17	47		3		11
43	43		7	41	23	5		3	37	19			17					31	47	29	11			
45		31	17	3	41			37	23		47		19	5	43	29				11				7
47	47	37		17	7		29	19			41	31		11		43		23	3					5
49		43	37	31		19	7		47	41		29	23	17	11	5								3
51			47		43	41	37			31	29			23		19	17		11		7	5	3	

$n = 54$

	1	5	7	11	13	17	19	23	25	29	31	35	37	41	43	47	49	53
1		5	7	11	13	17	19	23		29	31		37	41	43	47		53
5	5				11	31	41	7	17	37	47	13	23	43	53	19	29	
7	7			23	37	11		53	13	41		29	43	17	31	5	19	47
11	11		23	13			47	37	5		17	7	29	19	41	31	53	43
13	13	11	37		7	5	31	29		53		23		47	19	17	43	41
17	17	31	11		5	19	53	13	47	7	41				29	43	23	37
19	19	41		47	31	53	37	5	43	11		17		23	7	29	13	
23	23	7	53	37	29	13	5	43		19	11		41		17		47	31
25		17	13	5		47	43		31	23	19	11	7	53		41	37	29
29	29	37	41		53	7	11	19	23	31		43	47		5	13	17	
31	31	47		17		41		11	19		43	5	13	29	37	53	7	23
35		13	29	7	23		17		11	43	5	37	53	31	47		41	19
37	37	23	43	29				41	7	47	13	53	19	5		11	31	17
41	41	43	17	19	47		23		53		29	31	5	7		37	11	13
43	43	53	31	41	19	29	7	17		5	37	47			13	23		11
47	47	19	5	31	17	43	29		41	13	53		11	37	23			7
49		29	19	53	43	23	13	47	37	17	7	41	31	11				5
53	53		47	43	41	37		31	29		23	19	17	13	11	7	5	

$n = 56$

	1	3	5	9	11	13	15	17	19	23	25	27	29	31	33	37	39	41	43	45	47	51	53	55
1		3	5		11	13		17	19	23			29	31		37		41	43		47		53	
3	3									13	19		31	37	43		5	11	17	23	29	41	47	53
5	5						19	29		3	13	23		43	53	17		37	47		11	31	41	
9					43	5	23	41	3			19	37		17	53				13	31	11	29	47
11	11			43		31	53	19	41	29		17		5			37	3		47	13		23	
13	13			5	31			53	23	19			41	11	37		3	29				47	17	43
15			19	23	53			31	5			13	43	17	47				29	3		37	11	41
17	17		29	41	19	53	31		43			11		23		13	47		3	37			5	
19	19			3	41	23	5	43					47	29	11	31	13				53	17		37
23	23	13	3		29	19						5		41	31	11		47	37		17	53	43	
25		19	13									3	53	47	41	29	23	17	11	5		43	37	31
27			23	19	17		13	11		5	3			53		47		43	41		37		31	29
29	29	31		37		41	43		47		53			3	5		11	13		17	19	23		
31	31	37	43		5	11	17	23	29	41	47	53	3									13	19	
33		43	53	17		37	47		11	31	41		5						19	29		3	13	23
37	37		17	53				13	31	11	29	47					43	5	23	41	3			19
39		5			37	3		47	13		23		11			43		31	53	19	41	29		17
41	41	11	37		3	29				47	17	43	13			5	31			53	23	19		
43	43	17	47				29	3		37	11	41			19	23	53			31	5			13
45		23		13	47		3	37			5		17		29	41	19	53	31		43			11
47	47	29	11	31	13				53	17		37	19			3	41	23	5	43				
51		41	31	11		47	37		17	53	43		23	13	3		29	19						5
53	53	47	41	29	23	17	11	5		43	37	31		19	13									3
55		53		47		43	41		37		31	29			23	19	17		13	11		5	3	

$n = 58$ $(2p)$

	1	3	5	7	9	11	13	15	17	19	21	23	25	27	31	33	35	37	39	41	43	45	47	49	51	53	55	57
1		3	5	7		11	13		17	19		23			31			37		41	43		47			53		
3	3										5	11	17	23		41	47	53		7	13	19		31	37	43		
5	5						7	17		37	47			19				11		31	41		3	13	23		43	53
7	7				5	19		47	3	17	31				43		13		41		11			53		23	37	
9				5	23	41		19	37					11	47	7		43	3				17		53	13	31	
11	11			19	41	5			13				43	7			37		23			31	53	17		3		47
13	13		7				53		47		41			3		23		17	43	11	37	5	31				19	
15			17	47	19				23	53						31	3		5		7	37			11	41	13	43
17	17			3	37	13	47	23				43	19	53	5							11				31	7	41
19	19		37	17				53		13		31	11			47		7			5	43	23	3	41			
21		5	47	31			41					19	3		13			23	7			17		43		11	53	37
23	23	11							43	31	19	7	53	41	17	5					3		37		13		47	
25		17				43			19	11	3	53		37		13	5		47		31	23		7			41	
27		23	19		11	7	3		53			41	37				17	13		5				47	43			31
31	31			43	47				5		13	17				37	41			53		3	7	11		19	23	
33		41			7		23	31		47		5	13		37		53	3	11	19			43				17	
35		47		13		37		3					5	17	41	53	7	19	31	43							11	23
37	37	53	11		43		17			7	23			13		3	19					41			31	47	5	
39				41	3	23	43	5			7		47			11	31		13		53				17	37		19
41	41	7	31				11							5	53	19	43				23	47	13	37	3			17
43	43	13	41	11			37	7		5		3	31						53	23				19	47	17		
45		19				31	5	37	11	43	17		23		3			41		47		53				7		13
47	47		3		17	53	31			23		37			7	43				13			5	41	19			11
49		31	13	53		17				3	43		7	47	11					37	19		41	23	5			
51		37	23		53			11		41		13		43				31	17	3	47		19	5				7
53	53	43		23	13	3		41	31		11				19			47	37		17	7						5
55			43	37	31		19	13	7		53	47	41		23	17	11	5										3
57			53			47		43	41		37			31			23		19	17		13	11		7	5	3	

$n = 60$

	1	7	11	13	17	19	23	29	31	37	41	43	47	49	53	59
1		7	11	13	17	19	23	29	31	37	41	43	47		53	59
7	7		17	31	59	13	41	23	37	19	47		29	43	11	53
11	11	17		23	7	29	13	19	41	47	31	53	37	59	43	
13	13	31	23		41	7	59	17	43		53	19	11	37	29	47
17	17	59	7	41		23	31	13	47	29	37	11	19	53		43
19	19	13	29	7	23		17	11		43	59	37	53	31	47	41
23	23	41	13	59	31	17		7	53	11	43	29		47	19	37
29	29	23	19	17	13	11	7		59	53		47	43	41	37	31
31	31	37	41	43	47		53	59		7	11	13	17	19	23	29
37	37	19	47		29	43	11	53	7		17	31	59	13	41	23
41	41	47	31	53	37	59	43		11	17		23	7	29	13	19
43	43		53	19	11	37	29	47	13	31	23		41	7	59	17
47	47	29	37	11	19	53		43	17	59	7	41		23	31	13
49		43	59	37	53	31	47	41	19	13	29	7	23		17	11
53	53	11	43	29		47	19	37	23	41	13	59	31	17		7
59	59	53		47	43	41	37	31	29	23	19	17	13	11	7	

On dispose des connaissances éparses suivantes qui pourraient être utiles :

- → pour tous p, q, nombres premiers à n, on a $p^{(q-1)/2} \equiv \pm 1$ $(mod\ q)$ selon que p est (+1) ou n'est pas (-1) résidu quadratique de q ;
- → pour tout p premier à n, $p^{\varphi(n)} \equiv 1$ $(mod\ n)$;

- $\rightarrow$ si n est de la forme $4k+2$ (n double d'impair) alors pour $m \leq n/4$, $\left(\frac{x}{n}\right) = \left(\frac{x+m}{n}\right)$;
- $\rightarrow$ article 78 des Recherches arithmétiques : le produit des unités (des nombres premiers à n) est congru à -1 ($mod\ n$) pour n double d'une puissance de nombre premier différent de 2 (ainsi que pour $n = 4$ ou $n = p^m$) ; il est congru à 1 pour les autres nombres pairs ;
- $\rightarrow$ -1 est résidu quadratique des nombres premiers de la forme $4k+1$ ou bien des nombres composés de la forme $4k+1$ qui ne contiennent aucun premier $4k+3$ dans leur factorisation ;
- $\rightarrow$ -1 est non résidu quadratique des nombres pairs de la forme $4k$; il est résidu quadratique des nombres pairs de la forme $4k+2$ sauf s'ils contiennent un $4k+3$ dans leur factorisation et -1 est non-résidu quadratique de tous les autres nombres pairs qui ne contiennent aucun $4k+3$ dans leur factorisation.

Deviendrons-nous tous des produits ? (Denise Vella-Chemla, 7.8.18)

Recherchant une démonstration de la conjecture de Goldbach, désespérément, on calcule ce que vaut, modulo n, le produit des décomposants de Goldbach de n inférieurs à $n/2$ (c'est le reste de la division du produit en question par n).

On calcule également ce que vaut le quotient de cette division. Ci-après le résultat de l'exécution du programme ainsi que le programme lui-même.

```
6 -> 3 = 3 (mod 6)
     flotte ? 0.5
8 -> 3 = 3 (mod 8)
     flotte ? 0.375
10 -> 15 = 5 (mod 10)
     flotte ? 1.5
12 -> 5 = 5 (mod 12)
     flotte ? 0.416666666667
14 -> 21 = 7 (mod 14)
     flotte ? 1.5
16 -> 15 = 15 (mod 16)
     flotte ? 0.9375
18 -> 35 = 17 (mod 18)
     flotte ? 1.94444444444
20 -> 21 = 1 (mod 20)
     flotte ? 1.05
22 -> 165 = 11 (mod 22)
     flotte ? 7.5
24 -> 385 = 1 (mod 24)
     flotte ? 16.0416666667
26 -> 273 = 13 (mod 26)
     flotte ? 10.5
28 -> 55 = 27 (mod 28)
     flotte ? 1.96428571429
30 -> 1001 = 11 (mod 30)
     flotte ? 33.3666666667
32 -> 39 = 7 (mod 32)
     flotte ? 1.21875
34 -> 2805 = 17 (mod 34)
     flotte ? 82.5
36 -> 7735 = 31 (mod 36)
     flotte ? 214.861111111
38 -> 133 = 19 (mod 38)
     flotte ? 3.5
40 -> 561 = 1 (mod 40)
     flotte ? 14.025
42 -> 13585 = 19 (mod 42)
     flotte ? 323.452380952
44 -> 273 = 9 (mod 44)
     flotte ? 6.20454545455
46 -> 5865 = 23 (mod 46)
     flotte ? 127.5
48 -> 124355 = 35 (mod 48)
     flotte ? 2590.72916667
```

```
50 -> 5187 = 37 (mod 50)
     flotte ? 103.74
52 -> 1265 = 17 (mod 52)
     flotte ? 24.3269230769
54 -> 391391 = 53 (mod 54)
     flotte ? 7247.98148148
56 -> 741 = 13 (mod 56)
     flotte ? 13.2321428571
58 -> 27115 = 29 (mod 58)
     flotte ? 467.5
60 -> 19605131 = 11 (mod 60)
     flotte ? 326752.183333
62 -> 1767 = 31 (mod 62)
     flotte ? 28.5
64 -> 64515 = 3 (mod 64)
     flotte ? 1008.046875
66 -> 5766215 = 59 (mod 66)
     flotte ? 87366.8939394
68 -> 217 = 13 (mod 68)
     flotte ? 3.19117647059
70 -> 374187 = 37 (mod 70)
     flotte ? 5345.52857143
72 -> 12212915 = 59 (mod 72)
     flotte ? 169623.819444
74 -> 313131 = 37 (mod 74)
     flotte ? 4231.5
76 -> 170085 = 73 (mod 76)
     flotte ? 2237.96052632
78 -> 142635185 = 17 (mod 78)
     flotte ? 1828656.21795
80 -> 63973 = 53 (mod 80)
     flotte ? 799.6625
82 -> 902451 = 41 (mod 82)
     flotte ? 11005.5
84 -> 13147103255 = 83 (mod 84)
     flotte ? 156513133.988
86 -> 223041 = 43 (mod 86)
     flotte ? 2593.5
88 -> 101065 = 41 (mod 88)
     flotte ? 1148.46590909
90 -> 818183948197 = 67 (mod 90)
     flotte ? 9090932757.74
92 -> 22971 = 63 (mod 92)
     flotte ? 249.684782609
94 -> 2437655 = 47 (mod 94)
     flotte ? 25932.5
96 -> 1641671759 = 47 (mod 96)
     flotte ? 17100747.4896
98 -> 21793 = 37 (mod 98)
     flotte ? 222.37755102
100 -> 31350363 = 63 (mod 100)
     flotte ? 313503.63
```

On constate que le quotient flottant est de partie décimale égale à $1/2$ pour les doubles de premiers et pour eux seulement. Si on utilise les restes modulaires au fur et à mesure des multiplications, on obtient les quotients suivants dans l'intervalle $[0, 1]$ (on note également le produit des complémentaires à n des décomposants).

On constate qu'alors le résidu modulaire du produit des décomposants de Goldbach de n inférieurs ou égaux à $n/2$ vaut $n/2$. On vérifie qu'il n'y a pas de contre-exemples à cela jusqu'à 65912.

```
6 produit dg mod n = 3 flotte ? 0.5 produit compl dg mod n = 3 flotte ? 0.5

8 produit dg mod n = 3 flotte ? 0.375 produit compl dg mod n = 5 flotte ? 0.625

10 produit dg mod n = 5 flotte ? 0.5 produit compl dg mod n = 5 flotte ? 0.5

12 produit dg mod n = 5 flotte ? 0.416667 produit compl dg mod n = 7 flotte ? 0.583333

14 produit dg mod n = 7 flotte ? 0.5 produit compl dg mod n = 7 flotte ? 0.5

16 produit dg mod n = 15 flotte ? 0.9375 produit compl dg mod n = 15 flotte ? 0.9375

18 produit dg mod n = 17 flotte ? 0.944444 produit compl dg mod n = 17 flotte ? 0.944444

20 produit dg mod n = 1 flotte ? 0.05 produit compl dg mod n = 1 flotte ? 0.05

22 produit dg mod n = 11 flotte ? 0.5 produit compl dg mod n = 11 flotte ? 0.5

24 produit dg mod n = 1 flotte ? 0.0416667 produit compl dg mod n = 23 flotte ? 0.958333

26 produit dg mod n = 13 flotte ? 0.5 produit compl dg mod n = 13 flotte ? 0.5

28 produit dg mod n = 27 flotte ? 0.964286 produit compl dg mod n = 27 flotte ? 0.964286

30 produit dg mod n = 11 flotte ? 0.366667 produit compl dg mod n = 19 flotte ? 0.633333

32 produit dg mod n = 7 flotte ? 0.21875 produit compl dg mod n = 7 flotte ? 0.21875

34 produit dg mod n = 17 flotte ? 0.5 produit compl dg mod n = 17 flotte ? 0.5

36 produit dg mod n = 31 flotte ? 0.861111 produit compl dg mod n = 31 flotte ? 0.861111

38 produit dg mod n = 19 flotte ? 0.5 produit compl dg mod n = 19 flotte ? 0.5

40 produit dg mod n = 1 flotte ? 0.025 produit compl dg mod n = 39 flotte ? 0.975

42 produit dg mod n = 19 flotte ? 0.452381 produit compl dg mod n = 19 flotte ? 0.452381

44 produit dg mod n = 9 flotte ? 0.204545 produit compl dg mod n = 35 flotte ? 0.795455

46 produit dg mod n = 23 flotte ? 0.5 produit compl dg mod n = 23 flotte ? 0.5

48 produit dg mod n = 35 flotte ? 0.729167 produit compl dg mod n = 13 flotte ? 0.270833

50 produit dg mod n = 37 flotte ? 0.74 produit compl dg mod n = 37 flotte ? 0.74

52 produit dg mod n = 17 flotte ? 0.326923 produit compl dg mod n = 35 flotte ? 0.673077

54 produit dg mod n = 53 flotte ? 0.981481 produit compl dg mod n = 1 flotte ? 0.0185185

56 produit dg mod n = 13 flotte ? 0.232143 produit compl dg mod n = 43 flotte ? 0.767857

58 produit dg mod n = 29 flotte ? 0.5 produit compl dg mod n = 29 flotte ? 0.5

60 produit dg mod n = 11 flotte ? 0.183333 produit compl dg mod n = 11 flotte ? 0.183333
```

```
62 produit dg mod n = 31 flotte ? 0.5 produit compl dg mod n = 31 flotte ? 0.5

64 produit dg mod n = 3 flotte ? 0.046875 produit compl dg mod n = 61 flotte ? 0.953125

66 produit dg mod n = 59 flotte ? 0.893939 produit compl dg mod n = 59 flotte ? 0.893939

68 produit dg mod n = 13 flotte ? 0.191176 compl dg mod n = 13 flotte ? 0.191176

70 produit dg mod n = 37 flotte ? 0.528571 produit compl dg mod n = 33 flotte ? 0.471429

72 produit dg mod n = 59 flotte ? 0.819444 produit compl dg mod n = 59 flotte ? 0.819444

74 produit dg mod n = 37 flotte ? 0.5 produit compl dg mod n = 37 flotte ? 0.5

76 produit dg mod n = 73 flotte ? 0.960526 produit compl dg mod n = 3 flotte ? 0.0394737

78 produit dg mod n = 17 flotte ? 0.217949 produit compl dg mod n = 61 flotte ? 0.782051

80 produit dg mod n = 53 flotte ? 0.6625 produit compl dg mod n = 53 flotte ? 0.6625

82 produit dg mod n = 41 flotte ? 0.5 produit compl dg mod n = 41 flotte ? 0.5

84 produit dg mod n = 83 flotte ? 0.988095 produit compl dg mod n = 83 flotte ? 0.988095

86 produit dg mod n = 43 flotte ? 0.5 produit compl dg mod n = 43 flotte ? 0.5

88 produit dg mod n = 41 flotte ? 0.465909 produit compl dg mod n = 41 flotte ? 0.465909

90 produit dg mod n = 67 flotte ? 0.744444 produit compl dg mod n = 23 flotte ? 0.255556

92 produit dg mod n = 63 flotte ? 0.684783 produit compl dg mod n = 63 flotte ? 0.684783

94 produit dg mod n = 47 flotte ? 0.5 produit compl dg mod n = 47 flotte ? 0.5

96 produit dg mod n = 47 flotte ? 0.489583 produit compl dg mod n = 49 flotte ? 0.510417

98 produit dg mod n = 37 flotte ? 0.377551 produit compl dg mod n = 61 flotte ? 0.622449

100 produit dg mod n = 63 flotte ? 0.63 produit compl dg mod n = 63 flotte ? 0.63
```

Explication : Pour les doubles de nombres premiers de la forme $2p$, comme p est un décomposant de Goldbach trivial de $2p$, le produit des décomposants de Goldbach est de la forme $(2k+1)p$ car tous les décomposants de $2p$ autres que p étant impairs, leur produit est impair, et le produit de tous les décomposants de Goldbach est alors de la forme $(2k+1)p$ qui est congru à p $(mod\ 2p)$.

Pour les pairs non doubles de premiers, le quotient x du produit des décomposants de Goldbach de n est égal au quotient du produit de leurs complémentaires à n si le nombre de décomposants de Goldbach est pair tandis que l'un est l'autre sont complémentaires à 1 (x et $1-x$) si le nombre de décomposants de Goldbach de n est impair.

```
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

for n in range(6,102,2):
  produit = 1
  for x in range(1,n/2+1,1):
    if ((prime(x)) and (prime(n-x))):
      produit = produit*x
  s=str(n)
  s+=" -> "; s+=str(produit)
  s+=" = ";s+=str(produit % n);s+=" (mod ";s+=str(n);s+=")\n"
  s+="    flotte ? ";s+=str(produit/float(n));
  print(s)
```

Dans la mesure où on ne connaît pas la raison qui fait que le nombre de décomposants de Goldbach d'un nombre pair est pair ou impair, cette idée n'aide pas à faire avancer la compréhension.

Snurpf, exemple (Denise Vella-Chemla, 9.8.18)

On a appelé SNURPF notre Système de NUmération par les Restes modulaires dans les corps premiers [1]. Chaque nombre est codé par le n-uplet des restes de ses divisions par l'ensemble des nombres premiers inférieurs à sa racine.

On rappelle qu'un nombre premier p est un décomposant de Goldbach d'un nombre pair n s'il est inférieur à $n/2$ et ne partage avec n aucun de ses restes de divisions.

Voici un exemple, selon les nombres premiers 3, 5 et 7 (c'est la base de nombres premiers inférieurs à $\sqrt{100}$ dans laquelle on se place). On cherche les décomposants de Goldbach de 100.

$$100 \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}$$

Un décomposant de Goldbach de 100 trouvable par la méthode proposée ici est de la forme :

$$\begin{pmatrix} 2 \\ 1 \vee 2 \vee 3 \vee 4 \\ 1 \vee 3 \vee 4 \vee 5 \vee 6 \end{pmatrix}$$

Ecrivons les nombres premiers inférieurs à 50 et leurs restes, colorons en bleu les restes admissibles :

$$\begin{array}{cccccccccccccc}
3 & 5 & 7 & 11 & 13 & 17 & 19 & 23 & 29 & 31 & 37 & 41 & 43 & 47 \\
\begin{pmatrix} 0 \\ 3 \\ 3 \end{pmatrix} & \begin{pmatrix} 2 \\ 0 \\ 5 \end{pmatrix} & \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} & \begin{pmatrix} 2 \\ 1 \\ 4 \end{pmatrix} & \begin{pmatrix} 1 \\ 3 \\ 6 \end{pmatrix} & \begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix} & \begin{pmatrix} 1 \\ 4 \\ 5 \end{pmatrix} & \begin{pmatrix} 2 \\ 3 \\ 2 \end{pmatrix} & \begin{pmatrix} 2 \\ 4 \\ 1 \end{pmatrix} & \begin{pmatrix} 1 \\ 1 \\ 3 \end{pmatrix} & \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} & \begin{pmatrix} 2 \\ 1 \\ 6 \end{pmatrix} & \begin{pmatrix} 1 \\ 3 \\ 1 \end{pmatrix} & \begin{pmatrix} 2 \\ 2 \\ 5 \end{pmatrix} \\
 & & & \wedge & & \wedge & & & \wedge & & & \wedge & & \wedge
\end{array}$$

Les décomposants de Goldbach de 100 ont toute leur colonne colorée et sont indiqués par le signe $\wedge$ en bas de la colonne, exprimant que chacun de leur reste est différent des restes de 100.
Remarque : 3 qui est un décomposant de Goldbach de 100 n'est pas trouvé par cette méthode car tout reste nul est systématiquement éliminé comme possibilité.

Procédons de la même manière pour trouver les décomposants de Goldbach de 98 :

$$98 \begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix}$$

Un décomposant de Goldbach de 98 est donc de la forme :

$$\begin{pmatrix} 1 \\ 1 \vee 2 \vee 4 \\ 1 \vee 2 \vee 3 \vee 4 \vee 5 \vee 6 \end{pmatrix}$$

$$\begin{array}{cccccccccccccc}
3 & 5 & 7 & 11 & 13 & 17 & 19 & 23 & 29 & 31 & 37 & 41 & 43 & 47 \\
\begin{pmatrix} 0 \\ 3 \\ 3 \end{pmatrix} & \begin{pmatrix} 2 \\ 0 \\ 5 \end{pmatrix} & \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} & \begin{pmatrix} 2 \\ 1 \\ 4 \end{pmatrix} & \begin{pmatrix} 1 \\ 3 \\ 6 \end{pmatrix} & \begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix} & \begin{pmatrix} 1 \\ 4 \\ 5 \end{pmatrix} & \begin{pmatrix} 2 \\ 3 \\ 2 \end{pmatrix} & \begin{pmatrix} 2 \\ 4 \\ 1 \end{pmatrix} & \begin{pmatrix} 1 \\ 1 \\ 3 \end{pmatrix} & \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} & \begin{pmatrix} 2 \\ 1 \\ 6 \end{pmatrix} & \begin{pmatrix} 1 \\ 3 \\ 1 \end{pmatrix} & \begin{pmatrix} 2 \\ 2 \\ 5 \end{pmatrix} \\
 & & & & & & \wedge & & & \wedge & \wedge & & &
\end{array}$$

1. initialement PF pour Parties Finies de $\mathbb{N}$.

Tables des dg des nombres de 12 à 104 (Denise Vella-Chemla, 16.8.16)

$n = 12 = 2^2.3 \quad nbdg = 1$

9	7
3	5

$n = 14 = 2.7 \quad nbdg = 2$

11	9	7
3	5	7

$n = 16 = 2^4 \quad nbdg = 2$

13	11	9
3	5	7

$n = 18 = 2.3^2 \quad nbdg = 2$

15	13	11	9
3	5	7	9

$n = 20 = 2^2.5 \quad nbdg = 2$

17	15	13	11
3	5	7	9

$n = 22 = 2.11 \quad nbdg = 3$

19	17	15	13	11
3	5	7	9	11

$n = 24 = 2^3.3 \quad nbdg = 3$

21	19	17	15	13
3	5	7	9	11

$n = 26 = 2.13 \quad nbdg = 3$

23	21	19	17	15	13
3	5	7	9	11	13

$n = 28 = 2^2.7 \quad nbdg = 2$

25	23	21	19	17	15
3	5	7	9	11	13

$n = 30 = 2.3.5 \quad nbdg = 3$

27	25	23	21	19	17	15
3	5	7	9	11	13	15

$n = 32 = 2^5 \quad nbdg = 2$

29	27	25	23	21	19	17
3	5	7	9	11	13	15

$n = 34 = 2.17 \quad nbdg = 4$

31	29	27	25	23	21	19	17
3	5	7	9	11	13	15	17

$n = 36 = 2^2.3^2 \quad nbdg = 4$

33	31	29	27	25	23	21	19
3	5	7	9	11	13	15	17

$n = 38 = 2.19 \quad nbdg = 2$

35	33	31	29	27	25	23	21	19
3	5	7	9	11	13	15	17	19

$n = 40 = 2^3.5 \quad nbdg = 3$

37	35	33	31	29	27	25	23	21
3	5	7	9	11	13	15	17	19

$n = 42 = 2.3.7 \quad nbdg = 4$

39	37	35	33	31	29	27	25	23	21
3	5	7	9	11	13	15	17	19	21

$n = 44 = 2^2.11 \quad nbdg = 3$

41	39	37	35	33	31	29	27	25	23
3	5	7	9	11	13	15	17	19	21

$n = 46 = 2.23 \quad nbdg = 4$

43	41	39	37	35	33	31	29	27	25	23
3	5	7	9	11	13	15	17	19	21	23

$n = 48 = 2^4.3 \quad nbdg = 5$

45	43	41	39	37	35	33	31	29	27	25
3	5	7	9	11	13	15	17	19	21	23

$n = 50 = 2.5^2 \quad nbdg = 4$

47	45	43	41	39	37	35	33	31	29	27	25
3	5	7	9	11	13	15	17	19	21	23	25

$n = 52 = 2^2.13 \quad nbdg = 3$

49	47	45	43	41	39	37	35	33	31	29	27
3	5	7	9	11	13	15	17	19	21	23	25

$n = 54 = 2.3^3 \quad nbdg = 5$

51	49	47	45	43	41	39	37	35	33	31	29	27
3	5	7	9	11	13	15	17	19	21	23	25	27

$n = 56 = 2^3.7 \quad nbdg = 3$

53	51	49	47	45	43	41	39	37	35	33	31	29
3	5	7	9	11	13	15	17	19	21	23	25	27

$n = 58 = 2.29 \quad nbdg = 4$

55	53	51	49	47	45	43	41	39	37	35	33	31	29
3	5	7	9	11	13	15	17	19	21	23	25	27	29

$n = 60 = 2^2.3.5 \quad nbdg = 6$

57	55	53	51	49	47	45	43	41	39	37	35	33	31
3	5	7	9	11	13	15	17	19	21	23	25	27	29

$n = 62 = 2.31 \quad nbdg = 3$

59	57	55	53	51	49	47	45	43	41	39	37	35	33	31
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31

$n = 64 = 2^6 \quad nbdg = 5$

61	59	57	55	53	51	49	47	45	43	41	39	37	35	33
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31

$n = 66 = 2.3.11 \quad nbdg = 6$

63	61	59	57	55	53	51	49	47	45	43	41	39	37	35	33
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33

$n = 68 = 2^2.17 \quad nbdg = 2$

65	63	61	59	57	55	53	51	49	47	45	43	41	39	37	35
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33

$n = 70 = 2.5.7 \quad nbdg = 5$

67	65	63	61	59	57	55	53	51	49	47	45	43	41	39	37	35
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35

$n = 72 = 2^3.3^2 \quad nbdg = 6$

69	67	65	63	61	59	57	55	53	51	49	47	45	43	41	39	37
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35

$n = 74 = 2.37 \quad nbdg = 5$

71	69	67	65	63	61	59	57	55	53	51	49	47	45	43	41	39	37
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37

$n = 76 = 2^2.19 \quad nbdg = 5$

73	71	69	67	65	63	61	59	57	55	53	51	49	47	45	43	41	39
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37

$n = 78 = 2.3.13 \quad nbdg = 7$

75	73	71	69	67	65	63	61	59	57	55	53	51	49	47	45	43	41	39
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39

$n = 80 = 2^4.5 \quad nbdg = 4$

77	75	73	71	69	67	65	63	61	59	57	55	53	51	49	47	45	43	41
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39

$n = 82 = 2.41 \quad nbdg = 5$

79	77	75	73	71	69	67	65	63	61	59	57	55	53	51	49	47	45	43	41
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41

$n = 84 = 2^2.3.7 \quad nbdg = 8$

81	79	77	75	73	71	69	67	65	63	61	59	57	55	53	51	49	47	45	43
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41

$n = 86 = 2.43 \quad nbdg = 5$

83	81	79	77	75	73	71	69	67	65	63	61	59	57	55	53	51	49	47	45	43
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43

$n = 88 = 2^3.11 \quad nbdg = 4$

85	83	81	79	77	75	73	71	69	67	65	63	61	59	57	55	53	51	49	47	45
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43

$n = 90 = 2.3^2.5 \quad nbdg = 9$

87	85	83	81	79	77	75	73	71	69	67	65	63	61	59	57	55	53	51	49	47	45
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45

$n = 92 = 2^2.23 \quad nbdg = 4$

89	87	85	83	81	79	77	75	73	71	69	67	65	63	61	59	57	55	53	51	49	47
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45

$n = 94 = 2.47 \quad nbdg = 5$

91	89	87	85	83	81	79	77	75	73	71	69	67	65	63	61	59	57	55	53	51	49	47
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47

$n = 96 = 2^5.3 \quad nbdg = 7$

93	91	89	87	85	83	81	79	77	75	73	71	69	67	65	63	61	59	57	55	53	51	49
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47

$n = 98 = 2.7^2 \quad nbdg = 3$

95	93	91	89	87	85	83	81	79	77	75	73	71	69	67	65	63	61	59	57	55	53	51	49
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49

$n = 100 = 2^2.5^2 \quad nbdg = 6$

97	95	93	91	89	87	85	83	81	79	77	75	73	71	69	67	65	63	61	59	57	55	53	51
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49

$n = 102 = 2.3.17 \quad nbdg = 8$

99	97	95	93	91	89	87	85	83	81	79	77	75	73	71	69	67	65	63	61	59	57	55	53	51
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51

$n = 104 = 2^3.13 \quad nbdg = 5$

101	99	97	95	93	91	89	87	85	83	81	79	77	75	73	71	69	67	65	63	61	59	57	55	53
3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51

Snurpf, exemple (Denise Vella-Chemla, 9.8.18)

On a appelé SNURPF notre Système de NUmération par les Restes modulaires dans les corps premiers [1]. Chaque nombre est codé par le n-uplet des restes de ses divisions par l'ensemble des nombres premiers inférieurs à sa racine.

On rappelle qu'un nombre premier p est un décomposant de Goldbach d'un nombre pair n s'il est inférieur à $n/2$ et ne partage avec n aucun de ses restes de divisions.

Voici un exemple, selon les nombres premiers 3, 5 et 7 (c'est la base de nombres premiers inférieurs à $\sqrt{100}$ dans laquelle on se place). On cherche les décomposants de Goldbach de 100.

$$100\begin{pmatrix}1\\0\\2\end{pmatrix}$$

Un décomposant de Goldbach de 100 trouvable par la méthode proposée ici est de la forme :

$$\begin{pmatrix}2\\1\vee 2\vee 3\vee 4\\1\vee 3\vee 4\vee 5\vee 6\end{pmatrix}$$

Ecrivons les nombres premiers inférieurs à 50 et leurs restes, colorons en bleu les restes admissibles :

$$\begin{array}{cccccccccccccc}
3 & 5 & 7 & 11 & 13 & 17 & 19 & 23 & 29 & 31 & 37 & 41 & 43 & 47\\
\begin{pmatrix}0\\\color{cyan}3\\\color{cyan}3\end{pmatrix} &
\begin{pmatrix}\color{cyan}2\\0\\\color{cyan}5\end{pmatrix} &
\begin{pmatrix}1\\\color{cyan}2\\0\end{pmatrix} &
\begin{pmatrix}\color{cyan}2\\\color{cyan}1\\\color{cyan}4\end{pmatrix} &
\begin{pmatrix}1\\\color{cyan}3\\\color{cyan}6\end{pmatrix} &
\begin{pmatrix}\color{cyan}2\\\color{cyan}2\\\color{cyan}3\end{pmatrix} &
\begin{pmatrix}1\\\color{cyan}4\\\color{cyan}5\end{pmatrix} &
\begin{pmatrix}\color{cyan}2\\\color{cyan}3\\2\end{pmatrix} &
\begin{pmatrix}\color{cyan}2\\\color{cyan}4\\\color{cyan}1\end{pmatrix} &
\begin{pmatrix}1\\\color{cyan}1\\\color{cyan}3\end{pmatrix} &
\begin{pmatrix}1\\\color{cyan}2\\2\end{pmatrix} &
\begin{pmatrix}\color{cyan}2\\\color{cyan}1\\\color{cyan}6\end{pmatrix} &
\begin{pmatrix}1\\\color{cyan}3\\\color{cyan}1\end{pmatrix} &
\begin{pmatrix}\color{cyan}2\\\color{cyan}2\\\color{cyan}5\end{pmatrix}\\
 & & & \wedge & & \wedge & & & \wedge & & & \wedge & & \wedge
\end{array}$$

Les décomposants de Goldbach de 100 ont toute leur colonne colorée et sont indiqués par le signe $\wedge$ en bas de la colonne, exprimant que chacun de leur reste est différent des restes de 100.
Remarque : 3 qui est un décomposant de Goldbach de 100 n'est pas trouvé par cette méthode car tout reste nul est systématiquement éliminé comme possibilité.

Procédons de la même manière pour trouver les décomposants de Goldbach de 98 :

$$98\begin{pmatrix}2\\3\\0\end{pmatrix}$$

Un décomposant de Goldbach de 98 est donc de la forme :

$$\begin{pmatrix}1\\1\vee 2\vee 4\\1\vee 2\vee 3\vee 4\vee 5\vee 6\end{pmatrix}$$

$$\begin{array}{cccccccccccccc}
3 & 5 & 7 & 11 & 13 & 17 & 19 & 23 & 29 & 31 & 37 & 41 & 43 & 47\\
\begin{pmatrix}0\\3\\\color{cyan}3\end{pmatrix} &
\begin{pmatrix}2\\0\\\color{cyan}5\end{pmatrix} &
\begin{pmatrix}\color{cyan}1\\\color{cyan}2\\0\end{pmatrix} &
\begin{pmatrix}2\\\color{cyan}1\\\color{cyan}4\end{pmatrix} &
\begin{pmatrix}\color{cyan}1\\3\\\color{cyan}6\end{pmatrix} &
\begin{pmatrix}2\\\color{cyan}2\\\color{cyan}3\end{pmatrix} &
\begin{pmatrix}\color{cyan}1\\\color{cyan}4\\\color{cyan}5\end{pmatrix} &
\begin{pmatrix}2\\3\\\color{cyan}2\end{pmatrix} &
\begin{pmatrix}2\\\color{cyan}4\\\color{cyan}1\end{pmatrix} &
\begin{pmatrix}\color{cyan}1\\\color{cyan}1\\\color{cyan}3\end{pmatrix} &
\begin{pmatrix}\color{cyan}1\\\color{cyan}2\\\color{cyan}2\end{pmatrix} &
\begin{pmatrix}2\\\color{cyan}1\\\color{cyan}6\end{pmatrix} &
\begin{pmatrix}\color{cyan}1\\3\\\color{cyan}1\end{pmatrix} &
\begin{pmatrix}2\\\color{cyan}2\\\color{cyan}5\end{pmatrix}\\
 & & & & & & \wedge & & & \wedge & \wedge & & &
\end{array}$$

1. initialement PF pour Parties Finies de $\mathbb{N}$.

