Dancing links pour Conjecture de Goldbach (Denise Vella-Chemla, 31.12.2018)

Cette année, Donald Knuth a offert son traditionnel "arbre de Noël" : une conférence à l'Université de Stanford au sujet des Dancing links [1] [2].

Les Dancing links sont des listes informatiques doublement pointées (dans les deux sens), ce qui rend l'effacement ou le rétablissement d'un élément (opération inverse de l'effacement) dans les listes en question aisés. La force de la structure réside en la conservation des liens entre éléments qui ne sont pas perdus lors des effacements et sont de fait aisément rétablissables. Le Professeur Knuth décrit ces structures de données comme très adaptées à la résolution de problèmes de couverture exacte.

Il est alors tentant d'imaginer et de présenter, sans phrases, d'une manière très visuelle, ce que pourrait être la découverte des décomposants de Goldbach d'un nombre en utilisant les algorithmes portant sur des Dancing links.

On reprend notre exemple fétiche de la recherche des décomposants de Goldbach de 98.

$$\begin{cases} 98 \equiv 0 \pmod 2 \\ 98 \equiv 2 \pmod 3 \\ 98 \equiv 3 \pmod 5 \\ 98 \equiv 0 \pmod 7 \end{cases}$$

Appelons s un décomposant potentiel de 98. s peut être congru, hormis 0, à tout ce à quoi 98 n'est pas congru. Le signe $\vee$ dans le système ci-dessous est à lire comme un ou *exclusif*, son emploi étendu est à comprendre comme le fait de vérifier autant de systèmes de congruences que la combinatoire le permet.

$$\begin{cases} s \equiv 1 \pmod 2 \\ s \equiv 1 \pmod 3 \\ s \equiv 1 \vee 2 \vee 4 \pmod 5 \\ s \equiv 1 \vee 2 \vee 3 \vee 4 \vee 5 \vee 6 \pmod 7 \end{cases}$$

On se concentre sur les impairs, omettant la congruence à 1 (mod 2), les nombres premiers étant tous impairs sauf 2.

	1 (3)	1 (5)	1 (7)
3			
5			
7	1		
9			
11		1	
13	1		
15			1
17			
19	1		
21		1	
23			
25	1		
27			
29			1
31	1	1	
33			
35			
37	1		
39			
41		1	
43	1		1
45			
47			
49	1		

	1 (3)	2 (5)	1 (7)
3			
5			
7	1	1	
9			
11			
13	1		
15			1
17		1	
19	1		
21			
23			
25	1		
27		1	
29			1
31	1		
33			
35			
37	1	1	
39			
41			
43	1		1
45			
47		1	
49	1		

	1 (3)	4 (5)	1 (7)
3			
5			
7	1		
9		1	
11			
13	1		
15			1
17			
19	1	1	
21			
23			
25	1		
27			
29		1	1
31	1		
33			
35			
37	1		
39		1	
41			
43	1		1
45			
47			
49	1	1	

1. Voir ici http://denise.vella.chemla.free.fr/KDCt.html.
2. On s'était régalés, il y a longtemps, à essayer de résoudre le puzzle Eternity et JC, également admirateur de Knuth, avait codé la résolution de ce problème à l'aide de Dancing links.

	1 (3)	1 (5)	2 (7)
3			
5			
7	1		
9			1
11		1	
13	1		
15			
17			
19	1		
21		1	
23			1
25	1		
27			
29			
31	1	1	
33			
35			
37	1		1
39			
41		1	
43	1		
45			
47			
49	1		

	1 (3)	2 (5)	2 (7)
3			
5			
7	1	1	
9			1
11			
13	1		
15			
17		1	
19	1		
21			
23			1
25	1		
27		1	
29			
31	1		
33			
35			
37	1	1	1
39			
41			
43	1		
45			
47		1	
49	1		

	1 (3)	4 (5)	2 (7)
3			
5			
7	1		
9		1	1
11			
13	1		
15			
17			
19	1	1	
21			
23			1
25	1		
27			
29		1	
31	1		
33			
35			
37	1		1
39		1	
41			
43	1		
45			
47			
49	1	1	

	1 (3)	1 (5)	3 (7)
3			1
5			
7	1		
9			
11		1	
13	1		
15			
17			1
19	1		
21		1	
23			
25	1		
27			
29			
31	1	1	1
33			
35			
37	1		
39			
41		1	
43	1		
45			1
47			
49	1		

	1 (3)	2 (5)	3 (7)
3			1
5			
7	1	1	
9			
11			
13	1		
15			
17		1	1
19	1		
21			
23			
25	1		
27		1	
29			
31	1		1
33			
35			
37	1	1	
39			
41			
43	1		
45			1
47		1	
49	1		

	1 (3)	4 (5)	3 (7)
3			1
5			
7	1		
9		1	
11			
13	1		
15			
17			1
19	1	1	
21			
23			
25	1		
27			
29		1	
31	1		1
33			
35			
37	1		
39		1	
41			
43	1		
45			1
47			
49	1	1	

	1 (3)	1 (5)	4 (7)
3			
5			
7	1		
9			
11		1	1
13	1		
15			
17			
19	1		
21		1	
23			
25	1		1
27			
29			
31	1	1	
33			
35			
37	1		
39			1
41		1	
43	1		
45			
47			
49	1		

	1 (3)	2 (5)	4 (7)
3			
5			
7	1	1	
9			
11			1
13	1		
15			
17		1	
19	1		
21			
23			
25	1		1
27		1	
29			
31	1		
33			
35			
37	1	1	
39			1
41			
43	1		
45			
47		1	
49	1		

	1 (3)	4 (5)	4 (7)
3			
5			
7	1		
9		1	
11			1
13	1		
15			
17			
19	1	1	
21			
23			
25	1		1
27			
29		1	
31	1		
33			
35			
37	1		
39		1	1
41			
43	1		
45			
47			
49	1	1	

	1 (3)	1 (5)	5 (7)
3			
5			1
7	1		
9			
11		1	
13	1		
15			
17			
19	1		1
21		1	
23			
25	1		
27			
29			
31	1	1	
33			1
35			
37	1		
39			
41		1	
43	1		
45			
47			1
49	1		

	1 (3)	2 (5)	5 (7)
3			
5			1
7	1	1	
9			
11			
13	1		
15			
17		1	
19	1		1
21			
23			
25	1		
27		1	
29			
31	1		
33			1
35			
37	1	1	
39			
41			
43	1		
45			
47		1	1
49	1		

	1 (3)	4 (5)	5 (7)
3			
5			1
7	1		
9		1	
11			
13	1		
15			
17			
19	1	1	1
21			
23			
25	1		
27			
29		1	
31	1		
33			1
35			
37	1		
39		1	
41			
43	1		
45			
47			1
49	1	1	

	1 (3)	1 (5)	6 (7)
3			
5			
7	1		
9			
11		1	
13	1		1
15			
17			
19	1		
21		1	
23			
25	1		
27			1
29			
31	1	1	
33			
35			
37	1		
39			
41		1	1
43	1		
45			
47			
49	1		

	1 (3)	2 (5)	6 (7)
3			
5			
7	1	1	
9			
11			
13	1		1
15			
17		1	
19	1		
21			
23			
25	1		
27		1	1
29			
31	1		
33			
35			
37	1	1	
39			
41			1
43	1		
45			
47		1	
49	1		

	1 (3)	4 (5)	6 (7)
3			
5			
7	1		
9		1	
11			
13	1		1
15			
17			
19	1	1	
21			
23			
25	1		
27			1
29		1	
31	1		
33			
35			
37	1		
39		1	
41			1
43	1		
45			
47			
49	1	1	

Les décomposants de Goldbach de 98 (que sont 19, 31 et 37) ont été enluminés en rouge et bleu.
L'utilisation des couleurs permettrait peut-être de n'avoir qu'un seul tableau qui contiendrait directement les $\vee$ exclusifs selon chaque module premier, obligeant la couverture à contenir exactement un 1 dans la seconde colonne correspondant au module 3, exactement un 1 dans l'une des 3 colonnes correspondant au module 5 (colonnes 3, 4 et 5 du tableau ci-dessous) et exactement un 1 dans l'une des 6 colonnes correspondant au module 7 (colonnes 6ème et suivantes).

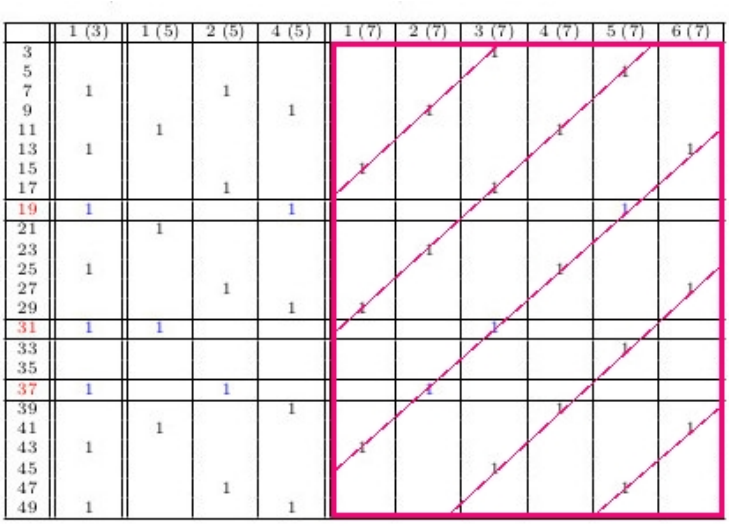
	1 (3)	1 (5)	2 (5)	4 (5)	1 (7)	2 (7)	3 (7)	4 (7)	5 (7)	6 (7)
3							1			
5									1	
7	1		1							
9				1		1				
11		1						1		
13	1									1
15					1					
17			1				1			
19	1			1					1	
21		1								
23						1				
25	1							1		
27			1							1
29				1	1					
31	1	1					1			
33									1	
35										
37	1		1			1				
39				1				1		
41		1								1
43	1				1					
45							1			
47			1						1	
49	1			1						

Dancing links pour Conjecture de Goldbach 2 (Denise Vella-Chemla, 2.1.2018)

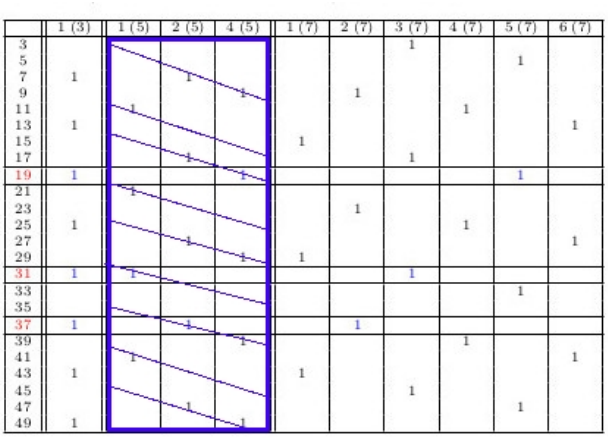
On poursuit à partir du tableau fourni à la fin de la note http://denise.vella.chemla.free.fr/DLpourCG.pdf dans le but d'y "voir les tores de chacun" (i.e. de chaque module).

	1 (3)	1 (5)	2 (5)	4 (5)	1 (7)	2 (7)	3 (7)	4 (7)	5 (7)	6 (7)
3							1			
5									1	
7	1		1							
9				1		1				
11		1						1		
13	1									1
15					1					
17			1				1			
19	1			1					1	
21		1								
23						1				
25	1							1		
27			1							1
29				1	1					
31	1	1					1			
33									1	
35										
37	1		1			1				
39				1				1		
41		1								1
43	1				1					
45							1			
47			1						1	
49	1			1						

Voici les tores.
Le tore selon le module 7 :



Le tore selon le module 5 :



Le tore selon le module 3 :

	1 (3)	1 (5)	2 (5)	4 (5)	1 (7)	2 (7)	3 (7)	4 (7)	5 (7)	6 (7)
3							1			
5									1	
7	1		1							
9				1		1				
11		1						1		
13	1									1
15					1					
17			1				1			
19	1			1					1	
21		1								
23						1				
25	1							1		
27			1							1
29				1	1					
31	1	1					1			
33									1	
35										
37	1		1			1				
39				1				1		
41		1			1					1
43	1						1			
45										
47			1						1	
49	1			1						

En mettant correctement les tores à l'échelle, on obtient le dessin suivant sur lequel apparaissent les décomposants de Goldbach de 98 que sont 19, 31 et 37.

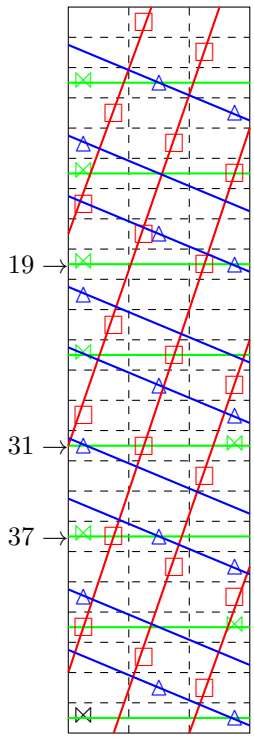
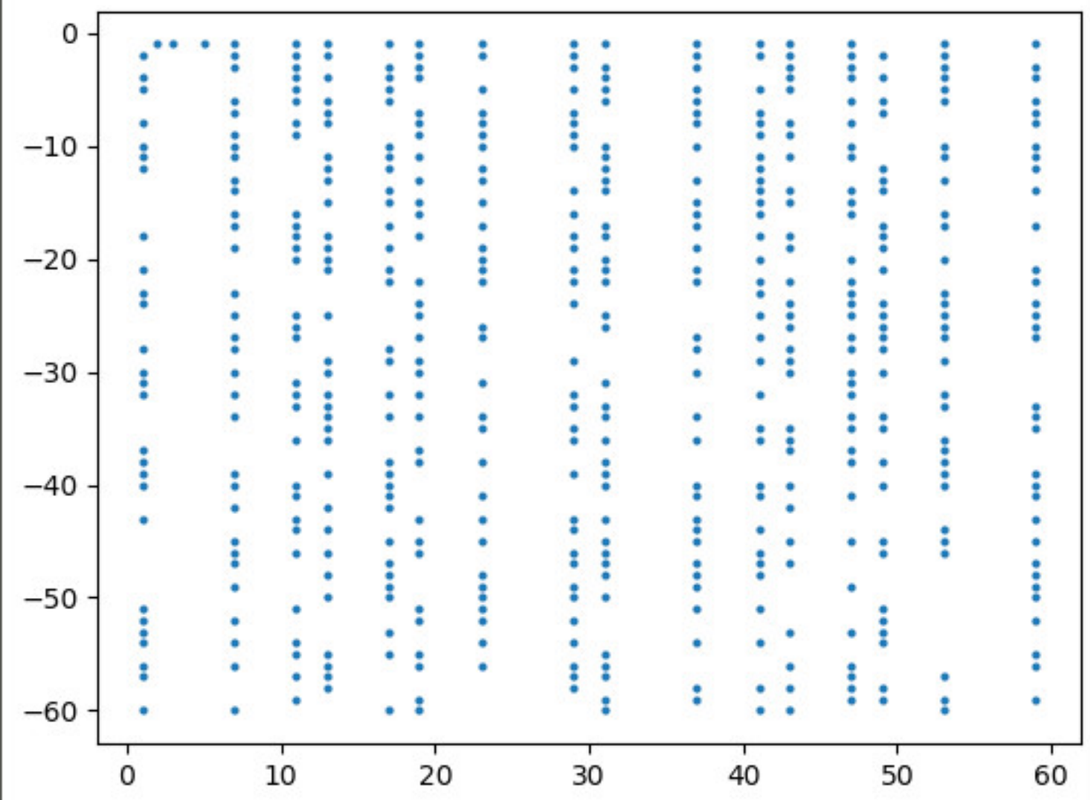


Figure 1



emacs25@vellachemla-X510UA

File Edit Options Buffers Tools Python Help

```
import matplotlib
import matplotlib.pyplot as plt


xs, ys = [], []
with open('pointsducrible', 'r') as f:
    for line in f.readlines():
        x, y = [int(mot) for mot in line.split()]
        xs.append(x)
        ys.append(y)
f.close()

plt.plot(xs, ys, 'o', label='', markersize=2)
plt.show()
```

-:--- dessineratosthene.py All L14 (Pytho

Wrote /home/vella-chemla/Bureau/dessineratostl

emacs25@vellachemla-X510UA

File Edit Options Buffers Tools Python Help

```
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(1,3601):
    if (prime(n)):
        x = (n%60)
        y = (-1)*((n/60)+1)
        print(str(x)+"  "+str(y))
```


coquelicots


nouvelle-zelande.jpg

princess-scientist.