L'été, revenir à des calculs simples (Denise Vella-Chemla, 12.8.18)

1) Plusieurs fonctions en une, à la recherche d'une fonction simple qui permettrait de caractériser les nombres premiers

En calculant la somme modulaire (selon n) des entiers inférieurs à $n/2$, on réalise que le calcul modulaire transforme une fonction quadratique en plusieurs fonctions affines.

On calcule par programme dans $\mathbb{Z}/n\mathbb{Z}$ la somme des $n/2$ premiers nombres $h(n) = \sum_{x=1}^{n/2} x \ (mod\ n)$.

n	$h(n)$	n	$h(n)$	n	$h(n)$	n	$h(n)$	n	$h(n)$
$s(1)$	0	$s(21)$	13	$s(41)$	5	$s(61)$	38	$s(81)$	10
$s(2)$	1	$s(22)$	0	$s(42)$	21	$s(62)$	0	$s(82)$	41
$s(3)$	1	$s(23)$	20	$s(43)$	16	$s(63)$	55	$s(83)$	31
$s(4)$	3	$s(24)$	6	$s(44)$	33	$s(64)$	16	$s(84)$	63
$s(5)$	3	$s(25)$	3	$s(45)$	28	$s(65)$	8	$s(85)$	53
$s(6)$	0	$s(26)$	13	$s(46)$	0	$s(66)$	33	$s(86)$	0
$s(7)$	6	$s(27)$	10	$s(47)$	41	$s(67)$	25	$s(87)$	76
$s(8)$	2	$s(28)$	21	$s(48)$	12	$s(68)$	51	$s(88)$	22
$s(9)$	1	$s(29)$	18	$s(49)$	6	$s(69)$	43	$s(89)$	11
$s(10)$	5	$s(30)$	0	$s(50)$	25	$s(70)$	0	$s(90)$	45
$s(11)$	4	$s(31)$	27	$s(51)$	19	$s(71)$	62	$s(91)$	34
$s(12)$	9	$s(32)$	8	$s(52)$	39	$s(72)$	18	$s(92)$	69
$s(13)$	8	$s(33)$	4	$s(53)$	33	$s(73)$	9	$s(93)$	58
$s(14)$	0	$s(34)$	17	$s(54)$	0	$s(74)$	37	$s(94)$	0
$s(15)$	13	$s(35)$	13	$s(55)$	48	$s(75)$	28	$s(95)$	83
$s(16)$	4	$s(36)$	27	$s(56)$	14	$s(76)$	57	$s(96)$	24
$s(17)$	2	$s(37)$	23	$s(57)$	7	$s(77)$	48	$s(97)$	12
$s(18)$	9	$s(38)$	0	$s(58)$	29	$s(78)$	0	$s(98)$	49
$s(19)$	7	$s(39)$	34	$s(59)$	22	$s(79)$	69	$s(99)$	37
$s(20)$	15	$s(40)$	10	$s(60)$	45	$s(80)$	20	$s(100)$	75

On note que $h(n)$ est égal à :
- k pour les $8k$ (soit $n/8$) ;
- k pour les $8k+1$;
- $4k+1$ pour les $8k+2$ (soit $n/2$) ;
- $3k+1$ pour les $8k+3$;
- $6k+3$ pour les $8k+4$ (soit $3n/4$) ;
- $5k+3$ pour les $8k+5$;
- 0 pour les $8k+6$;
- et $7k+6$ pour les $8k+7$.

La fonction $h(n)$ qui vaut $\frac{1}{4}n^2 + \frac{1}{2}n$ quand on la calcule sur l'ensemble des nombres entiers $\mathbb{N}$ s'est transformée dans $\mathbb{Z}/n\mathbb{Z}$ en une sorte d'agrégat de 8 fonctions affines différentes. On peut effectuer un traitement similiaire avec la somme des nombres compris entre $n/2$ et n [*]. Enfin, si on calcule la somme des nombres compris entre 1 et $n-1$, la fonction résultante est :

- Id pour les $8k, 8k+2$ et $8k+4$;
- $\frac{n-1}{2}$ pour les $8k+1, 8k+3$ (en fait, $4k$ pour les $8k+1$ et $4k+1$ pour les $8k+3$) ;
- $n + \frac{n-1}{2}$ pour les $8k+5, 8k+7$ (en fait, $12k+7$ pour les $8k+5$ et $12k+10$ pour les $8k+7$) ;
- et 0 pour les $8k+6$.

Les doubles de nombres premiers sont soit de la forme $8k+6$ (doubles de nombres premiers de la forme

∗. Les $8k$ ont pour image $6k$, les $8k+1$ ont pour image $3k$, les $8k+2$ ont pour image $4k+1$, les $8k+3$ ont pour image k, les $8k+4$ ont pour image $2k+1$, les $8k+5$ ont pour image $7k+4$, les $8k+6$ ont pour image 0 et les $8k+7$ ont pour image $5k+4$.

$4k+3$) soit de la forme $8k+2$ (doubles de nombres premiers de la forme $4k+1$).

Les résultats ci-dessus ne permettent pas de différencier les nombres premiers (resp. ou les doubles de nombres premiers) des nombres impairs composés (resp. des doubles de nombres impairs composés).

Pour voir si un autre élément permettrait de caractériser les nombres premiers, on calcule par programme dans $\mathbb{Z}/n\mathbb{Z}$ pour n pair le produit des $n/2$ nombres compris entre 1 et $n/2$, $k(n) = \prod_{x=1}^{n/2} x \ (mod\ n)$.

$k(n)$ est nul pour les nombres pairs. Voyons dans le tableau ci-dessous sa valeur pour les nombres impairs.

n	$k(n)$	n	$k(n)$	n	$k(n)$	n	$k(n)$	n	$k(n)$
$k(1)$	1	$k(21)$	0	$k(41)$	9	$k(61)$	11	$k(81)$	0
$k(3)$	1	$k(23)$	1	$k(43)$	42	$k(63)$	0	$k(83)$	1
$k(5)$	2	$k(25)$	0	$k(45)$	0	$k(65)$	0	$k(85)$	0
$k(7)$	6	$k(27)$	0	$k(47)$	46	$k(67)$	66	$k(87)$	0
$k(9)$	6	$k(29)$	12	$k(49)$	0	$k(69)$	0	$k(89)$	34
$k(11)$	10	$k(31)$	1	$k(51)$	0	$k(71)$	1	$k(91)$	0
$k(13)$	5	$k(33)$	0	$k(53)$	23	$k(73)$	27	$k(93)$	0
$k(15)$	0	$k(35)$	0	$k(55)$	0	$k(75)$	0	$k(95)$	0
$k(17)$	13	$k(37)$	31	$k(57)$	0	$k(77)$	0	$k(97)$	22
$k(19)$	18	$k(39)$	0	$k(59)$	1	$k(79)$	78	$k(99)$	0

Cette “moitié de factorielle” † de n est non-nulle pour les nombres premiers (sauf les nombres 1 et 9 ‡) tandis qu’elle est nulle pour les nombres composés.

Elle est égale à 1 ou $p-1$ pour les premiers $4k+3$ et à un nombre différent de 1 ou $p-1$ pour les premiers $4k+1$.

2) Nombre de puissances pures

On a trouvé à Noël passé une caractérisation des nombres premiers et de leurs puissances qu’on résume dans le tableau ci-dessous en terme de nombre de solutions de l’équation $x^{10} \equiv 1 \ (mod\ n)$ § :

	premiers ou puissances de premiers	*composés*
$dernier\ chiffre\ 1$	10 *solutions*	*autre chose que* 10
$dernier\ chiffre\ 3,5,7$	2 *solutions*	*autre chose que* 2

Comme la possibilité ci-dessus ne permet pas de distinguer les nombres premiers de leurs puissances pures, on voulait avoir à l’esprit le nombre de telles puissances pures de premiers jusqu’à un nombre donné (si elles étaient très peu nombreuses par rapport au nombre de premiers, le nombre de solutions ci-dessus pourrait servir à caractériser les premiers et peut-être à les compter, avec une faible erreur ¶).

Rappelons comment calculer le nombre $PP(n)$ de puissances pures de nombres premiers inférieures à n

†. La présente note fait suite à deux notes écrites à l’été 2017 http://denise.vella.chemla.free.fr/valpadiquefacto.pdf et http://denise.vella.chemla.free.fr/facto.pdf.

‡. car il n’y a pas au moins 2 multiples de 3 inférieurs à la moitié de 9.

§. A ce moment-là, on avait d’abord découvert par programme que seuls les nombres premiers $n = p$ et leurs puissances $n = p^k$ sont tels que $x^2 \equiv 1 \ (mod\ n)$ a exactement deux racines. Pour les nombres composés, cette même équation modulaire a 2^k solutions avec k le nombre de nombres premiers différents de la factorisation de n. On avait alors également vérifié par programme (c’est un résultat qui doit être déduisible des Recherches arithmétiques) que pour les $p = 4k+3$ et leurs puissances, l’équation $x^4 \equiv 1 \ (mod\ n)$ a toujours 2 solutions ; concernant les $p = 4k+1$ et leurs puissances, la même équation modulaire a toujours 4 solutions mais c’est également le cas pour les nombres composés qui ont un nombre pair de premiers de la forme $4k+3$ dans leur factorisation ; c’est ce défaut de caractérisation des premiers qui nous a fait envisager l’équation $x^5 \equiv 1 \ (mod\ n)$, puis $x^{10} \equiv 1 \ (mod\ n)$. Se reporter à http://denise.vella.chemla.free.fr/racinesdixiemesde1.pdf

¶. tout ça est bien connu, mais j’essaie d’imaginer quels ont pu être les cheminements des pensées.

(i.e. qui ne sont pas des nombres premiers). On a :

$$\begin{aligned} PP(n) &= \#\{p^k \ / \ p^k \leq n, p \leq \sqrt{n}, 1 < k < log_p n\} \\ &= \sum_{k=2}^{log_p n} \Pi\,(\sqrt[k]{n}) \end{aligned}$$

Note : On note aussi $\sqrt[k]{n}$ par $n^{\frac{1}{k}}$. $\Pi(n)$ désigne le nombre de nombres premiers inférieurs ou égaux à n.

Il y a "très peu" de puissances pures parmi les nombres (voici les 10 puissances pures inférieures à 100 : 49, 25, 9, 27, 81, 4, 8, 16, 32 et 64). Ci-dessous un tableau qui fournit quelques-uns de leur nombre (en troisième colonne, on note le pourcentage d'erreurs que l'on ferait si l'on confondait les puissances pures de nombres premiers avec des nombres premiers, sous prétexte qu'elles partageraient une caractéristique avec eux par exemple, comme le nombre de solutions de l'équation modulaire $x^{10} \equiv 1$) :

n	$PP(n)$	% *d'erreur*
10^2	10	10 *pour* 100
10^3	25	2 *pour* 100
10^4	51	5 *pour* 1000
10^5	108	1 *pour* 1000
10^8	1404	1 *pour* 100000
10^{12}	80070	8 *pour* 10^8

3) Somme des exposants des factorisations

Dans ce paragraphe, il s'agit de présenter une fonction qui rappelle le logarithme. On fournit dans le tableau ci-dessous pour chaque entier n sa factorisation $f(n) = \prod p_i^{\alpha_i}$ et la somme des exposants des différentes puissances des nombres premiers contenues dans sa factorisation $s(n) = \sum \alpha_i$.

n	$f(n)$	$s(n)$	n	$f(n)$	$s(n)$	n	$f(n)$	$s(n)$	n	$f(n)$	$s(n)$	n	$f(n)$	$s(n)$
$s(1)$	1	1	$s(21)$	3.7	2	$s(41)$	41	1	$s(61)$	61	1	$s(81)$	3^4	4
$s(2)$	2	1	$s(22)$	2.11	2	$s(42)$	2.3.7	3	$s(62)$	2.31	2	$s(82)$	2.41	2
$s(3)$	3	1	$s(23)$	23	1	$s(43)$	43	1	$s(63)$	$3^2.7$	3	$s(83)$	83	1
$s(4)$	2^2	2	$s(24)$	$2^3.3$	4	$s(44)$	$2^2.11$	3	$s(64)$	2^6	6	$s(84)$	$2^2.3.7$	4
$s(5)$	5	1	$s(25)$	5^2	2	$s(45)$	$3^2.5$	3	$s(65)$	5.13	2	$s(85)$	5.17	2
$s(6)$	2.3	2	$s(26)$	2.13	2	$s(46)$	2.23	2	$s(66)$	2.3.11	3	$s(86)$	2.43	2
$s(7)$	7	1	$s(27)$	3^3	3	$s(47)$	47	1	$s(67)$	67	1	$s(87)$	3.29	2
$s(8)$	2^3	3	$s(28)$	$2^2.7$	3	$s(48)$	$2^4.3$	5	$s(68)$	$2^2.17$	3	$s(88)$	$2^3.11$	4
$s(9)$	3^2	2	$s(29)$	29	1	$s(49)$	7^2	2	$s(69)$	3.23	2	$s(89)$	89	1
$s(10)$	2.5	2	$s(30)$	2.3.5	3	$s(50)$	2.5^2	3	$s(70)$	2.5.7	3	$s(90)$	$2.3^2.5$	4
$s(11)$	11	1	$s(31)$	31	1	$s(51)$	3.17	2	$s(71)$	71	1	$s(91)$	7.13	2
$s(12)$	$2^2.3$	3	$s(32)$	2^5	5	$s(52)$	$2^2.13$	3	$s(72)$	$2^3.3^2$	5	$s(92)$	$2^2.23$	3
$s(13)$	13	1	$s(33)$	3.11	2	$s(53)$	53	1	$s(73)$	73	1	$s(93)$	3.31	2
$s(14)$	2.7	2	$s(34)$	2.17	2	$s(54)$	2.3^3	4	$s(74)$	2.37	2	$s(94)$	2.47	2
$s(15)$	3.5	2	$s(35)$	5.7	2	$s(55)$	5.11	2	$s(75)$	3.5^2	3	$s(95)$	5.19	2
$s(16)$	2^4	4	$s(36)$	$2^2.3^2$	4	$s(56)$	$2^3.7$	4	$s(76)$	$2^2.19$	3	$s(96)$	$2^5.3$	6
$s(17)$	17	1	$s(37)$	37	1	$s(57)$	3.19	2	$s(77)$	7.11	2	$s(97)$	97	1
$s(18)$	2.3^2	3	$s(38)$	2.19	2	$s(58)$	2.29	2	$s(78)$	2.3.13	3	$s(98)$	2.7^2	3
$s(19)$	19	1	$s(39)$	3.13	2	$s(59)$	59	1	$s(79)$	79	1	$s(99)$	$3^2.11$	3
$s(20)$	$2^2.5$	3	$s(40)$	$2^3.5$	4	$s(60)$	$2^2.3.5$	4	$s(80)$	$2^4.5$	5	$s(100)$	$2^2.5^2$	4

On $f(ab) = f(a) + f(b)$. Un texte qui en explique très pédagogiquement la raison, en présentant la factorisation d'un point de vue ensembliste, peut être trouvé ici :

$$http://denise.vella.chemla.free.fr/Laisant1.pdf.$$

Pour résumer, en utilisant le calcul modulaire dans les corps premiers, grâce à la cyclicité que celui-ci apporte, on sait bien tout compter mais les demi-factorielles présentées ici n'apportent rien que n'apportait déjà le théorème de Wilson.

Memo pour les puissances $10^{èmes}$ (Denise Vella-Chemla, 15.8.18)

On rappelle le nombre de solutions de $x^{10} \equiv 1 \ (mod\ n)$:

	premiers ou puissances de premiers	*composés*
dernier chiffre 1	10 *solutions*	*autre chose que* 10
dernier chiffre 3, 5, 7	2 *solutions*	*autre chose que* 2

On a quelque soit n :

$$x^{2k} \equiv (n-x)^{2k} \ (mod\ n)$$

et

$$x^{2k+1} \equiv n - x^{2k+1} \ (mod\ n).$$

Modulo 11 (premier) :

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

Modulo 21 (composé impair) :

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

Modulo 13 (premier) :

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

Modulo 33 (composé impair) :

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

Modulo 7 (premier) :

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

Modulo 27 (puissance de premier) :

	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
1	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
2	1	4	9	16	25	9	22	10	0	19	13	9	7	7	9	13	19	0	10	22	9	25	16	9	4	1
3	1	8	0	10	17	0	19	26	0	1	8	0	10	17	0	19	26	0	1	8	0	10	17	0	19	26
4	1	16	0	13	4	0	25	19	0	10	7	0	22	22	0	7	10	0	19	25	0	4	13	0	16	1
5	1	5	0	25	20	0	13	17	0	19	23	0	16	11	0	4	8	0	10	14	0	7	2	0	22	26
6	1	10	0	19	19	0	10	1	0	1	10	0	19	19	0	10	1	0	1	10	0	19	19	0	10	1
7	1	20	0	22	14	0	16	8	0	10	2	0	4	23	0	25	17	0	19	11	0	13	5	0	7	26
8	1	13	0	7	16	0	4	10	0	19	22	0	25	25	0	22	19	0	10	4	0	16	7	0	13	1
9	1	26	0	1	26	0	1	26	0	1	26	0	1	26	0	1	26	0	1	26	0	1	26	0	1	26
10	1	25	0	4	22	0	7	19	0	10	16	0	13	13	0	16	10	0	19	7	0	22	4	0	25	1
	*																									*

Modulo 57 (composé impair) :

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	...
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	...
1	4	9	16	25	36	49	7	24	43	7	30	55	25	54	28	4	39	19	1	42	28	16	6	55	49	45	43	43	...
1	8	27	7	11	45	1	56	45	31	20	18	31	8	12	49	11	18	19	20	27	46	26	30	7	20	18	7	50	...
1	16	24	28	55	42	7	49	6	25	49	45	4	55	9	43	16	39	19	1	54	43	28	36	4	7	30	25	25	...
1	32	15	55	47	24	49	50	54	22	26	27	52	29	21	4	44	18	19	20	51	34	17	9	43	11	12	16	41	...
1	7	45	49	7	30	1	1	30	49	1	39	49	7	30	7	7	39	19	1	45	7	49	45	49	1	39	49	49	...
1	14	21	25	35	9	7	8	42	34	11	12	10	41	51	55	5	18	19	20	33	40	44	54	28	26	27	4	53	...
1	28	6	43	4	54	49	7	36	55	7	30	16	4	24	25	28	39	19	1	9	25	43	42	16	49	45	55	55	...
1	56	18	1	20	39	1	56	39	37	20	18	37	56	18	1	20	18	19	20	18	37	20	39	1	20	18	1	56	...
1	55	54	4	43	6	7	49	9	28	49	45	25	43	42	16	55	39	19	1	36	16	4	24	25	7	30	28	28	...
*																			*										...

Modulo 9 (puissance de premier) :

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	1	4	0	7	7	0	4	1
3	1	8	0	1	8	0	1	8
4	1	7	0	4	4	0	7	1
5	1	5	0	7	2	0	4	8
6	1	1	0	1	1	0	1	1
7	1	2	0	4	5	0	7	8
8	1	4	0	7	7	0	4	1
9	1	8	0	1	8	0	1	8
10	1	7	0	4	4	0	7	1
	*							*

Modulo 29 (premier) :

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

Modulo 39 (composé impair) :

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

Modulo 6 (composé pair) :

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

Modulo 8 (composé pair) :

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	1	4	1	0	1	4	1
3	1	0	3	0	5	0	7
4	1	0	1	0	1	0	1
5	1	0	3	0	5	0	7
6	1	0	1	0	1	0	1
7	1	0	3	0	5	0	7
8	1	0	1	0	1	0	1
9	1	0	3	0	5	0	7
10	1	0	1	0	1	0	1
	*		*		*		*

Memo pour les puissances $10^{\text{èmes}}$ *(Denise Vella-Chemla, 15.8.18)*

On rappelle le nombre de solutions de $x^{10} \equiv 1 \ (mod\, n)$:

	premiers *ou puissances de premiers*	*composés*
$dernier\ chiffre\ 1$	10 *solutions*	*autre chose que* 10
$dernier\ chiffre\ 3, 5, 7$	2 *solutions*	*autre chose que* 2

On a quelque soit n :

$$x^{2k} \equiv (n-x)^{2k} \ (mod\, n)$$

et

$$x^{2k+1} \equiv n - x^{2k+1} \ (mod\, n).$$

Modulo 11 (premier) :

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

Modulo 21 (composé impair) :

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

Modulo 13 (premier) :

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

Modulo 33 (composé impair) :

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

Modulo 7 (premier) :

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

Modulo 27 (puissance de premier) :

	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
1	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
2	1	4	9	16	25	9	22	10	0	19	13	9	7	7	9	13	19	0	10	22	9	25	16	9	4	1
3	1	8	0	10	17	0	19	26	0	1	8	0	10	17	0	19	26	0	1	8	0	10	17	0	19	26
4	1	16	0	13	4	0	25	19	0	10	7	0	22	22	0	7	10	0	19	25	0	4	13	0	16	1
5	1	5	0	25	20	0	13	17	0	19	23	0	16	11	0	4	8	0	10	14	0	7	2	0	22	26
6	1	10	0	19	19	0	10	1	0	1	10	0	19	19	0	10	1	0	1	10	0	19	19	0	10	1
7	1	20	0	22	14	0	16	8	0	10	2	0	4	23	0	25	17	0	19	11	0	13	5	0	7	26
8	1	13	0	7	16	0	4	10	0	19	22	0	25	25	0	22	19	0	10	4	0	16	7	0	13	1
9	1	26	0	1	26	0	1	26	0	1	26	0	1	26	0	1	26	0	1	26	0	1	26	0	1	26
10	1	25	0	4	22	0	7	19	0	10	16	0	13	13	0	16	10	0	19	7	0	22	4	0	25	1
	*																									*

Modulo 57 (composé impair) :

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	...
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	...
1	4	9	16	25	36	49	7	24	43	7	30	55	25	54	28	4	39	19	1	42	28	16	6	55	49	45	43	43	...
1	8	27	7	11	45	1	56	45	31	20	18	31	8	12	49	11	18	19	20	27	46	26	30	7	20	18	7	50	...
1	16	24	28	55	42	7	49	6	25	49	45	4	55	9	43	16	39	19	1	54	43	28	36	4	7	30	25	25	...
1	32	15	55	47	24	49	50	54	22	26	27	52	29	21	4	44	18	19	20	51	34	17	9	43	11	12	16	41	...
1	7	45	49	7	30	1	1	30	49	1	39	49	7	30	7	7	39	19	1	45	7	49	45	49	1	39	49	49	...
1	14	21	25	35	9	7	8	42	34	11	12	10	41	51	55	5	18	19	20	33	40	44	54	28	26	27	4	53	...
1	28	6	43	4	54	49	7	36	55	7	30	16	4	24	25	28	39	19	1	9	25	43	42	16	49	45	55	55	...
1	56	18	1	20	39	1	56	39	37	20	18	37	56	18	1	20	18	19	20	18	37	20	39	1	20	18	1	56	...
1	55	54	4	43	6	7	49	9	28	49	45	25	43	42	16	55	39	19	1	36	16	4	24	25	7	30	28	28	...
*																			*										...

Modulo 9 (puissance de premier) :

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	1	4	0	7	7	0	4	1
3	1	8	0	1	8	0	1	8
4	1	7	0	4	4	0	7	1
5	1	5	0	7	2	0	4	8
6	1	1	0	1	1	0	1	1
7	1	2	0	4	5	0	7	8
8	1	4	0	7	7	0	4	1
9	1	8	0	1	8	0	1	8
10	1	7	0	4	4	0	7	1
	*							*

Modulo 29 (premier) :

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

Modulo 39 (composé impair) :

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

Modulo 6 (composé pair) :

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

Modulo 8 (composé pair) :

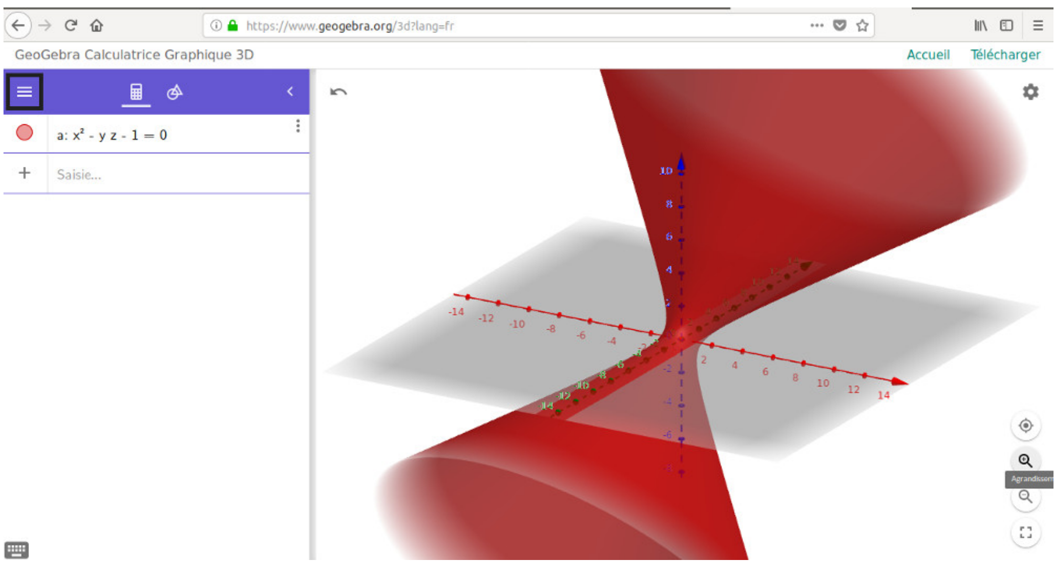
	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	1	4	1	0	1	4	1
3	1	0	3	0	5	0	7
4	1	0	1	0	1	0	1
5	1	0	3	0	5	0	7
6	1	0	1	0	1	0	1
7	1	0	3	0	5	0	7
8	1	0	1	0	1	0	1
9	1	0	3	0	5	0	7
10	1	0	1	0	1	0	1
	*		*		*		*

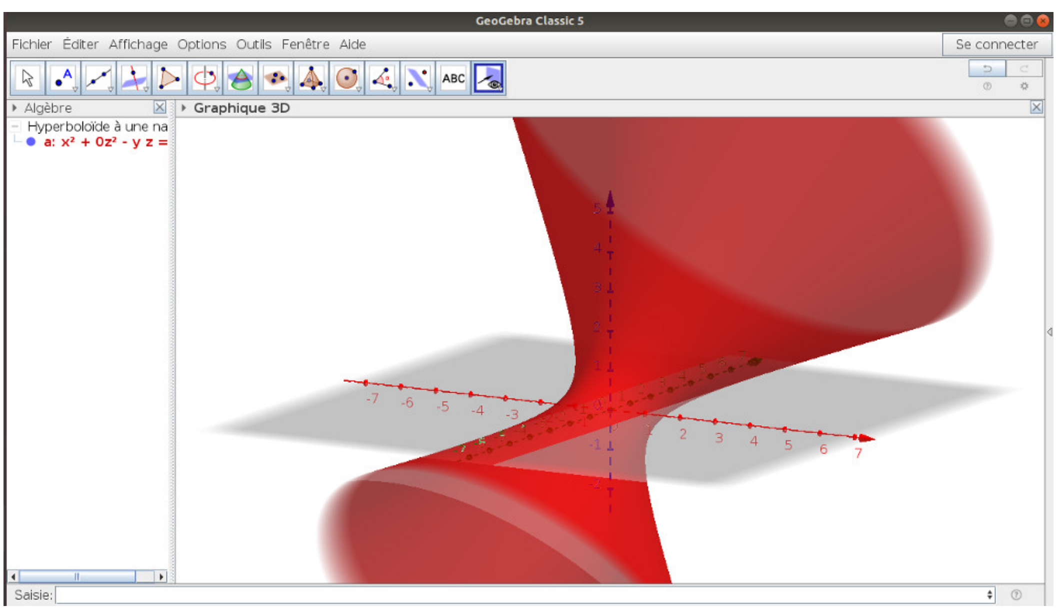
Hyperboloide à une nappe (Denise Vella-Chemla, 18.8.18)

On avait découvert par programme à la recherche initiale des points fixes et de leur nombre dans les anneaux $\mathbb{Z}/n\mathbb{Z}$, puis à la recherche des racines carrées de 1 et de leur nombre dans ces anneaux, que 1 a exactement 2 racines carrées seulement dans les corps premiers $\mathbb{Z}/p\mathbb{Z}$[*] ou dans les anneaux $\mathbb{Z}/p^k\mathbb{Z}$ avec p^k une puissance de nombre premier. Dans les anneaux $\mathbb{Z}/n\mathbb{Z}$, 1 a 2^k racines carrées avec k le nombre de nombres premiers intervenant dans la factorisation de n. On nous a fourni l'explication conceptuelle de ces faits, qui découle de l'isomorphisme d'anneaux entre $\mathbb{Z}/n\mathbb{Z}$ et le produit des anneaux $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ si $n = \prod p_i^{\alpha_i}$ (les cas $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/p^k\mathbb{Z}$ sont inclus dans le cas général).

On souhaiterait comprendre ce qui se passe si on sort de ces sortes de “rouleaux” cycliques que sont les $\mathbb{Z}/n\mathbb{Z}$. On a fait dessiner à Geogebra-3D la surface d'équation $x^2 - yz - 1 = 0$. Cette surface est un hyperboloide à une nappe (en un seul morceau), ou sorte de sablier infini, qui passe par les points $(1, 0, 0)$ et $(-1, 0, 0)$. Il faut imaginer une grille sur cette surface, grille dont les intersections sont les points à coordonnées entières.

Pour l'instant, on ne peut que fournir les visualisations en question ci-dessus.





*. Ce résultat se trouve dans l'article 62 des Recherches arithmétiques de Gauss.

Conjecture de Goldbach et chip-firing games (Denise Vella-Chemla, 19.8.18)

1) Chip-firing games 4×4

On compte dans les coefficients de matrices 4×4 les nombres d'occurrences de certaines configurations de prédicats de primalité sur les nombres. Dans des recherches précédentes, on avait représenté pour étudier la conjecture de Goldbach les nombres pairs par des mots dans un langage à 4 lettres.

Exemple : à 40 est associé le mot *accbacdac*. On associe ainsi à 40 la matrice

$$40 \quad \begin{pmatrix} 0 & 0 & 3 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

qui correspond au fait que le mot de 40 contient 3 doublons de lettres *ac*, 1 doublon *ba*, 1 doublon *cb*, 1 doublon *cc*, 1 doublon *cd* et 1 doublon *da*.

Procéder à une transformation de chip-firing-game sur une matrice consiste à la modifier de la façon suivante : le nombre d'une case (i, j) peut être diminué d'autant que sont augmentées les valeurs des cases de ses voisins directs $(i-1, j), (i+1, j), (i, j-1), (i, j+1), (i-1, j-1), (i-1, j+1), (i+1, j-1), (i+1, j+1)$.

On devrait ici parler de *nearly-chip-firing-game* car comme il s'agit de modéliser des sommes $x + y$ de deux nombres impairs égales à n (avec $3 \leq x \leq n/2$, un nombre pair qui augmente, la somme totale des coefficients de la matrice se trouve être augmentée de 1 une fois sur deux.

Observons ces transformations sur les matrices des nombres 90 à 100. On colorie les nombres qui distribuent leurs points à leurs voisins.

$$90 \quad \begin{pmatrix} \colorbox{cyan}{2} & 0 & 1 & \colorbox{cyan}{6} \\ 0 & 0 & 0 & 0 \\ 2 & 0 & 1 & \colorbox{cyan}{1} \\ \colorbox{cyan}{5} & 0 & 1 & \colorbox{cyan}{2} \end{pmatrix} \qquad 92 \quad \begin{pmatrix} 0 & \colorbox{cyan}{2} & 1 & 1 \\ 0 & 0 & 3 & \colorbox{cyan}{2} \\ \colorbox{cyan}{3} & \colorbox{cyan}{4} & 2 & 0 \\ 0 & 0 & \colorbox{cyan}{3} & 0 \end{pmatrix}$$

$$94 \quad \begin{pmatrix} 0 & 0 & \colorbox{cyan}{3} & 1 \\ 1 & \colorbox{cyan}{1} & \colorbox{cyan}{3} & 0 \\ 1 & \colorbox{cyan}{3} & \colorbox{cyan}{2} & \colorbox{cyan}{3} \\ 3 & 1 & 0 & 0 \end{pmatrix} \qquad 96 \quad \begin{pmatrix} 0 & 1 & \colorbox{cyan}{2} & \colorbox{cyan}{4} \\ \colorbox{cyan}{1} & 0 & 0 & \colorbox{cyan}{1} \\ \colorbox{cyan}{3} & 0 & 1 & \colorbox{cyan}{2} \\ \colorbox{cyan}{3} & \colorbox{cyan}{1} & \colorbox{cyan}{3} & 0 \end{pmatrix}$$

$$98 \quad \begin{pmatrix} 0 & \colorbox{cyan}{1} & 0 & \colorbox{cyan}{2} \\ 0 & \colorbox{cyan}{1} & \colorbox{cyan}{5} & 0 \\ \colorbox{cyan}{2} & \colorbox{cyan}{4} & \colorbox{cyan}{4} & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} \qquad 100 \quad \begin{pmatrix} 0 & 0 & 5 & 1 \\ 2 & 0 & 1 & 1 \\ 0 & 3 & 1 & 4 \\ 3 & 1 & 1 & 0 \end{pmatrix}$$

Puis à nouveau sur les matrices des nombres 9996, 9998, 10000.

$$9996 \quad \begin{pmatrix} \colorbox{cyan}{9} & 16 & \colorbox{cyan}{31} & \colorbox{cyan}{199} \\ \colorbox{cyan}{25} & 29 & 33 & 218 \\ 30 & 43 & 56 & \colorbox{cyan}{283} \\ \colorbox{cyan}{191} & \colorbox{cyan}{218} & 291 & \colorbox{cyan}{825} \end{pmatrix}$$

$$9998 \quad \begin{pmatrix} 0 & \colorbox{cyan}{34} & 0 & 64 \\ 0 & \colorbox{cyan}{45} & \colorbox{cyan}{127} & \colorbox{cyan}{290} \\ \colorbox{cyan}{40} & \colorbox{cyan}{181} & 86 & 262 \\ 59 & 202 & \colorbox{cyan}{355} & \colorbox{cyan}{753} \end{pmatrix}$$

$$10000 \quad \begin{pmatrix} 0 & 0 & 37 & 90 \\ 37 & 42 & 123 & 231 \\ 0 & 98 & 89 & 353 \\ 90 & 293 & 291 & 724 \end{pmatrix}$$

Démontrer la conjecture de Goldbach en utilisant une telle modélisation équivaut à démontrer qu'il n'est pas possible qu'à un nombre pair soit associée par ce procédé une matrice qui contiendrait un gnomon de 0 en haut à gauche, c'est-à-dire qui aurait la configuration suivante :

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & - & - & - \\ 0 & - & - & - \\ 0 & - & - & - \end{pmatrix}$$

2) Chip-firing games 2×2

Concernant la conjecture de Goldbach, on peut ne s'intéresser qu'aux décompositions de n un nombre pair en sommes de deux nombres impairs $p+y$ avec p premier. Cela nous permet de travailler sur des matrices 2×2 plutôt que 4×4.

On note dans une matrice 2×2 les comptages suivants :

$$\begin{pmatrix} f_{aa}(n) & f_{ab}(n) \\ f_{ba}(n) & f_{bb}(n) \end{pmatrix}$$

avec :
- $f_{aa}(n) = \#\{(p+q=n) \ \wedge \ (p \ premier) \ \wedge \ (q \ premier) \ \wedge \ (((n+2)-p) \ premier)\}$;
- $f_{ab}(n) = \#\{(p+q=n) \ \wedge \ (p \ premier) \ \wedge \ (q \ premier) \ \wedge \ (((n+2)-p) \ compos\acute{e})\}$;
- $f_{ba}(n) = \#\{(p+q=n) \ \wedge \ (p \ premier) \ \wedge \ (q \ compos\acute{e}) \ \wedge \ (((n+2)-p) \ premier)\}$;
- $f_{bb}(n) = \#\{(p+q=n) \ \wedge \ (p \ premier) \ \wedge \ (q \ compos\acute{e}) \ \wedge \ (((n+2)-p) \ compos\acute{e})\}$.