Une gourmandise[1] *(Denise Vella-Chemla, 3.1.2018)*

On appelle *méridien du tore* un cercle de section du tore obtenu si on coupe des tranches de tore comme on coupe un gâteau 3-frères[2].

Du fait de ce à quoi on a réfléchi en 2019, la conjecture de Goldbach pourrait se modéliser ainsi[3] :

Soit n un entier pair (>2) dont on cherche des décomposants de Goldbach.

Appelons $p_1, p_2, \ldots, p_k$ les nombres premiers compris entre 5 et $\left\lfloor \sqrt{\frac{n}{2}} \right\rfloor$, au nombre de $\pi\left(\left\lfloor \sqrt{\frac{n}{2}} \right\rfloor\right) - 2$. On a oublié le nombre premier 2 car tous les nombres premiers potentiellement solutions sont impairs et on a oublié le nombre premier 3 car il servira à couper les tranches de biscuit.

Soit un tore. Imaginer sur ce tore un premier feuilletage non parallèle à un méridien du tore ; seules p_1 ou $2p_1$ feuilles de ce premier feuilletage contiennent au moins un point. Imaginer un second feuilletage, différent du premier, non parallèle à un méridien du tore ; seules p_2 ou $2p_2$ feuilles de ce second feuilletage contiennent au moins un point.

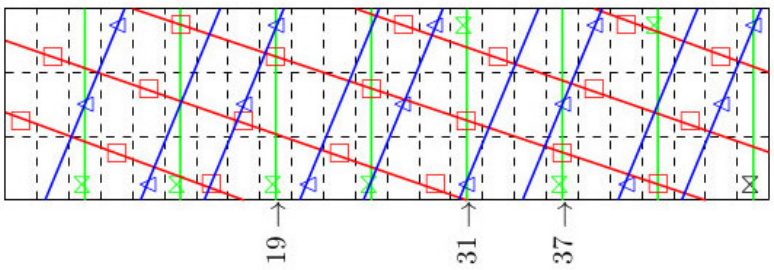
Imaginer sur ce tore un k-ième feuilletage non parallèle à un méridien du tore, différent de tous les feuilletages précédents. Seules p_k ou $2p_k$ feuilles de ce k-ième feuilletage contiennent au moins un point.

Imaginer enfin sur le tore un feuilletage parallèle à un méridien du tore, qu'on appellera le *feuilletage principal*. Certaines feuilles de ce feuilletage contiennent un point et d'autres non ; en fait, une feuille sur 3 contient un point.

Tous les feuilletages sont différents 2 à 2. Un feuilletage compte p_k feuilles lorsque p_k ne divise pas n et en compte $2p_k$ lorsque p_k divise n. On rappelle pour mémoire que pour tout feuilletage, certaines feuilles de ce feuilletage contiennent au moins un point tandis que d'autres feuilles n'en contiennent pas.

Pour démontrer la conjecture de Goldbach, il faudrait démontrer qu'une feuille au moins du feuilletage principal (i.e. *selon un méridien*) contient $k+1$ points, tous sur autant de feuilletages non parallèles 2 à 2.

Illustration dans le cas où $n = 98$: seules les feuilles "à points" sont visualisées, celles du feuilletage principal (module 3) sont vertes et celles des $\pi(\left\lfloor \sqrt{98/2} \right\rfloor) - 2 = 2$ autres feuilletages sont bleues (module 5) et rouges (module 7).

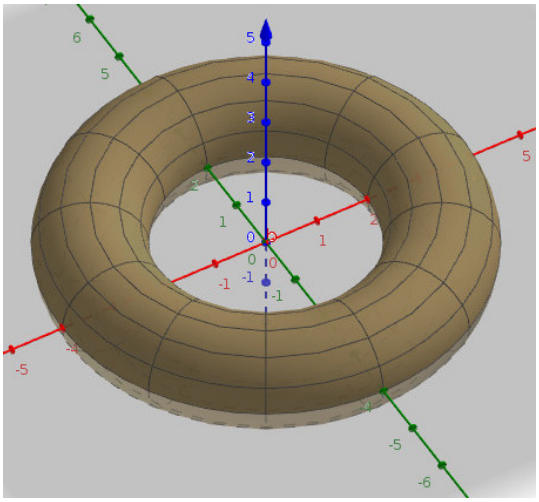


1. C'est un très joli roman, de Muriel Barbery, dans lequel un cuisinier cherche désespérément à retrouver un certain goût de son enfance.
2. Le trois-frères est un gâteau créé au XIX$^{\text{ème}}$ siècle par les trois frères Julien, célèbres pâtissiers parisiens, et qui est toujours cuit dans un moule spécial, en forme de grosse couronne torsadée ou non.
3. On ne sait pas si une telle modélisation permettrait la démonstration de la conjecture de Goldbach.

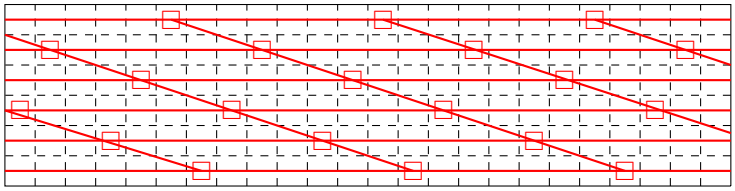
Repriser : patchwork plutôt que brins de laine (Denise Vella-Chemla, 3.1.2018)

Il y a plusieurs problèmes dans la modélisation par courbes sur tore proposée précédemment [1] : d'abord, le tore pose problème au niveau des "jointures", les bords ne se replient pas bien l'un sur l'autre, et verticalement, et horizontalement, c'était une erreur de le croire ; d'autre part, la distance entre les différentes feuilles des feuilletages n'est pas aisée à exprimer dans cette modélisation, alors que cette distance importe beaucoup.

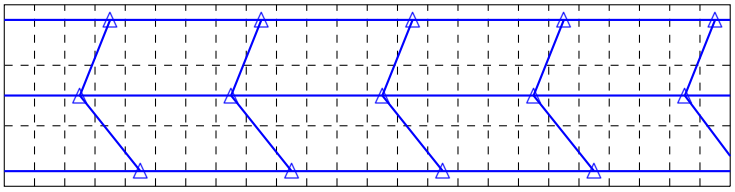
Peut-être vaudrait-il mieux considérer un maillage du tore par des polytopes dont les faces sont des parallélogrammes. Les longueurs de certains côtés des parallélogrammes seraient fixées par les modules (des nombres premiers) et les faces en question ne seraient pas des rectangles pour tous les modules sauf pour le module 3. Le maillage du tore selon le module 3 contiendrait des rectangles quant à lui comme sur la figure ci-dessous.



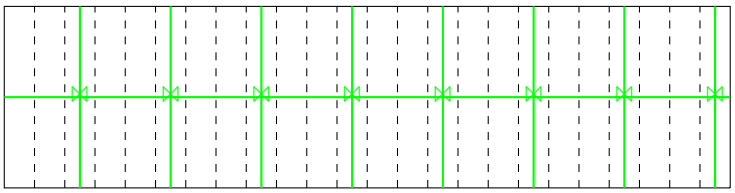
Par exemple, voici le maillage selon le module 7 à la recherche des décomposants de Goldbach de 98.



Voici le maillage selon le module 5 pour la modélisation de ce problème.



Voici le maillage selon le module 3 pour la modélisation de ce problème.

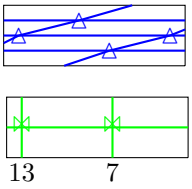


Démontrer la conjecture de Goldbach consisterait alors à démontrer qu'il existe toujours une section du tore selon un méridien [2] qui contient un sommet de chaque polytope.

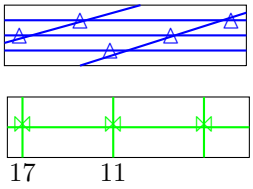
1. Cf. http://denise.vella.chemla.free.fr/topo.pdf.
2. On appelle méridien un petit cercle qui supporte le tore.

Exemples : pavages du plan par des parallélogrammes pour les doubles de nombres premiers (Denise Vella-Chemla, 4.1.2019)

$n = 26$
$n \equiv 2\ (3),\ n \equiv 1\ (5)$
$sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5)$



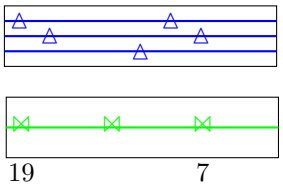
$n = 34$
$n \equiv 1\ (3),\ n \equiv 4\ (5)$
$sol \equiv 2\ (3),\ sol \equiv 1, 2, 3\ (5)$



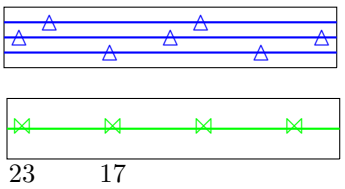
Pour les nombres suivants, on omet les petits côtés des parallélogrammes. La distance horizontale entre deux noeuds-papillon verts est toujours 3, la distance horizontale entre deux triangles bleus d'une même ligne est toujours 5, la distance horizontale entre deux carrés rouges d'une même ligne est toujours 7.

Le maillage du tore qu'on avait envisagé s'est simplifié en un pavage du plan par différents réseaux de parallélogrammes et la démonstration de la conjecture de Goldbach consiste alors à démontrer qu'on a toujours un alignement de sommets, un dans chaque pavage selon un module premier inférieur à la racine carrée du nombre pair dont on cherche les décomposants de Goldbach. Les modules premiers en question contraignent (sont) les longueurs (horizontales ici) des parallélogrammes.

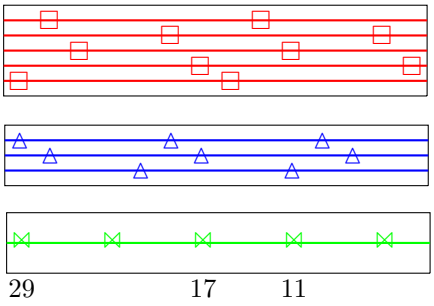
$n = 38$
$n \equiv 2\ (3),\ n \equiv 3\ (5)$
$sol \equiv 1\ (3),\ sol \equiv 1, 2, 4\ (5)$



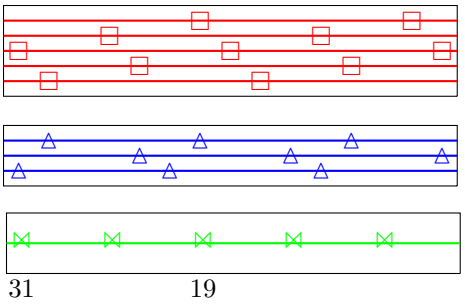
$n = 46$
$n \equiv 1\ (3),\ n \equiv 1\ (5)$
$sol \equiv 2\ (3),\ sol \equiv 2, 3, 4(5)$



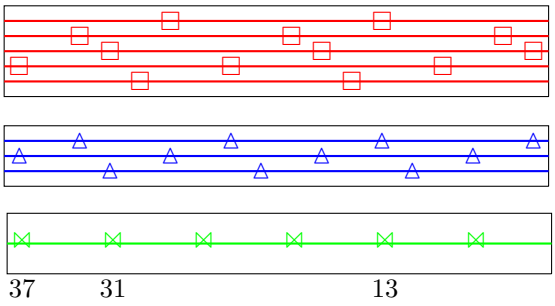
$n = 58$
$n \equiv 1\ (3),\ n \equiv 3\ (5),\ n \equiv 2\ (7)$
$sol \equiv 2\ (3),\ sol \equiv 1, 2, 4\ (5),\ sol \equiv 1, 3, 4, 5, 6\ (7)$



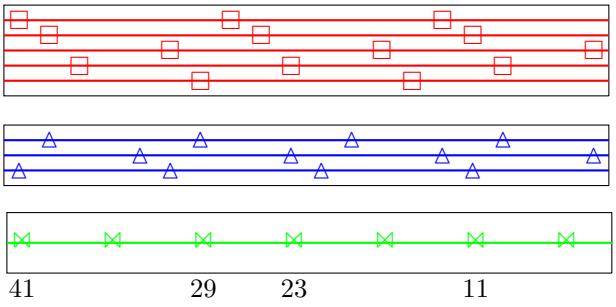
$n = 62$
$n \equiv 2\ (3),\ n \equiv 2\ (5),\ n \equiv 6\ (7)$
$sol \equiv 1\ (3),\ sol \equiv 1, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 5\ (7)$



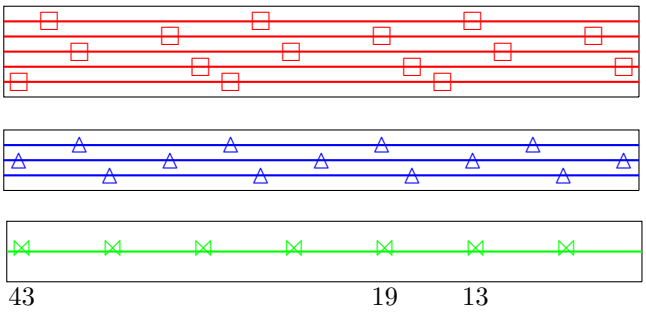
$n = 74$
$n \equiv 2\ (3),\ n \equiv 4\ (5),\ n \equiv 4\ (7)$
$sol \equiv 1\ (3),\ sol \equiv 1, 2, 3\ (5),\ n \equiv 1, 2, 3, 5, 6\ (7)$



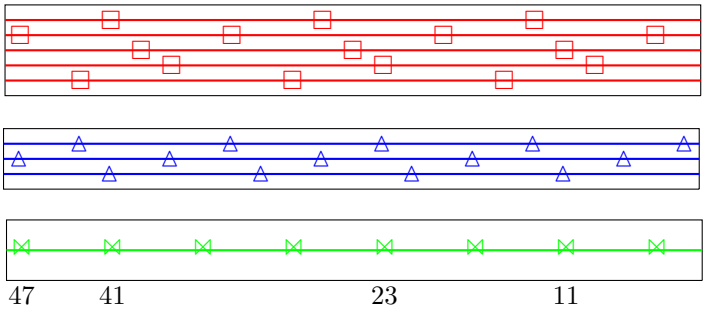
$n = 82$
$n \equiv 1\ (3),\ n \equiv 2\ (5),\ n \equiv 5\ (7)$
$sol \equiv 2\ (3),\ sol \equiv 1, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 6\ (7)$



$n = 86$
$n \equiv 2\ (3),\ n \equiv 1\ (5),\ n \equiv 2\ (7)$
$sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5),\ sol \equiv 1, 3, 4, 5, 6\ (7)$



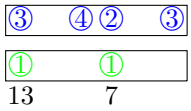
$n = 94$
$n \equiv 1\ (3),\ n \equiv 4\ (5),\ n \equiv 3\ (7)$
$sol \equiv 2\ (3),\ sol \equiv 1, 2, 3\ (5),\ sol \equiv 1, 2, 4, 5, 6\ (7)$



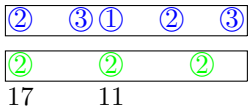
Mots périodiques ou comment projeter tous les restes sur 0 ou 1 (Denise Vella-Chemla, 4.1.2019)

Note : la méthode présentée ci-dessous de recherche de décomposants de Goldbach des nombres doubles de nombres premiers ne permet pas de trouver comme décomposant de Goldbach de n un nombre premier p inférieur à $\lfloor\sqrt{n}\rfloor$ (on oublie systématiquement les congruences à 0). Par exemple, juste ci-dessous, 3 n'est pas noté comme décomposant de Goldbach de 26 le double de 13 alors qu'il en est un : $26 = 3 + 23$.

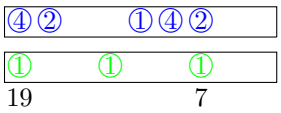
$n = 26$
$n \equiv 2\ (3),\ n \equiv 1\ (5)$
$sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5)$



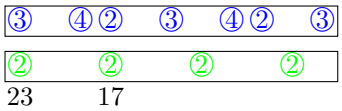
$n = 34$
$n \equiv 1\ (3),\ n \equiv 4\ (5)$
$sol \equiv 2\ (3),\ sol \equiv 1, 2, 3\ (5)$



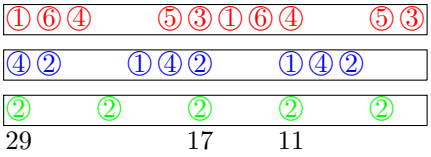
$n = 38$
$n \equiv 2\ (3),\ n \equiv 3\ (5)$
$sol \equiv 1\ (3),\ sol \equiv 1, 2, 4\ (5)$



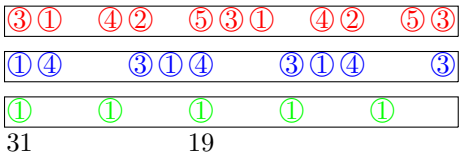
$n = 46$
$n \equiv 1\ (3),\ n \equiv 1\ (5)$
$sol \equiv 2\ (3),\ sol \equiv 2, 3, 4\ (5)$



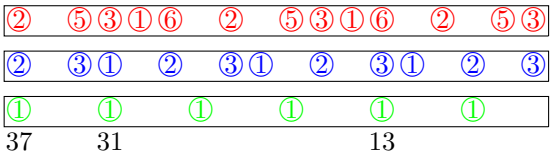
$n = 58$
$n \equiv 1\ (3),\ n \equiv 3\ (5),\ n \equiv 2\ (7)$
$sol \equiv 2\ (3),\ sol \equiv 1, 2, 4\ (5),\ sol \equiv 1, 3, 4, 5, 6\ (7)$



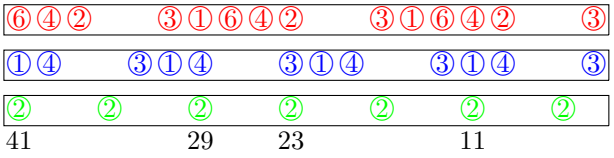
$n = 62$
$n \equiv 2\ (3),\ n \equiv 2\ (5),\ n \equiv 6\ (7)$
$sol \equiv 1\ (3),\ sol \equiv 1, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 5\ (7)$



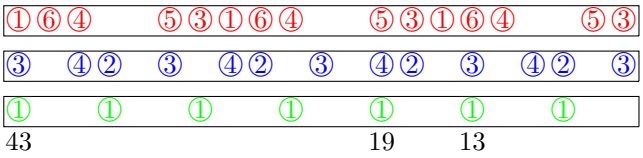
$n = 74$
$n \equiv 2\ (3),\ n \equiv 4\ (5),\ n \equiv 4\ (7)$
$sol \equiv 1\ (3),\ sol \equiv 1, 2, 3\ (5),\ n \equiv 1, 2, 3, 5, 6\ (7)$



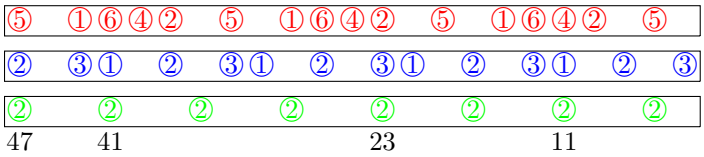
$n = 82$
$n \equiv 1\ (3),\ n \equiv 2\ (5),\ n \equiv 5\ (7)$
$sol \equiv 2\ (3),\ sol \equiv 1, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 6\ (7)$

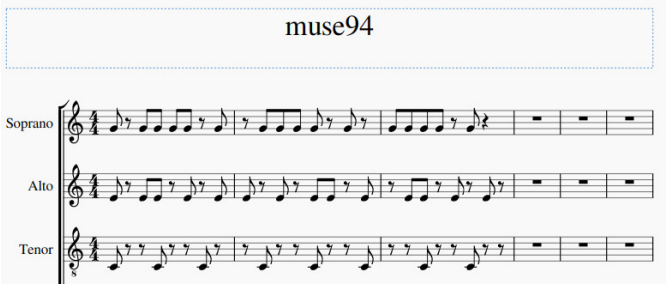


$n = 86$
$n \equiv 2\ (3),\ n \equiv 1\ (5),\ n \equiv 2\ (7)$
$sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5),\ sol \equiv 1, 3, 4, 5, 6\ (7)$



$n = 94$
$n \equiv 1\ (3),\ n \equiv 4\ (5),\ n \equiv 3\ (7)$
$sol \equiv 2\ (3),\ sol \equiv 1, 2, 3\ (5),\ sol \equiv 1, 2, 4, 5, 6\ (7)$





10111101011110101111010
10110101101011010110101
10010010010010010010010

L'expression informatique de la conjecture de Goldbach est :

> *Soit un ensemble de chaînes booléennes périodiques de périodes des mots de longueur impaire telles que le mot période de chaque chaîne contient exactement 2 lettres 0.*
> *A démontrer : la chaîne conjonction ($\wedge$ logique) de toutes ces chaînes contient une lettre 1 au moins.*

Retrouver les palindromes[1]

On commence par voir si l'idée tient pour des chaînes périodiques petites, de longueur 3 et 5.

Les trois chaînes possibles "à 2 zéros" de longueur 3 sont :

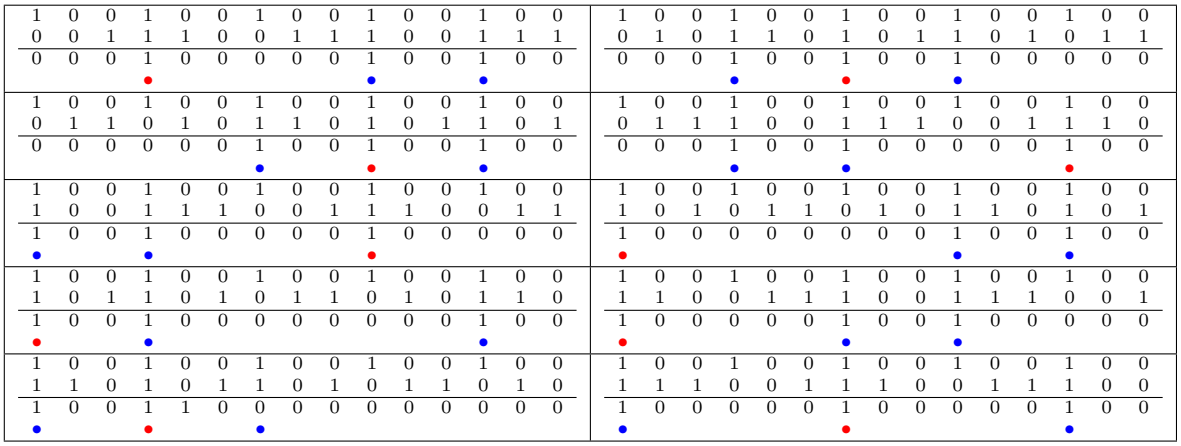
- 100,
- 010,
- 001.

Les 10 chaînes possibles "à 2 zéros" de longueur 5 sont :

- 00111,
- 01011,
- 01101,
- 01110,
- 10011,
- 10101,
- 10110,
- 11001,
- 11010,
- 11100.

Le nombre de chaînes de longueur n est $\frac{n(n-1)}{2}$ car le premier 0 a $n-1$ positions possibles dans le mot et qu'une fois sa position fixée, le second 0 a une position possible de moins que le premier zéro, ce qui fait $1+2+\ldots+(n-1)=\frac{n(n-1)}{2}$ possibilités en tout.

Voici les 10 premières combinaisons, de la première chaîne de longueur 3 avec toutes les chaînes possibles de longueur 5. La chaîne résultante est de longueur 15.



On est tenté d'appeler les lettres rouges "*centres*" des mots auxquels elles appartiennent dans le sens où si on mettait le mot sur un cercle[2] il se lirait identiquement que l'on parcoure le cercle dans le sens des aiguilles d'une montre ou bien dans le sens inverse (sorte de palindrome circulant). Les solutions sont les sommets d'un triangle isocèle porté par le cercle.

1. déjà rencontrés lors de précédentes recherches autour de la conjecture de Goldbach en février 2006, avril et mai 2009 et novembre 2017.

2. Mathématiquement, on appelle *collier* un mot sur un cercle, c'est l'orbite de l'action du groupe cyclique ; on appelle *bracelet* une classe de colliers équivalents par réflexion, le bracelet est l'orbite de l'action du groupe diédral ; l'existence de ces 3 points sommets d'un triangle isocèle sur le cercle se déduit peut-être du théorème de Borsuk-Ulam de partage discret du collier : le *centre* et un point opposé au centre à égale distance des deux points bleus sont antipodaux et existent toujours selon ce théorème.

Cette propriété a pour conséquence (il faudrait le démontrer) qu'il y a toujours une solution de position très basse par rapport à la longueur du mot considéré.

Poursuivons d'un niveau : prenons l'une des chaînes de longueur 15 qu'on avait trouvée (celle en "conjonctant" 001 à 01101) et qui est 001000000001001. C'est une chaîne à 15 caractères. On en fait la conjonction avec une chaîne au hasard de longueur 7 qui contient exactement 2 zéros et qui est 1101110. On obtient une chaîne de longueur 105 ci-dessous. Elle contient 15 solutions indiquées en bleu dont un centre coloré en rouge. La chaîne résultante est effectivement palindrome et se lit indifféremment dans un sens ou l'autre depuis le centre (ou depuis son antipode, indiqué d'un trait rouge entre deux caractères).

On a peut-être enfin trouvé les "rythmes non-rétrogadables" de Messiaen, qu'Alain Connes, Jacques Dixmier et Danye Chéreau évoquent dans leur roman Le Spectre d'Atacama. ([1], [2]).

0	0	1	0	0	0	0	0	0	0	0	1	0	0	1
1	1	0	1	1	1	0	1	1	0	1	1	1	0	1
											•		3	•

0	0	1	0	0	0	0	0	0	0	0	1	0	0	1
1	0	1	1	1	0	1	1	0	1	1	1	0	1	1
	3	•					9				•		3	•

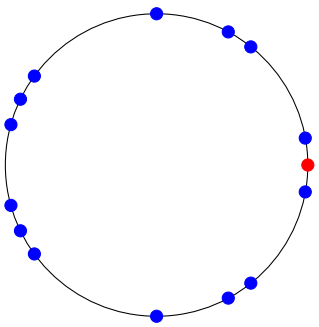
0	0	1	0	0	0	0	0	0	0	0	1	0	0	1
0	1	1	1	0	1	1	0	1	1	1	0	1	1	0
	3	•						15						

0	0	1	0	0	0	0	0	0	0	0	1	0	0	1
1	1	1	0	1	1	0	1	1	1	0	1	1	0	1
		•				9					•		3	•

0	0	1	0	0	0	0	0	0	0	0	1	0	0	1
1	1	0	1	1	0	1	1	1	0	1	1	0	1	1
				12							•		3	•

0	0	1	0	0	0	0	0	0	0	0	1	0	0	1
1	0	1	1	0	1	1	1	0	1	1	0	1	1	1
	3	•						12						•

0	0	1	0	0	0	0	0	0	0	0	1	0	0	1
0	1	1	0	1	1	1	0	1	1	0	1	1	1	0
	3	•				9						•	15	



Référence

[1] Alain Connes, Danye Chéreau, Jacques Dixmier, *Le Spectre d'Atacama*, janvier 2018, éditions Odile Jacob.

[2] Alain Connes, *Motivic rhythms*, décembre 2018, https://arxiv.org/pdf/1812.09946.pdf.

Annexe 1 : ajout d'un niveau

Pour se convaincre davantage, on reprend la chaîne conjonctive des chaînes de longueurs 3, 5 et 7, qui avait ses 1 aux positions suivantes : 12, 15, 18, 27, 30, 33, 48, 57, 60, 72, 75, 78, 90, 93, 102 (et qui est 000000000001001001000000001001001000000000000001000000001001000000000001001001000000000001001000000001000).

On la "conjoint" avec la chaîne périodique de longueur 1155 et de période 11101101111 choisie au hasard et contenant bien 2 lettres 0.

On obtient une chaîne dont les 0 sont aux positions : 12, 27, 30, 33, 57, 60, 72, 75, 78, 90, 93, 102, 120, 123, 132, 135, 138, 153, 162, 165, 177, 195, 198, 207, 222, 225, 228, 237, 240, 243, 258, 267, 270, 285, 288, 300, 303, 327, 330, 333, 342, 363, 372, 375, 387, 390, 393, 405, 408, 417, 432, 435, 438, 450, 453, 468, 492, 495, 498, 522, 537, 540, 552, 555, 558, 573, 582, 585, 597, 600, 603, 615, 618, 627, 648, 657, 660, 663, 687, 690, 702, 705, 720, 723, 732, 747, 750, 753, 762, 765, 768, 783, 792, 795, 813, 825, 828, 837, 852, 855, 858, 867, 870, 888, 897, 900, 912, 915, 918, 930, 933, 957, 960, 963, 978, 993, 1002, 1017, 1020, 1023, 1035, 1047, 1062, 1065, 1068, 1077, 1080, 1083, 1098, 1110, 1122, 1125, 1128, 1143, 1152.

On écrit les écarts, on note le centre en rouge et son antipode d'un trait entre 2 nombres.

15, 15, 3, 3, 24, 3, 12, 3,3, 12, 3, 9, 18, 3, 9, 3, 3, 15, 9, 3, 12, 18, 3, 9, 15, 3, 3, 9, 3, 3, 15, 9, 3, 15, 3, 12, 3, 24, 3, 3, 9, 21, 9, 3, 12, 3, 3, 12, 3, 9, 15, 3, 3, 12, 3, 15, 24, 3|3, 24, 15, 3, 12, 3, 3, 15, 9, 3, 12, 3, 3, 12, 3, 9, 21, 9, 3, 3, 24, 3, 12, 3, 15, 3, 9, 15, 3, 3, 9, 3, 3, 15, 9, 3, 18, 12, 3, 9, 15, 3, 3, 9, 3, 18, 9, 3, 12, 3, 3, 12, 3, 24, 3, 3, 15, 15, 9, 15, 3, 3, 12, 12, 15, 3, 3, ⑨, 3, 3, 15, 12, 12, 3, 3, 15, 9.

On a bien la propriété de palindromie autour du centre (ou autour de son antipode).

On doit comprendre qu'en passant du niveau correspondant à un nombre premier au niveau correspondant au nombre premier suivant, on va obtenir une chaîne qui sera la conjonction de 2 chaînes $s1$ et $s2$; l'une, $s1$, est la concaténation de mots palindromes (elle est périodique de période un palindrome) tandis que l'autre, $s2$, est la concaténation de plusieurs occurrences d'un mot contenant 2 zéros (elle est périodique de période un mot contenant 2 zéros).

La possibilité que 2 lettres 1 se trouvent à même position dans les chaînes $s1$ et $s2$ en question est assez hasardeuse et il faut avoir à l'esprit que trouver un décomposant de Goldbach d'un nombre consiste à trouver une occurrence de 2 lettres 1 à même position dans une sous-chaîne quelconque de la chaîne $s1 \wedge s2$ dont il vient d'être question.

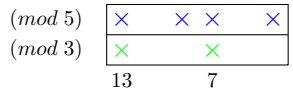
On peut cependant vérifier que ces idées sont correctes en comptant le nombre de solutions pour la chaîne calculée ci-dessus : elle contient 136 solutions (les lettres 1 à la même position dans $s1$ et $s2$) pour une longueur de $1155 = 3 \times 5 \times 7 \times 11$, $\frac{136}{1155} = 0.117$ et ce nombre est bien à peu près égal au produit des $\frac{p-2}{p}$ qui vaut environ $\frac{1}{3}.\frac{3}{5}.\frac{5}{7}.\frac{9}{11} = \frac{9}{77} = 0.117$.

On pense que la conjecture de Goldbach est vraie parce que les conjonctions de 1 se trouvent bien réparties autour du cercle, et il y en a toujours au moins une qui est à une position suffisamment petite pour être inférieure à $n/2$ pour un pair donné n.

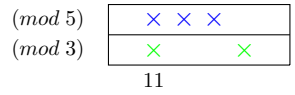
Mots périodiques ou comment projeter tous les restes sur 0 ou 1 (suite) (Denise Vella-Chemla, 9.1.2019)

Note : la méthode présentée ci-dessous de recherche de décomposants de Goldbach des nombres pairs ne permet pas de trouver comme décomposant de Goldbach de n un nombre premier p inférieur à $\lfloor\sqrt{n}\rfloor$ (on oublie systématiquement les congruences à 0). Par exemple, juste ci-dessous, 3 n'est pas noté comme décomposant de Goldbach de 26 le double de 13 alors qu'il en est un : $26 = 3 + 23$. Le traitement des n doubles de premiers est différencié en rouge.