Les matrices sont fournies en annexe pour les nombres pairs compris entre 10 et 100.

Le nombre de décompositions de Goldbach de n est égal à $f_{aa}(n) + f_{ab}(n)$. Démontrer la conjecture de Goldbach revient à démontrer qu'on a toujours $f_{aa}(n) + f_{ab}(n) > 0$.

La somme des 4 éléments de chaque matrice est égal à $\pi(n/2) - 1$, elle augmente de 1 à chaque double de nombre premier.

Annexe : matrices 2×2 *associées aux nombres pairs compris entre 10 et 100*

10	$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$	12	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	14	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	16	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	18	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$
20	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	22	$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$	24	$\begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}$	26	$\begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix}$	28	$\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$
30	$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$	32	$\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$	34	$\begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}$	36	$\begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$	38	$\begin{pmatrix} 0 & 2 \\ 3 & 2 \end{pmatrix}$
40	$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$	42	$\begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$	44	$\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$	46	$\begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}$	48	$\begin{pmatrix} 2 & 3 \\ 2 & 1 \end{pmatrix}$
50	$\begin{pmatrix} 0 & 4 \\ 3 & 1 \end{pmatrix}$	52	$\begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$	54	$\begin{pmatrix} 1 & 4 \\ 2 & 1 \end{pmatrix}$	56	$\begin{pmatrix} 0 & 3 \\ 3 & 2 \end{pmatrix}$	58	$\begin{pmatrix} 2 & 2 \\ 4 & 1 \end{pmatrix}$
60	$\begin{pmatrix} 1 & 5 \\ 1 & 2 \end{pmatrix}$	62	$\begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}$	64	$\begin{pmatrix} 2 & 3 \\ 4 & 1 \end{pmatrix}$	66	$\begin{pmatrix} 1 & 5 \\ 1 & 3 \end{pmatrix}$	68	$\begin{pmatrix} 0 & 2 \\ 5 & 3 \end{pmatrix}$
70	$\begin{pmatrix} 2 & 3 \\ 4 & 1 \end{pmatrix}$	72	$\begin{pmatrix} 2 & 4 \\ 2 & 2 \end{pmatrix}$	74	$\begin{pmatrix} 1 & 4 \\ 4 & 2 \end{pmatrix}$	76	$\begin{pmatrix} 2 & 3 \\ 5 & 1 \end{pmatrix}$	78	$\begin{pmatrix} 3 & 4 \\ 1 & 3 \end{pmatrix}$
80	$\begin{pmatrix} 0 & 4 \\ 4 & 3 \end{pmatrix}$	82	$\begin{pmatrix} 3 & 2 \\ 5 & 2 \end{pmatrix}$	84	$\begin{pmatrix} 1 & 7 \\ 3 & 1 \end{pmatrix}$	86	$\begin{pmatrix} 0 & 5 \\ 4 & 4 \end{pmatrix}$	88	$\begin{pmatrix} 2 & 2 \\ 7 & 2 \end{pmatrix}$
90	$\begin{pmatrix} 2 & 7 \\ 2 & 2 \end{pmatrix}$	92	$\begin{pmatrix} 0 & 4 \\ 4 & 5 \end{pmatrix}$	94	$\begin{pmatrix} 1 & 4 \\ 6 & 3 \end{pmatrix}$	96	$\begin{pmatrix} 1 & 6 \\ 2 & 5 \end{pmatrix}$	98	$\begin{pmatrix} 0 & 3 \\ 6 & 5 \end{pmatrix}$
				100	$\begin{pmatrix} 2 & 4 \\ 6 & 2 \end{pmatrix}$				

Deux approches de la conjecture de Goldbach

Denise Vella

Mai 2006

1 Introduction

Dans une lettre à Euler du 7 juin 1742, Goldbach énonce *"il semble que tout nombre supérieur à* 2 *soit la somme de trois nombres premiers"*. Euler reformule cette conjecture en une forme équivalente qui est *"tout nombre entier naturel pair supérieur à 2 est la somme de deux nombres premiers"*[1].

2 Approche utilisant le nombre de facteurs de la factorisation d'une factorielle

Etudions quelques exemples. On cherche les sommes de deux nombres premiers valant 12 (on les appellera *décompositions Goldbach de* 12). Pour cela, on va disposer les nombres impairs dont la somme vaut 12 par colonnes ayant même total dans un tableau.

9	7
3	5

Calculons maintenant le nombre de facteurs du produit de ces nombres : 3.5.7.9. La factorisation de ce produit a 5 facteurs (potentiellement égaux). Or, le tableau contient quatre nombres disposés dans deux colonnes. Puisque $5 \leq 4+2$, il y a forcément deux nombres premiers dans une même colonne (en l'occurrence 5 et 7). Recherchons les décompositions Goldbach de 14. Les nombres sont alors disposés comme suit dans le tableau.

11	9	7
3	5	

La factorisation du produit des 5 nombres impairs fait intervenir 6 facteurs. $6 \leq 5+2$. Les 2 colonnes ne peuvent donc pas contenir chacune un composé.

Généralisons : si on a $2n$ nombres impairs (resp. $2n+1$ dans un cas sur deux, quand on cherche les décompositions Goldbach du double d'un nombre impair) disposés dans n colonnes, et que la factorisation du produit de ces nombres impairs fait intervenir moins de $3n$ (resp. $3n+1$ dans le cas du double d'un impair) facteurs premiers, alors deux nombres premiers se retrouveront dans la même colonne et constitueront une décomposition Goldbach du nombre pair égal au total de chaque colonne (qui est $4n+2$).

[1] Les recherches présentées ici ont été déclenchées par la lecture du roman de Doxiadis "Oncle Pétros et la Conjecture de Goldbach".

Problème : pour résoudre la conjecture, il faudrait donc :
1) être capable de trouver le nombre de facteurs du produit des $2n$ (ou $2n+1$) premiers nombres entiers impairs (on ne compte pas 1) ;
2) être capable de démontrer que ce nombre est toujours inférieur à $3n$ (ou $3n+1$).
Continuons par l'exemple : voyons les factorisations des nombres de 2 à 20 (ces factorisations nous intéressent pour trouver les décompositions Goldbach de 22).

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

Le nombre de facteurs de la factorielle de 20 se décompose de la façon suivante (en les comptant colonne par colonne)[2] :

$10 + 5 + 2 + 1 = 18$ facteurs 2
$6 + 2 = 8$ facteurs 3
4 facteurs 5
2 facteurs 7
1 facteur 11
1 facteur 13
1 facteur 17
1 facteur 19
Soit un total de : 36 facteurs.

Voyons maintenant le nombre de facteurs du produit des nombres entiers pairs de 2 à 20. On peut obtenir ce nombre de facteurs en ajoutant 10 (le nombre de facteurs 2) au nombre de facteurs de la factorielle de 10. On obtient $10+15 = 25$. Par soustraction, on obtient le nombre de facteurs du produit des nombres impairs compris entre 3 et 19, en l'occurrence $36 - 25 = 11$ facteurs pour le produit des 10 premiers nombres entiers impairs (on oublie 1). Ce nombre étant inférieur à $3 \times 4 + 1 = 13$ correspondant au nombre de facteurs assurant la

[2] Lucas fait état de résultats dans sa théorie des nombres concernant la divisibilité des factorielles. Par exemple, le plus grand exposant de la puissance d'un nombre premier p contenue dans le produit $n!$ des n premiers nombres a pour limite supérieure $\frac{n}{p-1}$ (p.362).

présence de 2 nombres premiers dans une même colonne (ici 9 impairs de 3 à 19 à placer dans 4 colonnes selon la méthode vue plus haut), on est assuré que le nombre 22 a au moins une décomposition Goldbach.
Il faut être capable de prouver que, quelque soit x :

$$NbFact\big(\prod_{i=2}^{x}(2i-1)\big) \leq \lfloor\frac{3}{2}(x-2)\rfloor$$

La fonction *NbFact* renvoie pour x entier le nombre de facteurs (potentiellement égaux) que contient la factorisation de x.
L'inégalité est plus lisible si on l'écrit :

$$NbFact((2x)!) - NbFact(x!) - x \leq \lfloor\frac{3}{2}(x-1)\rfloor$$

Notons les premières valeurs des deux membres de l'inégalité dans un tableau. On appellera le terme à gauche de l'inégalité NFFPI (pour Nombre de Facteurs de la Factorisation du Produit des Impairs !) en entête de la colonne 4.

x	$NbFact((2x)!)$	$NbFact(x!)$	$NFFPI$	$\frac{3}{2}(x-1)$
4	11	4	3	4
5	15	5	5	6
6	19	7	6	7
7	22	8	7	9
8	28	11	9	10
9	32	13	10	12
10	36	15	11	13
11	40	16	13	15
12	45	19	14	16
13	49	20	16	18
14	55	22	19	19
15	59	24	20	21
16	65	28	21	22
17	69	29	23	24
18	75	32	25	25
19	78	33	26	27
20	83	36	27	28
21	87	38	28	30
22	91	40	29	31
23	96	41	32	33
24	102	45	32	34
25	107	47	35	36

Malheureusement, il suffit d'effectuer le calcul pour la factorielle de 100 à peine pour se rendre compte que l'idée ne tient pas.
$NbFact(100!) - NbFact(50!) - 50 = 81 > 73$.
Etudions ce qui se produit pour les décompositions Goldbach de 100 : il y a 14 nombres premiers impairs de 3 à 50 et 10 nombres impairs non premiers dans le même intervalle. "En face", il y a 10 nombres premiers dont on aurait pu imaginer qu'ils se soient justement et très "malencontreusement" positionnés en face des composés, ce qui aurait fait échouer la conjecture.

Les premiers sont parfois symétriques les uns des autres autour de x non pas à cause du fait qu'ils sont un rien si nombreux qu'il ne pourrait en être autrement mais bel et bien à cause de contraintes fortes pesant sur leurs positions, qui fait qu'au moins l'un d'entre eux "se positionne en face d'un nombre premier inférieur à x".

Autre idée : trouver selon un raisonnement un peu similaire que le nombre de facteurs du produit $Produit(2x - p_i)$ quel que soit i inférieur à $\Pi(x)$ est inférieur à $2\Pi(x)$, ce qui nous garantirait que l'un au moins des $2x - p_i$ serait premier. On a écrit *Produit* au lieu de la notation habituelle du produit par la lettre Π pour éviter de confondre les deux acceptions mathématiques possibles du symbole. Dit autrement, ceux qui sont "en face des premiers plus petits que x" ne peuvent pas être tous composés simultanément. Malheureusement, autant on sait calculer le nombre de facteurs d'un produit, en utilisant la formule $NbFact(xy) = NbFact(x) + NbFact(y)$ (qui se décline en particulier pour p premier par $NbFact(px) = NbFact(x) + 1$), autant on ne sait pas trouver le nombre de facteurs d'une somme, ce qui nous permettrait de trouver le nombre de facteurs de chacun des $2x - p_i$.

Dernière piste basée sur le calcul d'un nombre de facteurs :
Pour montrer que les $2x - p_i$ (p_i impair inférieur à x) ne peuvent pas être tous composés simultanément, il faudrait montrer que le nombre de facteurs du produit des nombres compris entre x (non compris) et $2x$ est toujours strictement inférieur au résultat de l'expression suivante $NbFact(x!) - NbFact((x/2)!) + 3x/2$ (si tous les $2x - p_i$ (p_i impair) étaient composés, ils auraient au moins deux facteurs chacun, ce qui entraînerait un total d'au moins x facteurs, auquel il faut ajouter le nombre de facteurs 2 de la première colonne égal à $x/2$ auquel il faut ajouter le nombre de facteurs des nombres compris entre $x/2$ et x, ce dernier étant égal à $NbFact(x!) - NbFact((x/2)!)$.

• 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...

Valuations p-adiques dans les factorisations des factorielles (Denise Vella-Chemla, 13.7.2017)

Lucas consacre dans sa théorie des nombres un paragraphe à la divisibilité des factorielles. Il fournit une procédure pour trouver la puissance d'un nombre premier p dans la factorisation de la factorielle d'un nombre entier n. Prenons un exemple ; pour connaître la puissance de 7 dans la factorielle de 10000, on divise successivement 10000 par 7, en obtenant comme quotients successifs 1428, 204, 29 et 4 et on ajoute ces quotients pour obtenir la valuation p-adique de 7 dans 10000 ! et qui est 1428+204+29+4=1665.

En réfléchissant un peu à cette idée, on réalise qu'un nombre premier p est à puissance 0 dans la factorisation de la factorielle de tout nombre qui lui est inférieur, à puissance 1 dans toute factorisation de la factorielle d'un entier de l'intervalle $[p, 2p[$ et à puissance supérieure à 1 pour les factorielles des nombres supérieurs ou égaux à $2p$.

Un nombre composé se distingue d'un nombre premier par le fait qu'il est à puissance au moins 2 dans la factorisation de sa propre factorielle (par exemple, 6 dans la factorielle de 6 apparaît "en tant que lui-même" mais également comme produit de ses 2 sous-facteurs 2 et 3 qui sont dans la factorielle l'un et l'autre séparément).

Cette propriété qu'un nombre premier p apparaît à puissance de 1 dans la factorisation de sa factorielle fournit une fonction qui permet de distinguer les nombres premiers des nombres composés (cette fonction associe à un nombre sa factorielle, puis extrait du nombre obtenu la valuation p-adique du nombre en question) ; les nombres premiers sont les seuls antécédents de 1 par cette fonction.

Ces propriétés permettent à nouveau d'illustrer ce que l'on peut entendre par "coïncidence de fonctions" : représentons le début de la droite numérique ainsi que les premiers nombres premiers. Représentons par des intervalles de valeurs ce qui a été énoncé ci-dessus. La deuxième ligne montre que la valuation p-adique de 3 dans les factorisations des factorielles des nombres compris entre 3 inclus et 6 exclus vaut 1 (et 0 pour des nombres inférieurs à 3 et plus que 1 pour des nombres supérieurs ou égaux à 6).

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

203. Divisibilité des factorielles. — Nous commencerons par résoudre le problème suivant : *Déterminer le plus grand exposant de la puissance d'un nombre a qui ne surpasse pas un nombre donné n.*

Une première méthode, directe, consiste à calculer le Tableau des puissances successives de a, jusqu'à ce que l'on obtienne un exposant α tel que l'on ait

$$a^\alpha \leqslant n < a^{\alpha+1},$$

et l'exposant cherché est α; on peut déterminer ainsi, par exemple, le plus grand exposant de la puissance de 2 contenue dans un nombre donné (nº 189, Remarque II).

Mais, au lieu d'employer les multiplications successives par a, on peut aussi employer les divisions successives par a. Cette méthode repose sur le théorème suivant : *Si q désigne le quotient par défaut de la division de n par a, et si q' désigne le quotient par défaut de la division de q par b, le nombre q' est égal* *au quotient par défaut de la division de n par le produit ab.* En effet, on a par définition,

$$n = aq + r, \qquad q = bq' + s,$$

r désignant l'une des valeurs $0, 1, 2, \ldots, (a-1)$, et s l'une des valeurs $0, 1, 2, \ldots, (b-1)$. On déduit

$$n = abq' + (as + r);$$

mais le nombre non négatif $(as + r)$ est au plus égal à

$$a(b-1) + (a-1) \quad \text{ou} \quad (ab-1);$$

donc q' est le quotient exact, ou approché par défaut, de la division de n par ab.

On désigne habituellement le plus grand nombre entier contenu dans $\frac{n}{a}$ par la notation $\mathrm{E}\frac{n}{a}$, que l'on prononce *entier de n par a* : on a donc

$$\mathrm{E}\frac{\mathrm{E}\frac{n}{a}}{b} = \mathrm{E}\frac{n}{ab},$$

et cette formule s'applique, en général, à l'entier de $\frac{n}{abc\ldots}$.

Cela posé, nous résoudrons le problème suivant : *Déterminer le plus grand exposant de la puissance d'un nombre premier p contenue dans le produit n! des n premiers nombres.* Les entiers qui contiennent p en facteur dans la factorielle $n!$ sont tous les multiples de p

$$p,\ 2p,\ 3p,\ \ldots,\ \mathrm{E}\frac{n}{p}\,p, \qquad \text{en nombre } \mathrm{E}\frac{n}{p};$$

par suite, l'exposant de p dans cette factorielle est égal à l'exposant de p dans le produit

$$1.2.3\ldots\ \mathrm{E}\frac{n}{p},$$

augmenté du dernier facteur. En répétant le même raisonnement sur cette nouvelle factorielle, et en appliquant le théorème précédent, il en résulte que l'exposant du nombre premier p dans la factorielle $n!$ est égal à la somme

$$\mathrm{E}\,\frac{n}{p} + \mathrm{E}\,\frac{n}{p^2} + \mathrm{E}\,\frac{n}{p^3} + \ldots.$$

Lorsque n est une puissance de p, les quotients de n par $p, p^2, p^3, \ldots,$ sont tous entiers, et l'on trouve pour l'exposant cherché

$$\frac{n-1}{p-1}.$$

Si l'on écrit le nombre n dans le système de numération de base p, en supposant

$$n = a + bp + cp^2 + dp^3 + \ldots,$$

on trouve facilement que l'exposant cherché a pour valeur

$$\frac{n-(a+b+c+\ldots)}{p-1},$$

et a pour limite supérieure

$$\frac{n}{p-1}.$$

Exemple I. — Quel est l'exposant de 7 dans le produit des 10000 premiers nombres?

On dispose le calcul de la manière suivante :

$$\begin{array}{r|l}
10000 & 7 \\ \cline{2-2}
30 & 1428 \\
20 & \\
60 & \\
4 &
\end{array}
\qquad
\begin{array}{r|l}
1428 & 7 \\ \cline{2-2}
028 & 204 \\
0 &
\end{array}
\qquad
\begin{array}{r|l}
204 & 7 \\ \cline{2-2}
64 & 29 \\
1 &
\end{array}
\qquad
\begin{array}{r|l}
29 & 7 \\ \cline{2-2}
1 & 4
\end{array}$$

et le nombre cherché est

$$1428 + 204 + 29 + 4 = 1665.$$

Exemple II. — Le produit des 1000 premiers nombres se termine par 249 zéros.

Exemple III. — Trouver le plus grand exposant de la puissance du nombre premier p contenue dans le nombre combinatoire C_m^n.

On a

$$\mathrm{C}_m^n = \frac{m!}{n!(m-n)!},$$

Valuations p-adiques des nombres dans les factorielles (Denise Vella-Chemla, 12.8.2017)

Dans la table suivante, on fournit dans la case (i, j) la valuation i-adique de i dans la factorielle de j (ou $val_i(j!)$, pour $i \geqslant 2$). On la note $<$ si elle est inférieure à 1, 1 si elle vaut 1 et $>$ si elle est supérieure à 1.

$val_3(4!) = val_3(4.3.2.1) = val_3(2.2.3.2.1) = 1.$

$val_9(6!) = val_9(6.5.4.3.2.1) = val_9(3.2.5.2.2.3.2.1) = 1.$

$val_i(j!)$	1	2	3	4	5	6	7	8	9	10
2	$<$	1	1	$>$	$>$	$>$	$>$	$>$	$>$	$>$
3	$<$	$<$	1	1	1	$>$	$>$	$>$	$>$	$>$
4	$<$	$<$	$<$	1	1	1	1	$>$	$>$	$>$
5	$<$	$<$	$<$	$<$	1	1	1	1	1	$>$
6	$<$	$<$	1	1	1	1	1	1	$>$	$>$
7	$<$	$<$	$<$	$<$	$<$	$<$	1	1	1	1
8	$<$	$<$	$<$	1	1	1	1	1	1	1
9	$<$	$<$	$<$	$<$	$<$	1	1	1	$>$	$>$
10	$<$	$<$	$<$	$<$	1	1	1	1	1	$>$

On note que $val_{p^2}((2p)!) = 1$.

On simplifie à l'extrême en n'utilisant que 3 images. On aurait pu utiliser une fonction val' qui aurait associé aux nombres des images rationnelles ; par exemple,

$$val'_9(12!) = val_9(12.11.10.9.8.7.6.5.4.3.2) = val'_9(2.2.3.11.2.5.3.3.2.2.2.7.2.3.5.2.2.3.2) = \frac{5}{2}.$$

Les seuls nombres tels que $val_x(x!) = 1$ sont les nombres premiers.

Pour voir si un autre élément permettrait de caractériser les nombres premiers, on calcule par programme dans $\mathbb{Z}/n\mathbb{Z}$ pour n pair le produit des $n/2$ nombres compris entre 1 et $n/2$, $k(n) = \prod_{x=1}^{n/2} x \ (mod\ n)$.

$k(n)$ est nul pour les nombres pairs. Voyons dans le tableau ci-dessous sa valeur pour les nombres impairs.

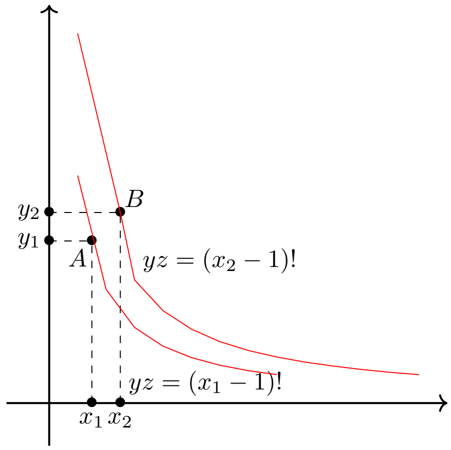
n	$k(n)$	n	$k(n)$	n	$k(n)$	n	$k(n)$	n	$k(n)$
$k(1)$	1	$k(21)$	0	$k(41)$	9	$k(61)$	11	$k(81)$	0
$k(3)$	1	$k(23)$	1	$k(43)$	42	$k(63)$	0	$k(83)$	1
$k(5)$	2	$k(25)$	0	$k(45)$	0	$k(65)$	0	$k(85)$	0
$k(7)$	6	$k(27)$	0	$k(47)$	46	$k(67)$	66	$k(87)$	0
$k(9)$	6	$k(29)$	12	$k(49)$	0	$k(69)$	0	$k(89)$	34
$k(11)$	10	$k(31)$	1	$k(51)$	0	$k(71)$	1	$k(91)$	0
$k(13)$	5	$k(33)$	0	$k(53)$	23	$k(73)$	27	$k(93)$	0
$k(15)$	0	$k(35)$	0	$k(55)$	0	$k(75)$	0	$k(95)$	0
$k(17)$	13	$k(37)$	31	$k(57)$	0	$k(77)$	0	$k(97)$	22
$k(19)$	18	$k(39)$	0	$k(59)$	1	$k(79)$	78	$k(99)$	0

Cette "moitié de factorielle"[†] de n est non-nulle pour les nombres premiers (sauf les nombres 1 et 9[‡]) tandis qu'elle est nulle pour les nombres composés.

Elle est égale à 1 ou $p-1$ pour les premiers $4k+3$ et à un nombre différent de 1 ou $p-1$ pour les premiers $4k+1$.

$\dfrac{(x-1)\,!}{x} \in \mathbb{N}?$ *(Denise Vella-Chemla (25.8.2018)*

x est composé s'il divise $(x-1)\,!$ et premier sinon. On peut représenter géométriquement cela sur le graphique ci-dessous : si y_1 l'ordonnée du point A d'abscisse x_1 sur l'hyperbole d'équation $yz = (x_1-1)!$ est un entier naturel alors x_1 est composé, tandis que si y_2 l'ordonnée du point B d'abscisse x_2 sur l'hyperbole d'équation $yz = (x_2-1)!$ n'est pas entier alors x_2 est premier.



Conjecture de Goldbach, chip-firing game, matrices 2×2 et descente infinie (Denise Vella-Chemla, 20.8.18)

On propose ici une nouvelle tentative de démontrer la conjecture de Goldbach.

Dans la suite de ce document, on ne s'intéresse qu'aux décompositions $p + (n - p)$ de chaque nombre pair n en sommes de 2 nombres impairs supérieurs ou égaux à 3 pour lesquelles p est un nombre premier inférieur ou égal à $n/2$.

Notre proposition utilise les éléments suivants :
- un langage $\mathcal{L}$ à deux lettres basé sur l'alphabet $\mathcal{A} = \{a, b\}$. La lettre a code les décompositions de la forme $p + (n - p)$ telles que $n - p$ est un nombre premier ; la lettre b code les décompositions de la forme $p + (n - p)$ telles que $n - p$ est composé ;
- des matrices de transition 2×2 à coefficients entiers [*] ; chaque matrice intègre dans ses coefficients une certaine connaissance sur les décompositions de n ainsi qu'une certaine connaissance sur les décompositions de $n + 2$, nous verrons comment ;
- la notion de chip-firing game [†] : on n'utilisera pas ici de résultats provenant de la théorie liée à cette notion, mais elle nous a été utile par son potentiel suggestif d'une part, et d'autre part, elle permettra de comprendre aisément comment s'effectue le passage de la matrice associée au nombre pair n à celle associée au nombre pair $n + 2$.

Pour fixer les idées, commençons par étudier deux exemples :

- au nombre pair 30 est associée la matrice $M_{30} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$.

- au nombre pair 32 est associée la matrice $M_{32} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$.

Penser la transition de M_{30} à M_{32} en terme de chip-firing game consiste à se dire que le 2 en haut à droite de M_{30} "a donné" 1 (chip ou jeton) au 1 en bas à gauche de M_{30}, ce qui a fait passer cet élément en bas à gauche de 1 à 2, et ce qui l'a lui-même fait passer en haut à droite de 2 à 1.

Explicitons à quoi correspondent les 4 éléments de la matrice M_{30} et les 4 éléments de la matrice M_{32}.

$n = 30$

p	$n - p$	$(n + 2) - p$	*doublon*
3	27	29	*ba*
5	25	27	*bb*
7	23	25	*ab*
11	19	21	*ab*
13	17	19	*aa*

$$\begin{pmatrix} aa\ 1 & ab\ 2 \\ ba\ 1 & bb\ 1 \end{pmatrix}$$

$n = 32$

p	$n - p$	$(n + 2) - p$	*doublon*
3	29	31	*aa*
5	27	29	*ba*
7	25	27	*bb*
11	21	23	*ba*
13	19	21	*ab*

$$\begin{pmatrix} aa\ 1 & ab\ 1 \\ ba\ 2 & bb\ 1 \end{pmatrix}$$

Comme on le voit dans ces exemples, chaque matrice intègre dans ses coefficients une certaine connaissance sur les décompositions de n (dans les lettres de gauche des doublons de lettres que comptent ses coefficients) ainsi qu'une certaine connaissance sur les décompositions de $n + 2$ (dans les lettres de droite des doublons de lettres que comptent ses coefficients).

*. Se reporter par exemple à A. Connes, Noncommutative geometry year 2000, [2], http://alainconnes.org/docs/2000.pdf, p.8, pour trouver des matrices telles que $f_{ab}(n) \neq f_{ba}(n)$ mais il s'agit alors d'opérateurs. Cette idée a eu un fort potentiel suggestif pour nous.

†. A. Björner, L. Lovász, P. W. Shor : Chip-firing games on graphs. European Journal of Combinatorics archive, Volume 12 Issue 4, July 1991, Pages 283–291.

Ecrivons mathématiquement ce que comptent les 4 coefficients de chaque matrice 2×2 :

$$M_n \begin{pmatrix} f_{aa}(n) & f_{ab}(n) \\ f_{ba}(n) & f_{bb}(n) \end{pmatrix}$$

avec :

- $f_{aa}(n) = \#\{(p+q=n) \wedge (p\ premier) \wedge (3 \leq p \leq n/2) \wedge (q\ premier) \wedge (((n+2)-p)\ premier)\}$;
- $f_{ab}(n) = \#\{(p+q=n) \wedge (p\ premier) \wedge (3 \leq p \leq n/2) \wedge (q\ premier) \wedge (((n+2)-p)\ compos\acute{e})\}$;
- $f_{ba}(n) = \#\{(p+q=n) \wedge (p\ premier) \wedge (3 \leq p \leq n/2) \wedge (q\ compos\acute{e}) \wedge (((n+2)-p)\ premier)\}$;
- $f_{bb}(n) = \#\{(p+q=n) \wedge (p\ premier) \wedge (3 \leq p \leq n/2) \wedge (q\ compos\acute{e}) \wedge (((n+2)-p)\ compos\acute{e})\}$.

On comprend aisément que la somme $f_{ba}(n) + f_{bb}(n)$ compte les couples $(x, x+2)$ tels que $x \geq n/2$ et $n - x$ est premier.

La somme des 4 éléments des matrices est égale à $\pi(n/2) - 1$ (avec $\pi(x)$ la notation habituelle pour le nombre de nombres premiers inférieurs ou égaux à x), puisqu'on ne s'intéresse qu'aux décompositions des nombres pairs "basées" sur un petit sommant qui est un nombre premier.

Cette somme augmente de 1 à chaque nombre pair double d'un nombre premier.

Sont fournies en annexe les matrices associées aux nombres pairs compris entre 10 et 100.

Le nombre de décompositions de Goldbach de n est égal à $f_{aa}(n) + f_{ab}(n)$. Démontrer la conjecture de Goldbach revient à démontrer qu'on a toujours $f_{aa}(n) + f_{ab}(n) > 0$.

Essayons maintenant de décomposer le processus à l'œuvre lors du passage d'un nombre pair n au nombre pair suivant $n+2$ en terme de transformation de chaque élément de la matrice pris séparément.

Reportons-nous aux matrices exemples M_{30} et M_{32} en observant la colonne des doublons de lettres à droite des décompositions.

Si un nombre n'avait pas de décomposition de Goldbach, on aurait $f_{aa}(n) = f_{ab}(n) = 0$. Seuls $f_{ba}(n)$ et $f_{bb}(n)$ seraient non nuls. Il y aurait alors, à droite de la matrice M_n, uniquement des doublons ba et des doublons bb. Mais on a vu qu'il y a identité entre les lettres gauches des doublons de $n+2$ et les lettres droites des doublons de n (puisque ces lettres codent les mêmes décompositions).

Précisons maintenant la circulation des jetons, en terme de chip-firing game, on a que (les ou sont inclusifs) :

- les ba se déversent dans les aa ou les ab ;
- les bb se déversent dans les ba ou les bb ;
- les aa se déversent dans les aa ou les ab ;
- les ab se déversent dans les ba ou les bb.

On peut représenter cette circulation par le schéma ci-dessous :

$$\begin{tikzcd}
aa \arrow[loop above] \arrow[r] & ab \arrow[d] \arrow[dl, Rightarrow] \\
ba \arrow[u] \arrow[ur, Rightarrow] & bb \arrow[l] \arrow[loop below]
\end{tikzcd}$$

En observant la manière dont les "chips circulent" dans le schéma, on comprend que le seul moyen d'aboutir à une matrice M_n telle que $f_{aa}(n)$ et $f_{ab}(n)$ sont nuls est de partir d'une matrice M_{n-2} telle que $f_{aa}(n-2)$ et $f_{ab}(n-2)$ sont nuls également.

La contradiction [‡] provient alors d'un mode de raisonnement appelé descente infinie de Fermat : on a vu que si la conjecture de Goldbach n'était pas vérifiée par un entier pair, elle ne le serait pas non plus par

‡. On aurait souhaité initialement établir la contradiction à partir du fait que puisque la somme totale des 4 éléments de chaque matrice est égale à $\pi(n/2) - 1$, et qu'on a vu que la somme $f_{ba}(n) + f_{bb}(n)$ compte les couples $(x, x+2)$ tels que

l'entier pair qui le précède. Or, il n'existe pas de suite infinie décroissante d'entiers positifs qui vérifient simultanément une même propriété (ici, le fait pour un nombre pair supérieur à 4 de se décomposer en une somme de 2 nombres premiers impairs, propriété dont on rappelle qu'elle est vraie pour tous les nombres pairs jusqu'à 100 par ailleurs). L'ensemble $\mathbb{N}$ des entiers naturels et toutes ses parties propres non vides possèdent une propriété remarquable : ils admettent un plus petit élément. On a raisonné par l'absurde : en supposant que la matrice associée à n est telle que $f_{aa}(n) = f_{ab}(n) = 0$, on a vu qu'il serait nécessaire que la matrice associée à $n-2$ soit elle aussi telle que $f_{aa}(n-2) = f_{ab}(n-2) = 0$. Or $n-2 < n$. On aboutit ainsi à une contradiction par descente infinie et un tel raisonnement devrait assurer que la conjecture de Goldbach est vraie.

Par le seul jeu des manipulations de lettres, on a effectivement la sensation de quelque-chose *qui tourne*, c'est-à-dire qui est comme *circulant dans le temps*.

Annexe 1 : matrices 2×2 associées aux nombres pairs compris entre 10 et 100

$$
\begin{array}{cccccccccc}
10 & \begin{pmatrix}1 & 1\\0 & 0\end{pmatrix} & 12 & \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} & 14 & \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix} & 16 & \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix} & 18 & \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}\\
20 & \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix} & 22 & \begin{pmatrix}2 & 1\\1 & 0\end{pmatrix} & 24 & \begin{pmatrix}1 & 2\\1 & 0\end{pmatrix} & 26 & \begin{pmatrix}0 & 3\\2 & 0\end{pmatrix} & 28 & \begin{pmatrix}1 & 1\\2 & 1\end{pmatrix}\\
30 & \begin{pmatrix}1 & 2\\1 & 1\end{pmatrix} & 32 & \begin{pmatrix}1 & 1\\2 & 1\end{pmatrix} & 34 & \begin{pmatrix}2 & 2\\2 & 0\end{pmatrix} & 36 & \begin{pmatrix}1 & 3\\0 & 2\end{pmatrix} & 38 & \begin{pmatrix}0 & 2\\3 & 2\end{pmatrix}\\
40 & \begin{pmatrix}1 & 2\\3 & 1\end{pmatrix} & 42 & \begin{pmatrix}1 & 3\\2 & 1\end{pmatrix} & 44 & \begin{pmatrix}1 & 2\\2 & 2\end{pmatrix} & 46 & \begin{pmatrix}2 & 2\\3 & 1\end{pmatrix} & 48 & \begin{pmatrix}2 & 3\\2 & 1\end{pmatrix}\\
50 & \begin{pmatrix}0 & 4\\3 & 1\end{pmatrix} & 52 & \begin{pmatrix}2 & 1\\3 & 2\end{pmatrix} & 54 & \begin{pmatrix}1 & 4\\2 & 1\end{pmatrix} & 56 & \begin{pmatrix}0 & 3\\3 & 2\end{pmatrix} & 58 & \begin{pmatrix}2 & 2\\4 & 1\end{pmatrix}\\
60 & \begin{pmatrix}1 & 5\\1 & 2\end{pmatrix} & 62 & \begin{pmatrix}1 & 2\\4 & 3\end{pmatrix} & 64 & \begin{pmatrix}2 & 3\\4 & 1\end{pmatrix} & 66 & \begin{pmatrix}1 & 5\\1 & 3\end{pmatrix} & 68 & \begin{pmatrix}0 & 2\\5 & 3\end{pmatrix}\\
70 & \begin{pmatrix}2 & 3\\4 & 1\end{pmatrix} & 72 & \begin{pmatrix}2 & 4\\2 & 2\end{pmatrix} & 74 & \begin{pmatrix}1 & 4\\4 & 2\end{pmatrix} & 76 & \begin{pmatrix}2 & 3\\5 & 1\end{pmatrix} & 78 & \begin{pmatrix}3 & 4\\1 & 3\end{pmatrix}\\
80 & \begin{pmatrix}0 & 4\\4 & 3\end{pmatrix} & 82 & \begin{pmatrix}3 & 2\\5 & 2\end{pmatrix} & 84 & \begin{pmatrix}1 & 7\\3 & 1\end{pmatrix} & 86 & \begin{pmatrix}0 & 5\\4 & 4\end{pmatrix} & 88 & \begin{pmatrix}2 & 2\\7 & 2\end{pmatrix}\\
90 & \begin{pmatrix}2 & 7\\2 & 2\end{pmatrix} & 92 & \begin{pmatrix}0 & 4\\4 & 5\end{pmatrix} & 94 & \begin{pmatrix}1 & 4\\6 & 3\end{pmatrix} & 96 & \begin{pmatrix}1 & 6\\2 & 5\end{pmatrix} & 98 & \begin{pmatrix}0 & 3\\6 & 5\end{pmatrix}\\
 & & & & 100 & \begin{pmatrix}2 & 4\\6 & 2\end{pmatrix} & & & &
\end{array}
$$

$n-x$ est premier, si seuls $f_{ba}(n)$ et $f_{bb}(n)$ étaient non nuls, cela signifierait qu'il y a autant de nombres premiers de 3 à $n/2$ que de $n/2$ à n, ce qui ne saurait être, le nombre de nombres premiers allant diminuant sur deux intervalles consécutifs de même longueur. Mais on ne trouve pas dans la littérature si $\pi(n) - \pi(n/2) < \pi(n/2)$ est un fait démontré.

Annexe 2 : Programme python de calcul des matrices

```
import math
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

for n in range(10,102,2):
  aa = 0 ; ab = 0 ; ba = 0 ; bb = 0 ;
  for x in range(3,n/2+1,2):
    if (prime(x)):
      if ((prime(n-x)) and (not(prime((n+2)-x)))):
        ab=ab+1
      elif ((prime(n-x)) and (prime((n+2)-x))):
        aa=aa+1
      elif ((not(prime(n-x))) and (prime((n+2)-x))):
        ba=ba+1
      elif ((not(prime(n-x))) and (not(prime((n+2)-x)))):
        bb=bb+1
  s=str(n)+'--->'
  print(s)
  s=str(aa)+' '+str(ab)
  print(s)
  s=str(ba)+' '+str(bb)
  print(s)
```

Bibliographie

[1] : A. Björner, L. Lovász, P. W. Shor : Chip-firing games on graphs. European Journal of Combinatorics archive, Volume 12 Issue 4, July 1991, Pages 283–291.

[2] : A. Connes, Noncommutative geometry year 2000, In : Alon N., Bourgain J., Connes A., Gromov M., Milman V. (eds) Visions in Mathematics. Modern Birkhäuser Classics. Birkhäuser Basel, 2000, p.481-559.

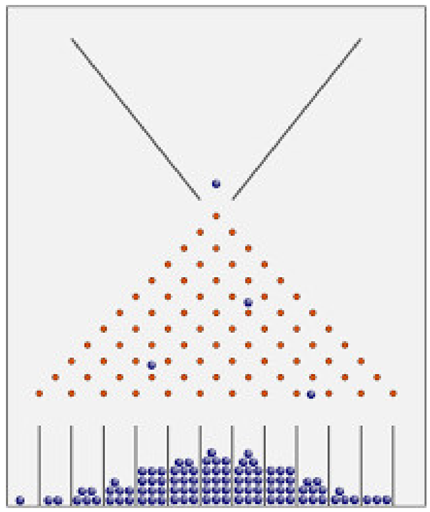
90

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

92

Décomposants de Goldbach sur planche de Galton (Denise Vella-Chemla, 27.8.18)

On a pris récemment la pleine mesure de la manière dont l'aléa gouverne les décompositions de Goldbach (i.e. ou décompositions d'un nombre pair en somme de deux nombres premiers) ainsi que leur nombre, en les étudiant selon un point de vue utilisant des matrices 2×2 de transitions codant des sortes d'échanges de jetons.
On souhaite étudier ici, pour appréhender davantage encore cet aléa, la manière dont les décomposants de Goldbach quantifiés (coupés en unités) remplissent une sorte de "planche de Galton" ; c'est une planche dans laquelle des billes tombent, et se répartissent plus il y en a selon une courbe de Gauss (courbe en cloche). Cette idée est venue de l'association souvent faite dans la littérature entre les concepts de chip-firing game et de sandpile (pile de sable) qui s'effondre petit à petit, les grains glissant les uns sur les autres *.

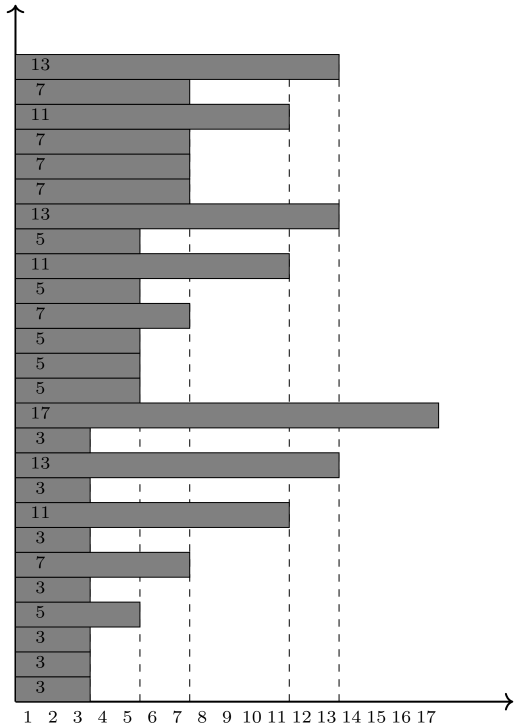


Illustrons sur un diagramme les comptages qu'on va effectuer par programme, avec les décompositions de Goldbach des nombres pairs compris entre 6 et 20. Voici les décompositions de Goldbach de ces nombres :

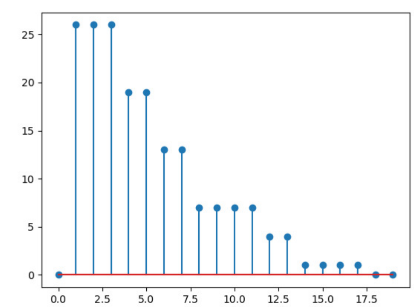
$$
\begin{aligned}
&6 = 3 + 3\\
&8 = 3 + 5\\
&10 = 3 + 7 = 5 + 5\\
&12 = 5 + 7\\
&14 = 3 + 11 = 7 + 7\\
&16 = 3 + 13 = 5 + 11\\
&18 = 5 + 13 = 7 + 11\\
&20 = 3 + 17 = 7 + 13
\end{aligned}
$$

Empilons-les toutes les unes sur les autres ainsi :

*. sans compter qu'on a souvent eu l'impression, lors de ces recherches, de concepts qui nous filent entre les doigts comme du sable...



Faisons descendre les quanta de décompositions le plus bas possible pour les compter, on obtient par programme le graphique suivant :



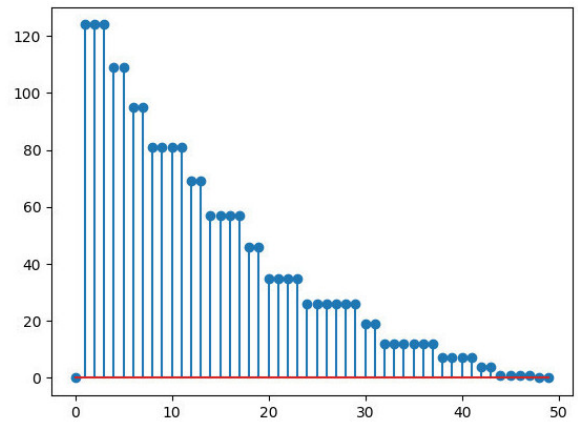
Notons les valeurs de la fonction que représente ce diagramme dans un tableau et explicitons ce que représentent ses valeurs (le sigle *dg* dans le tableau signifie *décomposant de Goldbach*) :

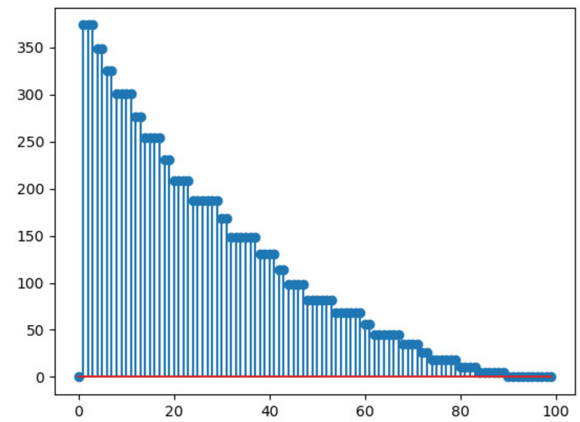
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
26	26	26	19	19	13	13	7	7	7	7	4	4	1	1	1	1
nb. dg ≥ 3			*nb. dg* ≥ 5		*nb. dg* ≥ 7		*nb. dg* ≥ 11				*nb. dg* ≥ 13		*nb. dg* ≥ 17			

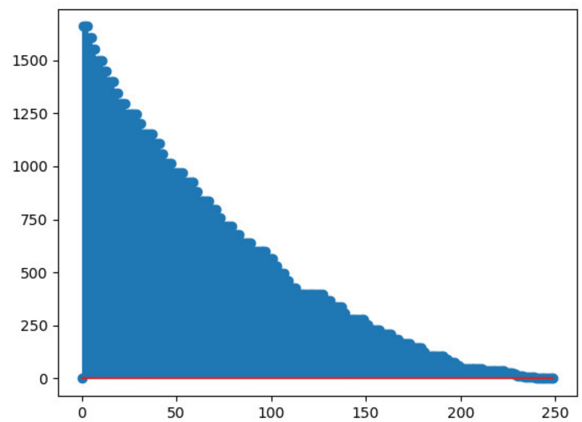
Le total de 26 compte les sommants des décompositions supérieurs ou égaux à 3 (on ne l'a noté que pour $f(2)$ mais il est identique pour $f(1)$ et $f(3)$), le total de 19 compte les sommants des décompositions supérieurs ou égaux à 5 (resp. 13 pour le nombre de sommants ≥ 7, 7 pour le nombre de sommants ≥ 11, 4 pour le nombre de sommants ≥ 13, 1 pour le nombre de sommants ≥ 17).

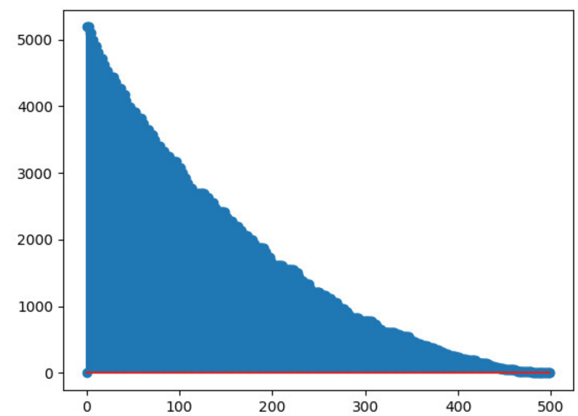
La fonction compte dans toutes les décompositions de Goldbach recensées des nombres de 6 à 20, pour un nombre x compris entre 2 nombres premiers successifs p_k et p_{k+1}, le nombre de sommants des décompositions qui sont supérieurs ou égaux à p_{k+1}. Par exemple, 4 sommants sont supérieurs ou égaux à 13 (les seconds sommants de décompositions de 16, 18 et 20) et la fonction attribue donc 4 comme image au nombre 12 et au nombre 13.

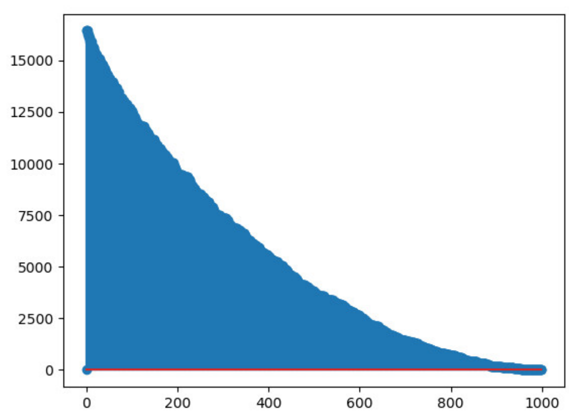
On fournit ci-dessous la tendance générale qui semble se dessiner pour cette fonction, bien qu'on n'ait pas pu la tester très loin (courbes jusqu'à 50, 100, 250, 500, 1000 et 10000).

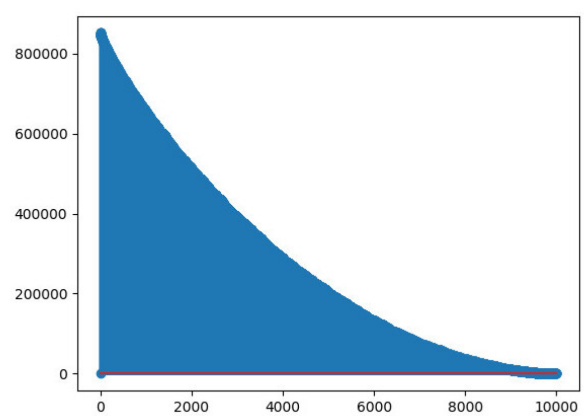












On approxime bien les premières courbes $f(x)$ par des formules comme :

$$(x - maxx) * (x - maxx)/(2.58498 * sqrt(maxx))$$

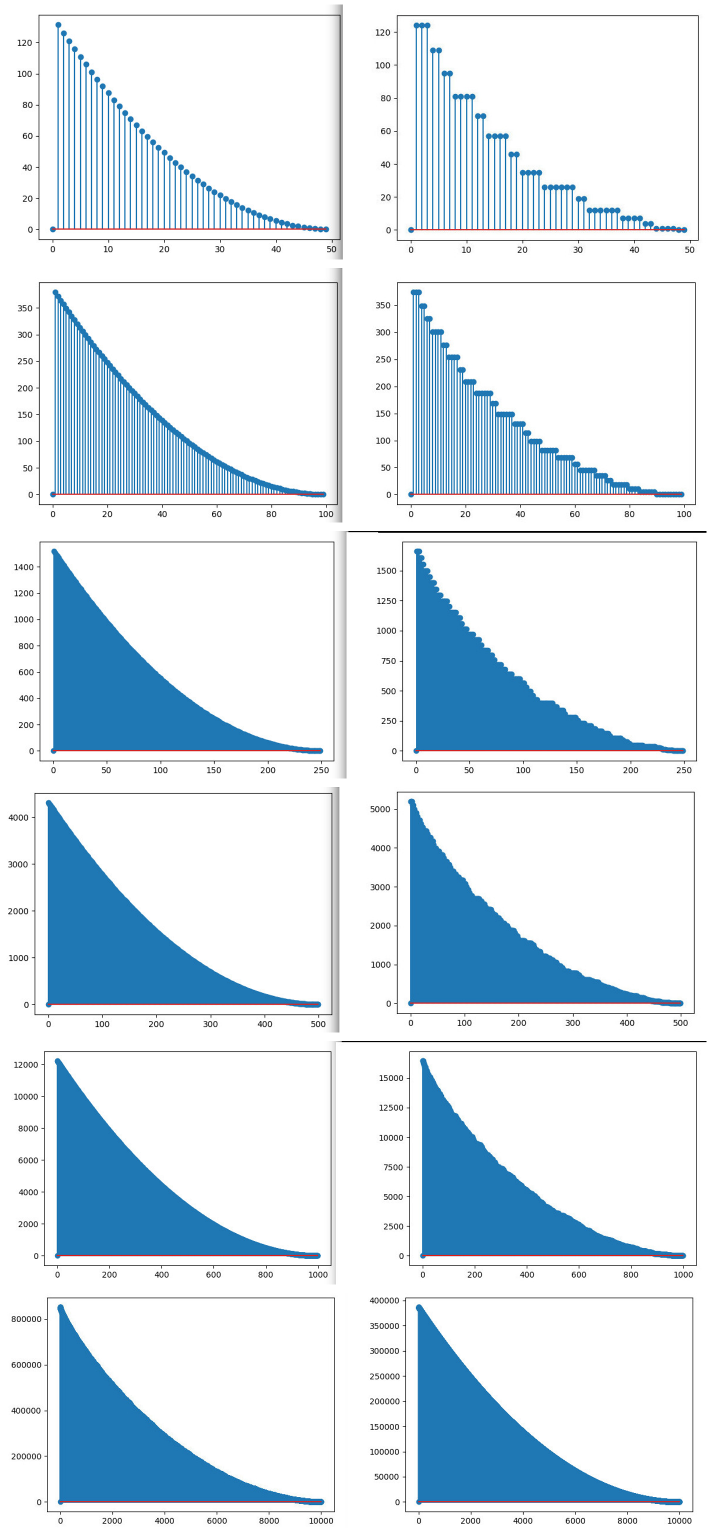
pour les petites valeurs de $maxx$ (50, 100, 250) (avec 2.58498 qui est la constante de Sierpinski [†]) mais cela ne va plus dès le graphique correspondant à $maxx = 500$ (regarder les ordonnées pour les petites

†. voir wikipedia : la constante de Sierpinski est la constante K définie par $K = \lim_{n\to\infty} \left[\sum_{k=1}^{n} \frac{r_2(k)}{k} - \pi \ln n\right]$ où $r_2(k)$ est le nombre de représentations de k comme une somme de deux carrés $a^2 + b^2$ avec a et b entiers naturels.
Sa valeur est :

$$K = \pi\left(2\ln 2 + 3\ln \pi + 2\gamma - 4\ln \Gamma\left(\frac{1}{4}\right)\right) \approx 2.58498,$$

où γ désigne la constante d'Euler-Mascheroni et Γ la fonction gamma.

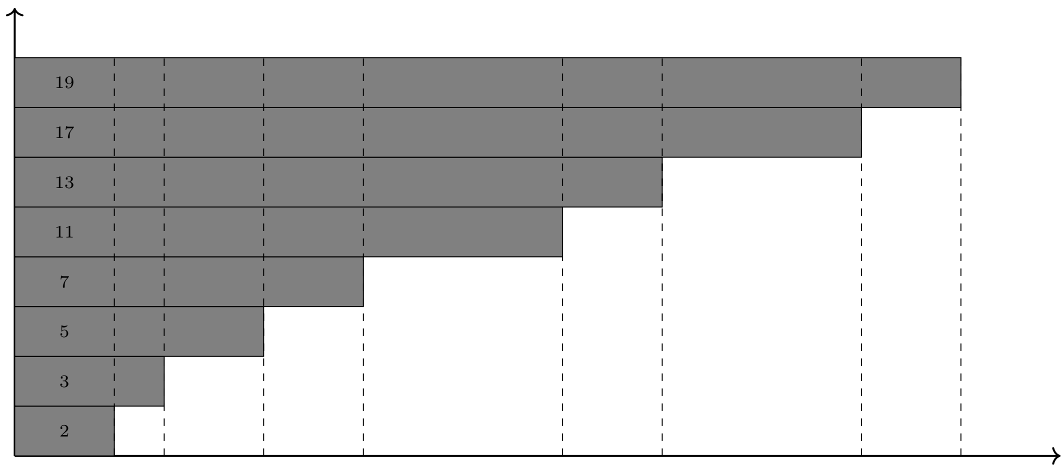
valeurs, à gauche des graphiques).



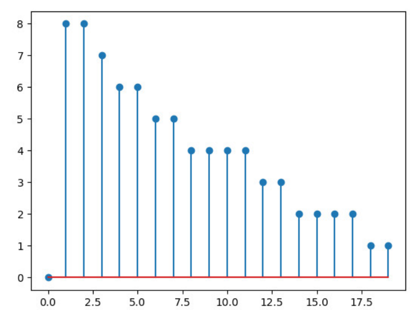
Quantifier les nombres premiers (Denise Vella-Chemla, 28.8.2018)

On a découvert récemment une façon de quantifier les décomposants de Goldbach (i.e. ou décompositions d'un nombre pair en somme de deux nombres premiers), c'est-à-dire de compter certains de leur nombre en les coupant en morceaux.
On souhaite étudier ici de la même manière les nombres premiers eux-mêmes.

Empilons-les tous les uns sur les autres ainsi :

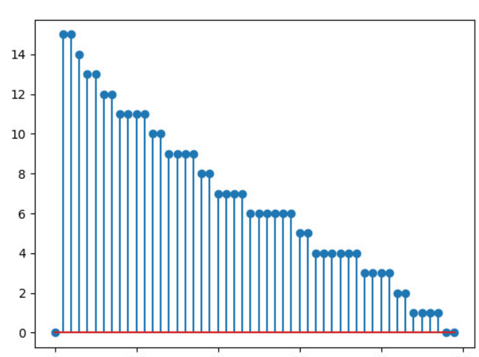


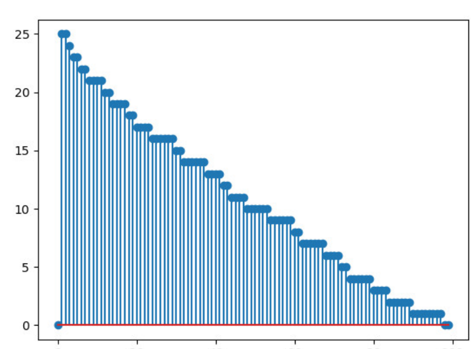
Faisons descendre les quanta le plus bas possible (par une sorte de gravité !) et comptons, on obtient par programme le graphique suivant :

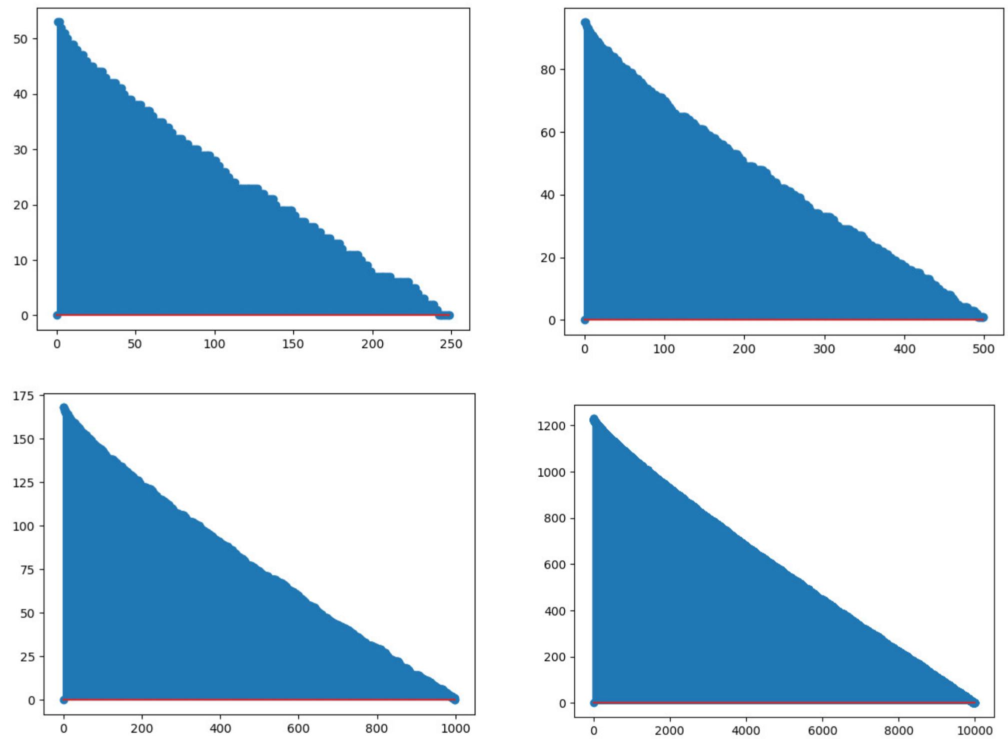


C'est le graphique d'une fonction, $f_{20}(x)$ qui fournit pour tout $x \leq 20$ le nombre de nombres premiers qui sont compris entre x et 20. L'abscisse à l'origine est ainsi égale à $\pi(20)$ (avec $\pi(x)$ la notation habituelle pour le nombre de nombres premiers inférieurs ou égaux à x).

On fournit ci-dessous les courbes correspondant à des comptages similaires jusqu'à 50, 100, 250, 500, 1000 et 10000.





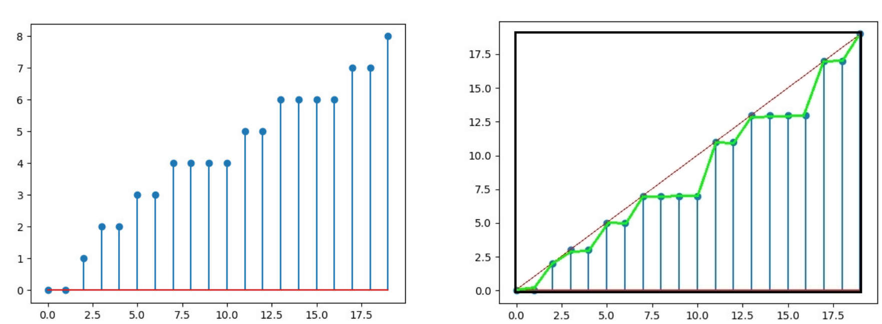


Comme attendu, ont été obtenus les graphiques de fonctions $f_n(x)$ presque linéaires décroissantes, d'équations qui semblent être de la forme $f(x) = -\dfrac{\pi(n)}{n}x + \pi(n)$ avec n l'abscisse la plus grande, alors qu'elles sont en réalité de la forme $f(x) = \pi(n) - \pi(x)$.

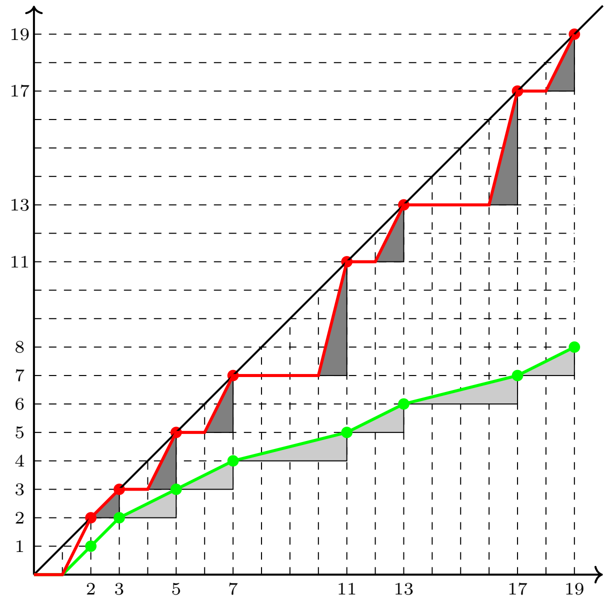
On peut étirer $\pi(x)$ de la façon suivante : pour que les valeurs des images couvrent la totalité de l'intervalle $[0, 20]$ par exemple, lorsqu'on rencontre un nombre premier, on cumule des sauts verticaux de 1 de manière à ce que les marches d'escalier plutôt que d'être de hauteur 1 (comme dans la fonction $\pi(x)$) soient plutôt de hauteur $p_k - p_{k-1}$, cela permet de rester toujours proche de la diagonale, qui est de longueur $\sqrt{2}n$.

La fonction correspondante consiste à associer à x le plus grand nombre premier inférieur ou égal à x. Les nombres premiers se retrouvent ainsi sur la diagonale du graphique.

On illustre cette idée sur le diagramme de la fonction $\pi(x)$ étirée pour x inférieur ou égal à 19 (à droite) en regard de $\pi(x)$ (à gauche).



Etirement (Denise Vella-Chemla, 30.8.2018)



La courbe verte représente la fonction $\pi(x)$ définie par $f(x) = \#\{p_k/p_k\ \textit{premier et}\ p_k \leq x\}$.

La courbe rouge (qu'on appelle $\pi(x)$ *rendue carrée*) est définie par $g(x) = max\{p_k/p_k\ \textit{premier},\ p_k \leq x\}$.

La taille de la surface différence entre les deux surfaces sous les deux courbes verte et rouge (en oubliant les petits triangles de surface totale $p_{max}/2$, ici $19/2$) est :

$$\Delta = \sum_k (p_k - k)(p_{k+1} - p_k)$$

Tendre vers 0.5 (Denise Vella-Chemla, 2.9.2018)

On fournit ici une nouvelle fonction définie sur l'ensemble des nombres premiers, à valeurs réelles, et qui semble avoir 1/2 pour limite : elle associe à un nombre n la moyenne des parties décimales des moyennes des ensembles de nombres premiers inférieurs à ce nombre n, le plus petit de ces ensembles étant le singleton $\{2\}$ et le plus grand étant l'ensemble des nombres premiers inférieurs ou égaux à n.

Cette fonction associe les valeurs suivantes aux nombres de 2 à 103 :

n	$\sum$	*nb. premiers*	*moyenne*	*moyenne décimales*
2	2	1	2	0
3	5	2	2.5	0.25
5	10	3	3.33333	0.277778
7	17	4	4.25	0.270833
11	28	5	5.6	0.336667
13	41	6	6.83333	0.419444
17	58	7	8.28571	0.40034
19	77	8	9.625	0.428423
23	100	9	11.1111	0.393166
29	129	10	12.9	0.443849
31	160	11	14.5455	0.453086
37	197	12	16.4167	0.450051
41	238	13	18.3077	0.4391
43	281	14	20.0714	0.412838
47	328	15	21.8667	0.443093
53	381	16	23.8125	0.466181
59	440	17	25.8824	0.490662
61	501	18	27.8333	0.5097
67	568	19	29.8947	0.529965
71	639	20	31.95	0.550966
73	712	21	33.9048	0.567814
79	791	22	35.9545	0.585393
83	874	23	38	0.559941
89	963	24	40.125	0.541818
97	1060	25	42.4	0.536145
101	1161	26	44.6538	0.540672
103	1264	27	46.8148	0.550826

Il semblerait que la moyenne des parties décimales des moyennes des ensembles de nombres premiers successifs tende vers 1/2.

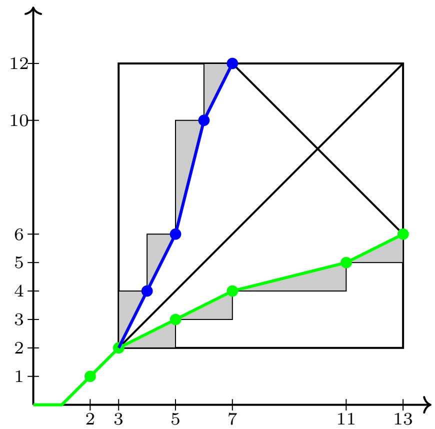
Elle est égale à 0.501183 pour 10^5, et à 0.500481 pour 225079.

On ne sait pas démontrer que la valeur asymptotique de la fonction est 1/2 dans le cas où elle le serait effectivement.

Surface à faire vibrer (Denise Vella-Chemla, 30.8.2018)

Bien que je ne sache pas du tout comment il faut procéder pour trouver les noeuds de vibration, les harmoniques, etc, je propose le carré tronqué comme surface à faire vibrer, peut-être, comme autre manière d'"entendre" les nombres premiers.

Dessin pour $p = 13$:

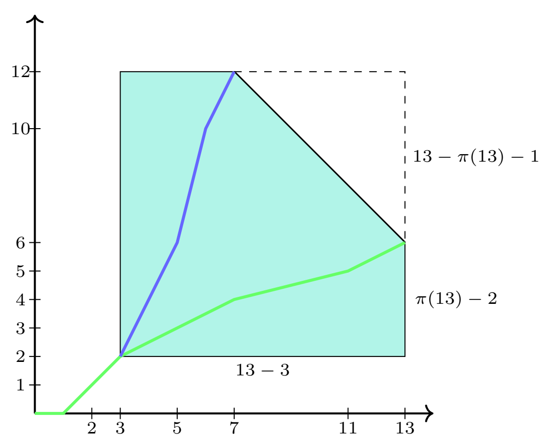


La courbe verte représente la fonction $\pi(x)$ définie par $f(x) = \#\{p_k/p_k \textit{ premier et } p_k \leq x\}$.

La courbe bleue est symétrique de $\pi(x)$ par rapport à la diagonale.

La taille totale des petits triangles rectangles de côtés adjacents horizontaux est $(p_{max} - 3)/2$, là 5.

On aimerait faire vibrer la surface "carré tronqué" colorée en bleu pâle ci-dessous. Les mesures sur les côtés du carré tronqué permettent de calculer la taille des surfaces des différents polygones pour un nombre premier p_{max} donné.

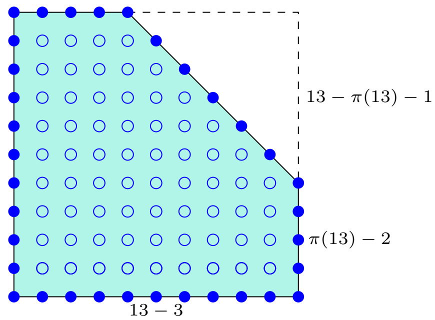


La formule de calcul de l'aire de la surface du carré tronqué donne (on la calcule pour le cas présenté $p_k = 13$) :

$$\begin{aligned}(x-3)^2 - \frac{1}{2}(x - (\pi(x)+1))^2 \quad &= \frac{1}{2}x^2 - \pi(x)(1-x) - \frac{1}{2}\pi(x)^2 - 5x + \frac{17}{2} \\ &= 82\end{aligned}$$

On peut aussi vérifier que cette formule est correcte en calculant également l'aire de la surface grâce à la formule fourni par le théorème de Pick (Ext est le nombre de points entiers du pourtour de la surface tandis que Int est le nombre de points entiers à l'intérieur de la surface) :

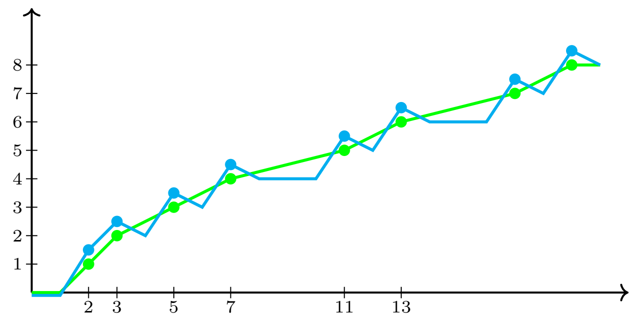
$$\begin{aligned}
Ext &= 34\\
Int &= 66\\
Aire &= Int + \frac{1}{2}Ext - 1\\
&= 66 + 17 - 1\\
&= 82
\end{aligned}$$



Petit memo (Denise Vella-Chemla, 12.09.2018)

Riemann ne compte pas les premiers comme “habituellement”, il ajoute 0.5 à la fonction de comptage lors du passage sur un nombre premier ; on compare dans le tableau ci-dessous la fonction $\pi(x)$ (de couleur verte), celle proposée dans l'article fondateur de Riemann qu'on nomme $\pi_{BR}(x)$ (de couleur cyan), et les valeurs des aires sous les courbes de ces deux fonctions.

x	$\pi(x)$	$\pi_{BR}(x)$	$F1(x) = Aire\ sous\ \pi(x)$	$F2(x) = Aire\ sous\ \pi_{BR}(x)$	$(F1(x+1)+F1(x-1))/2$	$(F2(x+1)+F2(x-1))/2$
2	1	1.5	0.5	0.75	1	1.375
3	2	2.5	2	2.75	2.25	2.875
4	2	2	4	5	4	4.25
5	3	3.5	6	7.75	6.5	8
6	3	3	9	11	9	11.25
7	4	4.5	12	14.75	12.5	15
8	4	4	16	19	16	18.875
9	4	4	20	23	20	23
10	4	4	24	27	24	27.375
11	5	5.5	28	31.75	27.5	32
12	5	5	33	37	33	37.25
13	6	6.5	38	42.75	38.5	43
14	6	6	44	49	44	48.875
15	6	6	50	55	50	55
16	6	6	56	61	56	61.375
17	7	7.5	62	67.75	62.5	68
18	7	7	69	75	69	75.25
19	8	8.5	76	82.75	76.5	83
20	8	8	84	91		



On constate que pour les premiers, avec la fonction de comptage proposée dans l'article de Riemann, la différence des aires sous la courbe de leur succ et de leur prec vaut le double de leur rang.

$$\forall p_k\ premier, Aire_{BR}(p_k+1) - Aire_{BR}(p_k-1) = 2k$$

On constate également qu'avec la fonction $\pi(x)$ telle qu'elle est habituellement définie, la moyenne des aires sous la courbe du succ et du prec d'un nombre (à part pour les nombres premiers 2 et 3) a toujours pour partie fractionnaire 0.5.

Compter les nombres premiers

Denise Vella-Chemla

19.9.2018

On définit ci-dessous une fonction $f_b(x)$ paramétrée par un entier b (la base, qui n'est pas forcément un nombre premier).

Cette fonction est définie sur l'ensemble des entiers naturels $\mathbb{N}$.