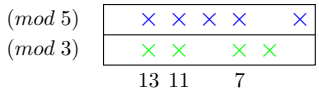
$n = 26,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\quad$ $sol \equiv 1\ (3),\ sol \equiv 2,3,4\ (5)$



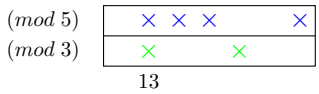
$n = 28,\ n \equiv 1\ (3),\ n \equiv 3\ (5)$ $\quad$ $sol \equiv 2\ (3),\ sol \equiv 1,2,4\ (5)$



$n = 30,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\quad$ $sol \equiv 1\ (3),\ sol \equiv 2,3,4\ (5)$

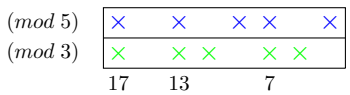


$n = 32,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\quad$ $sol \equiv 1\ (3),\ sol \equiv 2,3,4\ (5)$

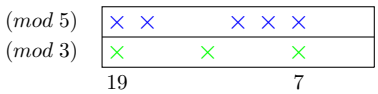


$n = 34,\ n \equiv 1\ (3),\ n \equiv 4\ (5)$ $\quad$ $sol \equiv 2\ (3),\ sol \equiv 1,2,3\ (5)$

$n = 36,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\quad$ $sol \equiv 1\ (3),\ sol \equiv 2,3,4\ (5)$

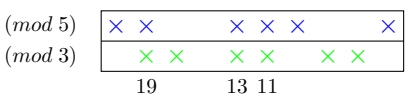


$n = 38,\ n \equiv 2\ (3),\ n \equiv 3\ (5)$ $\quad$ $sol \equiv 1\ (3),\ sol \equiv 1,2,4\ (5)$

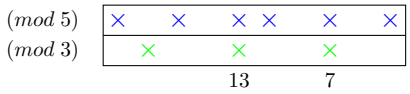


$n = 40,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\quad$ $sol \equiv 1\ (3),\ sol \equiv 2,3,4\ (5)$

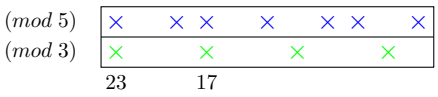
$n = 42,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\quad$ $sol \equiv 1\ (3),\ sol \equiv 2,3,4\ (5)$



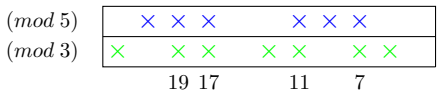
$n = 44,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\qquad$ $sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5)$



$n = 46,\ n \equiv 1\ (3),\ n \equiv 1\ (5)$ $\qquad$ $sol \equiv 2\ (3),\ sol \equiv 2, 3, 4 (5)$

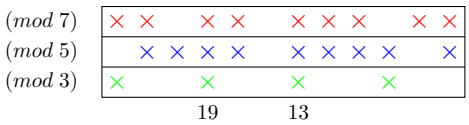


$n = 48,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\qquad$ $sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5)$



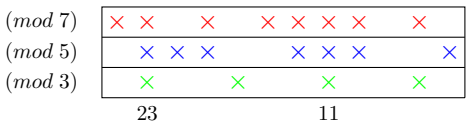
$n = 50,\ n \equiv 2\ (3),\ n \equiv 1\ (5),\ n \equiv 1\ (7)$

$sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5),\ sol \equiv 2, 3, 4, 5, 6\ (7)$



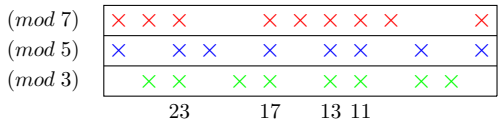
$n = 52,\ n \equiv 1\ (3),\ n \equiv 2\ (5),\ n \equiv 3\ (7)$

$sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5),\ sol \equiv 1, 2, 4, 5, 6\ (7)$



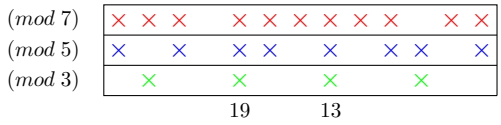
$n = 54,\ n \equiv 0\ (3),\ n \equiv 4\ (5),\ n \equiv 5\ (7)$

$sol \equiv 1, 2\ (3),\ sol \equiv 1, 2, 3\ (5),\ sol \equiv 1, 2, 3, 4, 6\ (7)$



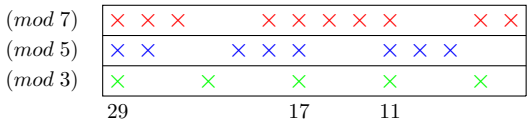
$n = 56,\ n \equiv 2\ (3),\ n \equiv 1\ (5),\ n \equiv 0\ (7)$

$sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 5, 6\ (7)$



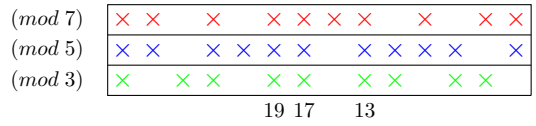
$n = 58,\ n \equiv 1\ (3),\ n \equiv 3\ (5),\ n \equiv 2\ (7)$

$sol \equiv 2\ (3),\ sol \equiv 1, 2, 4\ (5),\ sol \equiv 1, 3, 4, 5, 6\ (7)$



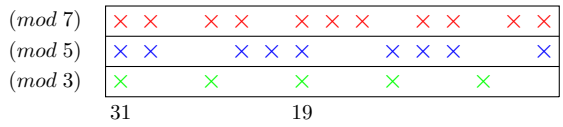
$n = 60,\ n \equiv 0\ (3),\ n \equiv 0\ (5),\ n \equiv 4\ (7)$

$$sol \equiv 1, 2\ (3),\ sol \equiv 1, 2, 3, 4\ (5),\ sol \equiv 1, 2, 4, 5, 6\ (7)$$



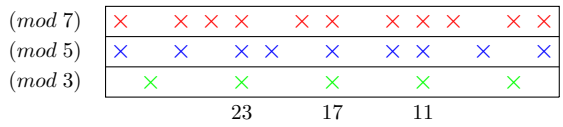
$n = 62,\ n \equiv 2\ (3),\ n \equiv 2\ (5),\ n \equiv 6\ (7)$

$$sol \equiv 1\ (3),\ sol \equiv 1, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 5\ (7)$$



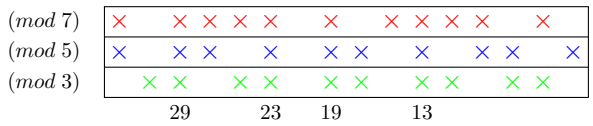
$n = 64,\ n \equiv 1\ (3),\ n \equiv 4\ (5),\ n \equiv 1\ (7)$

$$sol \equiv 2\ (3),\ sol \equiv 1, 2, 3\ (5),\ sol \equiv 2, 3, 4, 5, 6\ (7)$$



$n = 66,\ n \equiv 0\ (3),\ n \equiv 1\ (5),\ n \equiv 3\ (7)$

$$sol \equiv 1, 2\ (3),\ sol \equiv 2, 3, 4\ (5),\ sol \equiv 1, 2, 4, 5, 6\ (7)$$

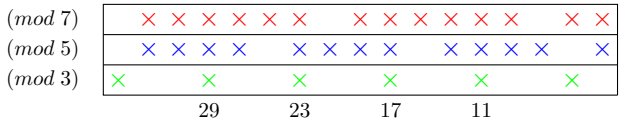


$n = 68,\ n \equiv 2\ (3),\ n \equiv 3\ (5),\ n \equiv 5\ (7)$

$$sol \equiv 1\ (3),\ sol \equiv 1, 2, 4\ (5),\ sol \equiv 1, 2, 3, 4, 6\ (7)$$

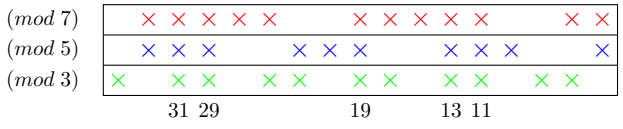
$n = 70,\ n \equiv 1\ (3),\ n \equiv 0\ (5),\ n \equiv 0\ (7)$

$$sol \equiv 2\ (3),\ sol \equiv 1, 2, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 5, 6\ (7)$$



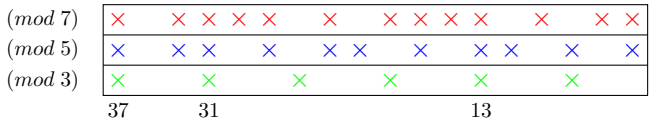
$n = 72,\ n \equiv 0\ (3),\ n \equiv 2\ (5),\ n \equiv 2\ (7)$

$$sol \equiv 1, 2\ (3),\ sol \equiv 1, 3, 4\ (5),\ sol \equiv 1, 3, 4, 5, 6\ (7)$$



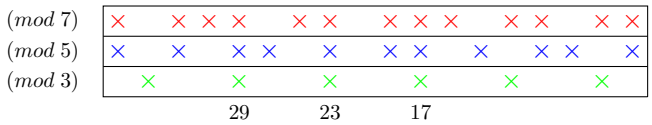
$n = 74,\ n \equiv 2\ (3),\ n \equiv 4\ (5),\ n \equiv 4\ (7)$

$sol \equiv 1\ (3),\ sol \equiv 1, 2, 3\ (5),\ sol \equiv 1, 2, 3, 5, 6\ (7)$



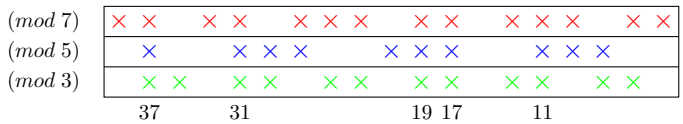
$n = 76,\ n \equiv 1\ (3),\ n \equiv 1\ (5),\ n \equiv 6\ (7)$

$sol \equiv 2\ (3),\ sol \equiv 2, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 5\ (7)$



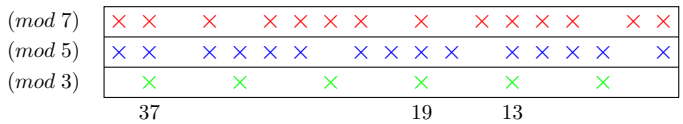
$n = 78,\ n \equiv 0\ (3),\ n \equiv 3\ (5),\ n \equiv 1\ (7)$

$sol \equiv 1, 2\ (3),\ sol \equiv 1, 2, 4\ (5),\ sol \equiv 2, 3, 4, 5, 6\ (7)$



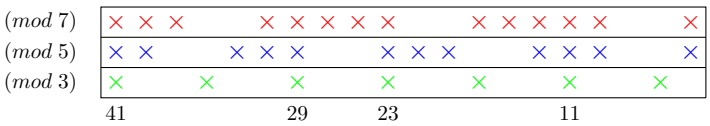
$n = 80,\ n \equiv 2\ (3),\ n \equiv 0\ (5),\ n \equiv 3\ (7)$

$sol \equiv 1\ (3),\ sol \equiv 1, 2, 3, 4\ (5),\ sol \equiv 1, 2, 4, 5, 6\ (7)$



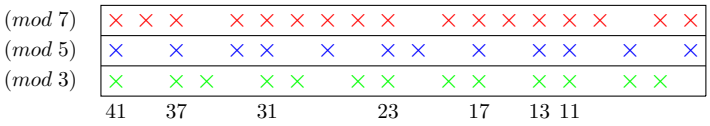
$n = 82,\ n \equiv 1\ (3),\ n \equiv 2\ (5),\ n \equiv 5\ (7)$

$sol \equiv 2\ (3),\ sol \equiv 1, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 6\ (7)$



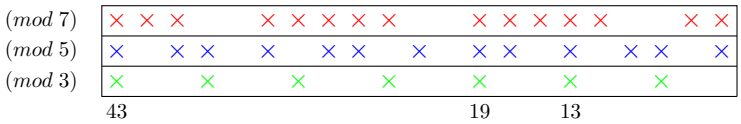
$n = 84,\ n \equiv 0\ (3),\ n \equiv 4\ (5),\ n \equiv 0\ (7)$

$sol \equiv 1, 2\ (3),\ sol \equiv 1, 2, 3\ (5),\ sol \equiv 1, 2, 3, 4, 5, 6\ (7)$



$n = 86,\ n \equiv 2\ (3),\ n \equiv 4\ (5),\ n \equiv 2\ (7)$

$sol \equiv 1\ (3),\ sol \equiv 1, 2, 3\ (5),\ sol \equiv 1, 3, 4, 5, 6\ (7)$

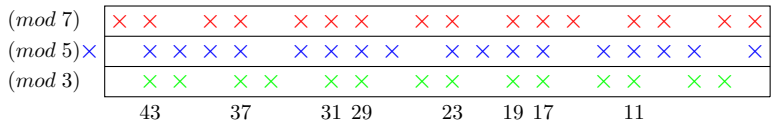


$n = 88,\ n \equiv 1\ (3),\ n \equiv 3\ (5),\ n \equiv 4\ (7)$

$$sol \equiv 2\ (3),\ sol \equiv 1, 2, 4\ (5),\ sol \equiv 1, 2, 3, 5, 6\ (7)$$

$n = 90,\ n \equiv 0\ (3),\ n \equiv 0\ (5),\ n \equiv 6\ (7)$

$$sol \equiv 1, 2\ (3),\ sol \equiv 1, 2, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 5\ (7)$$

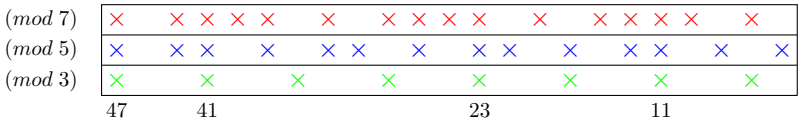


$n = 92,\ n \equiv 2\ (3),\ n \equiv 2\ (5),\ n \equiv 1\ (7)$

$$sol \equiv 1\ (3),\ sol \equiv 1, 3, 4\ (5),\ sol \equiv 2, 3, 4, 5, 6\ (7)$$

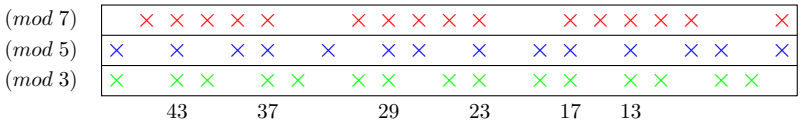
$n = 94,\ n \equiv 1\ (3),\ n \equiv 4\ (5),\ n \equiv 3\ (7)$

$$sol \equiv 2\ (3),\ sol \equiv 1, 2, 3\ (5),\ sol \equiv 1, 2, 4, 5, 6\ (7)$$



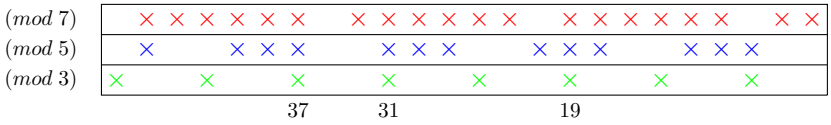
$n = 96,\ n \equiv 0\ (3),\ n \equiv 1\ (5),\ n \equiv 5\ (7)$

$$sol \equiv 1, 2\ (3),\ sol \equiv 2, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 6\ (7)$$



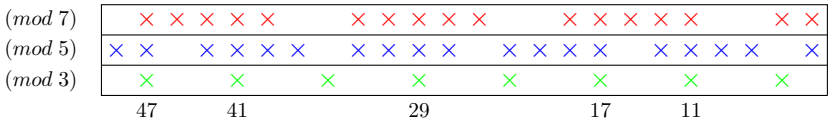
$n = 98,\ n \equiv 2\ (3),\ n \equiv 3\ (5),\ n \equiv 0\ (7)$