Elle permet d'"isoler" une puissance de la base dans l'écriture d'un nombre entier sous la forme d'un produit ainsi [*] :

$$f_b(kb^y) = y \text{ avec } b \not| k.$$

Cette fonction coïncide avec la valuation p-adique $v_p(n)$ qui est définie sur $\mathbb{Q}$ et selon p un nombre premier [†].

$$y \text{ est l'exposant maximum tel que } \; b^y \mid n.$$

Les images des 30 premiers entiers par les fonctions f_2, f_3, f_4, f_5 sont :

x	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
$f_2(x)$	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
$f_3(x)$	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
$f_4(x)$	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	2	0	0	0	1	0	0	0	1	0	0	0	1	0	0
$f_5(x)$	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	2	0	0	0	0	1

Ces fonctions ont un comportement similaire à celui du logarithme : par exemple, $f_k(kx) = f_k(x) + 1$.

On remarque dans chaque séquence les multiples occurrences d'une sous-séquence répétitive, qui rappelle la notion de motif musical, ces motifs étant palindromiques [‡] :

- multiples occurrences du "motif" 010 dans la séquence des $f_2(x)$, entre lesquelles s'intercalent les valeurs 2, 3, 2, 4, etc.
- multiples occurrences du "motif" 00100100 dans la séquence des $f_3(x)$, entre lesquelles s'intercalent les valeurs 2, 2, 3, 2, 2, 3, 2, 2, 4, etc.
- multiples occurrences du "motif" $(0^{p-1}1)^{p-1}0^{p-1}$ dans la séquence des $f_p(x)$, entre lesquelles s'intercalent les valeurs 2 ($p-1$ fois), etc.

La fonction $Sf(n)$ qui associe à n la somme des valeurs des $f_x(n)$ pour x un entier compris entre 2 et $\left\lfloor \frac{n}{2} \right\rfloor$, associe comme image 0 aux nombres premiers (> 1) et associe comme image un entier non nul aux nombres composés.

$$Sf(n) = \sum_{2 \leq x \leq \left\lfloor \frac{n}{2} \right\rfloor} f_x(n)$$

Les valeurs $Sf(x)$ sont fournies ci-dessous pour les premiers entiers :

x	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
$Sf(x)$	0	0	2	0	1	0	3	2	1	0	3	0	1	1	6	0	3	0	3	1	1	0	5	2	1	3	3	0	3

Maintenant qu'on a trouvé une fonction qui s'annule pour les nombres premiers et ne s'annule pas pour les autres nombres, on définit une fonction toute simple basée sur elle, et qui compte les nombres premiers

∗. La présente note reprend les idées d'une note de février 2006, Fractale, symétrie et conjecture de Goldbach, http://denisevellachemla.eu/fevrier2006.pdf.

†. Les fonctions définies ici ne doivent pas être confondues avec celles fournissant pour un entier les coefficients intervenant dans leur écriture en base p, i.e. leur écriture comme combinaison linéaire de puissances de p.

‡. Les fonctions discrètes proposées ici rappellent par leur forme les spectres de fréquences de *fonctions sinusoïdales modulées en amplitude. Cf. dessin en annexe et article wikipedia sur la Modulation d'amplitude https://fr.wikipedia.org/wiki/Modulation$'_d$amplitude*

inférieurs ou égaux à un entier donné :

$$\pi_D(x) = \sum_{k=2}^{n/2} \frac{1}{|1 - Sf(x)^{15}|}$$

L'exposant au dénominateur est destiné à augmenter la précision : s'il est trop petit, par exemple s'il est égal à 2, la fonction $\pi_D(x)$ dépasse trop $\pi(x)$; s'il vaut 10, la fonction $\pi_D(x)$ a une différence de 2 avec $\pi(x)$ (1231 au lieu de 1229) pour $x = 10^4$, une différence de 22 (9614 au lieu de 9592 et une différence de 124 (78622 au lieu de 78498) ; s'il vaut 15, il n'y a plus de différence entre $\pi_D(x)$ et $\pi(x)$ jusqu'à 10^6 [§]).*Annexe 1 : programme de calcul de* $\pi_D(x)$

```
#include <iostream>
#include <stdio.h>
#include <cmath>
#include <math.h>

int prime(int atester) {
    bool pastrouve=true;
    unsigned long k = 2;

    if (atester == 1) return 0;
    if (atester == 2) return 1;
    if (atester == 3) return 1;
    if (atester == 5) return 1;
    if (atester == 7) return 1;
    while (pastrouve) {
        if ((k * k) > atester)
            return 1;
        else
            if ((atester % k) == 0)
                return 0 ;
            else k++;
    }
}

int main (int argc, char* argv[]) {
    int n, nmax, p, puiss, tempo, somme ;
    float compte ;
    int valpadique[1000002] ;

    compte = 0.0 ; nmax = 1000000 ;
    for (n = 2 ; n <= nmax ; ++n) {
        for (p = 2 ; p <= n/2 ; ++p)
            valpadique[p] = 0 ;
        somme = 0 ;
        for (p = 2 ; p <= n/2 ; ++p) {
            puiss = 1 ;
            tempo = n ;
            while ((tempo/p > 0) && ((tempo % p) == 0)) {
                tempo = tempo/p ;
                puiss = puiss+1 ;
            }
            valpadique[p] = puiss-1 ;
            somme = somme+valpadique[p] ;
    }
```

§. Avec un exposant au dénominateur de 10, on obtient par $\pi_D(x)$ de meilleures approximations de $\pi(x)$ que celles obtenues par la fonction $Li(10^4) = 1245$, $Li(10^5) = 9629$ ou $Li(10^6) = 78627$, fonction $Li(x)$ bien connue des mathématiciens [¶], ce qui est normal puisqu'on a utilisé les exposants de tous les facteurs intervenant dans les factorisations des nombres...

```

        std::cout << n << "-> " ;
        //ligne au-dessous : precision a 15
        compte = compte+1.0/abs(1.0-pow((float)somme,15)) ;
        if (prime(n))
            std::cout << "\npremier" ;
        else
            std::cout << "\ncompose" ;
        std::cout << " somme " << somme << "\n" ;
        std::cout << " compte " << compte << "\n" ;
    }
}
```

Annexe 2 : quelques illustrations pour fixer les idées
Dessin initial de février 2006

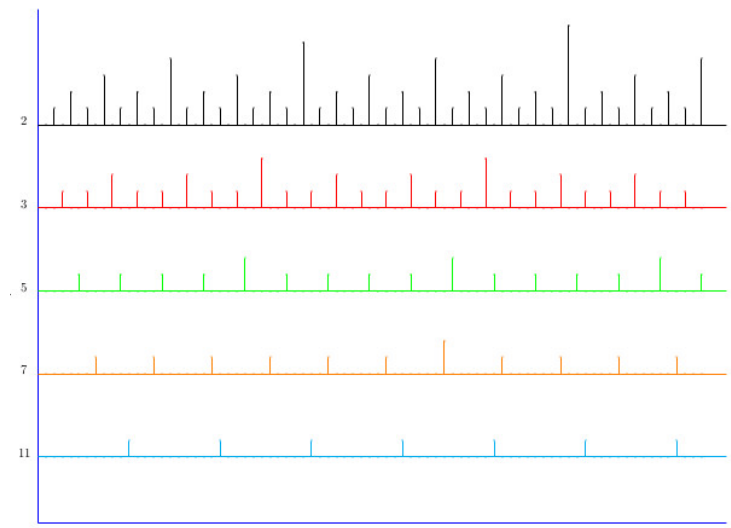
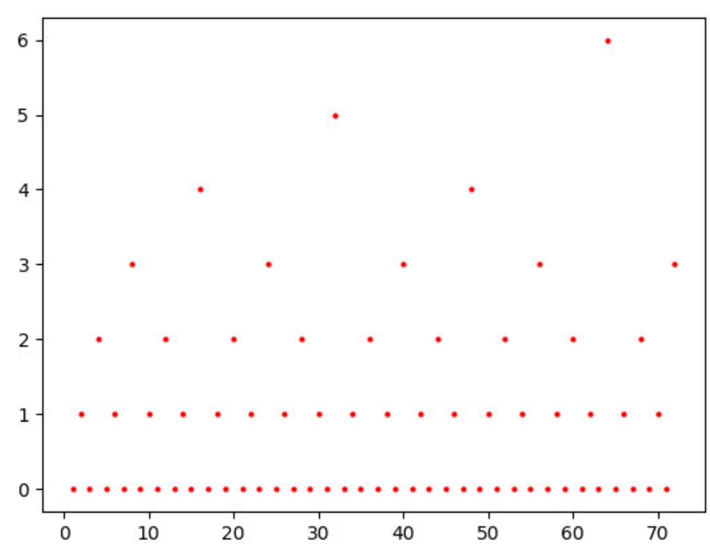
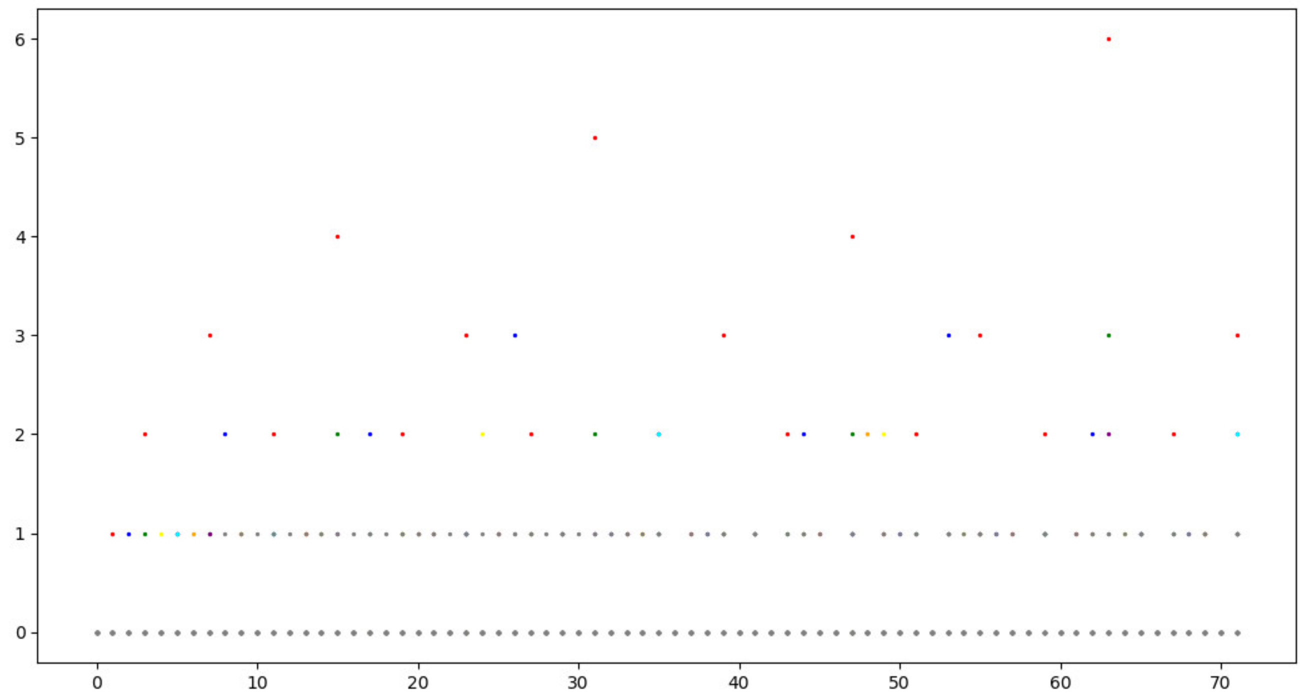


Figure 1 : Séquences fractales de valuations p-adiques

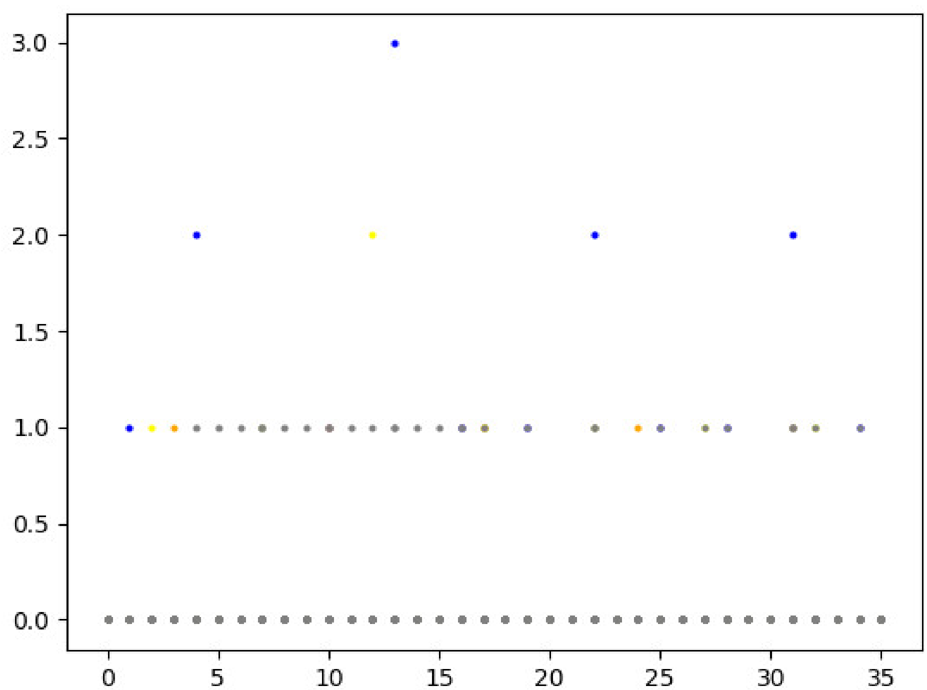
Sortes de valuations 2-adiques (i.e. plus grande puissance de 2 divisant un nombre) des entiers de 1 à 72



Valuations de 1 à 36-adiques des nombres de 1 à 72



Valuations pour les nombres impairs de 3-adiques à 35-adiques des entiers impairs compris entre 1 à 71



Les nombres premiers compris entre 36 et 72 apparaissent "sans points" sur la ligne d'ordonnée égale à 1, $p = 2x + 1$ étant à l'ordonnée x (37 à l'ordonnée 18, 41 à l'ordonnée 20, etc. jusqu'à 71 à l'ordonnée 35).

Compter les nombres composés (Denise Vella-Chemla, 19.9.2018)

On va ici étudier ce qu'il faudrait faire pour compter le nombre de nombres composés compris entre 1 et 100. On souhaite vraiment présenter quel a été notre cheminement.

On fournit d'abord le résultat attendu : de 1 à 100, il y a 25 nombres premiers : 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, soit $\pi(100) = 25$. On oublie 1.

- on compte les puissances "pures" (au moins carrées) de 2, au nombre de 5 (les nombres 4, 8, 16, 32 et 64).
- on compte les puissances de 3, au nombre de 3 (les nombres 9, 27 et 81) ;
- on compte une seule puissance de 5 (son carré 25) ;
- on compte une seule puissance de 7 (son carré 49) ;
- à partir de 11, plus de puissances pures à compter (121 dépasse 100).

On cherche alors à dénombrer les composés, d'une manière combinatoire, en dénombrant tous les produits de 2, 3, ou 4 nombres parmi les possibilités suivantes :

- pour 2, on peut utiliser l'une de ses puissances possibles dans [1,2,3,4,5] ;
- pour 3, on peut utiliser l'une de ses puissances possibles dans [1,2] ;
- pour 5, on pense qu'on ne peut l'utiliser qu'à la puissance 1 ;
- pour 7, on pense qu'on ne peut l'utiliser qu'à la puissance 1 ;

Voici les combinaisons que l'on obtient (l'ordre est sans importance, l'essentiel est de n'oublier aucune possibilité de la combinatoire proposée ci-dessus) :

- un élément dans chacune de deux lignes sur les 4 lignes possibles :

$2{\times}7 = 14$ $2^2 \times 7 = 28$ $2^3 \times 7 = 56$ $2^4 \times 7$ *trop grand* $2{\times}5 = 10$ $2^2 \times 5 = 20$ $2^3 \times 5 = 40$ $2^4 \times 5 = 80$	$2{\times}3 = 6$ $2^2 \times 3 = 12$ $2^3 \times 3 = 24$ $2^4 \times 7 = 48$ $2{\times}3^2 = 18$ $2^2 \times 3^2 = 36$ $2^3 \times 3^2 = 72$ $2^4 \times 3^2$ *trop grand*	$3{\times}7 = 21$ $3^2 \times 7 = 63$ $3{\times}5 = 15$ $3^2 \times 5 = 45$ $5{\times}7 = 35$

- un élément dans chacune de trois lignes sur les 4 lignes possibles :

$2{\times}5 \times 7 = 70$ $2{\times}3 \times 7 = 42$ $2{\times}3 \times 5 = 30$ $2{\times}3^2 \times 7$ *trop grand* $2{\times}3^2 \times 5 = 90$	$2^2 \times 3 \times 7 = 84$ $2^2 \times 3 \times 5 = 60$ $2^2 \times 3^2 \times 7$ *trop grand* $2^2 \times 3^2 \times 5$ *trop grand*	$2^3 \times 3 \times 7$ *trop grand* $2^3 \times 3 \times 5$ *trop grand* $2^3 \times 3^2 \times 7$ *trop grand* $2^3 \times 3^2 \times 5$ *trop grand*	$2^4 \times 3 \times 7$ *trop grand* $2^4 \times 3 \times 5$ *trop grand* $2^4 \times 3^2 \times 7$ *trop grand* $2^4 \times 3^2 \times 5$ *trop grand*

- un élément dans chacune des 4 lignes possibles :

$2{\times}3 \times 5 \times 7$ *trop grand* $2{\times}3^2 \times 5 \times 7$ *trop grand*	$2^2 \times 3 \times 5 \times 7$ *trop grand* $2^2 \times 3^2 \times 5 \times 7$ *trop grand*
$2^3 \times 3 \times 5 \times 7$ *trop grand* $2^3 \times 3^2 \times 5 \times 7$ *trop grand*	$2^4 \times 3 \times 5 \times 7$ *trop grand* $2^4 \times 3^2 \times 5 \times 7$ *trop grand*

Là, on réalise qu'on a oublié de nombreuses possibilités *, que l'on liste ci-dessous, avant de fournir le raisonnement qu'il fallait plutôt mener :

$2 \times 11 = 22$	$3 \times 11 = 33$	$5 \times 11 = 55$	$7 \times 11 = 77$	$2^2 \times 11 = 44$
$2 \times 13 = 26$	$3 \times 13 = 39$	$5 \times 13 = 65$	$7 \times 13 = 91$	$2 \times 5^2 = 50$
$2 \times 17 = 34$	$3 \times 17 = 51$	$5 \times 17 = 85$		$2^2 \times 13 = 52$
$2 \times 19 = 38$	$3 \times 19 = 57$	$5 \times 19 = 95$		$2 \times 3^3 = 54$
$2 \times 23 = 46$	$3 \times 23 = 69$			$2 \times 3 \times 11 = 66$
$2 \times 29 = 58$	$3 \times 29 = 87$			$2^2 \times 17 = 68$
$2 \times 31 = 62$	$3 \times 31 = 93$			$3 \times 5^2 = 75$
$2 \times 37 = 74$				$2^2 \times 19 = 76$
$2 \times 41 = 82$				$2 \times 3 \times 13 = 78$
$2 \times 43 = 86$				$2^3 \times 11 = 88$
$2 \times 47 = 94$				$2^2 \times 23 = 92$
				$2^5 \times 3 = 96$
				$2 \times 7^2 = 98$
				$3^2 \times 11 = 99$
				$2^2 \times 5^2 = 100$

Le raisonnement qu'il fallait plutôt mener est le suivant : supposons que l'on connaisse les nombres premiers (ainsi que leur nombre) qui sont compris entre 1 et $n/2$ (ici 50) et que l'on souhaite connaître le nombre de nombre composés compris entre $n/2$ et n en étudiant combinatoirement les factorisations des nombres composés inférieurs à 100, il faudrait :

- choisir un exposant α_2 pour le nombre premier 2 parmi les nombres de 0 à 6 ;
- choisir un exposant α_3 pour le nombre premier 3 parmi les nombres de 0 à 4 ;
- choisir deux exposants α_5 pour le nombre premier 5 et α_7 pour le nombre premier 7 parmi les nombres de 0 à 2 ;
- choisir 11 exposants $\alpha_{11}, \alpha_{13}, \alpha_{17}, \alpha_{19}, \alpha_{23}, \alpha_{29}, \alpha_{31}, \alpha_{37}, \alpha_{41}, \alpha_{43}, \alpha_{47}$ pour les nombre premiers 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 parmi les nombres de 0 à 1.

Le nombre de combinaisons possibles s'élève à $2^{11} \times 3^2 \times 5 \times 7$.

Parmi toutes ces possibilités, seules celles vérifiant $\sum_i \alpha_i \geq 2$ et $\sum_i p_i^{\alpha_i} \leq 100$ conviennent. Le facteur premier 2 a plus de poids que les autres. On a bien dénombré tous les nombres composés entre 1 et 100 (1 (le nombre) + 10 puissances pures + 64 composés produits = 75) qui retranché de 100 fournit le nombre de nombres premiers 25 mais cette méthode est bien hasardeuse (l'hyper-volume contenant les points tels que $\prod_i p_i^{\alpha_i} \leq 100$ étant difficile à appréhender).

*. 39 %, sans commentaire.

Sommes par lignes d'une matrice et nombres premiers (Denise Vella-Chemla, 23.9.2018)

Soit la matrice M_n suivante, qu'on imagine de taille infinie mais qui sera de taille finie pour les exemples founis ici, et qui contient des 1 en première colonne et dans les autres colonnes, en position $M[i, j]$ la plus grande puissance de j qui divise i.

Fournissons l'exemple d'une telle matrice pour $n = 10$.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 3 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Effectuer les sommes par lignes de M_n fournit une matrice d'une seule colonne dont tous les éléments égaux à 2 sont d'indice un nombre premier. Le programme python qui code cette idée est très court et il semble efficace.

```
import numpy as np

def pgp(x, y):
  e = 0
  while (x/y > 0):
    x = x / y
    e = e + 1
  return e

def elt(x, y):
  return 1 if y == 1 else (pgp(x, y) if x % y == 0 else 0)

import time
tmps1=time.time()
n = input("Entrer n : ")
m = np.array([[elt(x, y) for y in range(1, n+1)] for x in range(1, n+1)])
c1 = np.sum(m, axis=1)
p = [i+1 for i in range(c1.size) if c1[i] == 2]
print(p)
print(len(p))
print(c1.size)
tmps2=time.time()-tmps1
print "Temps d'execution avec matrices = %f" %tmps2
```

Voici la table des sommes par lignes pour les entiers de 1 à 100.

lod(1) = 1	lod(21) = 4	lod(41) = 2	lod(61) = 2	lod(81) = 9
lod(2) = 2	lod(22) = 4	lod(42) = 8	lod(62) = 4	lod(82) = 4
lod(3) = 2	lod(23) = 2	lod(43) = 2	lod(63) = 7	lod(83) = 2
lod(4) = 4	lod(24) = 10	lod(44) = 7	lod(64) = 15	lod(84) = 13
lod(5) = 2	lod(25) = 4	lod(45) = 7	lod(65) = 4	lod(85) = 4
lod(6) = 4	lod(26) = 4	lod(46) = 4	lod(66) = 8	lod(86) = 4
lod(7) = 2	lod(27) = 6	lod(47) = 2	lod(67) = 2	lod(87) = 4
lod(8) = 6	lod(28) = 7	lod(48) = 4	lod(68) = 7	lod(88) = 10
lod(9) = 4	lod(29) = 2	lod(49) = 4	lod(69) = 4	lod(89) = 2
lod(10) = 4	lod(30) = 8	lod(50) = 7	lod(70) = 8	lod(90) = 13
lod(11) = 2	lod(31) = 2	lod(51) = 4	lod(71) = 2	lod(91) = 4
lod(12) = 7	lod(32) = 11	lod(52) = 7	lod(72) = 16	lod(92) = 7
lod(13) = 2	lod(33) = 4	lod(53) = 2	lod(73) = 2	lod(93) = 4
lod(14) = 4	lod(34) = 4	lod(54) = 10	lod(74) = 4	lod(94) = 4
lod(15) = 4	lod(35) = 4	lod(55) = 4	lod(75) = 7	lod(95) = 4
lod(16) = 9	lod(36) = 12	lod(56) = 10	lod(76) = 7	lod(96) = 17
lod(17) = 2	lod(37) = 2	lod(57) = 4	lod(77) = 4	lod(97) = 2
lod(18) = 7	lod(38) = 4	lod(58) = 4	lod(78) = 8	lod(98) = 7
lod(19) = 2	lod(39) = 4	lod(59) = 2	lod(79) = 2	lod(99) = 7
lod(20) = 7	lod(40) = 10	lod(60) = 13	lod(80) = 14	lod(100) = 12

La définition des éléments de la matrice M qu'on a utilisée est :

$$\begin{array}{lll}
\forall y \in \mathbb{N}, & M[1,y] & = 1 \\
\forall x > 1, y \in \mathbb{N}, & M[yx,y] & = 0 \qquad \textit{si y ne divise pas x} \ \ (\mathrm{y} \nmid x) \\
 & & = M[x,y]+1 \quad \textit{sinon}
\end{array}$$

Si on remplace dans le programme l'appel à la fonction $pgp(x,y)$ (qui fournit la plus grande puissance de y divisant x) par 1, on peut définir ainsi la valeur des éléments de la matrice P :

$$\begin{array}{lll}
\forall x \in \mathbb{N}, & P[x,x] & = 1 \\
\forall x,y \in \mathbb{N}\times\mathbb{N}, & P[x,y] & = 0 \qquad \textit{si } y > x \\
 & & = P[x-y,y] \quad \textit{sinon.}
\end{array}$$

$$P = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

En calculant les sommes par lignes de cette matrice, on obtient comme attendu ligne par ligne le nombre de diviseurs de chaque entier et à nouveau, les éléments d'image 2 sont les nombres premiers :

nbdiv(1) = 1	nbdiv(21) = 4	nbdiv(41) = 2	nbdiv(61) = 2	nbdiv(81) = 5
nbdiv(2) = 2	nbdiv(22) = 4	nbdiv(42) = 8	nbdiv(62) = 4	nbdiv(82) = 4
nbdiv(3) = 2	nbdiv(23) = 2	nbdiv(43) = 2	nbdiv(63) = 6	nbdiv(83) = 2
nbdiv(4) = 3	nbdiv(24) = 8	nbdiv(44) = 6	nbdiv(64) = 7	nbdiv(84) = 12
nbdiv(5) = 2	nbdiv(25) = 3	nbdiv(45) = 6	nbdiv(65) = 4	nbdiv(85) = 4
nbdiv(6) = 4	nbdiv(26) = 4	nbdiv(46) = 4	nbdiv(66) = 8	nbdiv(86) = 4
nbdiv(7) = 2	nbdiv(27) = 4	nbdiv(47) = 2	nbdiv(67) = 2	nbdiv(87) = 4
nbdiv(8) = 4	nbdiv(28) = 6	nbdiv(48) = 10	nbdiv(68) = 6	nbdiv(88) = 8
nbdiv(9) = 3	nbdiv(29) = 2	nbdiv(49) = 3	nbdiv(69) = 4	nbdiv(89) = 2
nbdiv(10) = 4	nbdiv(30) = 8	nbdiv(50) = 6	nbdiv(70) = 8	nbdiv(90) = 12
nbdiv(11) = 2	nbdiv(31) = 2	nbdiv(51) = 4	nbdiv(71) = 2	nbdiv(91) = 4
nbdiv(12) = 6	nbdiv(32) = 6	nbdiv(52) = 6	nbdiv(72) = 12	nbdiv(92) = 6
nbdiv(13) = 2	nbdiv(33) = 4	nbdiv(53) = 2	nbdiv(73) = 2	nbdiv(93) = 4
nbdiv(14) = 4	nbdiv(34) = 4	nbdiv(54) = 8	nbdiv(74) = 4	nbdiv(94) = 4
nbdiv(15) = 4	nbdiv(35) = 4	nbdiv(55) = 4	nbdiv(75) = 6	nbdiv(95) = 4
nbdiv(16) = 5	nbdiv(36) = 9	nbdiv(56) = 8	nbdiv(76) = 6	nbdiv(96) = 12
nbdiv(17) = 2	nbdiv(37) = 2	nbdiv(57) = 4	nbdiv(77) = 4	nbdiv(97) = 2
nbdiv(18) = 6	nbdiv(38) = 4	nbdiv(58) = 4	nbdiv(78) = 8	nbdiv(98) = 6
nbdiv(19) = 2	nbdiv(39) = 4	nbdiv(59) = 2	nbdiv(79) = 2	nbdiv(99) = 6
nbdiv(20) = 6	nbdiv(40) = 8	nbdiv(60) = 12	nbdiv(80) = 10	nbdiv(100) = 9

Une fonction de comptage des nombres premiers (Denise Vella-Chemla, 14.9.2018)

On définit ci-dessous une fonction $f_b(x)$ paramétrée par un entier b (la base, qui n'est pas forcément un nombre premier).

Cette fonction est définie sur l'ensemble des entiers naturels $\mathbb{N}$.

Elle permet d'"isoler" une puissance de la base dans l'écriture d'un nombre entier sous la forme d'un produit ainsi * :

$$f_b(kb^y) = y \text{ avec } b \not| \, k.$$

Cette fonction coïncide avec la valuation p-adique $v_p(n)$ qui est définie sur $\mathbb{Q}$ et selon p un nombre premier †.

$$y \text{ est l'exposant maximum tel que } \; b^y \mid n.$$

Les images des 30 premiers entiers par les fonctions f_2, f_3, f_4, f_5 sont :

x	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
$f_2(x)$	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
$f_3(x)$	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
$f_4(x)$	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	2	0	0	0	1	0	0	0	1	0	0	0	1	0	0
$f_5(x)$	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	2	0	0	0	0	1

Ces fonctions ont un comportement similaire à celui du logarithme : par exemple, $f_k(kx) = f_k(x) + 1$. Cependant, elles ne coïncident avec les logarithmes en base k que pour les x qui sont des puissances des différents k. Entre ces puissances, les logarithmes en base k croissent lentement sur $\mathbb{R}$ tandis que les $f_k(x)$ sont très souvent nulles et entrecoupées de valeurs erratiques tous les k nombres.

On remarque dans chaque séquence les multiples occurrences d'une sous-séquence répétitive, qui rappelle la notion de motif musical, ces motifs étant palindromiques ‡ :

- multiples occurrences du "motif" 010 dans la séquence des $f_2(x)$, entre lesquelles s'intercalent les valeurs 2, 3, 2, 4, etc.
- multiples occurrences du "motif" 00100100 dans la séquence des $f_3(x)$, entre lesquelles s'intercalent les valeurs 2, 2, 3, 2, 2, 3, 2, 2, 4, etc.
- multiples occurrences du "motif" $(0^{p-1}1)^{p-1}0^{p-1}$ dans la séquence des $f_p(x)$, entre lesquelles s'intercalent les valeurs 2 ($p-1$ fois), etc.

La fonction $Sf(n,x)$ qui associe à n la somme des valeurs des $f(n,x)$ pour x un entier compris entre 2 et $\lfloor \sqrt{n} \rfloor$, associe comme image 1 aux nombres premiers (> 1) et associe comme image un entier strictement supérieur à 1 aux nombres composés.

$$Sf(n) = \sum_{2 \leq x \leq \lfloor \sqrt{n} \rfloor} f(n,x)$$

Les valeurs $Sf(x)$ sont fournies ci-dessous pour les premiers entiers :

x	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
$Sf(x)$	1	1	3	1	2	1	4	3	2	1	4	1	2	2	7	1	4	1	4	2	2	1	6	3	2	4	4	1	4

Maintenant qu'on a trouvé une fonction qui vaut 1 pour les nombres premiers et est strictement supérieure à 1 pour les nombres composés, on définit une fonction toute simple basée sur elle, et qui compte les nombres premiers inférieurs ou égaux à un entier donné :

$$\pi_D(x) = \left\lfloor \sum \frac{1}{Sf(x)} \right\rfloor$$

Cette fonction compte le nombre de nombres premiers inférieurs ou égaux à x.

*. La présente note reprend les idées d'une note de février 2006, Fractales, symétrie et conjecture de Goldbach, http://denisevellachemla.eu/fevrier2006.pdf.

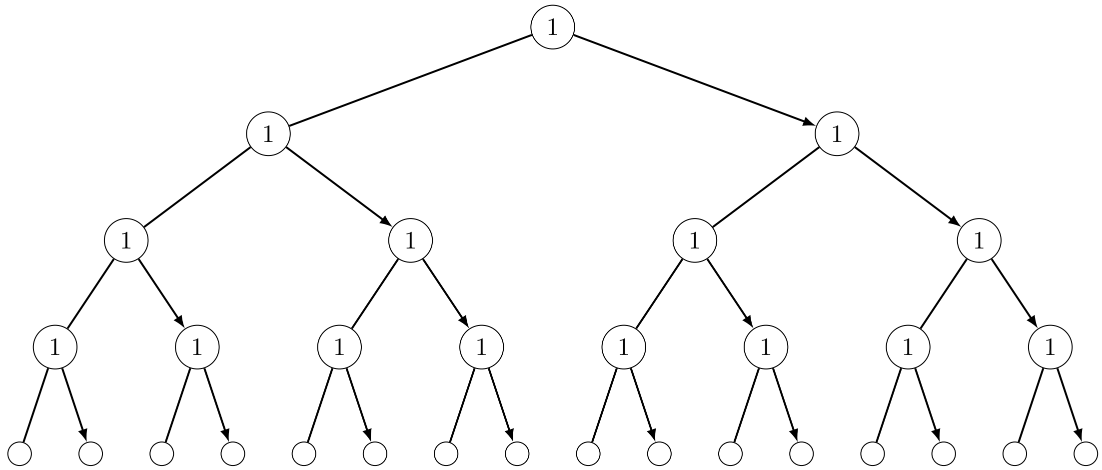
†. Les fonctions définies ici ne doivent pas être confondues avec celles fournissant pour un entier les coefficients intervenant dans leur écriture en base p, i.e. leur écriture comme combinaison linéaire de puissances de p.

‡. Les fonctions discrètes proposées ici rappellent par leur forme les spectres de fréquences de *fonctions sinusoïdales modulées en amplitude. Cf. dessin en annexe et article wikipedia sur la Modulation d'amplitude https://fr.wikipedia.org/wiki/Modulation$'_d$amplitude*

Annexe : programme de calcul de $\pi_D(x)$

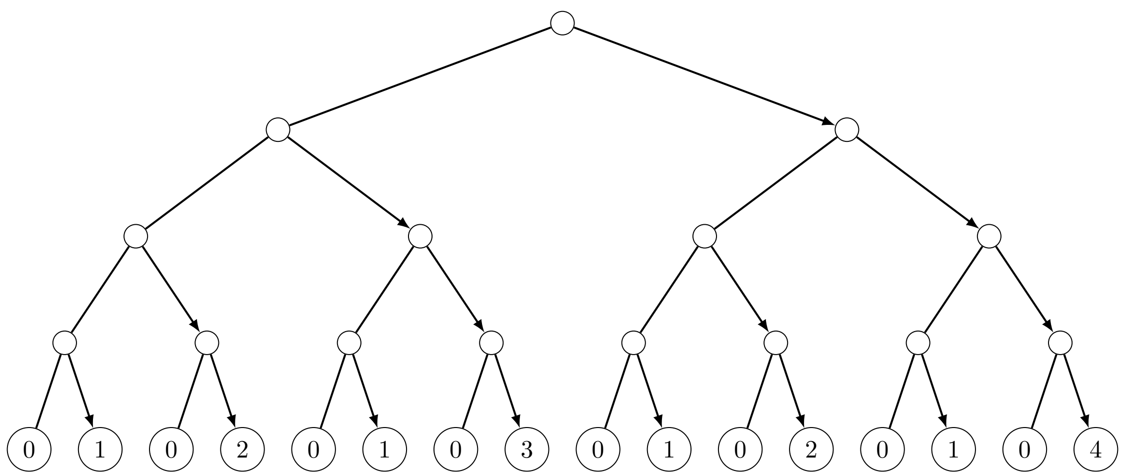
```
#include <iostream>
#include <stdio.h>
#include <cmath>
#include <math.h>

int prime(int atester) {
  bool pastrouve=true;
  unsigned long k = 2;

  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve)
    if ((k * k) > atester)
      return 1;
    else
      if ((atester % k) == 0) return 0 ;
      else k++;
}

int main (int argc, char* argv[]) {
  int n, nmax, p, puiss, tempo, somme ;
  float compte ;
  int valpadique[1000002] ;

  compte = 0.0 ;
  nmax = 1000 ;
  for (n = 2 ; n <= nmax ; ++n) {
      std::cout << "\n" << n << " -> " ;
      for (p = 2 ; p <= sqrt(n) ; ++p)
        valpadique[p] = 0 ;
      somme = 1 ;
      for (p = 2 ; p <= sqrt(n) ; ++p) {
        puiss = 1 ;
        tempo = n ;
        while ((tempo/p > 0) && ((tempo % p) == 0)) {
          tempo = tempo/p ;
          puiss = puiss+1 ;
        }
      valpadique[p] = puiss-1 ;
      somme = somme+valpadique[p] ;
    }
    compte = compte+floor(1.0/(float)somme) ;
    if (prime(n))
      std::cout << " premier" ;
    else
      std::cout << " compose" ;
    std::cout << "   somme " << somme ;
    std::cout << "   compte " << compte << "\n" ;
  }
}
```

Arbres (Denise Vella-Chemla, 29.9.2018)

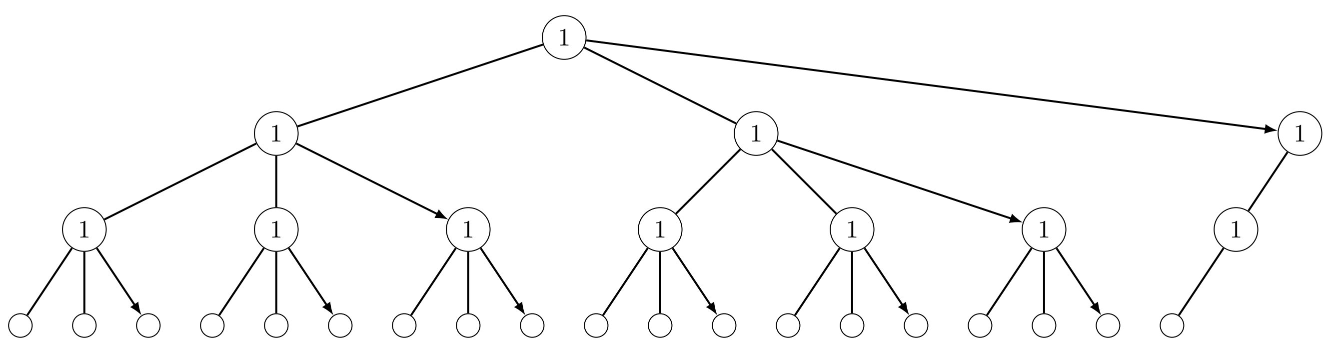


Ci-dessus, un arbre binaire sur lequel on applique un “transfert de jetons” le plus longtemps possible pour en étiqueter les feuilles [*].

On obtient l'arbre à feuilles étiquetées suivant :

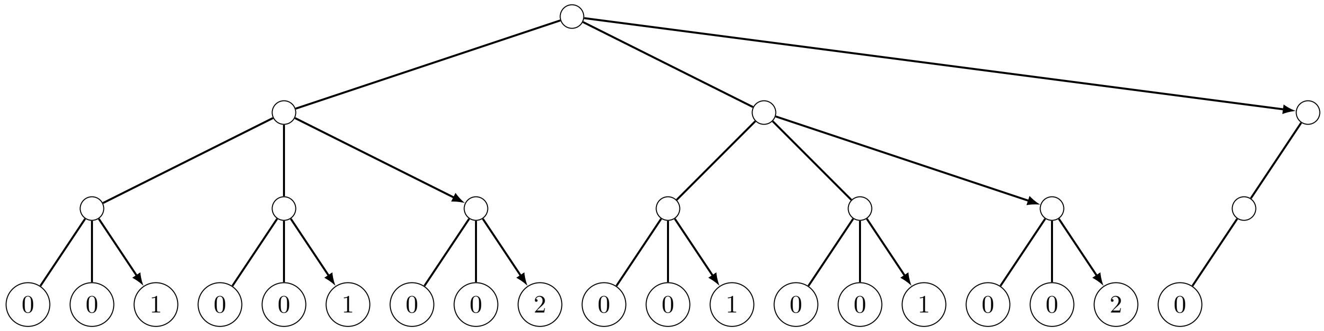


Procédons maintenant sur un arbre ayant le même nombre de feuilles (16) que l'arbre précédent, mais qui est un arbre ternaire,



On obtient les étiquettes suivantes pour les feuilles :

*. On a utilisé le site http://math.et.info.free.fr/TikZ/Arbre/ très pratique pour générer le code TikZ.



On imagine des arbres 4-naires, 5-naires, etc., fabriqués selon la même idée : les jetons des noeuds intérieurs de l'arbre n'ont le droit d'être distribués qu'aux "derniers" fils à chaque fois (fils à l'extrémité droite d'une fratrie). Le chip-firing "calcule" de cette étrange manière, comme étiquette de la n-ième feuille, dans l'arbre x-naire, quelle est la plus grande puissance de x qui divise n.

Ennuyée (Denise Vella-Chemla, 4.10.2018)

On voudrait expliquer ce qui nous bloque là.
Idéalement, pour compter aisément les nombres premiers, on aurait besoin, selon le diviseur 2, d'avoir une fonction qui associe comme images aux entiers successifs la suite :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
0	1	0	2	0	1	0	3	0	1	0	2	0	1	0	4	...

A la place de cette fonction, on dispose du *log* en base 2, bien régulier, et qui fournit ces valeurs :

1 0	2 1	3 1, ...	4 2	5 2, ...	6 2, ...	7 2, ...	8 3	9 3, ...	10 3, ...	11 3, ...	12 3, ...	13 3, ...	14 3, ...	15 3, ...	16 4
17 4, ...	... ...														

Les deux fonctions coïncident sur les puissances de 2. Entre deux puissances de 2, il y a $2^{k+1} - 2^k - 1$ nombres non entiers de parties entières égales.
Selon le diviseur 3, on voudrait :

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
0	0	1	0	0	1	0	0	2	0	0	1	0	0	1	0	...

alors qu'on a :

1	2	3	...	9	...	27	...	81	...
0	0, ...	1	1, ...	2	2, ...	3	3, ...	4	...
	(*au nombre de* 5)		(*au nombre de* 17)		(*au nombre de* 53)				

Les fonctions qui nous intéresseraient associent presque tout le temps aux nombres l'image 0 ; de temps en temps, elles associent aux nombres l'image 1, moins souvent, elles leur associent l'image 2, encore moins souvent, l'image 3, etc.

Par moins souvent, il faut comprendre logarithmiquement en base x moins souvent.

Le nombre de nombres à virgules de même partie entière qui se succèdent (ce qu'on a noté entre parenthèses par des *"au nombre de"*) est toujours égal à $x^{k+1} - x^k - 1$.

Et ce qui reste extraordinaire, c'est le fait de réussir à approximer $\pi(x)$ par $Li(x) = li(x) - li(2)$.

$li(x)$ prend les valeurs suivantes :

li(1)=-inf	li(21)=10.2363	li(41)=16.1097	li(61)=21.2091	li(81)=25.9064
li(2)=1.0451	li(22)=10.5623	li(42)=16.3781	li(62)=21.4519	li(82)=26.1336
li(3)=2.1635	li(23)=10.8835	li(43)=16.6448	li(63)=21.6937	li(83)=26.3602
li(4)=2.9675	li(24)=11.2003	li(44)=16.9098	li(64)=21.9346	li(84)=26.5862
li(5)=3.6345	li(25)=11.5129	li(45)=17.1733	li(65)=22.1746	li(85)=26.8116
li(6)=4.2222	li(26)=11.8217	li(46)=17.4353	li(66)=22.4137	li(86)=27.0364
li(7)=4.7570	li(27)=12.1268	li(47)=17.6957	li(67)=22.6520	li(87)=27.2606
li(8)=5.2537	li(28)=12.4286	li(48)=17.9547	li(68)=22.8894	li(88)=27.4843
li(9)=5.7212	li(29)=12.7271	li(49)=18.2124	li(69)=23.1260	li(89)=27.7073
li(10)=6.1655	li(30)=13.0226	li(50)=18.4686	li(70)=23.3618	li(90)=27.9298
li(11)=6.5910	li(31)=13.3152	li(51)=18.7236	li(71)=23.5967	li(91)=28.1518
li(12)=7.00054	li(32)=13.6050	li(52)=18.9773	li(72)=23.8310	li(92)=28.3732
li(13)=7.3965	li(33)=13.8923	li(53)=19.2298	li(73)=24.0644	li(93)=28.5941
li(14)=7.7808	li(34)=14.1771	li(54)=19.4811	li(74)=24.2971	li(94)=28.8145
li(15)=8.1548	li(35)=14.4595	li(55)=19.7312	li(75)=24.5291	li(95)=29.0343
li(16)=8.5197	li(36)=14.7396	li(56)=19.9802	li(76)=24.7603	li(96)=29.2537
li(17)=8.8764	li(37)=15.0176	li(57)=20.2281	li(77)=24.9909	li(97)=29.4725
li(18)=9.2258	li(38)=15.2936	li(58)=20.4749	li(78)=25.2208	li(98)=29.6908
li(19)=9.5686	li(39)=15.5675	li(59)=20.7206	li(79)=25.4500	li(99)=29.9087
li(20)=9.9052	li(40)=15.8395	li(60)=20.9654	li(80)=25.6785	li(100)=30.1261

On réalise par programme que si l'on remplace le signe de l'intégrale définissant $li(x) = \displaystyle\int_0^x \frac{dt}{ln\ t}$ par un signe somme et qu'on somme à partir de 2, la somme obtenue semble approximer le nombre de nombres premiers inférieurs ou égaux à x de la même façon que le fait le logarithme intégral.

Il faudrait du coup réussir à comprendre pourquoi $g(x) = \displaystyle\sum_{k=2}^{x} \frac{1}{ln\ k}$ permet de compter $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x.

La somme des inverses des logarithmes népériens vaut par exemple 78627 pour 10^6 quand $\pi(x)$ vaut 78498.

Elle vaut 664918 pour 10^7 quand $\pi(x)$ vaut 664579.

Réfléchissons aux fonctions $f_y(x) = \dfrac{1}{log_y(x)}$, par exemple aux fonctions $f_2(x) = \dfrac{1}{log_2(x)}$ ou $f_3(x) = \dfrac{1}{log_3(x)}$.

On a $f_2(4) = \dfrac{1}{2}$ ou $f_2(8) = \dfrac{1}{3}$ car $4^{\frac{1}{2}} = 2$ ou $8^{\frac{1}{3}} = 2$.

On a de même $f_3(9) = \dfrac{1}{2}$ ou $f_3(27) = \dfrac{1}{3}$ car $9^{\frac{1}{2}} = 3$ ou $27^{\frac{1}{3}} = 3$.

La fonction plus générale (en base e) $f(x) = \dfrac{1}{ln\ x}$ associe à x la puissance à laquelle il faut élever x pour trouver e.

La fonction qu'on a proposée $g(x) = \displaystyle\sum_{k=2}^{x} \frac{1}{ln\ k}$ calcule quant à elle pour un nombre donné x la somme pour les nombres entiers successifs jusqu'à x des puissances auxquelles il faut élever ces nombres pour trouver e.

Comment faire intervenir la factorielle dans tout ça ? On sait qu'un nombre premier est à puissance 1 dans sa propre factorielle tandis qu'un nombre composé est à puissance au moins 2 dans sa propre factorielle.

$$\begin{array}{cccccc} g(x) & = \dfrac{1}{ln\ 2} & + \dfrac{1}{ln\ 3} & + \dfrac{1}{ln\ 4} & + \ldots & + \dfrac{1}{ln\ x} \\ & f(2) & f(3) & f(4) & \ldots & f(x) \end{array}$$

On rappelle que :

$$\begin{array}{l} e^{f(2)} = 2 \\ e^{f(3)} = 3 \\ e^{f(4)} = 4 \\ \ldots \\ e^{f(x)} = x \end{array}$$

On a donc :

$$x! = \Gamma(x) = e^{f(2)}.e^{f(3)}.e^{f(3)}.\ldots.e^{f(x)}$$

Mais on n'arrive vraiment pas bien à voir ce qui se passe : on a l'impression que les nombres premiers sont les points fixes d'une fonction spéciale (qui associe à un nombre laquelle de ses puissances intervient dans la factorisation de sa propre factorielle) ; ou bien on peut également considérer que les nombres premiers sont les seuls nombres qui ont pour image l'élément neutre (si on s'intéresse plutôt à la fonction qui associe à un nombre la puissance à laquelle il se trouve élevé dans la factorisation de sa propre factorielle) ; et cela a peut-être pour conséquence que les zéros sont sur la droite critique, mais tout ça n'est pas clair du tout...

Toujours est-il qu'on aimerait comprendre pourquoi le spectre de cet opérateur, si on considère qu'on a présenté ici un opérateur matriciel dont la matrice est diagonale et qui associe à un entier l'inverse de son logarithme népérien, fournit des valeurs très approchées de $\pi(x)$.

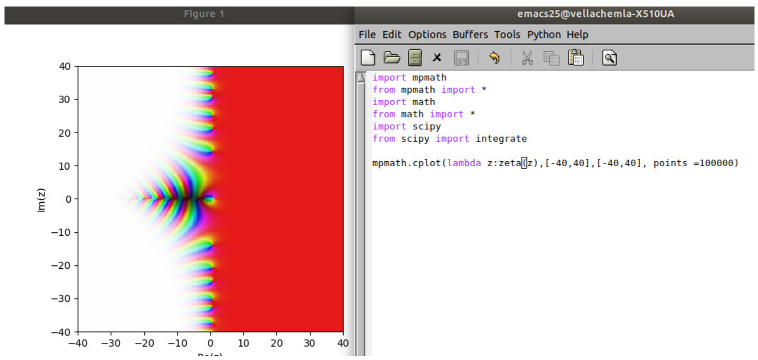
Danses serpentines (Denise Vella-Chemla, 6.10.2018)

On a constaté par programme que l'on peut compter les nombres premiers sur les entiers par une somme plutôt simple :

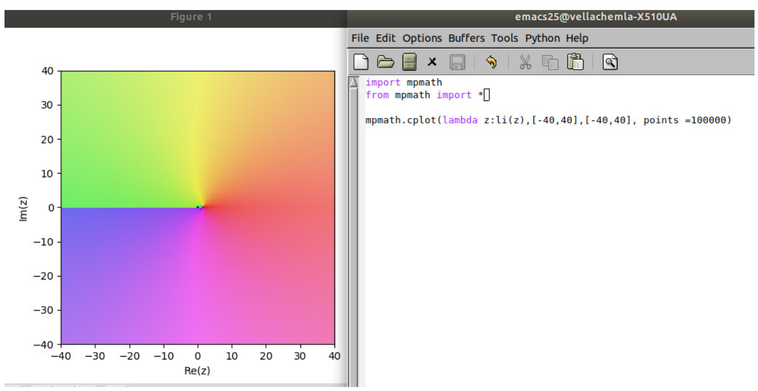
$$\pi(x) \approx \sum_{k=2}^{x} \frac{1}{ln\ k}$$

On voudrait comprendre pourquoi la fonction zêta a tous ses zéros sur la droite critique (droite des complexes de partie réelle 1/2). On exécute plusieurs programmes python à la recherche de ce qui "donne leur forme" à différentes fonctions.

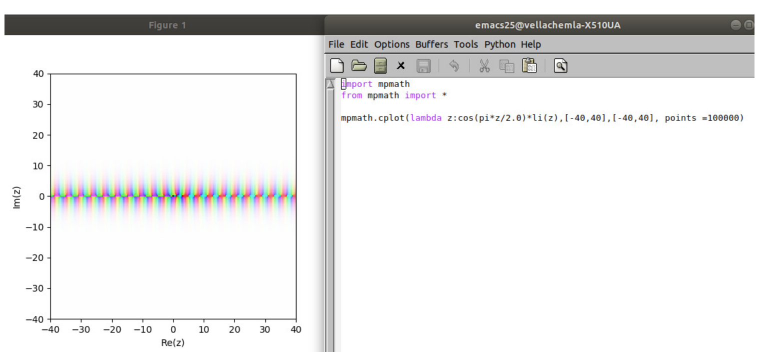
1) *fonction* $\zeta(s)$



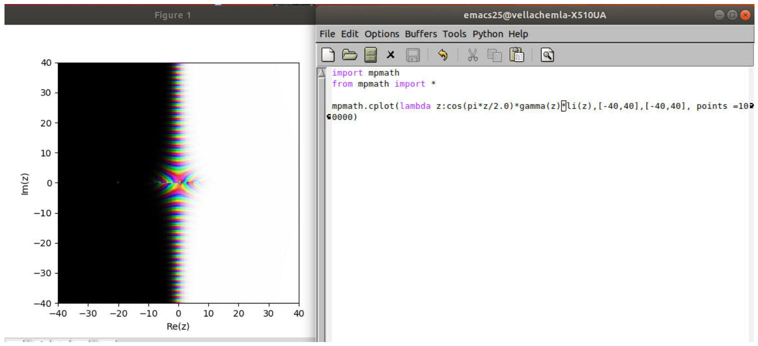
2) *fonction li s*



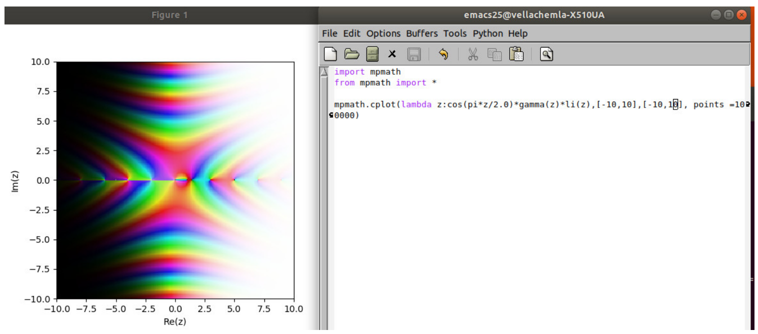
3) *fonction* $\cos \dfrac{\pi\ s}{2}\ li\ s$



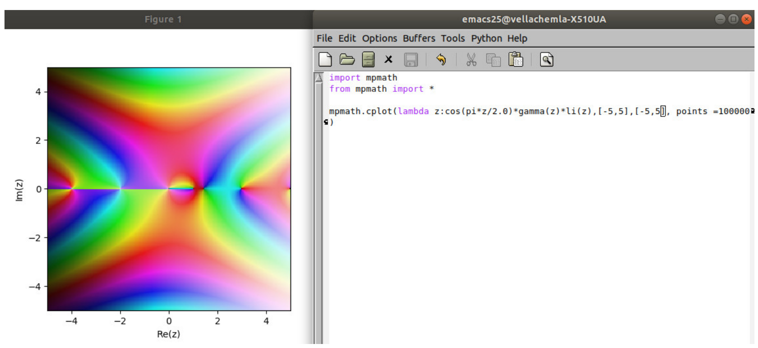
4) *fonction* $\cos\dfrac{\pi\ s}{2}\ \Gamma(s)\ li\ s$



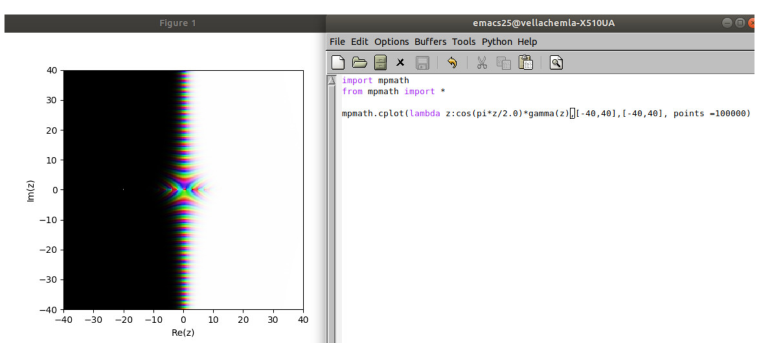
5) *idem zoomée*



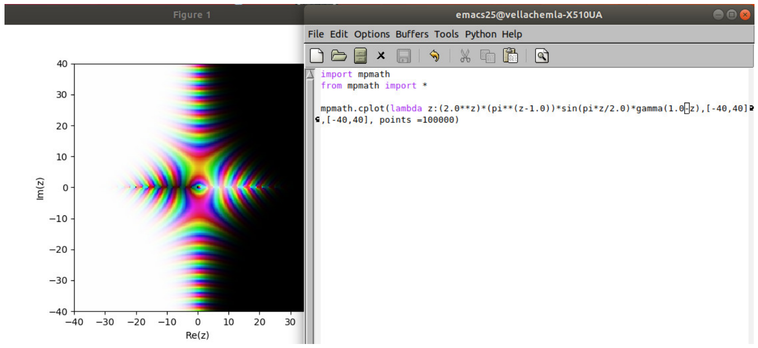
6) *idem très zoomée*



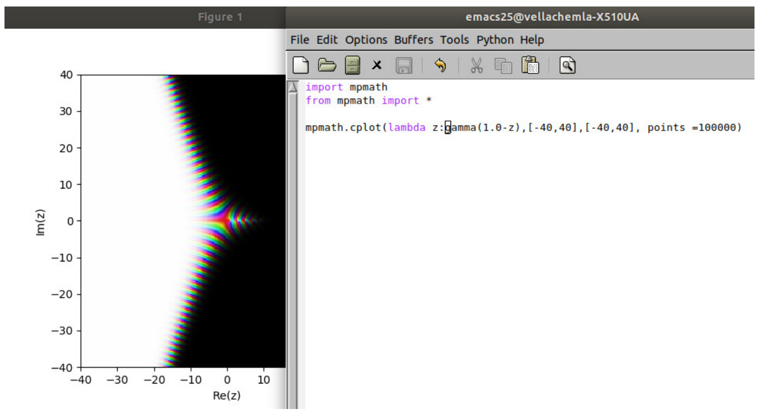
7) *fonction* $\cos\dfrac{\pi\ s}{2}\ \Gamma(s)$



8) *fonction* $2^s \pi^{s-1} \sin \dfrac{\pi\ s}{2}\ \Gamma(1-s)$



9) *fonction* $\Gamma(1-s)$



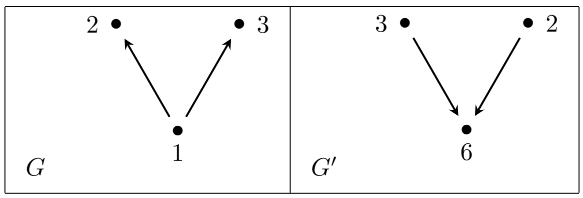
note : plutôt que de penser aux robes de Jean-Paul Gaultier, se concentrer sur l'objectif...

Arêtes (Denise Vella-Chemla, 14.10.2018)

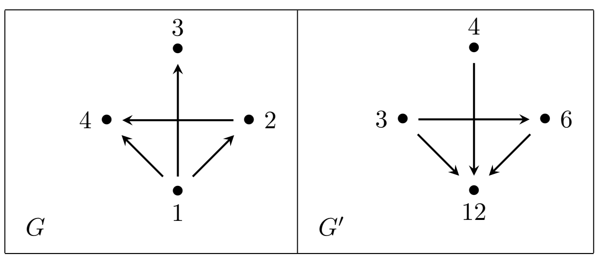
Quand on fait calculer au logiciel WolframAlpha Mathematica[*] les solutions complexes de l'équation $1+\dfrac{1}{2^s}+\dfrac{1}{3^s}=0$, le logiciel réécrit l'équation en $6^{-s}(2^s+3^s+6^s)=0$. Cela nous a intriguée et amenée à étudier les graphes de divisibilité des entiers successifs dont on ajoute, dans les équations ci-dessus, soit des puissances complexes, soit des inverses de puissances complexes.

Fournissons les premiers graphes et pour chacun d'eux un graphe qu'on va appeler son *graphe inversé*. Si on note $ppcm(\{1,\ldots,i\})$ le plus petit commun multiple des entiers de 1 à i, à chacun des sommets du graphe G associé à un entier k compris entre 1 et i correspond le sommet du graphe inversé G' correspondant à l'entier $\dfrac{ppcm(\{1,\ldots,i\})}{k}$. A toute arête orientée du graphe G entre les sommets A et B exprimant que $A|B$ correspond l'arête orientée dans le sens opposé du graphe inversé exprimant le fait que $B'|A'$.

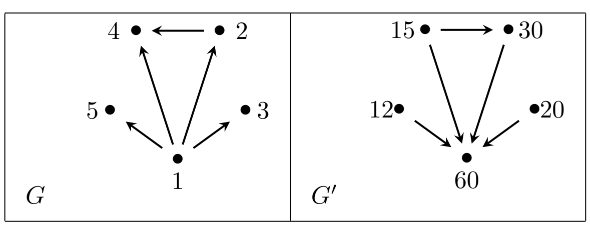
Le plus petit commun multiple des 3 premiers entiers est 6.
On a les graphes orientés ci-dessous pour les relations de divisibilité :



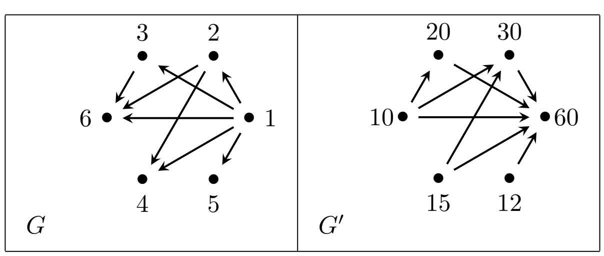
Le plus petit commun multiple des 4 premiers entiers est 12.



Le plus petit commun multiple des 5 premiers entiers est 60.

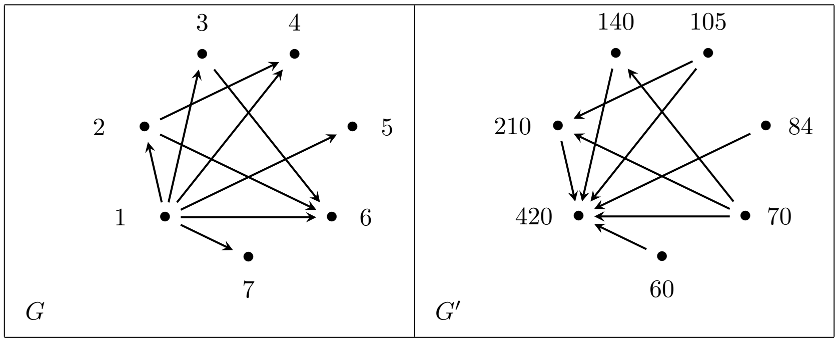


Le plus petit commun multiple des 6 premiers entiers est 60.



∗. version en ligne à l'adresse https://www.wolframalpha.com/

Le plus petit commun multiple des 7 premiers entiers est 420.



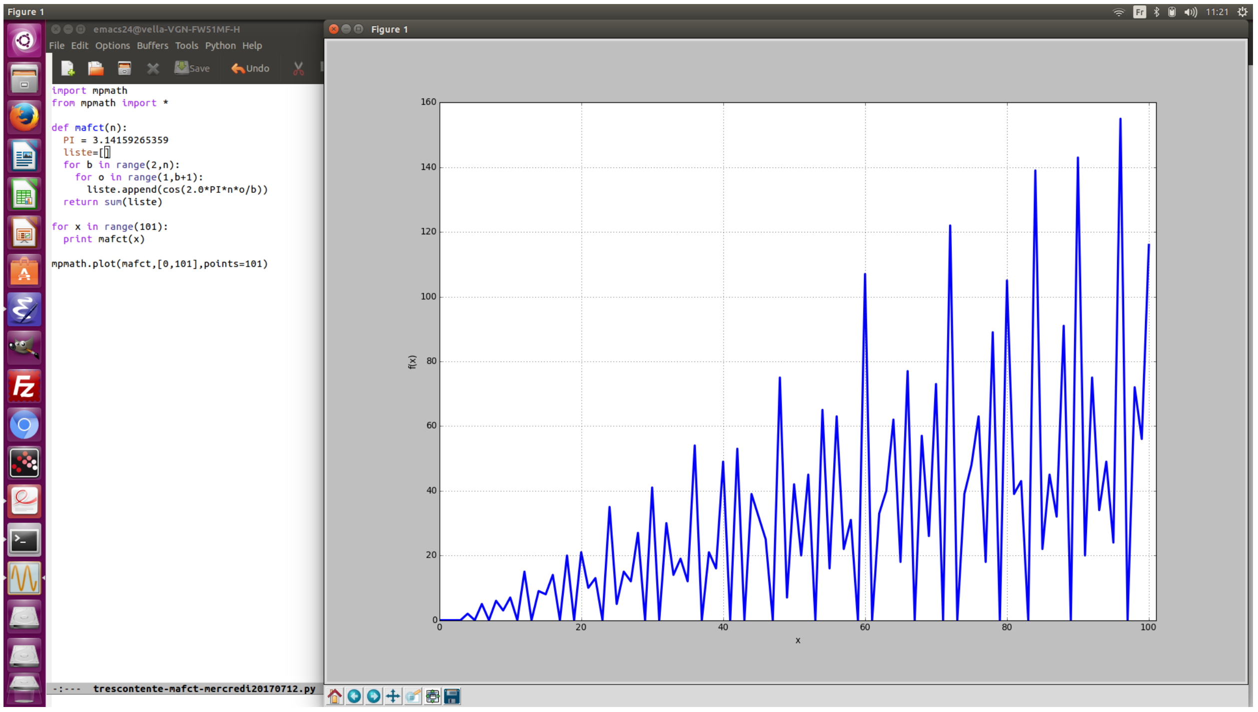
Ci-dessous les nombres d'arêtes des graphes pour les nombres de 1 à 100. Si $A(k) - A(k-1) = 1$ alors k est premier (on a retrouvé ces nombres dans la suite de l'On-Line Encyclopedia of Integer Sequences $A002541$).

A(1)=0	A(21)=49	A(41)=119	A(61)=202	A(81)=292
A(2)=1	A(22)=52	A(42)=126	A(62)=205	A(82)=295
A(3)=2	A(23)=53	A(43)=127	A(63)=210	A(83)=296
A(4)=4	A(24)=60	A(44)=132	A(64)=216	A(84)=307
A(5)=5	A(25)=62	A(45)=137	A(65)=219	A(85)=310
A(6)=8	A(26)=65	A(46)=140	A(66)=226	A(86)=313
A(7)=9	A(27)=68	A(47)=141	A(67)=227	A(87)=316
A(8)=12	A(28)=73	A(48)=150	A(68)=232	A(88)=323
A(9)=14	A(29)=74	A(49)=152	A(69)=235	A(89)=324
A(10)=17	A(30)=81	A(50)=157	A(70)=242	A(90)=335
A(11)=18	A(31)=82	A(51)=160	A(71)=243	A(91)=338
A(12)=23	A(32)=87	A(52)=165	A(72)=254	A(92)=343
A(13)=24	A(33)=90	A(53)=166	A(73)=255	A(93)=346
A(14)=27	A(34)=93	A(54)=173	A(74)=258	A(94)=349
A(15)=30	A(35)=96	A(55)=176	A(75)=263	A(95)=352
A(16)=34	A(36)=104	A(56)=183	A(76)=268	A(96)=363
A(17)=35	A(37)=105	A(57)=186	A(77)=271	A(97)=364
A(18)=40	A(38)=108	A(58)=189	A(78)=278	A(98)=369
A(19)=41	A(39)=111	A(59)=190	A(79)=279	A(99)=374
A(20)=46	A(40)=118	A(60)=201	A(80)=288	A(100)=382

Alterner les termes de la somme de cosinus qui s'annule pour les nombres premiers (Denise Vella-Chemla, 28.10.2018)

On a proposé en juillet 2014 [*] la caractérisation suivante des nombres premiers (motivée par le fait que si p est un nombre premier, $\sigma(p) = p + 1$ [†]) :

$$n \text{ est premier} \iff \sum_{b=2}^{n-1} \sum_{o=1}^{b} cos \frac{2\pi n o}{b} = 0$$



On trouve ici une démonstration du fait que cette caractérisation des nombres premiers en est bien une : http://denise.vella.chemla.free.fr/VictorVarinKeldyshSumsumcos.pdf.

Il s'agit d'une caractérisation triviale des nombres premiers dans le sens où elle calcule la somme des diviseurs des entiers successifs par le biais de calcul d'angles et par le test du fait que ces angles sont ou non multiples de 2π. Cela revient au même pour tester si un nombre est premier qu'à étudier sa division par tous les entiers qui lui sont inférieurs [‡].

Voyons comment la somme de cosinus calcule la somme des diviseurs de 2, 3, 4 et 5. On note les angles en degrés pour que la divisibilité se voie mieux. θ dénote les angles dont sont calculés les cosinus.

∗. cf http://denise.vella.chemla.free.fr/primesommecos.pdf.

†. $\sigma(n)$ est la notation habituelle pour la somme des diviseurs de n.