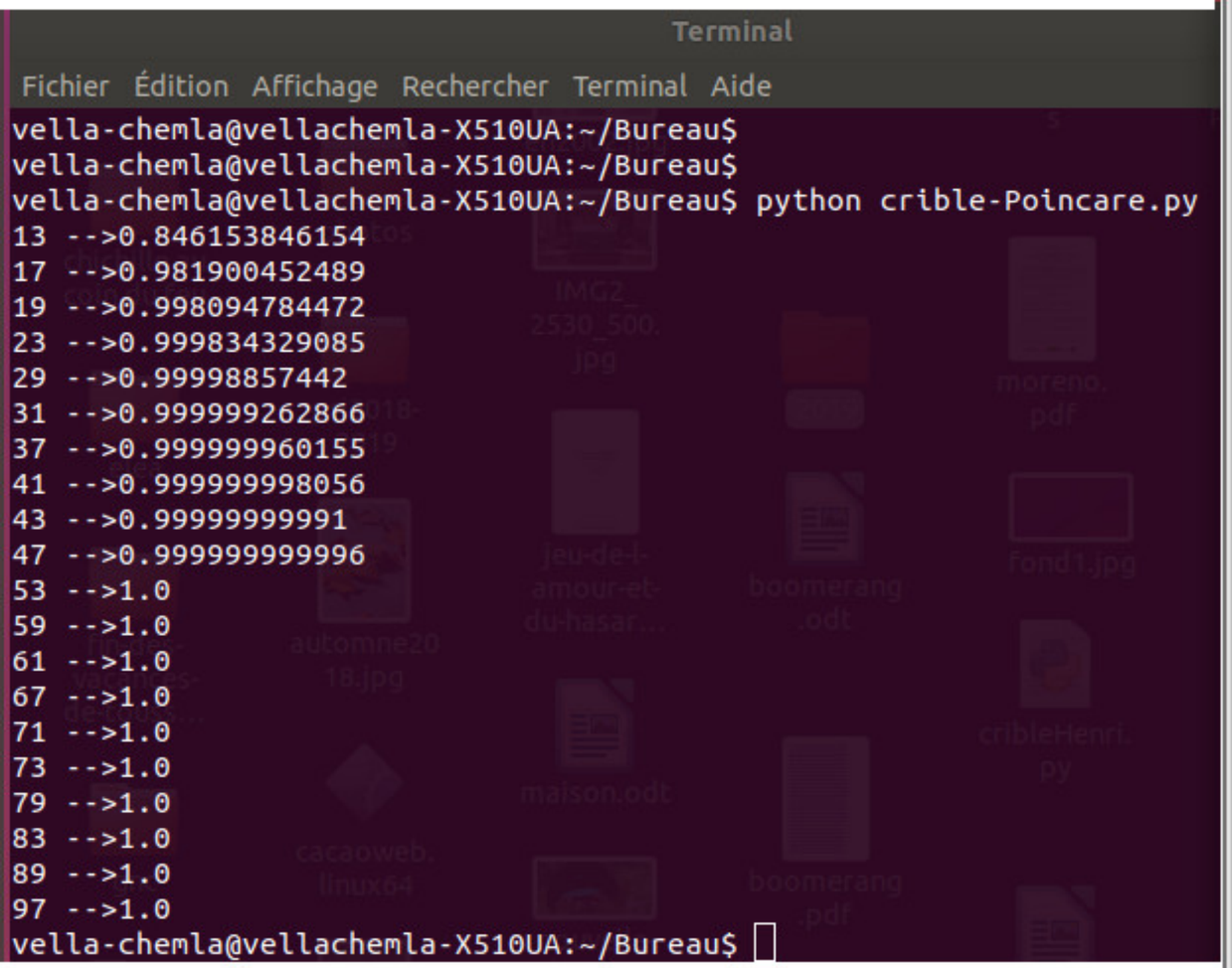
$$sol \equiv 1\ (3),\ sol \equiv 1, 2, 4\ (5),\ sol \equiv 1, 2, 3, 4, 5, 6\ (7)$$

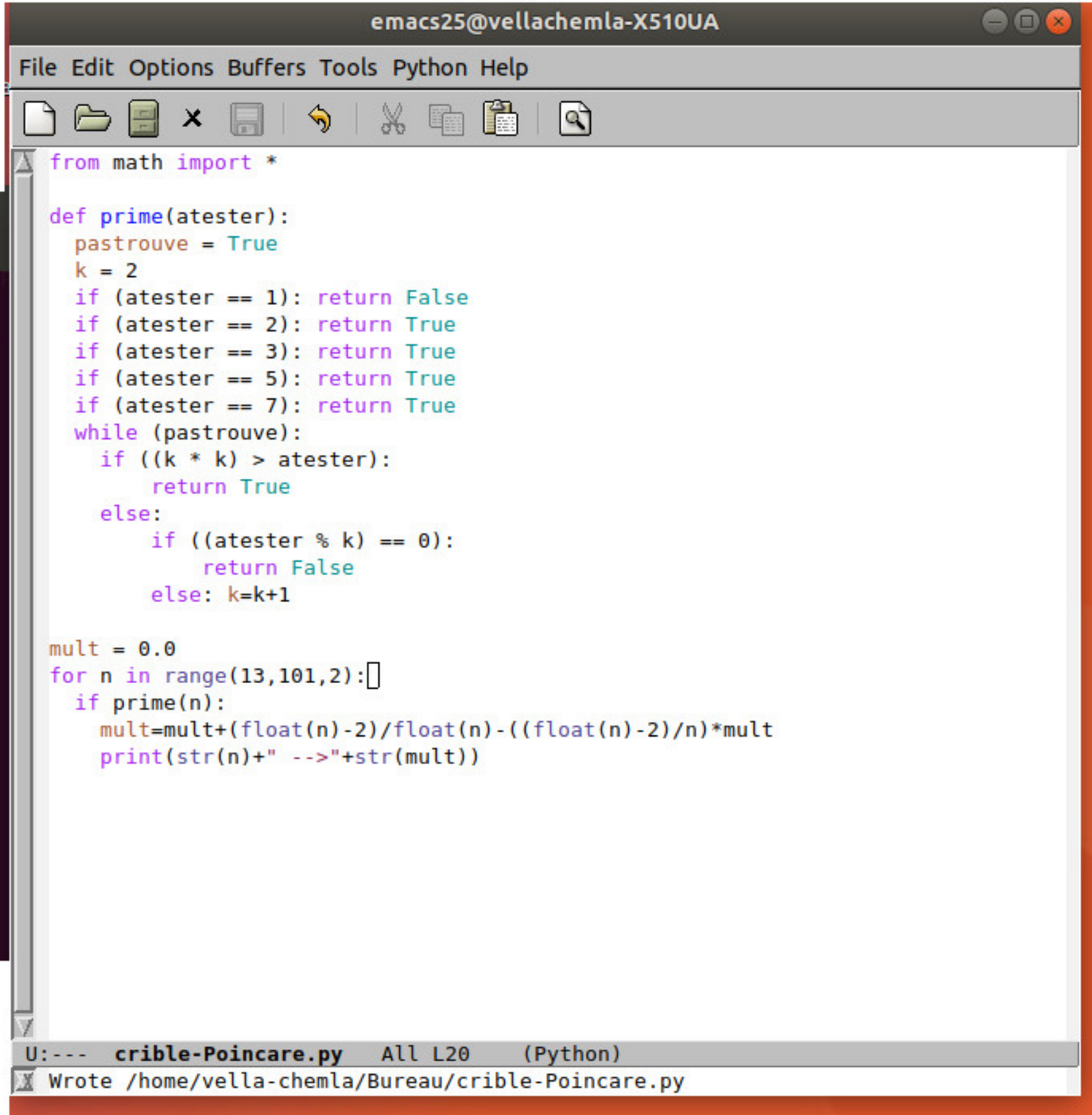


$n = 100,\ n \equiv 1\ (3),\ n \equiv 0\ (5),\ n \equiv 2\ (7)$

$$sol \equiv 2\ (3),\ sol \equiv 1, 2, 3, 4\ (5),\ sol \equiv 1, 3, 4, 5, 6\ (7)$$




Terminal
Fichier Édition Affichage Rechercher Terminal Aide
vella-chemla@vellachemla-X510UA:~/Bureau$
vella-chemla@vellachemla-X510UA:~/Bureau$
vella-chemla@vellachemla-X510UA:~/Bureau$ python crible-Poincare.py
13 -->0.846153846154
17 -->0.981900452489
19 -->0.998094784472
23 -->0.999834329085
29 -->0.99998857442
31 -->0.999999262866
37 -->0.999999960155
41 -->0.999999998056
43 -->0.99999999991
47 -->0.999999999996
53 -->1.0
59 -->1.0
61 -->1.0
67 -->1.0
71 -->1.0
73 -->1.0
79 -->1.0
83 -->1.0
89 -->1.0
97 -->1.0
vella-chemla@vellachemla-X510UA:~/Bureau$

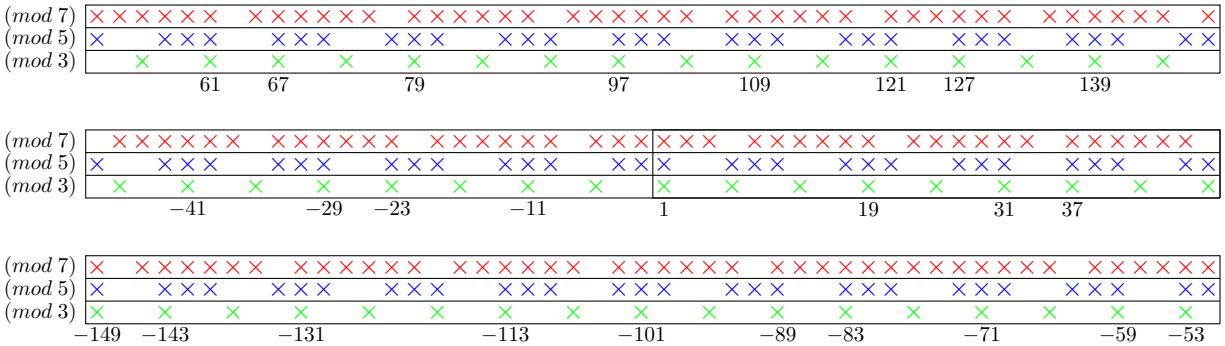

emacs25@vellachemla-X510UA
File Edit Options Buffers Tools Python Help
from math import *
def prime(atester):
pastrouve = True
k = 2
if (atester == 1): return False
if (atester == 2): return True
if (atester == 3): return True
if (atester == 5): return True
if (atester == 7): return True
while (pastrouve):
if ((k * k) > atester):
return True
else:
if ((atester % k) == 0):
return False
else: k=k+1
mult = 0.0
for n in range(13,101,2):
if prime(n):
mult=mult+(float(n)-2)/float(n)-((float(n)-2)/n)*mult
print(str(n)+" -->"+str(mult))
U:--- crible-Poincare.py All L20 (Python)
Wrote /home/vella-chemla/Bureau/crible-Poincare.py

Palindromie dans les séquences booléennes conjonctions de séquences périodiques (Denise Vella-Chemla, 13.1.2019)

On montre sur notre exemple fétiche $n = 98$ la difficulté que représente la nécessité de se cantonner à l'intervalle $[3, 49]$ pour trouver des décomposants de Goldbach ainsi que l'apparition de propriétés de périodicité et de palindromie lorsqu'on effectue la conjonction ($\wedge$ logique) de séquences périodiques de booléens.

$n = 98,\ n \equiv 2\ (3),\ n \equiv 3\ (5),\ n \equiv 0\ (7)$

$sol \equiv 1\ (3),\ sol \equiv 1, 2, 4\ (5),\ sol \equiv 1, 2, 3, 4, 5, 6\ (7)$



Les décompositions apparaissant sur le dessin sont des décompositions de 98 en somme de deux nombres non divisibles par 2, 3, 5 ou 7 et la projection de cet ensemble de nombres sur l'intervalle $[0, 49]$ permet d'obtenir des nombres premiers dans la mesure où 7 est le plus grand nombre premier inférieur à $\sqrt{98}$.

On voit apparaître de nouvelles décompositions de Goldbach de 98 qui contiennent des nombres premiers négatifs. On constate certaines périodicités (par exemple, -149,-143, -89, -83, -59, -53, 31, 37, 61, 67, 121, 127) ainsi qu'une propriété de palindromie des écarts présentée ci-dessous.

$$\begin{aligned}
98 &= 19 + 79\\
98 &= 31 + 67\\
98 &= 37 + 61\\
98 &= 1 + 97\ ^{1}\\
98 &= 109 + (-11)\\
98 &= 127 + (-29)\\
98 &= 151 + (-149)\\
98 &= 173 + (-71)\\
98 &= 191 + (-89)\\
&\dots
\end{aligned}$$

En considérant 1 comme un nombre premier, en marquant où se situe l'entier 0 de façon à se repérer un peu dans le dessin ci-dessus, et en notant les écarts entre les décompositions qui sont ici $\dots, 12, 12, (0), 18, 12, 6, 24, 6, 12, 18, 12, 12, 6, 12, \dots$, on constate la palindromie des écarts autour de l'écart 24. On le colore en bleu pour bien voir cette palindromie autour de lui.

$$\dots, 12, 12, 18, 12, 6, 24, 6, 12, 18, 12, 12, 6, 12, \dots$$

Cette palindromie a ainsi pour centre 49, soit $\frac{n}{2}$ pour $n = 98$. Elle a comme autre centre de palindromie -56 avec $49 + (-56) = 105 = 3 \times 5 \times 7$, les seuls nombres premiers (avec 2 mais on s'est concentré sur les impairs) qu'on a considérés ici.

Conjonctions de mots booléens (Denise Vella-Chemla, 16.1.2019)

On voudrait essayer d'exposer ici ce qui nous bloque.

On a abouti récemment à l'expression informatique suivante pour la conjecture de Goldbach :

On cherche à décomposer un nombre pair n.

Soit un ensemble de chaînes booléennes périodiques s_k de périodes des mots m_k de longueurs impaires l_k [a].

Ces chaînes de booléens sont telles que tout mot période de chaque chaîne contient 1 ou 2 lettres 0.

A démontrer :
La chaîne conjonction ($\wedge$ logique) de toutes ces chaînes contient une lettre 1 au moins à une position inférieure à $\frac{n}{2}$.

a. En fait, les mots en question ont pour longueurs les nombres premiers successifs mais comme les nombres composés ne modifient pas les positions des "trous", on peut simplifier le problème en acceptant toutes les longueurs impaires successives.

La difficulté essentielle nous semble résider dans la nécessité de démontrer qu'une conjonction de booléens de valeur vraie a lieu "avant la moitié de n".

En effet, comme on élimine une ou deux classes de congruences selon tout module premier, le théorème des restes chinois assure qu'on a en tout

$$\prod_{p\ 1^{er},\ p\leqslant\sqrt{n}} (p-2)$$

solutions différentes [1] [2], une pour chaque système de congruences selon les modules p premiers inférieurs ou égaux à $\sqrt{n}$ et que ces solutions appartiennent à l'intervalle

$$\prod_{p\ 1^{er},\ p\leqslant\sqrt{n}} p.$$

Mais il faut cependant être assuré qu'une solution au moins appartient bien à l'intervalle $\left[3, \frac{n}{2}\right]$.

Pour envisager comment cela pourrait ne pas être le cas, on considère les entiers jusqu'à n et on programme des calculs de conjonctions de chaînes booléennes qui éliminent deux classes de congruence selon tout module premier inférieur à $\sqrt{n}$, on choisit les classes 0 et, arbitrairement, $p-1$ $(mod\ p)$. Si le plus grand écart entre 2 solutions dans ce "pire des cas arbitraire" s'avérait inférieur à $\frac{n}{2}$, on serait assuré de toujours avoir un décomposant de Goldbach dans l'intervalle $\left[3, \frac{n}{2}\right]$. Ce programme "pire des cas", en faisant occuper un maximum de place aux "trous" (nombres que le crible doit éliminer) est tel que la première solution trouvée est l'écart maximum recherché.

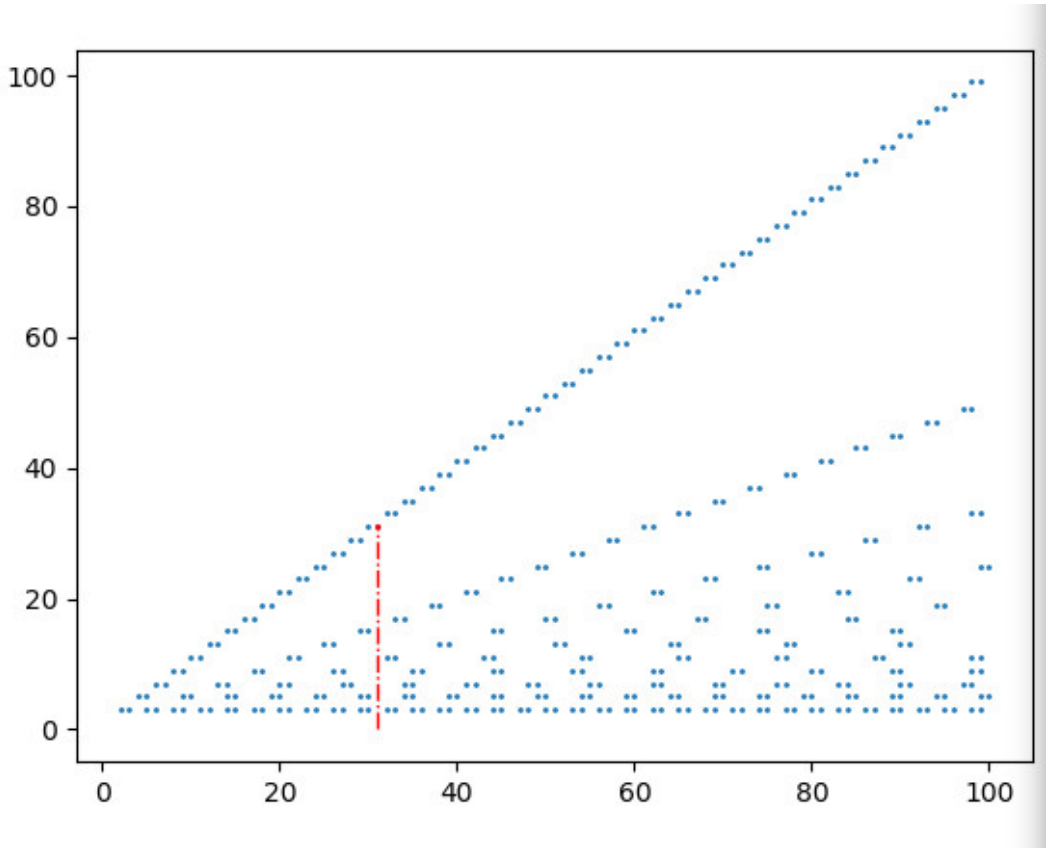
Le tableau suivant fournit, pour différentes valeurs de n quel est le plus petit premier qui n'est jamais

1. $\prod$ désigne le produit ici, et ne doit pas être confondu avec $\pi(n)$ utilisé pour dénoter le nombre de nombres premiers inférieurs ou égaux à n.
2. Le fait d'éliminer une seule classe de congruence selon un certain module a pour effet de remplacer $p-2$ par $p-1$ dans le produit à effectuer, cela augmente le nombre de solutions ; l'élimination des nombres appartenant à une ou deux classes de congruences est fonction des restes de n selon les différents modules inférieurs à $\sqrt{n}$. On élimine les nombres d'une seule classe de congruence lorsque le module divise n et 2 classes lorsque le module ne divise pas n. Se reporter à denise.vella.chemla.free.fr/doublescomposes.pdf.

congru à $p-1$ $(mod\ p)$ selon tout module premier inférieur à $\sqrt{n}$.

n	*plus petit premier* $> n$ *et jamais congru* à $p-1$ $(mod\ p)$
de 26 à 48	7
de 50 à 960	31
de 962 à 1368	73
de 1370 à 10000	127

Voici un graphique montrant par colonnes vides jusqu'à la plus haute diagonale ce qu'on entend par éliminer deux classes de congruences selon chaque module impair (la classe 0 et la classe $p-1$ $(mod\ p)$). On a choisi $n = 100$, on repère 31, le plus petit nombre premier non congru à 2 $(mod\ 3)$, non congru à 4 $(mod\ 5)$ et non congru à 6 $(mod\ 7)$, les trois modules inférieurs à $\sqrt{100}$.



Balade dans le jardin des premiers[1] *(Denise Vella-Chemla, 17.1.2019)*

On voudrait se rappeler ici d'un petit retour vers la physique.

Ce qu'on aimerait trouver, c'est une opération qui permettrait de passer directement d'un premier à un autre.

Voyons 1, qui n'est pas premier, comme le seul nombre entier qui, divisé par tous les autres nombres, dont les nombres premiers, a pour reste 1.

En ce moment, on est confronté à un problème particulier qui est "Etant donné un ensemble $\{p_1, p_2, \ldots, p_k\}$ de nombres premiers successifs[2], quel est le plus petit nombre premier supérieur à p_k et qui, quel que soit p_k, n'est pas congru à $p_k - 1$ $(mod\ p_k)$?". On voudrait simplement effectuer une petite promenade à partir de 1 à base de sauts additifs qui amènerait au nombre premier minimum recherché.

Pourquoi des sauts additifs ? Parce que la multiplication fait sortir de l'ensemble des nombres premiers : un nombre premier, multiplié par quoi que ce soit, donne un nombre composé, et ça n'est pas ce qu'on cherche.

Pour simplifier notre problème, on va ne considérer que les nombres impairs, et on va se fixer sur les nombres premiers $3, 5, 7$.

Ce qu'il faut alors avoir à l'esprit, c'est la notion de saut quantique, ou saut discret : l'électron saute de couche en couche et pour ce faire, il absorbe une quantité d'énergie de valeur fixée.

Ici, c'est pareil : quand on saute de 3 en 3 à partir d'un nombre, le reste des nombres obtenus dans leur division par 3 ne change pas. Quand on saute de 5 en 5, c'est le reste des nombres obtenus dans leur division par 5 qui ne change pas et plus généralement, quand on saute de p en p, c'est le reste des nombres obtenus dans leur division par p qui ne change pas. Dit quantiquement, pour qu'un nombre donne son reste modulo p à un autre nombre, il faut lui ajouter un multiple de p.

On part de 1, on doit sauter de nombre en nombre à la recherche d'une solution qui est un nombre premier supérieur à 7 (dont le reste n'est pas 0 dans les divisions par 3, 5 et 7) et dont le reste n'est pas 2 $(mod\ 3)$, 4 $(mod\ 5)$ et 6 $(mod\ 7)$. Quels choix s'offrent à nous ? Soit faire des sauts de 6 en 6 pour conserver le reste modulo 3 (tout en étant impair), soit faire des sauts de 10 en 10 pour conserver le reste modulo 5 (tout en étant impair), soit faire des sauts de 14 en 14 pour conserver le reste modulo 7 (tout en étant impair).

On sait qu'on trouvera forcément une solution qui vérifie les différentes contraintes du point de vue des congruences, c'est le théorème des restes chinois qui l'assure, et une solution qui soit un nombre premier (car toute suite arithmétique en contient) mais ce qui nous intéresse ici, c'est un moyen sûr de parvenir (directement ?) à la solution minimale car on cherche à majorer cette valeur minimale[3].

1. ou bien balade dans le premier des jardins, ou bien écrire en prose pour ne pas oublier, ou bien écrire en prose pour ne pas être oubliée.

2. supérieurs ou égaux à 3, on oublie 2, et on fera des sauts pairs pour rester dans les impairs.

3. Pour résoudre la conjecture de Goldbach, il faudrait être capable de majorer la solution recherchée par $\frac{n}{2}$ lorsqu'on cherche les décomposants de Goldbach de n, les nombres premiers à considérer alors étant les nombres premiers inférieurs à $\sqrt{n}$.

Déroulons l'algorithme de recherche en traitant le module 3 d'abord :

$1+2\times 3=7$	$\to 7\equiv 1\not\equiv 0,2\ (3)$ $\to 7\equiv 2\not\equiv 0,4\ (5)$ $\to 7\equiv 0\ (7)$	$\to ok\ (3)$ $\to ok\ (5)$ $\to raté\ (7)$
$1+4\times 3=13$	$\to 13\equiv 1\ (3)\not\equiv 0,2\ (3)$ $\to 13\equiv 3\not\equiv 0,4\ (5)$ $\to 13\equiv 6\ (7)$	$\to ok\ (3)$ $\to ok\ (5)$ $\to raté\ (7)$
$1+6\times 3=19$	$\to 19\equiv 1\not\equiv 2\ (3)$ $\to 19\equiv 4\ (5)$	$\to ok\ (3)$ $\to raté\ (5)$
$1+8\times 3=25$	$\to 25\equiv 1\not\equiv 0,2\ (3)$ $\to 25\equiv 0\ (5)$	$\to ok\ (3)$ $\to raté\ (5)$
$1+10\times 3=31$	$\to 31\equiv 1\not\equiv 2\ (3)$ $\to 31\equiv 1\not\equiv 0,4\ (5)$ $\to 31\equiv 3\not\equiv 0,6\ (7)$	$\to ok\ (3)$ $\to ok\ (5)$ $\to ok\ (7)$

Déroulons l'algorithme de recherche en traitant le module 5 d'abord :

$1+2\times 5=11$	$\to 11\equiv 2\ (3)$	$\to raté$
$1+4\times 5=21$	$\to 21\equiv 0\ (7)$	$\to raté$
$1+6\times 5=31$	$\to 31$	$\to ok$

Déroulons l'algorithme de recherche en traitant le module 7 d'abord :

$1+2\times 7=15$	$\to 15\equiv 0\ (3)$	$\to raté$
$1+4\times 7=29$	$\to 29\equiv 2\ (3)$	$\to raté$
$1+6\times 7=43$	$\to 43\equiv 1\ (3), 43\equiv 3\ (5), 43\equiv 1\ (7)$	$\to ok$

La solution obtenue en commençant par le module 7 (qui est 43) est plus grande que celle obtenue en commençant par le module 3 (qui est 31).

Est-ce toujours le cas (solution la plus petite en commençant par le module le plus petit sous prétexte que les deux congruences à éliminer sont 0 et $p-1$ $(mod\ p)$?
Quelle est la solution minimale pour le problème considéré ?
A force de sauts, ne va-t-on pas atterrir sur des nombres supérieurs à p_{max}^2 (avec p_{max} le plus grand nombre premier de l'ensemble considéré), dont il faudrait alors s'assurer de leur indivisibilité par des nombres premier supérieurs à p_{max} ? Quelle est la solution minimale si la seconde congruence à éliminer par module n'est pas $p-1$ mais une classe de congruence quelconque ?

On pense à un arbre de décision. Pour chaque module, soit le nombre obtenu vérifie la contrainte imposée (non congruence à 0 et $p-1$), soit pas. On imagine un arbre binaire à 2^k feuilles, mais on n'arrive pas bien à voir encore comment mélanger cet arbre de décision à notre arbre de promenade par sauts quantiques...

On a l'impression qu'il faut mener un raisonnement combinatoire : $1+2\times 3\times 5$ respecte les contraintes modulo 3 et 5, on s'interroge sur son respect des contraintes modulo 7 ; $1+2\times 3\times 7$ respecte les contraintes modulo 3 et 7, on s'interroge sur son respect des contraintes modulo 5 ; $1+2\times 5\times 7$ respecte les contraintes modulo 5 et 7, on s'interroge sur son respect des contraintes modulo 3. Serait-il possible que les trois nombres pêchent simultanément selon le module sur lequel on n'a pas d'assurance ? Est-ce que le maximum de ces 3 nombres est la borne cherchée ? De toute façon, utiliser les primorielles augmente trop la valeur des nombres. Ne pourrait-on être assuré de trouver une solution avec un ou deux pas selon chaque module, ou guère plus, sous prétexte qu'un saut de longueur $2p_i$ change le reste modulo tout p_j avec j différent de i ?

Ce genre de raisonnement montre bien qu'on est ennuyé car il faut répondre à plusieurs questions simultanément et que la réponse à l'une des questions amène une incertitude sur l'une des autres questions posées et dont on nécessite cependant d'avoir la réponse aussi. On a là une illustration de l'aspect si quantique des nombres premiers.

Cela nous ramène aussi à de vieux souvenirs de parcours d'arêtes de polytopes (des simplexes), en recherche opérationnelle, à la recherche là-aussi d'une solution optimale selon une certaine fonction de coût,

et qui vérifiait certaines contraintes, si ce n'est que les contraintes en question étaient des inéquations linéaires, et qu'on se plaçait donc dans des espaces vectoriels, alors qu'ici, l'action se situe dans des produits cartésiens de corps premiers, sur lesquels il n'y a pas de notion d'ordre...

C'est comme un mirage, quand on s'approche, ça s'éloigne.

Dés (Denise Vella-Chemla, 19.1.2019)

Il s'agit aujourd'hui de montrer où les probabilités ainsi que le non-discret interviennent dans la recherche de décomposants de Goldbach.

On a vu dans des notes précédentes que chercher un décomposant de Goldbach d'un nombre n consiste à éliminer 2 classes de congruences au plus par module p premier, pour tout p inférieur ou égal à $\sqrt{n}$.

On se fixe sur les nombres premiers 3, 5 et 7. On va étudier la manière dont se combinent des motifs rythmiques de périodes de longueur 3, 5 ou 7 sur un mot (une séquence) de longueur $105 = 3.5.7$ ("instant" à partir duquel on retrouvera le même motif rythmique global) et on se fixe pour but de compter précisément les occurrences de certains sous-motifs rythmiques dans le rythme global.

On représente le fait qu'un nombre sur 3 n'est pas satisfaisant pour être un décomposant potentiel de Goldbach tandis que 2 nombres sur 3 le sont par le couple $\begin{pmatrix} \frac{1}{3} & \frac{2}{3} \end{pmatrix}$.

On représente le fait que deux nombres sur 5 ne sont pas satisfaisants pour être un décomposant potentiel de Goldbach tandis que 3 nombres sur 5 le sont par le couple $\begin{pmatrix} \frac{2}{5} & \frac{3}{5} \end{pmatrix}$.

Enfin, on représente le fait que deux nombres sur 7 ne sont pas satisfaisants pour être un décomposant potentiel de Goldbach tandis que 5 nombres sur 7 le sont par le couple $\begin{pmatrix} \frac{2}{7} & \frac{5}{7} \end{pmatrix}$.

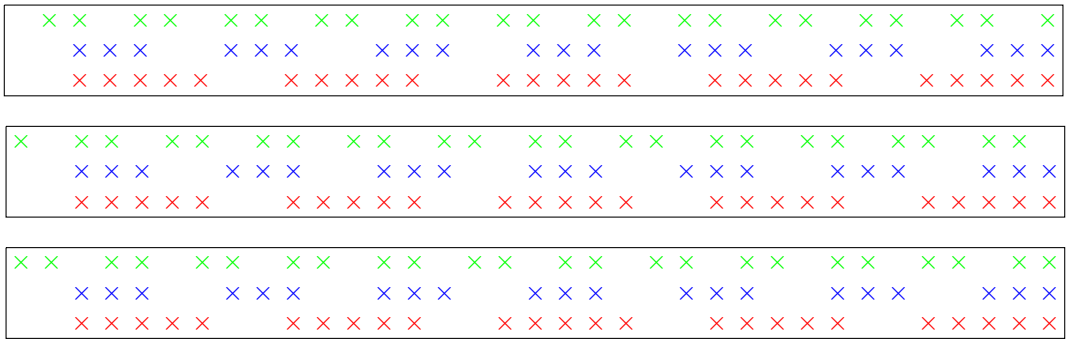
On calcule les probabilités par une sorte de produit tensoriel représenté à notre manière ainsi :

$$\begin{aligned} \begin{pmatrix} \frac{1}{3} & \frac{2}{3} \end{pmatrix} \begin{pmatrix} \frac{2}{5} & \frac{3}{5} \end{pmatrix} \begin{pmatrix} \frac{2}{7} & \frac{5}{7} \end{pmatrix} &= \begin{pmatrix} \frac{2}{15} & \frac{4}{15} & \frac{3}{15} & \frac{6}{15} \end{pmatrix} \begin{pmatrix} \frac{2}{7} & \frac{5}{7} \end{pmatrix} \\ &= \begin{pmatrix} \frac{4}{105} & \frac{8}{105} & \frac{6}{105} & \frac{12}{105} & \frac{10}{105} & \frac{20}{105} & \frac{15}{105} & \frac{30}{105} \end{pmatrix} \end{aligned}$$

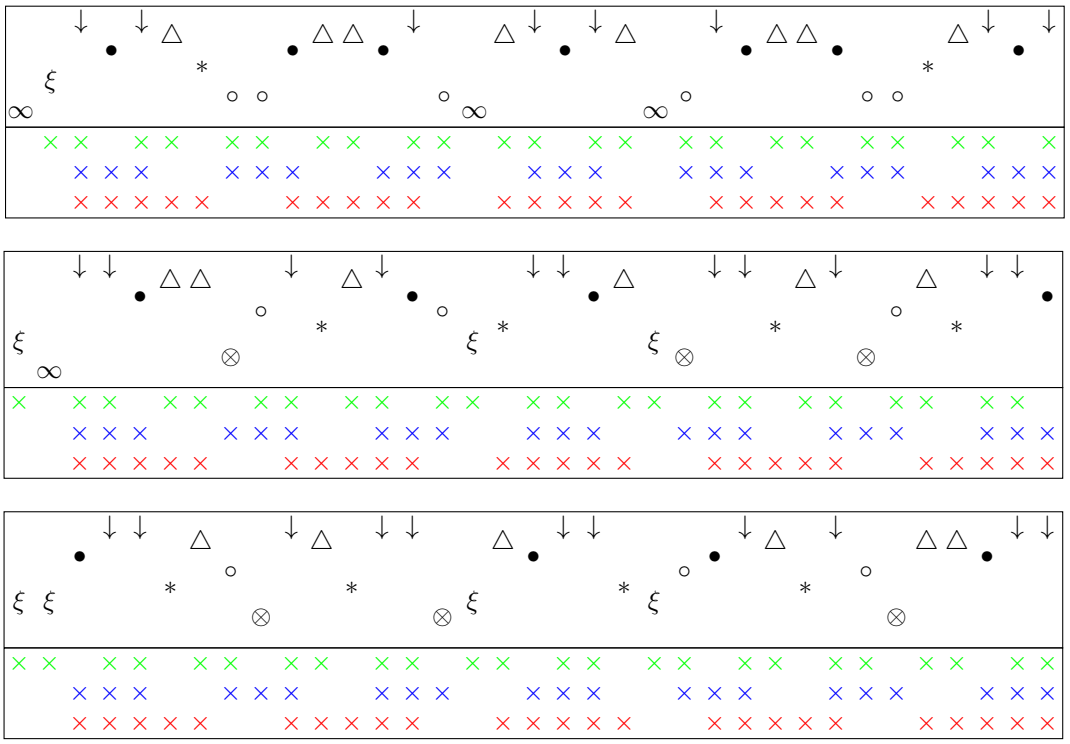
On a bien sûr obtenu 2^3 quantités (des cardinaux ensemblistes), à retrouver précisément parmi les colonnes de la première à la 105-ième.