‡. Cf page 9 de la première note qu'on avait écrite au sujet de la conjecture de Goldbach en septembre 2005.

n	$o,b \to \theta$	cos	$o,b \to \theta$	cos	$o,b \to \theta$	cos	$o,b \to \theta$	cos	$o,b \to \theta$	cos	$\sigma(n)$
2	$1,1 \to 720$	1									
	$1,2 \to 360$	1	$2,2 \to 720$	1							3
3	$1,1 \to 1080$	1									
	$1,2 \to 540$	-1	$2,2 \to 1080$	1							
	$1,3 \to 360$	1	$2,3 \to 720$	1	$3,3 \to 1080$	1					4
4	$1,1 \to 1440$	1									
	$1,2 \to 720$	1	$2,2 \to 1440$	1							
	$1,3 \to 480$	-0.5	$2,3 \to 960$	-0.5	$3,3 \to 1440$	1					
	$1,4 \to 360$	1	$2,4 \to 720$	1	$3,4 \to 1080$	1	$4,4 \to 1440$	1			7
5	$1,1 \to 1800$	1									
	$1,2 \to 900$	-1	$2,2 \to 1800$	1							
	$1,3 \to 600$	-0.5	$2,3 \to 1200$	-0.5	$3,3 \to 1800$	1					
	$1,4 \to 450$	0	$2,4 \to 900$	-1	$3,4 \to 1350$	0	$4,4 \to 1800$	1			
	$1,5 \to 360$	1	$2,5 \to 720$	1	$3,5 \to 1080$	1	$4,5 \to 1440$	1	$5,5 \to 1800$	1	6

On constate par programme qu'en alternant les signes $+$ et $-$ devant chaque terme de la somme et en soustrayant 1 au résultat global, on obtient que les nombres premiers de la forme $4k+1$ ont pour image 0 quand les nombres premiers de la forme $4k+3$ ont pour image 1 selon le programme suivant :

```
import mpmath
from mpmath import *

def mafct(n):
  oppose = 1
  liste=[]
  for b in range(2,n):
    for o in range(1,b+1):
      oppose = (-1) * oppose
      liste.append(oppose*cos(2*pi*n*o/b))
  res=sum(liste)-1
  return res

for x in range(101):
  print(str(x)+' a pour somme '+str(mafct(x)))

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

Résultat du programme ci-dessus : calcul d'une somme alternée de cosinus

```
1 a pour somme -1
2 a pour somme -1
3 a pour somme 1.0
4 a pour somme -2.0
5 a pour somme -2.66453525910038e-15
6 a pour somme -5.0
7 a pour somme 0.999999999999997
8 a pour somme -2.0
9 a pour somme 6.0
10 a pour somme -5.00000000000001
```

```
11 a pour somme 1.00000000000002
12 a pour somme -10.0
13 a pour somme 1.86517468137026e-14
14 a pour somme -4.99999999999998
15 a pour somme 16.9999999999999
16 a pour somme -2.00000000000003
17 a pour somme 1.06581410364015e-14
18 a pour somme -17.0
19 a pour somme 1.00000000000006
20 a pour somme -10.0000000000001
21 a pour somme 20.0
22 a pour somme -5.00000000000012
23 a pour somme 1.00000000000001
24 a pour somme -18.0000000000001
25 a pour somme 9.99999999999995
26 a pour somme -4.99999999999988
27 a pour somme 24.9999999999999
28 a pour somme -10.0000000000001
29 a pour somme -8.21565038222616e-14
30 a pour somme -36.9999999999999
31 a pour somme 1.00000000000026
32 a pour somme -2.00000000000002
33 a pour somme 27.9999999999999
34 a pour somme -4.99999999999991
35 a pour somme 25.0
36 a pour somme -33.9999999999997
37 a pour somme -3.19744231092045e-14
38 a pour somme -5.00000000000025
39 a pour somme 33.0000000000003
40 a pour somme -17.9999999999999
41 a pour somme 1.75859327100625e-13
42 a pour somme -45.0
43 a pour somme 1.0000000000002
44 a pour somme -9.9999999999999
45 a pour somme 64.0000000000001
46 a pour somme -5.00000000000072
47 a pour somme 1.00000000000015
48 a pour somme -34.0000000000001
49 a pour somme 14.0000000000003
50 a pour somme -24.9999999999995
51 a pour somme 40.9999999999997
52 a pour somme -9.99999999999957
53 a pour somme 1.93622895494627e-13
54 a pour somme -52.9999999999998
55 a pour somme 33.0000000000002
56 a pour somme -17.9999999999994
57 a pour somme 43.9999999999999
58 a pour somme -4.99999999999929
59 a pour somme 0.999999999999813
60 a pour somme -73.9999999999995
61 a pour somme -5.10924635932497e-13
62 a pour somme -4.99999999999921
63 a pour somme 81.0
64 a pour somme -2.00000000000007
65 a pour somme 35.999999999999
66 a pour somme -60.9999999999997
67 a pour somme 1.00000000000103
68 a pour somme -10.0000000000005
69 a pour somme 51.9999999999997
70 a pour somme -53.0000000000017
```

```
71 a pour somme 0.999999999999956
72 a pour somme -65.9999999999991
73 a pour somme 5.77315972805081e-13
74 a pour somme -4.99999999999963
75 a pour somme 97.0
76 a pour somme -10.0000000000007
77 a pour somme 36.0000000000004
78 a pour somme -68.9999999999998
79 a pour somme 1.00000000000032
80 a pour somme -33.9999999999996
81 a pour somme 78.0000000000006
82 a pour somme -5.00000000000226
83 a pour somme 0.999999999998838
84 a pour somme -89.9999999999989
85 a pour somme 43.9999999999991
86 a pour somme -4.99999999999942
87 a pour somme 64.9999999999984
88 a pour somme -18.0000000000019
89 a pour somme -5.15143483426073e-14
90 a pour somme -132.999999999998
91 a pour somme 41.0000000000008
92 a pour somme -9.99999999999778
93 a pour somme 67.9999999999987
94 a pour somme -5.00000000000054
95 a pour somme 48.9999999999985
96 a pour somme -65.9999999999998
97 a pour somme 1.24611432283928e-12
98 a pour somme -32.9999999999993
99 a pour somme 112.999999999998
100 a pour somme -50.0000000000001
```

Si l'on initialise le signe du premier terme de la somme à -1 plutôt qu'à $+1$ et si l'on ajoute 2 à la somme globale plutôt que de lui soustraire 1, alors les rôles des nombres premiers de la forme $4k+1$ et $4k+3$ sont échangés, les premiers ayant alors pour image 1 au lieu de 0 et les seconds ayant pour image 0 au lieu de 1 selon le programme, les graphiques et le tableau des images par les deux fonctions sommes alternées de cosinus suivants :

```python
import mpmath
from mpmath import *

def mafct(n):
  oppose = -1
  liste=[]
  for b in range(2,n):
    for o in range(1,b+1):
      oppose = (-1) * oppose
      liste.append(oppose*cos(2*pi*n*o/b))
  res=sum(liste)-1
  return res

for x in range(101):
  print(str(x)+' a pour somme '+str(mafct(x)))

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

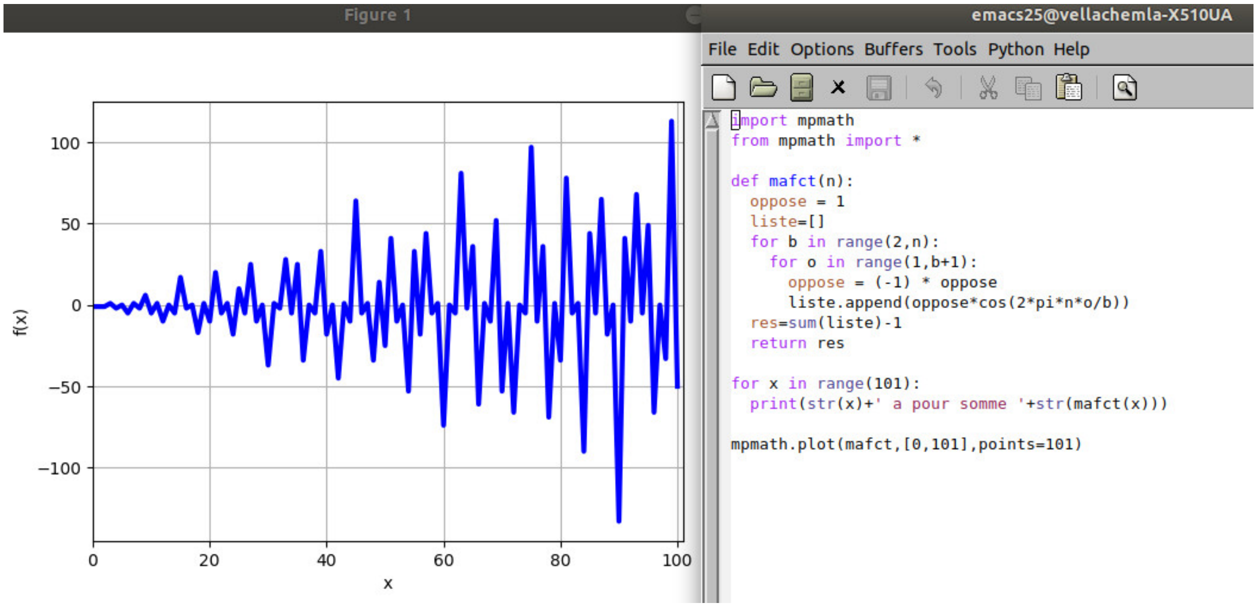


Figure 1
emacs25@vellachemla-X510UA
File Edit Options Buffers Tools Python Help
100
50
0
−50
−100
f(x)
0
20
40
60
80
100
x
import mpmath
from mpmath import *
def mafct(n):
oppose = 1
liste=[]
for b in range(2,n):
for o in range(1,b+1):
oppose = (-1) * oppose
liste.append(oppose*cos(2*pi*n*o/b))
res=sum(liste)-1
return res
for x in range(101):
print(str(x)+' a pour somme '+str(mafct(x)))
mpmath.plot(mafct,[0,101],points=101)

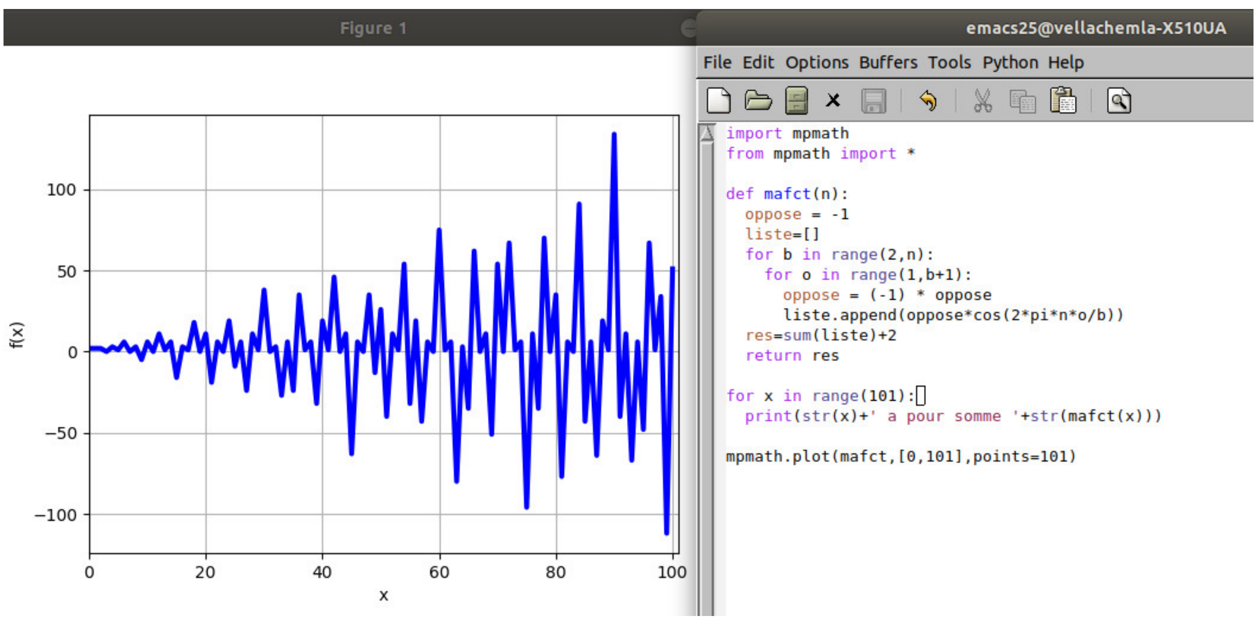


Figure 1
emacs25@vellachemla-X510UA
File Edit Options Buffers Tools Python Help
100
50
0
−50
−100
f(x)
0
20
40
60
80
100
x
import mpmath
from mpmath import *
def mafct(n):
oppose = -1
liste=[]
for b in range(2,n):
for o in range(1,b+1):
oppose = (-1) * oppose
liste.append(oppose*cos(2*pi*n*o/b))
res=sum(liste)+2
return res
for x in range(101):
print(str(x)+' a pour somme '+str(mafct(x)))
mpmath.plot(mafct,[0,101],points=101)

p	*somme alternée* 1	*somme alternée* 2
3	1	0
5	0	1
7	1	0
11	1	0
13	0	1
17	0	1
19	1	0
23	1	0
29	0	1
31	1	0
37	0	1
41	0	1
43	1	0
47	1	0
53	0	1
59	1	0
61	0	1
67	1	0
71	1	0
73	0	1
79	1	0
83	1	0
89	0	1
97	0	1

Annexe : extrait de la première note de septembre 2005 (il faut plutôt prendre le complexe 1 comme sommet commun des polygones)

Au tout début, nous réfléchissions à une manière élégante d'implémenter les horloges modulaires Gaussiennes. On peut voir l'horloge modulaire de n comme un polygone régulier à n côtés sur le cercle unité. Prenons comme convention que tous les polygones ont en commun le sommet correspondant à midi. Deux nombres sont premiers entre eux si leurs polygones réguliers respectifs n'ont aucun sommet commun hormis le sommet midi. Cette idée des polygones réguliers nous a fait faire un détour par les fractions à coefficients entiers. 4 n'est pas premier car $2/4 = 1/2$. Cela nous a amenée naturellement a nous rendre compte qu'un nombre était premier si toutes les fractions de $1/n$ à $(n-1)/n$ étaient non réductibles.

La considération des fractions entières $1/5$, $2/5$, $3/5$, $4/5$, nous a fait dériver vers les sinusoïdes. En effet, les sinusoïdes sont des fonctions qui passent régulièrement par zéro. La sinusoïde $\sin(5\pi x)$ s'annule justement pour les 4 fractions qui nous intéressent sur l'intervalle $]0,1[$. Un nombre n est ainsi premier si sa sinusoïde s'annule exactement $n-1$ fois dans l'intervalle $]0,1[$ et ce, jamais sur un point pour lequel s'annule la sinusoïde d'un nombre premier inférieur à lui.

Nous avons vite abandonné cette voie de recherche : le fait d'assimiler un nombre premier p à sa sinusoïde $\sin(p\pi x)$ semblait ne pas présenter d'intérêt ; en effet, même si cela a l'avantage de restreindre l'étude à l'intervalle $]0,1[$, dans la mesure où il y a une infinité de sinusoïdes qui s'annulent dans cet intervalle, on ne fait que transformer un problème sur des données infiniment grandes en un problème sur des données infiniment petites.

Voir également http://denisevellachemla.eu/dents-de-scie.pdf pour une tentative d'explication d'une valeur moyenne de $\frac{1}{2}$ pour les restes modulaires vus comme des fractions rationnelles.

Interrupteurs (Denise Vella-Chemla, 31.10.2018)

A la suite d'une note publiée en juillet 2014 [1], on propose la fonction somme alternée suivante qui associe $\dfrac{1}{2}$ aux nombres premiers et des valeurs différentes de $\dfrac{1}{2}$ aux nombres composés :

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

Les cosinus d'angles opposés s'éliminent "presque tous" pour les nombres premiers, du fait de leur insécabilité.

Au contraire, pour les nombres composés, leur divisibilité par des nombres qui leur sont inférieurs entraîne par l'ajout des cosinus l'ajout d'un certain nombre d'unités.

Cette propriété rend la somme des cosinus :

- égale à 2 pour les nombres premiers de la forme $4k+3$,
- et égale à 1 pour les nombres premiers de la forme $4k+1$.

Le fait d'ajouter en dernier lieu au résultat $-1+(-1)^{\frac{n}{2}}$ à la somme de cosinus permet de "ramener" les images des nombres premiers égales à 2 ou 1 sur l'image $\dfrac{1}{2}$.

1. http://denise.vella.chemla.free.fr/primesommecos.pdf

Programme en $C++$ pour les sommes alternées de cosinus (les $4k+3$ ont pour image 0 et les $4k+1$ ont pour image 1)

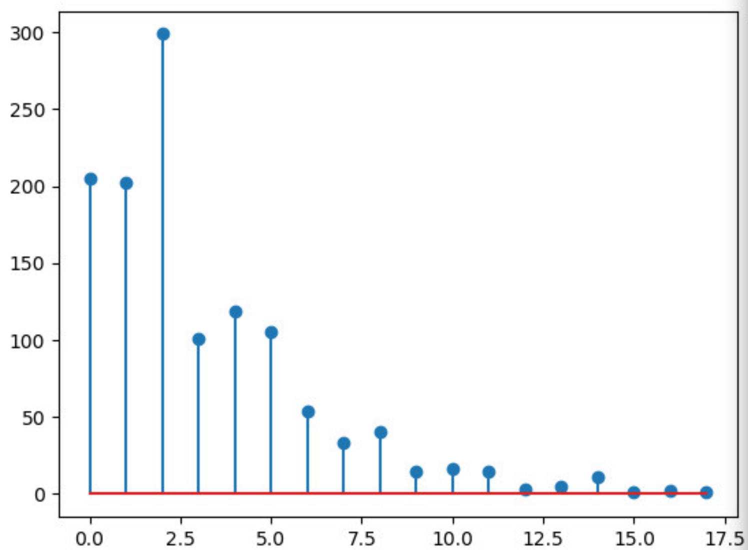
```cpp
#include <iostream>
#include <complex>
#include <cmath>
#include <stdio.h>

using namespace std ;
typedef complex<double> dcomp ;

int prime(int atester)
{
  unsigned long diviseur=2;
  unsigned long k = 2;
  bool pastrouve = true ;

  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve)
    {
    if ((k * k) > atester) return 1;
    else
      if ((atester % k) == 0) return 0 ;
      else k++;
    }
}

int main (int argc, char* argv[])
{
  int n, i, j ;
  double somme ;
  int oppose ;
  const double PI = 4.0 * atan(1.0);

  for (n = 2 ; n <= 50 ; n++)
    {
      oppose = 1 ;
      somme = 0.0 ;
      for (i = 2 ; i <= n-1 ; i++)
  {
    std::cout << "\n" ;
    for (j = 1 ; j <= i ; j++)
      {
        oppose = (-1) * oppose ;
        somme += oppose * cos(2.0 * PI * (double) n * (double) j / (double) i) ;
        std::cout << n << "," << i << "," << j << " -> " ;
        std::cout << 360 * (double) n * (double) j / (double) i << " " ;
        std::cout << oppose * cos(2.0 * PI * (double) n * (double) j / (double) i) << "\n" ;
      }
  }
      somme = somme-1-oppose*0.5 ;
      std::cout << n << " somme globale " << somme << "\n" ;
    }
}
```

```
3,2,1 -> 540  1
3,2,2 -> 1080  1
3 somme globale 0.5

4,2,1 -> 720  -1
4,2,2 -> 1440  1

4,3,1 -> 480  0.5
4,3,2 -> 960  -0.5
4,3,3 -> 1440  -1
4 somme globale -1.5

5,2,1 -> 900  1
5,2,2 -> 1800  1

5,3,1 -> 600  0.5
5,3,2 -> 1200  -0.5
5,3,3 -> 1800  -1

5,4,1 -> 450  3.06162e-16
5,4,2 -> 900  1
5,4,3 -> 1350  -2.69484e-15
5,4,4 -> 1800  -1
5 somme globale 0.5

6,2,1 -> 1080  -1
6,2,2 -> 2160  1

6,3,1 -> 720  -1
6,3,2 -> 1440  1
6,3,3 -> 2160  -1

6,4,1 -> 540  -1
6,4,2 -> 1080  -1
6,4,3 -> 1620  -1
6,4,4 -> 2160  -1

6,5,1 -> 432  0.309017
6,5,2 -> 864  0.809017
6,5,3 -> 1296  -0.809017
6,5,4 -> 1728  -0.309017
6,5,5 -> 2160  1
6 somme globale -5.5

7,2,1 -> 1260  1
7,2,2 -> 2520  1

7,3,1 -> 840  0.5
7,3,2 -> 1680  -0.5
7,3,3 -> 2520  -1

7,4,1 -> 630  -4.28626e-16
7,4,2 -> 1260  1
7,4,3 -> 1890  -4.90478e-16
7,4,4 -> 2520  -1

7,5,1 -> 504  -0.809017
7,5,2 -> 1008  -0.309017
7,5,3 -> 1512  0.309017
7,5,4 -> 2016  0.809017
7,5,5 -> 2520  1
```

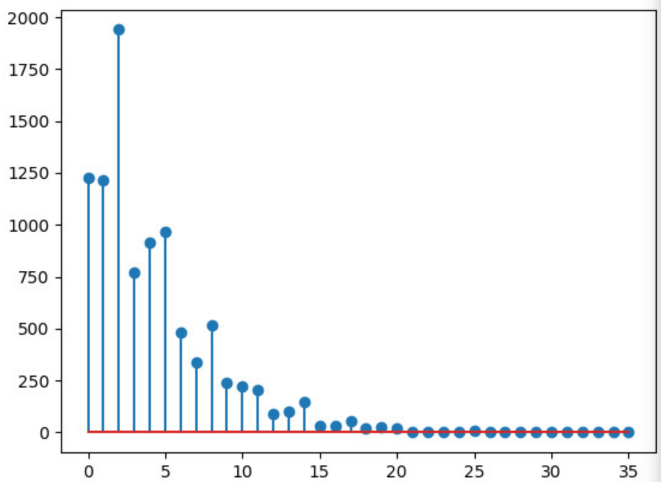
```
7,6,1 -> 420  -0.5
7,6,2 -> 840  -0.5
7,6,3 -> 1260  1
7,6,4 -> 1680  -0.5
7,6,5 -> 2100  -0.5
7,6,6 -> 2520  1
7 somme globale 0.5

8,2,1 -> 1440  -1
8,2,2 -> 2880  1

8,3,1 -> 960  0.5
8,3,2 -> 1920  -0.5
8,3,3 -> 2880  -1

8,4,1 -> 720  1
8,4,2 -> 1440  -1
8,4,3 -> 2160  1
8,4,4 -> 2880  -1

8,5,1 -> 576  -0.809017
8,5,2 -> 1152  -0.309017
8,5,3 -> 1728  0.309017
8,5,4 -> 2304  0.809017
8,5,5 -> 2880  1

8,6,1 -> 480  0.5
8,6,2 -> 960  -0.5
8,6,3 -> 1440  -1
8,6,4 -> 1920  -0.5
8,6,5 -> 2400  0.5
8,6,6 -> 2880  1

8,7,1 -> 411.429  -0.62349
8,7,2 -> 822.857  -0.222521
8,7,3 -> 1234.29  0.900969
8,7,4 -> 1645.71  -0.900969
8,7,5 -> 2057.14  0.222521
8,7,6 -> 2468.57  0.62349
8,7,7 -> 2880  -1
8 somme globale -1.5

9,2,1 -> 1620  1
9,2,2 -> 3240  1

9,3,1 -> 1080  -1
9,3,2 -> 2160  1
9,3,3 -> 3240  -1

9,4,1 -> 810  5.51091e-16
9,4,2 -> 1620  1
9,4,3 -> 2430  -3.42963e-15
9,4,4 -> 3240  -1

9,5,1 -> 648  0.309017
9,5,2 -> 1296  0.809017
9,5,3 -> 1944  -0.809017
9,5,4 -> 2592  -0.309017
9,5,5 -> 3240  1
```

```
9,6,1 -> 540  1
9,6,2 -> 1080  1
9,6,3 -> 1620  1
9,6,4 -> 2160  1
9,6,5 -> 2700  1
9,6,6 -> 3240  1

9,7,1 -> 462.857  0.222521
9,7,2 -> 925.714  -0.900969
9,7,3 -> 1388.57  -0.62349
9,7,4 -> 1851.43  0.62349
9,7,5 -> 2314.29  0.900969
9,7,6 -> 2777.14  -0.222521
9,7,7 -> 3240  -1

9,8,1 -> 405  0.707107
9,8,2 -> 810  -5.51091e-16
9,8,3 -> 1215  -0.707107
9,8,4 -> 1620  1
9,8,5 -> 2025  -0.707107
9,8,6 -> 2430  3.42963e-15
9,8,7 -> 2835  0.707107
9,8,8 -> 3240  -1
9 somme globale 6.5

10,2,1 -> 1800  -1
10,2,2 -> 3600  1

10,3,1 -> 1200  0.5
10,3,2 -> 2400  -0.5
10,3,3 -> 3600  -1

10,4,1 -> 900  -1
10,4,2 -> 1800  -1
10,4,3 -> 2700  -1
10,4,4 -> 3600  -1

10,5,1 -> 720  1
10,5,2 -> 1440  -1
10,5,3 -> 2160  1
10,5,4 -> 2880  -1
10,5,5 -> 3600  1


10,6,1 -> 600  0.5
10,6,2 -> 1200  -0.5
10,6,3 -> 1800  -1
10,6,4 -> 2400  -0.5
10,6,5 -> 3000  0.5
10,6,6 -> 3600  1

10,7,1 -> 514.286  0.900969
10,7,2 -> 1028.57  0.62349
10,7,3 -> 1542.86  0.222521
10,7,4 -> 2057.14  -0.222521
10,7,5 -> 2571.43  -0.62349
10,7,6 -> 3085.71  -0.900969
10,7,7 -> 3600  -1
```

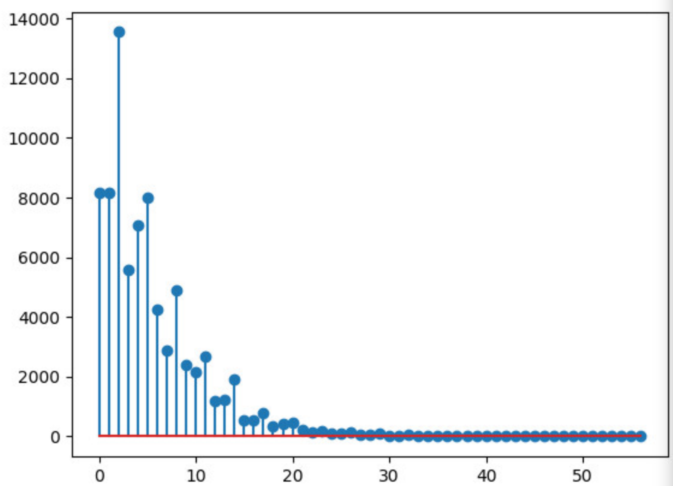
```
10,8,1 -> 450  3.06162e-16
10,8,2 -> 900  1
10,8,3 -> 1350  -2.69484e-15
10,8,4 -> 1800  -1
10,8,5 -> 2250  -2.45548e-16
10,8,6 -> 2700  1
10,8,7 -> 3150  -3.91949e-15
10,8,8 -> 3600  -1

10,9,1 -> 400  0.766044
10,9,2 -> 800  -0.173648
10,9,3 -> 1200  -0.5
10,9,4 -> 1600  0.939693
10,9,5 -> 2000  -0.939693
10,9,6 -> 2400  0.5
10,9,7 -> 2800  0.173648
10,9,8 -> 3200  -0.766044
10,9,9 -> 3600  1
10 somme globale -5.5
```

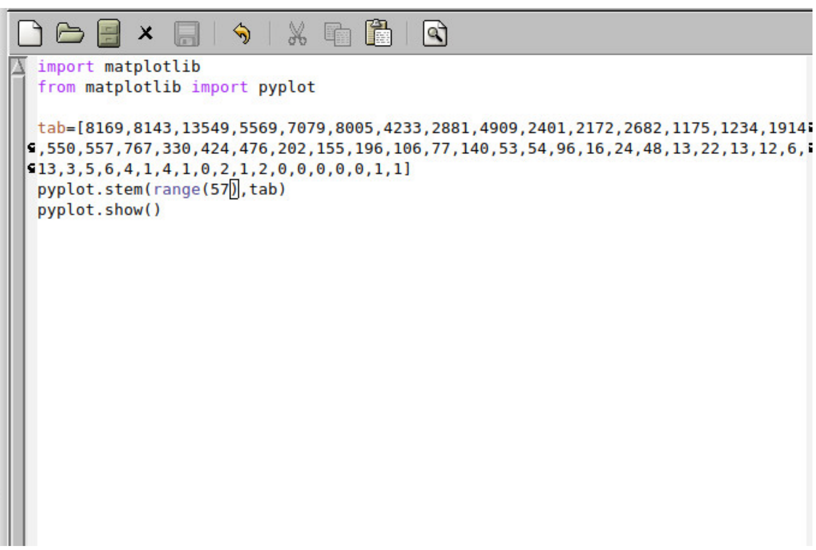



```python
import matplotlib
from matplotlib import pyplot

tab=[205,202,299,101,119,105,54,33,40,15,16,15,3,5,11,1,2,1]
pyplot.stem(range(18),tab)
pyplot.show()
```




```
import matplotlib
from matplotlib import pyplot

tab=[1224,1215,1940,773,916,964,484,339,514,238,223,206,88,98,146,32,33,54,19,28,19,5,4,3,5,7,4,1,4,1,1,1,0,0,0,1]
pyplot.stem(range(36),tab)
pyplot.show()
```





```
import matplotlib
from matplotlib import pyplot

tab=[8169,8143,13549,5569,7079,8005,4233,2881,4909,2401,2172,2682,1175,1234,1914
,550,557,767,330,424,476,202,155,196,106,77,140,53,54,96,16,24,48,13,22,13,12,6,
13,3,5,6,4,1,4,1,0,2,1,2,0,0,0,0,0,1,1]
pyplot.stem(range(57),tab)
pyplot.show()
```

Interrupteurs ou bien une somme alternée de cosinus assez surprenante (Denise Vella-Chemla, 4.11.2018)

A la suite d'une note publiée en juillet 2014 [1], on propose la fonction somme alternée suivante qui associe $\dfrac{1}{2}$ aux nombres premiers et des valeurs différentes de $\dfrac{1}{2}$ aux nombres composés :

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

Les cosinus d'angles opposés s'éliminent "presque tous" pour les nombres premiers, du fait de leur insécabilité.

Au contraire, pour les nombres composés, leur divisibilité par des nombres qui leur sont inférieurs entraîne par l'ajout des cosinus l'ajout d'un certain nombre d'unités.

Cette propriété rend la somme des cosinus :

- égale à 2 pour les nombres premiers de la forme $4k+3$,
- et égale à 1 pour les nombres premiers de la forme $4k+1$.

Le fait d'ajouter en dernier lieu au résultat $-1+\left((-1)^{\frac{n}{2}} \times \dfrac{1}{2}\right)$ à la somme de cosinus permet de "ramener" les images des nombres premiers égales à 2 ou 1 sur l'image $\dfrac{1}{2}$.

On fait calculer par programme cette somme alternée de cosinus pour les entiers jusqu'à 10000 [2].

Cette somme alternée présente la propriété suivante : pour les puissances de nombres premiers, la fonction $f_D(n)$ coïncide avec des fonctions affines ; ainsi, $f_D(9) = 6.5, f_D(27) = 24.5, f_D(81) = 78.5$, i.e. $f_D(x = 3^k) = x - 2.5$; ou bien $f_D(25) = 10.5, f_D(125) = 60.5, f_D(625) = 310.5, f_D(3125) = 1560.5$, i.e. $f_D(x = 5^k) = \frac{1}{2}x - 2$; etc.

On trouve la formule générale pour les puissances de premiers $x = p^k$: si on note $f_D(x) = ax - b$, a est égal à $\dfrac{2}{p-1}$ et b est égal à $\dfrac{3p+1}{2p-2}$.

Pour les nombres dont la factorisation fait intervenir plusieurs nombres premiers différents, on n'arrive pas à dégager de formule générale qui coïnciderait avec la somme alternée de cosinus qu'on a proposée.

On est intrigué par ces résultats et on revient à l'idée initiale qui consistait à calculer la somme suivante :

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

On fait calculer à nouveau par programme cette somme de cosinus pour les entiers jusqu'à 1000 [3].

Les images des puissances de nombres premiers obéissent à la formule :

$$g_D(p^k) = \frac{p^k - p}{p-1}$$

Les images des produits simples de nombres premiers (à la puissance 1) obéissent à la formule :

$$g_D(pq) = p + q$$

1. http://denise.vella.chemla.free.fr/primesommecos.pdf
2. Le programme de calcul de $f_D(n)$ peut être trouvé ici http://denise.vella.chemla.free.fr/trouveformuleoppose.pdf. Le résultat du programme peut être trouvé ici http://denise.vella.chemla.free.fr/affin.pdf
3. Le programme de calcul de $g_D(n)$ peut être trouvé ici http://denise.vella.chemla.free.fr/sumsumcos.pdf. Le résultat du programme peut être trouvé ici http://denise.vella.chemla.free.fr/ressumsumcos.pdf

Par exemple, $g_D(21) = g_D(3 \times 7) = 3 + 7 = 10$ ou bien $g_D(10) = g_D(2 \times 5) = 2 + 5 = 7$.

Le calcul de $g_D(210) = g_D(2 \times 3 \times 5 \times 7) = 2+3+5+7+6+10+14+15+21+35+30+42+70+105 = 365$.

La fonction $g_D(n)$ est ainsi très simple à calculer pour les produits de nombres premiers simples.
Pour les produits faisant intervenir des puissances, on peut appliquer la formule :

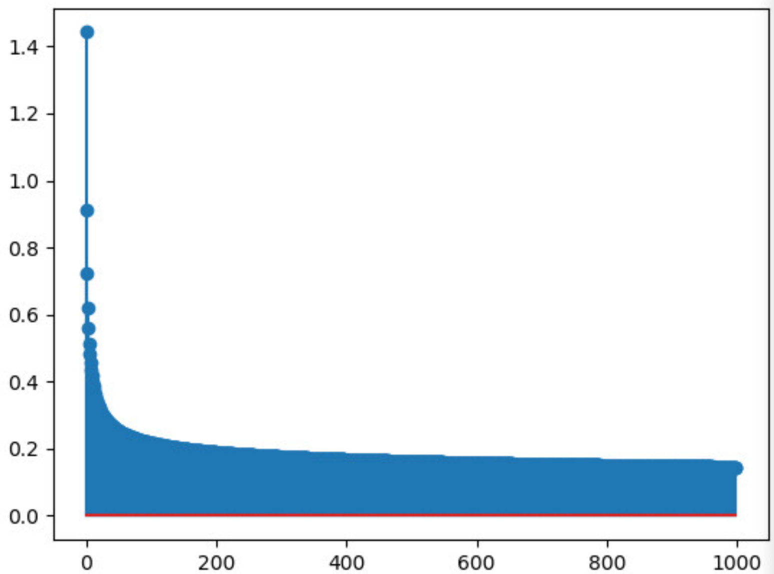
$$g_D(p^k \times x) = (p+1)g_D(p^{k-1} \times x).$$

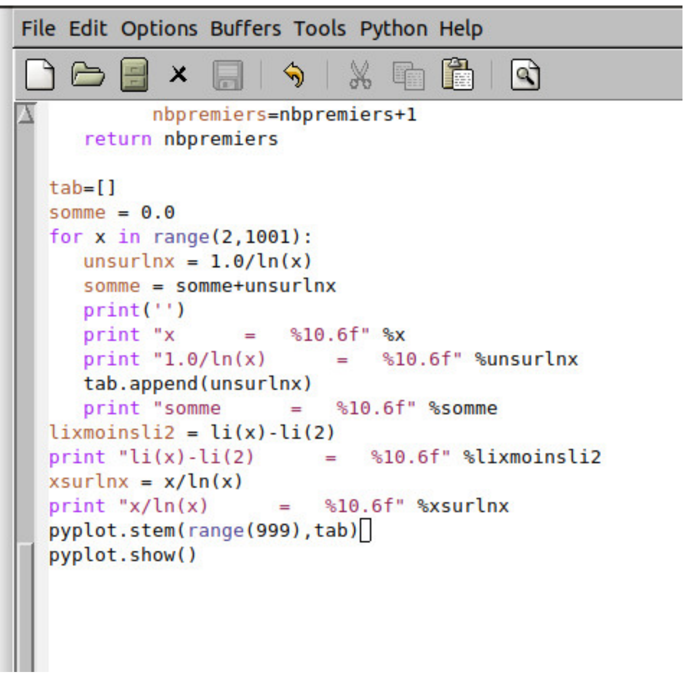
Différence de logarithmes intégrals (Denise Vella-Chemla, 6.11.2018)

```
import mpmath
from mpmath import *
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

def pi(x):
   nbpremiers = 0
   for y in range(1,x):
      if prime(y):
         nbpremiers=nbpremiers+1
   return nbpremiers

x=int(input())
res = li(x)-li(2)
a = pi(x)
b = int(sqrt(x))
c = li(b)-li(2)
resultat=res-(1.0/2.0)*c
print "li(x)-li(2) = %10.6f" %res
print "li(sqrt(x))-li(2) = %10.6f" %c
print "(li(x)-li(2))-(li(sqrt(x))-li(2)) = %10.6f" %resultat
print "pi(x) = %d" %a
erreur1 = (res-a)/a
erreur2 = (resultat-a)/a
print "(li(x)-li(2)-pi(x))/pi(x)  =   %10.6f" %erreur1
print "(li(x)-li(sqrt(x)-pi(x))/pi(x) = %10.6f" %erreur2
```

Résultat de l'exécution du programme ci-dessus

```
x = 100
li(x)-li(2) = 29.080978
li(sqrt(x))-li(2) = 5.120436
(li(x)-li(2))-(li(sqrt(x))-li(2)) = 26.520760
pi(x) = 25
(li(x)-li(2)-pi(x))/pi(x)   =   0.163239
(li(x)-li(sqrt(x)-pi(x))/pi(x) = 0.060830

x = 1000
li(x)-li(2) = 176.564494
li(sqrt(x))-li(2) = 12.270067
(li(x)-li(2))-(li(sqrt(x))-li(2)) = 170.429461
pi(x) = 168
(li(x)-li(2)-pi(x))/pi(x)   =   0.050979
(li(x)-li(sqrt(x)-pi(x))/pi(x) = 0.014461

x = 10000
li(x)-li(2) = 1245.092052
li(sqrt(x))-li(2) = 29.080978
(li(x)-li(2))-(li(sqrt(x))-li(2)) = 1230.551563
pi(x) = 1229
(li(x)-li(2)-pi(x))/pi(x)   =   0.013094
(li(x)-li(sqrt(x)-pi(x))/pi(x) = 0.001262

x = 100000
li(x)-li(2) = 9628.763837
li(sqrt(x))-li(2) = 70.080798
(li(x)-li(2))-(li(sqrt(x))-li(2)) = 9593.723439
pi(x) = 9592
(li(x)-li(2))-pi(x)/pi(x)   =   0.003833
(li(x)-li(sqrt(x)-pi(x))/pi(x) = 0.000180

x = 1000000
li(x)-li(2) = 78626.503996
li(sqrt(x))-li(2) = 176.564494
(li(x)-li(2))-(li(sqrt(x))-li(2)) = 78538.221749
pi(x) = 78498
(li(x)-li(2)-pi(x))/pi(x)   =   0.001637
(li(x)-li(sqrt(x)-pi(x))/pi(x) = 0.000512

x = 10000000
li(x)-li(2) = 664917.359885
li(sqrt(x))-li(2) = 461.881189
(li(x)-li(2))-(li(sqrt(x))-li(2)) = 664686.419290
pi(x) = 664579
(li(x)-li(2)-pi(x))/pi(x)   =   0.000509
(li(x)-li(sqrt(x)-pi(x))/pi(x) = 0.000162
```






```
        nbpremiers=nbpremiers+1
    return nbpremiers

tab=[]
somme = 0.0
for x in range(2,1001):
   unsurlnx = 1.0/ln(x)
   somme = somme+unsurlnx
   print('')
   print "x      =   %10.6f" %x
   print "1.0/ln(x)      =   %10.6f" %unsurlnx
   tab.append(unsurlnx)
   print "somme      =   %10.6f" %somme
lixmoinsli2 = li(x)-li(2)
print "li(x)-li(2)      =   %10.6f" %lixmoinsli2
xsurlnx = x/ln(x)
print "x/ln(x)      =   %10.6f" %xsurlnx
pyplot.stem(range(999),tab)
pyplot.show()
```

Triplets Goldbachiques (Denise Vella-Chemla, 30.11.2018)

On souhaiterait appeler *triplets Goldbachiques* des triplets de nombres premiers (p_1, p_3, p_2) tels que

$$2p_3 = p_1 + p_2.$$

Voici les triplets Goldbachiques tels que $p_3 < 100$.