Attention : il est important de préciser qu'on compte ici des cardinaux d'ensembles obtenus par la combinatoire d'intersections ensemblistes et il ne faut en aucune manière essayer de voir à quels nombres les rangs des colonnes correspondent car on ne factorise rien ici.

D'abord, dessinons des croix dans 3 grilles à lire à la suite l'une de l'autre, et qui respectent bien les motifs rythmiques qu'on s'est fixé (1/3, 2/3 pour la première ligne de chaque grille, 2/5, 3/5 pour la seconde ligne, et 2/7, 5/7 pour la troisième ligne.



Maintenant, utilisons 8 symboles différents, qu'on place au-dessus des grilles, et qui dénotent les colonnes appartenant à la même classe, c'est-à-dire les colonnes qui ont leurs croix au même endroit.

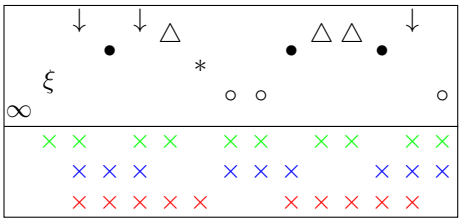


On retrouve nos cardinaux d'ensembles : 4 ∞, 6 $\otimes$, 8 ξ, 10 $*$, 12 $\circ$, 15 $\bullet$, 20 $\triangle$ et 30 $\downarrow$.

Il s'agit de bien observer que, même si dans chaque ligne existe une palindromie du mot complet autour d'un certain centre à retrouver, et ce pour chaque symbole, les séquences de symboles prises indépendamment présentent des motifs rythmiques très irréguliers.

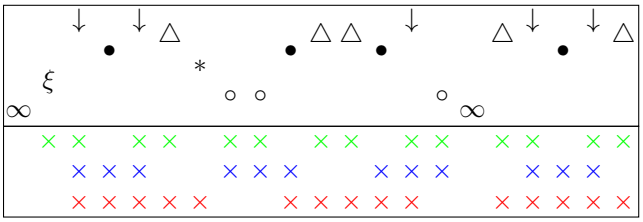
Imaginons maintenant que l'on ne veuille prendre qu'une sous-partie de la séquence des symboles, par exemple ses 15 premières colonnes, histoire de bien couper la séquence totale en 7, ou bien ses 21 premières colonnes (pour la couper en 5) ou enfin, ses 35 premières colonnes (pour la couper en 3, cette dernière possibilité correspondant à la première des 3 grilles vues précédemment et on ne la reproduira donc pas ci-dessous).

Voici les 15 premières colonnes :



Etudions les cardinaux des ensembles de symboles obtenus : 1 ∞, 1 ξ, 1 $*$, 3 $\circ$, 3 $\bullet$, 3 $\triangle$ et 3 $\downarrow$. Ces nombres ramenés aux cardinaux globaux sont en général à multiplier par des nombres entiers (par exemple, multiplier par 4 le nombre de $\circ$ pour obtenir le nombre global de $\circ$ qui est 12). Mais pour le symbole $\triangle$, la division ne tombe pas juste parce que le rythme est coupé n'importe où.

Voici les 21 premières colonnes :



Ici, les cardinaux des ensembles de symboles sont : 2 ∞, 1 ξ, 1 $*$, 3 $\circ$, 4 $\bullet$, 5 $\triangle$ et 5 $\downarrow$. Et c'est alors pour le symbole $\bullet$ que la division ne tombe pas juste parce que le motif rythmique est coupé n'importe où.

Enfin, pour la grille dont on prend les 35 premières colonnes, ce sont 4 motifs rythmiques sur les 8 qui sont coupés quelque part dans le motif, ce qui fait que les divisions ne tombent pas juste : les motifs rythmiques codés par les symboles $\infty, \bullet, \triangle$ et $\downarrow$.

Voici dans un tableau les ratios résumés. Si on fait la moyenne des multiplicandes entre parenthèses (nombre k par lequel il faudrait multiplier le nombre de symboles d'une certaine sorte pour obtenir le nombre total de symboles de cette sorte dans le mot global), on obtient bien un nombre proche de 3, proche de 5 ou proche de 7 suivant la colonne dans laquelle on se situe. On vérifie que le décompte des symboles est juste dans la dernière ligne. La dernière colonne totalise les symboles.

1 ∞ (4)	2 ∞ (2)	3 ∞ $(1,\ldots)$	4
0 $\otimes$ (0)	0 $\otimes$ (0)	0 $\otimes$ (0)	6
1 ξ (8)	1 ξ (2)	1 ξ (8)	8
1 $*$ (10)	1 $*$ (10)	2 $*$ (5)	10
3 $\circ$ (4)	3 $\circ$ (4)	6 $\circ$ (2)	12
3 $\bullet$ (5)	4 $\bullet$ $(3,\ldots)$	7 $\bullet$ $(1,\ldots)$	15
3 $\triangle$ $(6,\ldots)$	5 $\triangle$ (4)	8 $\triangle$ $(2,\ldots)$	20
3 $\downarrow$ (10)	5 $\downarrow$ (6)	8 $\downarrow$ $(3,\ldots)$	30
15 $(47/7 = 6,\ldots)$	21 $(31/7 = 4,\ldots)$	35 $(22/7 = 3,\ldots)$	105

Lorsqu'on cherche les décomposants de Goldbach, c'est exactement ce genre de raisonnement que l'on tient. On pourrait considérer toutes les périodes possibles (y compris les périodes de longueur impaire composée ou de longueur paire), mais c'est inutile puisque les périodes en question ne sont que redondantes par rapport aux périodes de longueurs des nombres premiers.

Un calcul simple donne (dans la première ligne, si l'on considère l'impair composé 9, et dans les lignes suivantes en ne gardant que les nombres premiers) :

$$\frac{1}{3}\frac{3}{5}\frac{5}{7}\frac{7}{9}\frac{9}{11} = \frac{1}{11}$$

$$\frac{1}{3}\frac{3}{5}\frac{5}{7}\frac{9}{11} = \frac{9}{7}\frac{1}{11} > \frac{1}{11}$$

$$\frac{1}{3}\frac{3}{5}\frac{5}{7}\frac{9}{11}\frac{11}{13} > \frac{1}{13}$$

$$\frac{1}{3}\frac{3}{5}\frac{5}{7}\frac{9}{11}\frac{11}{13}\frac{15}{17} = \frac{135}{91}\frac{1}{17} > \frac{1}{17}\cdots$$

On a pu voir dans les grilles que certains motifs rythmiques apparaissent très tardivement (ici le motif codé par le symbole $\otimes$) mais peut-être que le fait que le numérateur de la fraction obtenue dans les calculs ci-dessus soit toujours supérieur à 1 garantit cependant l'existence d'un décomposant de Goldbach.

Théorème de Morley dans $\mathbb{Z}/13\mathbb{Z}$ (Denise Vella-Chemla, 28.1.2019)

Dans une conférence au Collège de France [1] *"Langage et mathématique"*, Alain Connes évoque le fait que le théorème de Morley s'applique à tout corps possédant une racine cubique de l'unité. C'est le cas en particulier de tout corps premier $\mathbb{Z}/p\mathbb{Z}$ tel que 3 divise $p-1$.

Etudions le cas $\mathbb{Z}/13\mathbb{Z}$ qui possède 3 racines de l'unité : la racine triviale 1, et les deux racines 3 et 9. En effet, $3^3 = 27 \equiv 1\ (mod\ 13)$ et $9^3 = 729 \equiv 1\ (mod\ 13)$.

Il y a plein de solutions possibles, qui vérifient les spécifications énoncées dans l'article, mais on va simplement en montrer une, illustrative, et qui fixera [2] bien les idées.

On rappelle la table de 13, pour faciliter les calculs modulaires : 13, 26, 39, 52, 65, 78, 91, 104, 117, 130, 143, ...

On triche un peu : on connaît d'avance ce qu'on cherche : trois opérateurs f, g et h tels que $fgh = \begin{pmatrix} 3 & k \\ 0 & 1 \end{pmatrix}$.

Il faut aussi qu'on ait $f^3g^3h^3 = 1$ (autre notation pour $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$). Par programme, on obtient de très nombreuses solutions respectant ces deux contraintes. Fixons-nous sur une et voyons ce qu'il en est :

$$f = \begin{pmatrix} 5 & 4 \\ 0 & 1 \end{pmatrix}, \quad g = \begin{pmatrix} 2 & 6 \\ 0 & 1 \end{pmatrix}, \quad h = \begin{pmatrix} 12 & 5 \\ 0 & 1 \end{pmatrix}$$

On a bien $fgh = \begin{pmatrix} 5 & 4 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 6 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 12 & 5 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 0 & 1 \end{pmatrix}$.

On calcule pour $M = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ qu'on a $M^3 = \begin{pmatrix} a^3 & a^2b + b(a+1) \\ 0 & 1 \end{pmatrix}$

Ce qui donne comme cubes de f, g et h :

$$f^3 = \begin{pmatrix} 5 & 4 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 8 & 7 \\ 0 & 1 \end{pmatrix}$$
$$g^3 = \begin{pmatrix} 2 & 6 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 8 & 3 \\ 0 & 1 \end{pmatrix}$$
$$h^3 = \begin{pmatrix} 12 & 5 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 12 & 5 \\ 0 & 1 \end{pmatrix}.$$

On véririe qu'on a bien $f^3g^3h^3 = 1$ par le calcul :

$$\begin{pmatrix} 8 & 7 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 8 & 3 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 12 & 5 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

On calcule

$$fg = \begin{pmatrix} 5 & 4 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 6 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 10 & 8 \\ 0 & 1 \end{pmatrix}$$

qui a pour point fixe

$$fix(fg) = 2\ (\text{car } 10 \times 2 + 8 = 28 \equiv 2\ (\text{mod } 13)).$$

On calcule

$$gh = \begin{pmatrix} 2 & 6 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 12 & 5 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 11 & 3 \\ 0 & 1 \end{pmatrix}$$

qui a pour point fixe

$$fix(gh) = 1\ (\text{car } 11 \times 1 + 3 = 14 \equiv 1\ (\text{mod } 13)).$$

1. https://www.college-de-france.fr/site/colloque-2018/symposium-2018-10-18-10h00.htm
2. C'est le cas de le dire, dans la mesure où on cherche des opérateurs et leur point fixe !

On calcule

$$hf = \begin{pmatrix} 12 & 5 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 5 & 4 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 8 & 1 \\ 0 & 1 \end{pmatrix}$$

qui a pour point fixe

$$fix(hf) = 11 \text{ (car } 8 \times 11 + 1 = 89 \equiv 11 \text{ (mod } 13)).$$

Et là, ce qui est assez extraordinaire, c'est qu'on a bien notre racine de l'unité $j = 3$, qui vérifie $fix(gh) + j\ fix(hf) + j^2\ fix(fg) = 0$.

En effet, dans $\mathbb{Z}/13\mathbb{Z}$, $1+3\times11 + 9 \times 2 = 52 \equiv 0\ (mod\ 13)$.

On a donc bien un théorème de Morley qui s'applique dans le corps premier $\mathbb{Z}/13\mathbb{Z}$, et il a de multiples manières de s'appliquer.

On peut refaire les mêmes vérifications pour les matrices de coefficients $a_1 = 12, b_1 = 1, a_2 = 10, b_2 = 2, a_3 = 3, b_3 = 6$ et la racine cubique de l'unité 9.

Conjecture de Goldbach, où l'on retrouve ζ autrement (Denise Vella-Chemla, 26.1.2019)

On s'intéresse à la conjecture de Goldbach qui stipule que tout nombre pair supérieur strictement à 2 est la somme de deux nombres premiers.

On rappelle qu'un nombre premier inférieur à $\frac{n}{2}$, qui ne partage aucun de ses restes avec n un nombre pair supérieur à 2, dans toute division par un nombre premier inférieur à $\sqrt{n}$, est un décomposant de Goldbach de n.

En effet, si x inférieur à $\frac{n}{2}$ ne partage aucun de ses restes avec n dans toute division par un nombre premier inférieur à $\sqrt{n}$, alors $n - x$ est lui aussi premier.

La probabilité qu'un nombre x inférieur à $\frac{n}{2}$ soit premier est fournie par le théorème des nombres premiers ; elle vaut :

$$\frac{\frac{n}{2}}{ln\left(\frac{n}{2}\right)}$$

Supposons maintenant que x est premier. Etudions le non-partage d'un reste au moins entre x et n dans les divisions par les nombres premiers inférieurs à $\sqrt{n}$.

Puisque x est premier, on sait au moins qu'il n'a aucun reste nul dans toute division par un nombre premier inférieur à $\sqrt{n}$.

Dans une division par 3, il lui reste 2 possibilités de reste (1 et 2), et il a une chance sur deux (i.e. 1/2) d'obtenir l'un ou l'autre.

Dans une division par 5, il lui reste 4 possibilités de reste (1, 2, 3 ou 4), et il a une chance sur 4 (i.e. 1/4) d'obtenir l'un ou l'autre.

Dans une division par 7, il lui reste 6 possibilités de reste (1, 2, 3, 4, 5 et 6), et il a une chance sur 6 (i.e. 1/6) d'obtenir l'un ou l'autre.

Plus généralement, dans une division par p, il lui reste $p-1$ possibilités de reste (1, 2, ..., $p-1$), et il a une chance sur $p-1$ (i.e. 1/(p-1)) d'obtenir l'un ou l'autre.

Tous ces événements ayant des probabilités indépendantes, la probabilité d'obtenir leur conjonction est le produit des probabilités de chaque événement séparé (les événements considérés étant "x et n ont même reste dans une division par 3", "x et n ont même reste dans une division par 5", etc.).

Ce produit s'écrit :

$$\prod_{p\ premier\ <\sqrt{n}} \frac{1}{p-1}$$

On peut le réécrire :

$$\prod_{p\ premier\ <\sqrt{n}} \frac{1}{p^{-(-1)}-1}$$

puis

$$-\prod_{p\ premier\ <\sqrt{n}} \frac{1}{1-p^{-(-1)}}$$

et l'on reconnaît alors $-\zeta(-1)$. Ramanujan a démontré que $\zeta(-1) = -\frac{1}{12}$. La note [1] fournit une démonstration simple de ce fait.