$(3,5,7)$	$(3,37,71)$	$(17,53,89)$	$(11,71,131)$	$(59,83,107)$
$(3,7,11)$	$(7,37,67)$	$(23,53,83)$	$(29,71,113)$	$(5,89,173)$
$(3,11,19)$	$(13,37,61)$	$(47,53,59)$	$(41,71,101)$	$(11,89,167)$
$(5,11,17)$	$(31,37,43)$	$(5,59,113)$	$(53,71,89)$	$(29,89,149)$
$(3,13,23)$	$(3,41,79)$	$(11,59,107)$	$(59,71,83)$	$(41,89,137)$
$(7,13,19)$	$(11,41,71)$	$(17,59,101)$	$(7,73,139)$	$(47,89,131)$
$(3,17,31)$	$(23,41,59)$	$(29,59,89)$	$(19,73,127)$	$(71,89,107)$
$(5,17,29)$	$(29,41,53)$	$(47,59,71)$	$(37,73,109)$	$(3,97,191)$
$(11,17,23)$	$(3,43,83)$	$(13,61,109)$	$(43,73,103)$	$(13,97,181)$
$(7,19,31)$	$(7,43,79)$	$(19,61,103)$	$(67,73,79)$	$(31,97,163)$
$(3,23,43)$	$(13,43,73)$	$(43,61,79)$	$(7,79,151)$	$(37,97,157)$
$(5,23,41)$	$(19,43,67)$	$(3,67,131)$	$(19,79,139)$	$(43,97,151)$
$(17,23,29)$	$(5,47,89)$	$(7,67,127)$	$(31,79,127)$	$(67,97,127)$
$(5,29,53)$	$(11,47,83)$	$(31,67,103)$	$(61,79,97)$	
$(11,29,47)$	$(23,47,71)$	$(37,67,97)$	$(3,83,163)$	
$(17,29,41)$	$(41,47,53)$	$(61,67,73)$	$(17,83,149)$	
$(3,31,59)$	$(3,53,103)$	$(3,71,139)$	$(29,83,137)$	
$(19,31,43)$	$(5,53,101)$	$(5,71,137)$	$(53,83,113)$	

Deux triplets Goldbachiques en engendrent un troisième : par exemple, $(3,5,7)$ et $(7,13,19)$ engendrent $(3,11,19)$.

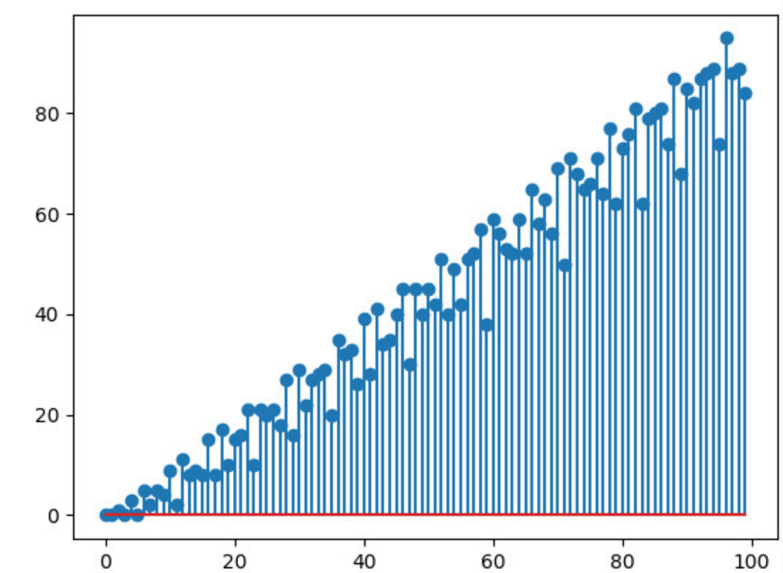
Coder le vrai par -1 (Denise Vella-Chemla, 2.12.2018)

On définit la fonction $divispin(n, x)$ valant -1 si x divise n et +1 sinon. On calcule pour les entiers n jusqu'à 100 la somme

$$ds(n) = \sum_{k=2}^{n-1} divispin(n, x)$$

$1 \to 0$	$21 \to 15$	$41 \to 39$	$61 \to 59$	$81 \to 73$
$2 \to 0$	$22 \to 16$	$42 \to 28$	$62 \to 56$	$82 \to 76$
$3 \to 1$	$23 \to 21$	$43 \to 41$	$63 \to 53$	$83 \to 81$
$4 \to 0$	$24 \to 10$	$44 \to 34$	$64 \to 52$	$84 \to 62$
$5 \to 3$	$25 \to 21$	$45 \to 35$	$65 \to 59$	$85 \to 79$
$6 \to 0$	$26 \to 20$	$46 \to 40$	$66 \to 52$	$86 \to 80$
$7 \to 5$	$27 \to 21$	$47 \to 45$	$67 \to 65$	$87 \to 81$
$8 \to 2$	$28 \to 18$	$48 \to 30$	$68 \to 58$	$88 \to 74$
$9 \to 5$	$29 \to 27$	$49 \to 45$	$69 \to 63$	$89 \to 87$
$10 \to 4$	$30 \to 16$	$50 \to 40$	$70 \to 56$	$90 \to 68$
$11 \to 9$	$31 \to 29$	$51 \to 45$	$71 \to 69$	$91 \to 85$
$12 \to 2$	$32 \to 22$	$52 \to 42$	$72 \to 50$	$92 \to 82$
$13 \to 11$	$33 \to 27$	$53 \to 51$	$73 \to 71$	$93 \to 87$
$14 \to 8$	$34 \to 28$	$54 \to 40$	$74 \to 68$	$94 \to 88$
$15 \to 9$	$35 \to 29$	$55 \to 49$	$75 \to 65$	$95 \to 89$
$16 \to 8$	$36 \to 20$	$56 \to 42$	$76 \to 66$	$96 \to 74$
$17 \to 15$	$37 \to 35$	$57 \to 51$	$77 \to 71$	$97 \to 95$
$18 \to 8$	$38 \to 32$	$58 \to 52$	$78 \to 64$	$98 \to 88$
$19 \to 17$	$39 \to 33$	$59 \to 57$	$79 \to 77$	$99 \to 89$
$20 \to 10$	$40 \to 26$	$60 \to 38$	$80 \to 62$	$100 \to 84$

La fonction ds associer à un entier n pair une image $ds(n)$ paire. La fonction ds associe à un nombre premier p l'image $p-2$ et est ainsi une fonction strictement croissante sur l'ensemble des nombres premiers tandis qu'elle associe à un entier impair composé n (sauf 1) un nombre strictement inférieur à $n-2$.



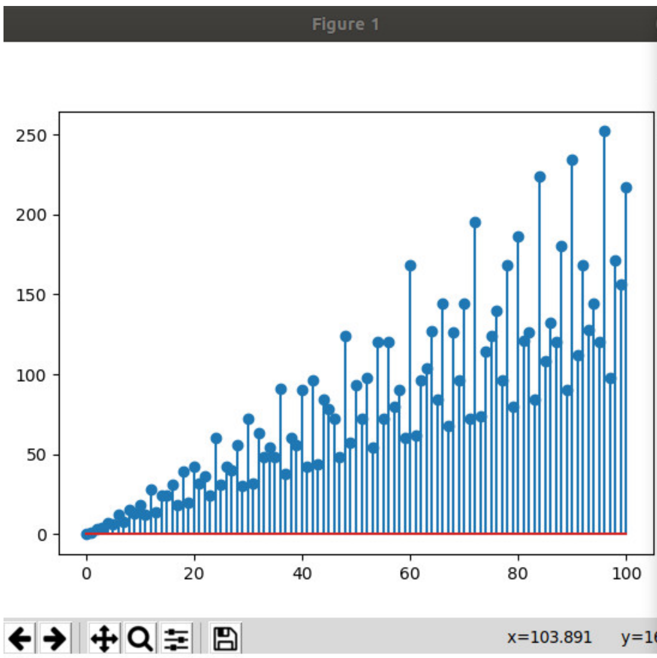
File Edit Options Buffers Tools Python Help

```python
import matplotlib
from matplotlib import pyplot

tab=[]
i=0
for x in range(1,101):
  somme = 0.0
  for k in range(2,x):
    if ((x % k) == 0):
      somme = somme-1
    else:
      somme = somme+1
  print(str(x)+" --> "+str(somme))
  tab.append(somme)
  i=i+1
pyplot.stem(range(i),tab)
pyplot.show()
```

-:--- **spins.py** All L13 (Python

Wrote /home/vella-chemla/Bureau/spins.

```
65 --> 59.0
66 --> 52.0
67 --> 65.0
68 --> 58.0
69 --> 63.0
70 --> 56.0
71 --> 69.0
72 --> 50.0
73 --> 71.0
74 --> 68.0
75 --> 65.0
76 --> 66.0
77 --> 71.0
78 --> 64.0
79 --> 77.0
80 --> 62.0
81 --> 73.0
82 --> 76.0
83 --> 81.0
84 --> 62.0
85 --> 79.0
86 --> 80.0
87 --> 81.0
88 --> 74.0
89 --> 87.0
90 --> 68.0
91 --> 85.0
92 --> 82.0
93 --> 87.0
94 --> 88.0
95 --> 89.0
96 --> 74.0
97 --> 95.0
98 --> 88.0
99 --> 89.0
100 --> 84.0
```



emacs25@vellachemla-X510UA

File Edit Options Buffers Tools Python Help

```python
import matplotlib
from matplotlib import pyplot

sigma=[0.0,0.0]
sigma[1] = 1.0
i=0
for n in range(2,101):
  somme = 0.0
  for k in range(1,n):
     somme = somme+(-(n*n)+5.0*k*n-5.0*k*k)*sigma[k]*sigma[n-k]
  res = (12.0*somme)/(n*n*(n-1.0))
  sigma.append(res)
  i=i+1
  print(str(n)+" --> "+str(res))
pyplot.stem(range(i+2),sigma)
pyplot.show()
```

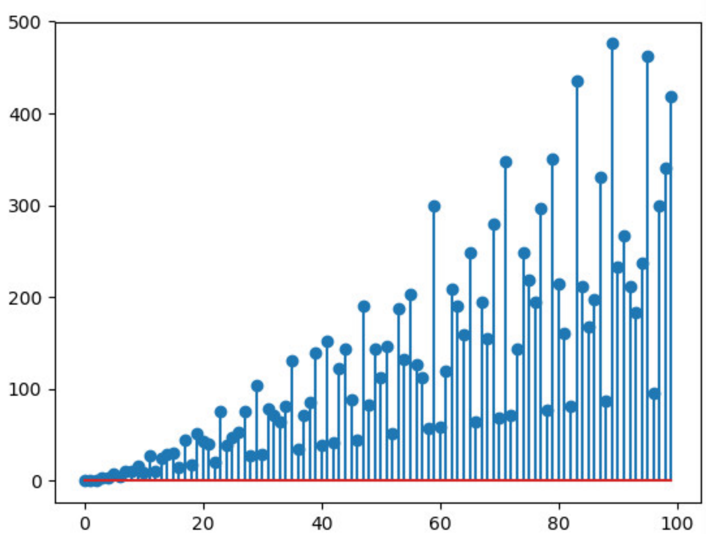
-:--- **dessinechazy.py** All L15 (Python)

Wrote /home/vella-chemla/Bureau/dessinechazy.py

Fichier Édition Af

```
65 --> 84.0
66 --> 144.0
67 --> 68.0
68 --> 126.0
69 --> 96.0
70 --> 144.0
71 --> 72.0
72 --> 195.0
73 --> 74.0
74 --> 114.0
75 --> 124.0
76 --> 140.0
77 --> 96.0
78 --> 168.0
79 --> 80.0
80 --> 186.0
81 --> 121.0
82 --> 126.0
83 --> 84.0
84 --> 224.0
85 --> 108.0
86 --> 132.0
87 --> 120.0
88 --> 180.0
89 --> 90.0
90 --> 234.0
91 --> 112.0
92 --> 168.0
93 --> 128.0
94 --> 144.0
95 --> 120.0
96 --> 252.0
97 --> 98.0
98 --> 171.0
99 --> 156.0
100 --> 217.0
```

Figure 1



emacs25@vella

File Edit Options Buffers Tools Python Help

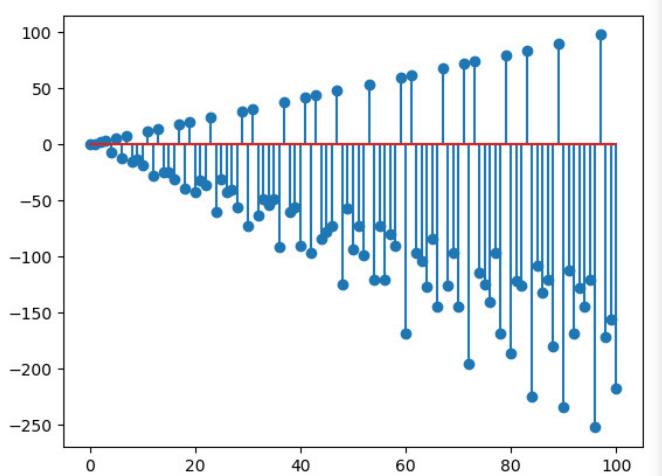
```python
import matplotlib
from matplotlib import pyplot

def pgcd(m, n):
  while (m  != 0):
    r = n % m ;
    n = m ;
    m = r ;
  return n ;

tab=[]
i=0
for x in range(1,101):
  somme = 0.0
  for k in range(2,x):
     somme = somme+pgcd(x, k)
  print(str(x)+" --> "+str(somme))
  tab.append(somme)
  i=i+1
pyplot.stem(range(i),tab)
pyplot.show()
```

Terminal

Fichier Édition Affichage Recherch

```
30 --> 104.0
31 --> 29.0
32 --> 79.0
33 --> 71.0
34 --> 64.0
35 --> 81.0
36 --> 131.0
37 --> 35.0
38 --> 72.0
39 --> 85.0
40 --> 139.0
41 --> 39.0
42 --> 152.0
43 --> 41.0
44 --> 123.0
45 --> 143.0
46 --> 88.0
47 --> 45.0
48 --> 191.0
49 --> 83.0
50 --> 144.0
51 --> 113.0
52 --> 147.0
53 --> 51.0
```

Figure 1



emacs25@vellachemla-X510UA

File Edit Options Buffers Tools Python Help

```
import matplotlib
from matplotlib import pyplot

sigma=[0.0,0.0]
sigma[1] = 1.0
dessinesigma=[0.0,0.0]
dessinesigma[1] = 1.0
i=0
for n in range(2,101):
  somme = 0.0
  for k in range(1,n):
     somme = somme+(-(n*n)+5.0*k*n-5.0*k*k)*sigma[k]*sigma[n-k]
  res = (12.0*somme)/(n*n*(n-1.0))
  if (res > n+1):
    stockeres = (-1)*res
  else:
    stockeres = res
  sigma.append(res)
  dessinesigma.append(stockeres)
  i=i+1
  print(str(n)+" --> "+str(stockeres))
pyplot.stem(range(i+2),dessinesigma)
pyplot.show()
```

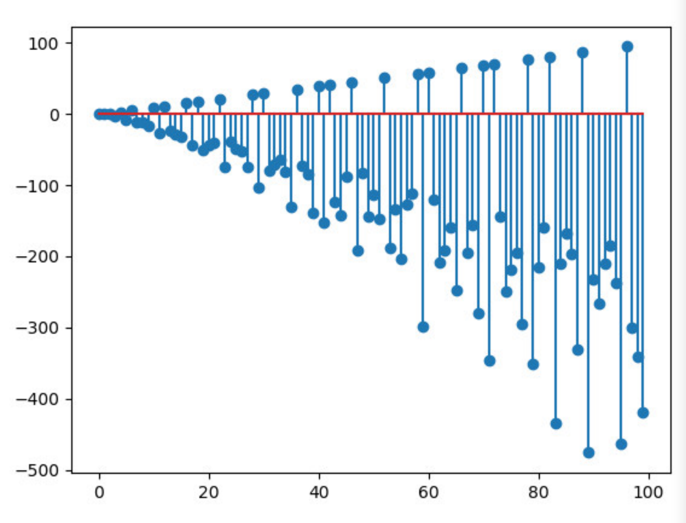
-:--- separeles.py All L22 (Python)

Wrote /home/vella-chemla/Bureau/beauxpyplot/separeles.py

Fichier Édition Affic

```
65 --> -84.0
66 --> -144.0
67 --> 68.0
68 --> -126.0
69 --> -96.0
70 --> -144.0
71 --> 72.0
72 --> -195.0
73 --> 74.0
74 --> -114.0
75 --> -124.0
76 --> -140.0
77 --> -96.0
78 --> -168.0
79 --> 80.0
80 --> -186.0
81 --> -121.0
82 --> -126.0
83 --> 84.0
84 --> -224.0
85 --> -108.0
86 --> -132.0
87 --> -120.0
88 --> -180.0
89 --> 90.0
90 --> -234.0
91 --> -112.0
92 --> -168.0
93 --> -128.0
94 --> -144.0
95 --> -120.0
96 --> -252.0
97 --> 98.0
98 --> -171.0
99 --> -156.0
100 --> -217.0
```

Figure 1



emacs25@vellachemla

File Edit Options Buffers Tools Python Help

```python
import matplotlib
from matplotlib import pyplot

def pgcd(m, n):
  while (m  != 0):
    r = n % m ;
    n = m ;
    m = r ;
  return n ;

tab=[]
dessinetab=[]
i=0
for x in range(1,101):
  somme = 0.0
  for k in range(2,x):
     somme = somme+pgcd(x, k)
  print(str(x)+" --> "+str(somme))
  tab.append(somme)
  if (somme > x-2):
    dessinetab.append((-1)*somme)
  else:
    dessinetab.append(somme)
  i=i+1
pyplot.stem(range(i),dessinetab)
pyplot.show()
```

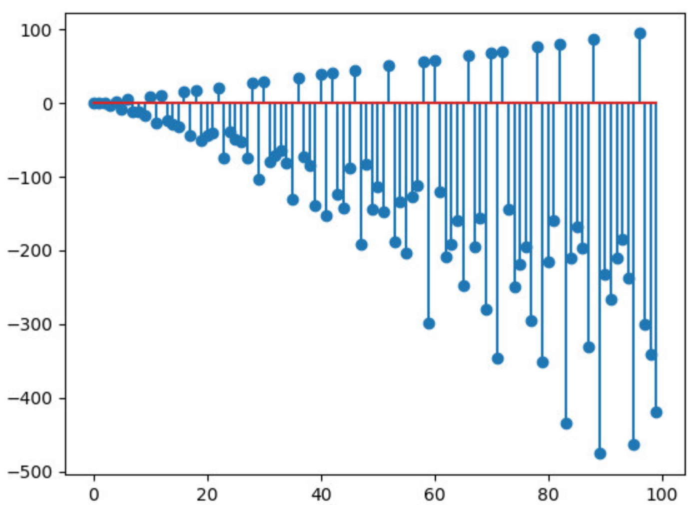
-:--- **separepgcd.py**   All L20   (Python)

Wrote /home/vella-chemla/Bureau/beauxpyplot/s

Fichier Édition Affichage Rechercher

```
65 --> 159.0
66 --> 248.0
67 --> 65.0
68 --> 195.0
69 --> 155.0
70 --> 280.0
71 --> 69.0
72 --> 347.0
73 --> 71.0
74 --> 144.0
75 --> 249.0
76 --> 219.0
77 --> 195.0
78 --> 296.0
79 --> 77.0
80 --> 351.0
81 --> 215.0
82 --> 160.0
83 --> 81.0
84 --> 435.0
85 --> 211.0
86 --> 168.0
87 --> 197.0
88 --> 331.0
89 --> 87.0
90 --> 476.0
91 --> 233.0
92 --> 267.0
93 --> 211.0
94 --> 184.0
95 --> 237.0
96 --> 463.0
97 --> 95.0
98 --> 300.0
99 --> 341.0
100 --> 419.0
```

Figure 1



emacs25@vellachemla-

File Edit Options Buffers Tools Python Help

```python
import matplotlib
from matplotlib import pyplot

def pgcd(m, n):
  while (not (m*n == 0)):
    if (n > m):
      n=n-m ;
    else:
      m = m-n ;
  if (n == 0):
    return m ;
  else:
    return n ;

tab=[]
dessinetab=[]
i=0
for x in range(1,101):
  somme = 0.0
  for k in range(2,x):
     somme = somme+pgcd(x, k)
  print(str(x)+" --> "+str(somme))
  tab.append(somme)
  if (somme > x-2):
    dessinetab.append((-1)*somme)
  else:
    dessinetab.append(somme)
  i=i+1
pyplot.stem(range(i),dessinetab)
pyplot.show()
```

-:--- separepgcdsansmod.py   All L1   (Python

5 1

Termi

Fichier Édition Affichage Re

```
65 --> 159.0
66 --> 248.0
67 --> 65.0
68 --> 195.0
69 --> 155.0
70 --> 280.0
71 --> 69.0
72 --> 347.0
73 --> 71.0
74 --> 144.0
75 --> 249.0
76 --> 219.0
77 --> 195.0
78 --> 296.0
79 --> 77.0
80 --> 351.0
81 --> 215.0
82 --> 160.0
83 --> 81.0
84 --> 435.0
85 --> 211.0
86 --> 168.0
87 --> 197.0
88 --> 331.0
89 --> 87.0
90 --> 476.0
91 --> 233.0
92 --> 267.0
93 --> 211.0
94 --> 184.0
95 --> 237.0
96 --> 463.0
97 --> 95.0
98 --> 300.0
99 --> 341.0
100 --> 419.0
```

PGCD d'Euclide et matrices (Wikipedia, Denise Vella-Chemla, 4.12.2018)

On veut calculer le plus grand commun diviseur (*pgcd*) de 9 et 6.

Les deux égalités obtenues par l'exécution de l'algorithme d'Euclide :

$$\begin{array}{c} 9 = 1 \times 6 + 3 \;\; (a = q_0 \times b + r_0) \\ 6 = 2 \times 3 + 0 \;\; (b = q_1 \times r_0 + r_1) \end{array}$$

sont codées par les matrices de la forme $\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$ suivantes $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$.

On effectue leur produit pour obtenir la matrice $M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$.

L'inverse de M est $M^{-1} = \begin{pmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix}$.

Le *pgcd* de 9 et 6 est ainsi trouvé en calculant le produit (dans lequel l'exposant de -1 est le nombre de matrices intervenant dans le produit calculant M ci-dessus) :

$$(-1)^2 \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 9 \\ 6 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \end{pmatrix}$$

Note : bien qu'on ait $pgcd(x, y) = pgcd(y, x)$, la multiplication des matrices, par exemple $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$ est non-commutative. Ainsi :

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$$

tandis que

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix}$$

On a :

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

On peut de cette manière voir les nombres premiers comme mettant en relation les nombres dont ils sont *pgcd*. Les nombres premiers sont les éléments minimaux de la relation d'ordre partiel induite sur les entiers par la relation de divisibilité.

Transcription de l'extrait de l'article de Wikipedia concernant le pgcd calculé par des matrices
L'identité de Bézout établit que le plus grand commun diviseur g de deux entiers a et b peut être représenté par une combinaison linéaire de a et b. En d'autres termes, on peut toujours trouver deux entiers s et t tels que $g = sa + tb$.

Les entiers solutions de l'identité de Bézout peuvent être trouvés en utilisant une méthode de calcul matriciel.
La séquence d'équations de l'algorithme d'Euclide

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ &\vdots \\ r_{N-2} &= q_N r_{N-1} + 0 \end{aligned}$$

peut s'écrire comme un produit de matrices quotients de taille 2×2 multipliées par un vecteur colonne reste de deux lignes.

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r_0 \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = \cdots = \prod_{i=0}^{N} \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{N-1} \\ 0 \end{pmatrix}.$$

$\mathbf{M}$ représente le produit de toutes les matrices quotient.

$$\mathbf{M} = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = \prod_{i=0}^{N} \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_N & 1 \\ 1 & 0 \end{pmatrix}.$$

L'algorithme d'Euclide se simplifie ainsi en la forme :

$$\begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{M} \begin{pmatrix} r_{N-1} \\ 0 \end{pmatrix} = \mathbf{M} \begin{pmatrix} g \\ 0 \end{pmatrix}.$$

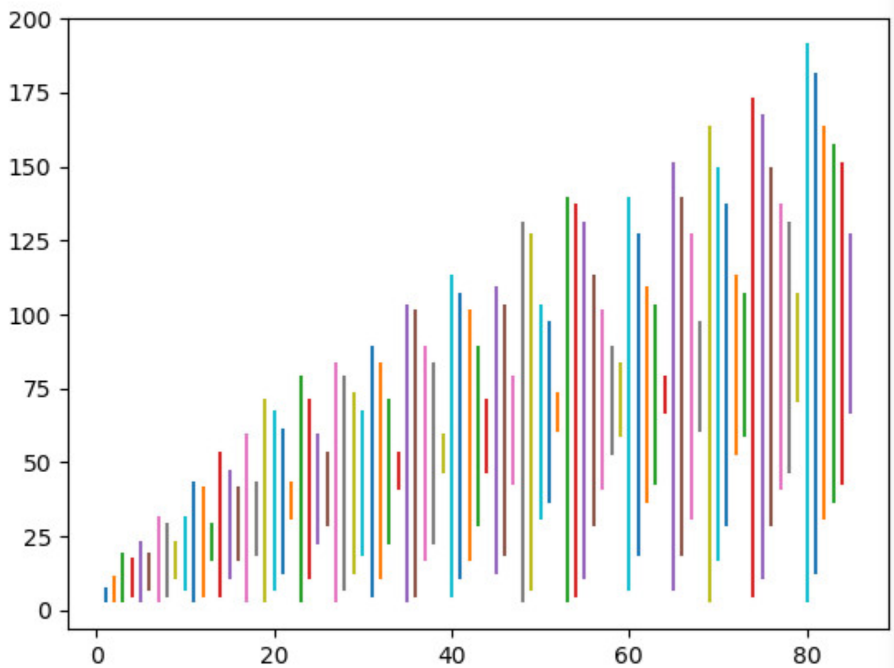
Pour exprimer g comme une combinaison linéaire de a et b, les deux côtés de l'équation peuvent être multipliés par l'inverse de la matrice $\mathbf{M}$. Le déterminant de $\mathbf{M}$ est égal à $(-1)^{N+1}$, puisqu'il est égal au produit des déterminants des matrices quotients, chacun de ces déterminants valant -1. Puisque le déterminant de $\mathbf{M}$ n'est jamais nul, le dernier vecteur des restes peut être calculé en utilisant l'inverse de $\mathbf{M}$.

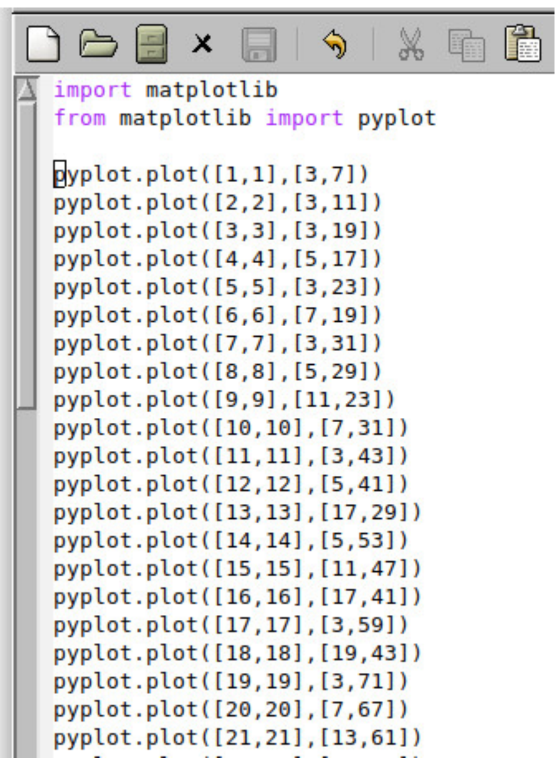
$$\begin{pmatrix} g \\ 0 \end{pmatrix} = \mathbf{M}^{-1} \begin{pmatrix} a \\ b \end{pmatrix} = (-1)^{N+1} \begin{pmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Puisque l'équation ci-dessus donne

$$g = (-1)^{N+1}(m_{22}a - m_{12}b),$$

les deux entiers solutions de l'identité de Bézout sont $s = (-1)^{N+1}m_{22}$ and $t = (-1)^N m_{12}$. La méthode par les matrices est aussi efficace que la méthode récursive, avec deux multiplications et deux additions à chaque étape de l'algorithme d'Euclide.





```
import matplotlib
from matplotlib import pyplot

pyplot.plot([1,1],[3,7])
pyplot.plot([2,2],[3,11])
pyplot.plot([3,3],[3,19])
pyplot.plot([4,4],[5,17])
pyplot.plot([5,5],[3,23])
pyplot.plot([6,6],[7,19])
pyplot.plot([7,7],[3,31])
pyplot.plot([8,8],[5,29])
pyplot.plot([9,9],[11,23])
pyplot.plot([10,10],[7,31])
pyplot.plot([11,11],[3,43])
pyplot.plot([12,12],[5,41])
pyplot.plot([13,13],[17,29])
pyplot.plot([14,14],[5,53])
pyplot.plot([15,15],[11,47])
pyplot.plot([16,16],[17,41])
pyplot.plot([17,17],[3,59])
pyplot.plot([18,18],[19,43])
pyplot.plot([19,19],[3,71])
pyplot.plot([20,20],[7,67])
pyplot.plot([21,21],[13,61])
```

Essayer de comprendre la formule de Riemann (Denise Vella-Chemla, 22.12.2018)

Ci-dessous la transcription de mes posts sur le forum *les-mathematiques.net* cette semaine [1].

On s'intéresse à la formule :

$$f(x) = Li(x) - \sum_{\alpha} \left[Li\left(x^{\frac{1}{2}+\alpha i}\right) + Li\left(x^{\frac{1}{2}-\alpha i}\right) \right] + \int_x^{\infty} \frac{1}{x^2-1} \frac{dx}{x \log x} + \log \xi(0),$$

de l'article de Riemann dans lequel il émet son illustre hypothèse.

Quand on calcule par programme la somme $\displaystyle\sum_{k=2}^{n-1} \frac{1}{ln\ k}$ [2], on trouve "quasiment" $\pi(n)$ le nombre de nombres premiers inférieurs à n, et cela semble signifier que dans la formule fournie par Riemann, les éléments que l'on soustrait et ceux que l'on ajoute à $Li(x)$ s'annulent.

Intéressons-nous à $S(x) = \displaystyle\sum_{\rho} \left[Li\left(x^{\rho}\right) + Li\left(x^{\overline{\rho}}\right) \right]$ et au fait que Riemann insiste sur le fait qu'il faille calculer cette somme selon chaque "zéro et son conjugué" un par un, en écrivant : "Mais, si l'on changeait cet ordre des termes de la série, on pourrait obtenir pour résultat n'importe quelle valeur réelle.".

On a

$$\begin{aligned} S(x) &= \sum_{\rho} 2cos\ arg(Li(x^{\rho})) \\ &= \sum_{\rho} 2cos\ arctan \frac{Li(x^{\rho}) - \overline{Li(x^{\rho})}}{i(Li(x^{\rho}) + \overline{Li(x^{\rho})})} \\ &= \sum_{\rho} \frac{2}{\sqrt{1 + \left(\frac{Li(x^{\rho}) - \overline{Li(x^{\rho})}}{i(Li(x^{\rho}) + \overline{Li(x^{\rho})})} \right)^2}} \end{aligned}$$

Si maintenant on note $z = a + bi$ l'un des $Li(x^{\rho})$ avec ρ un zéro de zêta non trivial de partie imaginaire positive, on a : $z - \overline{z} = (a+bi) - (a-bi) = 2bi$ et $z + \overline{z} = (a+bi) + (a-bi) = 2a$ et la somme $S(x)$ égale (les 2 et les i s'éliminant dans la fraction sous le signe $\sqrt{}$) :

$$S(x) = \sum_{\rho} \frac{2}{\sqrt{1 + \left(\frac{\Im(Li(x^{\rho}))}{\Re(Li(x^{\rho}))} \right)^2}}$$

avec ρ tel que $\zeta(\rho) = 0$ et $\Im(\rho) > 0$.

Il faudrait alors peut-être démontrer que cette somme et l'intégrale $T(x) = \displaystyle\int_x^{\infty} \frac{1}{x^2-1} \frac{dx}{x\ ln\ x}$ sont asymptotiquement égales pour ne conserver que $Li(x)$ dans la formule de $f(x)$.

Pour x entier inférieur à 1000, on fournit le programme python qui calcule l'intégrale $T(x)$ ainsi que son résultat ici :

- http://denise.vella.chemla.free.fr/pgmintegBR1000.pdf
- http://denise.vella.chemla.free.fr/resintegBR1000.pdf

Pour tenter de comparer $S(x)$ et $T(x)$, on fournit le programme python qui calcule la somme $S(x)$ pour les nombres entiers x inférieurs à 100, en utilisant les 1000 premiers zéros de zêta ou bien en utilisant les 100000 premiers zéros de zêta :

- http://denise.vella.chemla.free.fr/pgmcalcS.pdf

1. ici http://www.les-mathematiques.net/phorum/read.php?4,1747818.
2. On nous a expliqué qu'il est normal que cette somme calculée sur des entiers soit équivalente au fait de calculer l'intégrale qui définit $li(x)$ car la différence entre la somme et l'intégrale est contrôlée puisque la dérivée de $\frac{1}{ln\ x}$, qui est $\frac{-1}{(x\ (ln\ x)^2)}$, est intégrable.

— http://denise.vella.chemla.free.fr/respgmcalcS1.pdf
— http://denise.vella.chemla.free.fr/respgmcalcS2.pdf

On n'a pas l'impression que $S(x)$ et $T(x)$ puissent jamais s'annuler.

Fonction $\psi(x)$ et $\xi(t)$ de Riemann (Denise Vella-Chemla, 24.12.2018)

On aimerait avoir un aperçu de la fonction $\xi(t)$ définie ainsi à partir de la fonction $\psi(x)$, par Riemann dans son article fondateur concernant le nombre de nombres premiers inférieurs à un certain nombre :

$$\psi(x) = \sum_{n=1}^{\infty} e^{-n^2\pi x}$$

$$\xi(t) = \frac{1}{2} - \left(t^2 - \frac{1}{4}\right) \int_{x=1}^{\infty} \psi(x) x^{\frac{-3}{4}} \cos\left(\frac{1}{2} t \; log \; x\right) dx$$

Pour que les calculs ne soient pas trop longs, on prend 1000 pour valeur la plus grande de n dans le calcul de la fonction $\psi(x)$.

On calcule les valeurs de $\psi(x)$ et $\xi(t)$ pour t de 1 à 10000, le programme et son résultat pouvant être trouvés ici :

— http://denise.vella.chemla.free.fr/pgm-psixideRiemann.pdf,

— http://denise.vella.chemla.free.fr/res-psixideRiemann.pdf.

Les résultats obtenus sont souvent minuscules. On ne comprend malheureusement pas trop comment les interpréter.

On peut également calculer par programme les valeurs de la fonction $\xi(t)$ en utilisant la définition fournie par Riemann et qui est (si on appelle $s = \frac{1}{2} + it$ un zéro de zêta) :

$$\xi(t) = (s-1)\pi^{\frac{-s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s)$$

Le programme et son résultat pour un calcul de $\xi(t)$ pour les entiers de 1 à 10000.

— http://denise.vella.chemla.free.fr/pgmxientiers.pdf,

— http://denise.vella.chemla.free.fr/resxientiers.pdf.

Le programme et son résultat pour un calcul de $\xi(t)$ pour les parties imaginaires des 1000 premiers zéros.

— http://denise.vella.chemla.free.fr/pgmxizeroszeta.pdf,

— http://denise.vella.chemla.free.fr/resxizeroszeta.pdf.