On obtient donc comme probabilité globale qu'un nombre x soit d'une part premier, et d'autre part ne partage aucun de ses restes avec n dans une division par un nombre premier inférieur à $\sqrt{n}$ [2] :

$$\frac{\frac{n}{2}}{ln\left(\frac{n}{2}\right)} \times (-\zeta(-1))$$

soit :

$$\frac{n}{2\ ln\ n - 2\ ln\ 2} \times \frac{1}{12}.$$

Ceci semble rendre la conjecture de Goldach vraie à partir de $n = 92$ [3].

1. Par définition $S = 1 + 2 + 3 + 4 + 5 + ...$ On remarque qu'en faisant la différence terme à terme :

$$\begin{array}{rccccl} S - B = & 1+2 & +3+4 & +5+6 & ... & \\ & -1+2 & -3+4 & -5+6 & ... & \\ = & 0+4 & +0+8 & +0+12 & ... = 4(1+2+3+...) = 4S & \end{array}$$

Donc $S - 4S = B$, i.e. $-3S = B$, d'où $S = -\frac{B}{3} = -\frac{\frac{1}{4}}{3}$ Ainsi, on retrouve le résultat attendu : $S = -\frac{1}{12}$.

2. Le fait pour x de ne partager aucun reste avec n dans les divisions par les nombres premiers inférieurs à $\sqrt{n}$ n'a rien à voir avec le fait d'être premier à n. Cette condition est nécessaire (i.e. *impliquée*) mais non suffisante (i.e. *impliquante*). Par exemple, 17 et 81, dont la somme vaut 98, sont tous les deux premiers à 98, mais ils n'en sont pas pour autant des décomposants de Goldbach (de 98) puisque 17 partage le reste de 2 avec 98 lorsqu'on les divise par 3 (Gauss écrit cela $17 \equiv 98\ (mod\ 3)$, c'est lui qui a attiré l'attention de tous sur l'importance de travailler dans les corps premiers).

3. $\frac{92}{2\ ln\ 92 - 2\ ln\ 2}.\frac{1}{12} = 1.0012254835$ alors que $\frac{90}{2\ ln\ 90 - 2\ ln\ 2)}.\frac{1}{12} = 0.9851149163$.

Divisions euclidiennes représentées par des matrices (Denise Vella-Chemla, 5.2.2019)

On continue d'étudier le fait que 98 ait 3 décomposants de Goldbach (19, 31 et 37), c'est-à-dire 3 nombres premiers dont le complément à 98 est premier aussi (79, 67, 61) mais on représente maintenant les nombres par des matrices 2×2 de coefficients dans les corps premiers $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/7\mathbb{Z}$.

La matrice utilisée pour représenter 98 dans $\mathbb{Z}/3\mathbb{Z}$ est $\begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$ car $98 = 32 \times 3 + 2$ et $32 \equiv 2 \ (mod\ 3)$.

La matrice utilisée pour représenter 98 dans $\mathbb{Z}/5\mathbb{Z}$ est $\begin{pmatrix} 4 & 3 \\ 0 & 1 \end{pmatrix}$ car $98 = 19 \times 5 + 3$ et $19 \equiv 4 \ (mod\ 5)$.

La matrice utilisée pour représenter 98 dans $\mathbb{Z}/7\mathbb{Z}$ est $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ car $98 = 14 \times 7 + 0$ et $14 \equiv 0 \ (mod\ 7)$.

Les matrices associées aux nombres impairs dans $\mathbb{Z}/3\mathbb{Z}$ reviennent cycliquement tous les 9 impairs, selon le cycle :

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \dots$$

De même, pour $\mathbb{Z}/5\mathbb{Z}$ (resp. $\mathbb{Z}/7\mathbb{Z}$), le cycle qui fait revenir identiquement les matrices pour représenter les nombres impairs successifs est de longueur 25 (resp. 49) puisqu'on a deux nombres, le quotient et le reste qui parcourent $\mathbb{Z}/5\mathbb{Z}$ (resp. $\mathbb{Z}/7\mathbb{Z}$).

Si l'on observe uniquement le quotient (en haut à gauche des matrices) dans $\mathbb{Z}/3\mathbb{Z}$, en effectuant bien la réduction modulo le nombre premier considéré, ici 3, sa variation suit le cycle

$$+0, +1, +1, +0, +1, +1, +0, +1, +1, \dots$$

Si l'on observe uniquement le reste (en haut à droite des matrices), de nombre pair en nombre pair, naturellement, la variation est toujours

$$+2, +2, +2, \dots$$

et ce quel que soit le corps considéré.

Si l'on observe uniquement le quotient (en haut à gauche des matrices) dans $\mathbb{Z}/5\mathbb{Z}$, en effectuant bien la réduction modulo 5, sa variation suit le cycle

$$+1, +0, +0, +1, +0, +1, +0, +0, +1, +0, +1, +0, \dots$$

(qu'on peut résumer par le mot à 5 lettres 10010).
Si l'on observe uniquement le quotient (en haut à gauche des matrices) dans $\mathbb{Z}/7\mathbb{Z}$, en effectuant bien la réduction modulo 7, sa variation suit le cycle

$$+0, +1, +0, +0, +0, +1, +0, +0, +1, +0, +0, +0, \dots$$

(qu'on peut résumer par le mot à 7 lettres 1000100).

Les décomposants de Goldbach de 98 ont, comme attendu, leur matrice qui ont un coefficient haut droit non nul, pour que le nombre en question soit un nombre premier supérieur à $\sqrt{98}$; pour que le complémentaire du décomposant de Goldbach soit premier aussi, les matrices de 98 et du décomposant dans chaque corps premier doivent avoir un coefficient haut droit différent, c'est-à-dire que 98 et un décomposant de Goldbach de 98 supérieur à $\sqrt{98}$, quel qu'il soit s'il existe, n'ont aucun reste de division euclidienne en commun lorsqu'on les divise par les nombres premiers inférieurs à $\sqrt{98}$.

Voici, pour bien comprendre les processus à l'œuvre, les matrices associées aux nombres impairs de 3 à 49, moitié de 98. Les décomposants de Goldbach sont indiqués en rouge.

		11	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$ $\begin{pmatrix}2&1\\0&1\end{pmatrix}$ $\begin{pmatrix}1&4\\0&1\end{pmatrix}$	21	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$ $\begin{pmatrix}4&1\\0&1\end{pmatrix}$ $\begin{pmatrix}3&0\\0&1\end{pmatrix}$	31	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$ $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ $\begin{pmatrix}4&3\\0&1\end{pmatrix}$	41	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$ $\begin{pmatrix}3&1\\0&1\end{pmatrix}$ $\begin{pmatrix}5&6\\0&1\end{pmatrix}$	$(dans\ \mathbb{Z}/3\mathbb{Z})$ $(dans\ \mathbb{Z}/5\mathbb{Z})$ $(dans\ \mathbb{Z}/7\mathbb{Z})$
3	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$ $\begin{pmatrix}0&3\\0&1\end{pmatrix}$ $\begin{pmatrix}0&3\\0&1\end{pmatrix}$	13	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$ $\begin{pmatrix}2&3\\0&1\end{pmatrix}$ $\begin{pmatrix}1&6\\0&1\end{pmatrix}$	23	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$ $\begin{pmatrix}4&3\\0&1\end{pmatrix}$ $\begin{pmatrix}3&2\\0&1\end{pmatrix}$	33	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$ $\begin{pmatrix}1&3\\0&1\end{pmatrix}$ $\begin{pmatrix}4&5\\0&1\end{pmatrix}$	43	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$ $\begin{pmatrix}3&3\\0&1\end{pmatrix}$ $\begin{pmatrix}6&1\\0&1\end{pmatrix}$	$(dans\ \mathbb{Z}/3\mathbb{Z})$ $(dans\ \mathbb{Z}/5\mathbb{Z})$ $(dans\ \mathbb{Z}/7\mathbb{Z})$
5	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$ $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ $\begin{pmatrix}0&5\\0&1\end{pmatrix}$	15	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$ $\begin{pmatrix}3&0\\0&1\end{pmatrix}$ $\begin{pmatrix}2&1\\0&1\end{pmatrix}$	25	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$ $\begin{pmatrix}0&0\\0&1\end{pmatrix}$ $\begin{pmatrix}3&4\\0&1\end{pmatrix}$	35	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$ $\begin{pmatrix}2&0\\0&1\end{pmatrix}$ $\begin{pmatrix}5&0\\0&1\end{pmatrix}$	45	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$ $\begin{pmatrix}4&0\\0&1\end{pmatrix}$ $\begin{pmatrix}6&3\\0&1\end{pmatrix}$	$(dans\ \mathbb{Z}/3\mathbb{Z})$ $(dans\ \mathbb{Z}/5\mathbb{Z})$ $(dans\ \mathbb{Z}/7\mathbb{Z})$
7	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$ $\begin{pmatrix}1&2\\0&1\end{pmatrix}$ $\begin{pmatrix}1&0\\0&1\end{pmatrix}$	17	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$ $\begin{pmatrix}3&2\\0&1\end{pmatrix}$ $\begin{pmatrix}2&3\\0&1\end{pmatrix}$	27	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$ $\begin{pmatrix}0&2\\0&1\end{pmatrix}$ $\begin{pmatrix}3&6\\0&1\end{pmatrix}$	37	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$ $\begin{pmatrix}2&2\\0&1\end{pmatrix}$ $\begin{pmatrix}5&2\\0&1\end{pmatrix}$	47	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$ $\begin{pmatrix}4&2\\0&1\end{pmatrix}$ $\begin{pmatrix}6&5\\0&1\end{pmatrix}$	$(dans\ \mathbb{Z}/3\mathbb{Z})$ $(dans\ \mathbb{Z}/5\mathbb{Z})$ $(dans\ \mathbb{Z}/7\mathbb{Z})$
9	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$ $\begin{pmatrix}1&4\\0&1\end{pmatrix}$ $\begin{pmatrix}1&2\\0&1\end{pmatrix}$	19	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$ $\begin{pmatrix}3&4\\0&1\end{pmatrix}$ $\begin{pmatrix}2&5\\0&1\end{pmatrix}$	29	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$ $\begin{pmatrix}0&4\\0&1\end{pmatrix}$ $\begin{pmatrix}4&1\\0&1\end{pmatrix}$	39	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$ $\begin{pmatrix}2&4\\0&1\end{pmatrix}$ $\begin{pmatrix}5&4\\0&1\end{pmatrix}$	49	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$ $\begin{pmatrix}4&4\\0&1\end{pmatrix}$ $\begin{pmatrix}0&0\\0&0\end{pmatrix}$	$(dans\ \mathbb{Z}/3\mathbb{Z})$ $(dans\ \mathbb{Z}/5\mathbb{Z})$ $(dans\ \mathbb{Z}/7\mathbb{Z})$

Matrices du groupe affine... (Denise Vella-Chemla, 5.2.2019)

On continue de travailler sur la représentation des nombres par des matrices du groupe affine à coefficients dans les corps premiers.

On fournit dans le tableau ci-dessous les matrices associées aux nombres impairs de 3 à 99, dans le but d'observer une caractérisation des nombres premiers.

A un nombre, sont associées autant de matrices qu'il y a de nombres premiers inférieurs à la racine carrée de ce nombre. Ces matrices sont de la forme :

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

avec a et b appartenant aux différents $\mathbb{Z}/p_k\mathbb{Z}$ notés en tête des colonnes.

Pour alléger la présentation, on omet les coefficients bas des matrices, toujours égaux à 0 et 1.

On observe bien une cyclicité de longueur $18(= 2 \times 3^2)$ dans $\mathbb{Z}/3\mathbb{Z}$ (*nota* : elle est en fait de longueur 9 mais on la voit de 18 ici car on a omis les nombres pairs dans le tableau) : cette cyclicité est telle qu'à 21 est associée la même matrice qu'à 3 ou bien à 35 est associée la même matrice qu'à 17. Cette cyclicité est d'écart $50(= 2 \times 5^2)$ dans la colonne de $\mathbb{Z}/5\mathbb{Z}$, etc.

Une condition nécessaire et suffisante pour qu'un nombre supérieur à 3 soit premier est comme attendu qu'aucun des coefficients b d'aucune de ses matrices associées ne soit nul (ces coefficients sont colorés en bleu pour les nombres premiers supérieurs à 3).

n	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	n	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	n	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$
3	(1 0)			37	(0 1)	(2 2)		71	(2 2)	(4 1)	(3 1)
5	(1 2)			39	(1 0)	(2 4)		73	(0 1)	(4 3)	(3 3)
7	(2 1)			41	(1 2)	(3 1)		75	(1 0)	(0 0)	(3 5)
9	(0 0)			43	(2 1)	(3 3)		77	(1 2)	(0 2)	(4 0)
11	(0 2)			45	(0 0)	(4 0)		79	(2 1)	(0 4)	(4 2)
13	(1 1)			47	(0 2)	(4 2)		81	(0 0)	(1 1)	(4 4)
15	(2 0)			49	(1 1)	(4 4)	(0 0)	83	(0 2)	(1 3)	(4 6)
17	(2 2)			51	(2 0)	(0 1)	(0 2)	85	(1 1)	(2 0)	(5 1)
19	(0 1)			53	(2 2)	(0 3)	(0 4)	87	(2 0)	(2 2)	(5 3)
21	(1 0)			55	(0 1)	(1 0)	(0 6)	89	(2 2)	(2 4)	(5 5)
23	(1 2)			57	(1 0)	(1 2)	(1 1)	91	(0 1)	(3 1)	(6 0)
25	(2 1)	(0 0)		59	(1 2)	(1 4)	(1 3)	93	(1 0)	(3 3)	(6 2)
27	(0 0)	(0 2)		61	(2 1)	(2 1)	(1 5)	95	(1 2)	(4 0)	(6 4)
29	(0 2)	(0 4)		63	(0 0)	(2 3)	(2 0)	97	(2 1)	(4 2)	(6 6)
31	(1 1)	(1 1)		65	(0 2)	(3 0)	(2 2)	99	(0 0)	(4 4)	(0 1)
33	(2 0)	(1 3)		67	(1 1)	(3 2)	(2 4)				
35	(2 2)	(2 0)		69	(2 0)	(3 4)	(2 6)				

Le problème ici est qu'il est spécifié dans la littérature que le coefficient a (en haut à gauche des matrices 2×2, ou à gauche des couples correspondant aux premières lignes des matrices dans le tableau) ne doit pas être nul mais alors on ne voit pas quoi associer comme matrices aux nombres qui posent ce problème du a nul (comme 37 ou 81 par exemple).

Le *Snurpf*[1] qu'on avait proposé pour représenter les nombres était plus simple (représenter chaque nombre par la suite de ses représentations dans les différents corps premiers pour les nombres premiers inférieurs à sa racine) et on avait la même condition nécessaire et suffisante (aucune classe nulle, qui correspondait aux coefficients b ici, ou restes des divisions euclidiennes) pour qu'un nombre soit premier. Les cycles étaient dans chaque corps $\mathbb{Z}/p_k\mathbb{Z}$ de longueur p_k au lieu d'être de longueur p_k^2 dans la mesure où seul le reste était pris en compte (ici, reste et quotient sont pris en compte, d'où le carré pour la combinatoire).

Continuons cependant à la recherche d'une modélisation convenable.

On aimerait, idéalement, "agréger" toutes les matrices associées à un nombre en une seule matrice qui résumerait l'information associée à ce nombre.

1. *Système de Numération par les Restes dans les Parties Finies de* $\mathbb{N}$.

On rappelle que c'est la présence d'un $b = 0$ qui correspond à la divisibilité par un nombre premier. Voyons d'abord la non-commutativité de la multiplication matricielle à l'oeuvre sur un exemple : si on multiplie à droite ou bien à gauche par une matrice ayant un coefficient nul en haut à droite, on n'obtient pas le même résultat [2].

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & ab' \\ 0 & 1 \end{pmatrix}$$

alors que

$$\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a'a & b' \\ 0 & 1 \end{pmatrix}$$

Un moyen d'obtenir que la divisibilité par un nombre premier (le fait d'être composé) absorde toute autre information, du fait de l'ordre très particulier dans lequel s'effectue les calculs intermédiaire d'une multiplication matriciel, serait d'intervertir les positions des coefficients a et b. On aurait alors :

$$\begin{pmatrix} 0 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b' & a' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 1 \end{pmatrix}$$

On corrige le tableau en conséquence et on associe à chaque nombre le produit de ses matrices (colonne). La multiplication par une matrice indiquant qu'un nombre est composé est absorbante, qu'elle s'effectue à droite ou à gauche, en ce qui concerne le coefficient en haut à gauche des matrices.

En effet, on a :

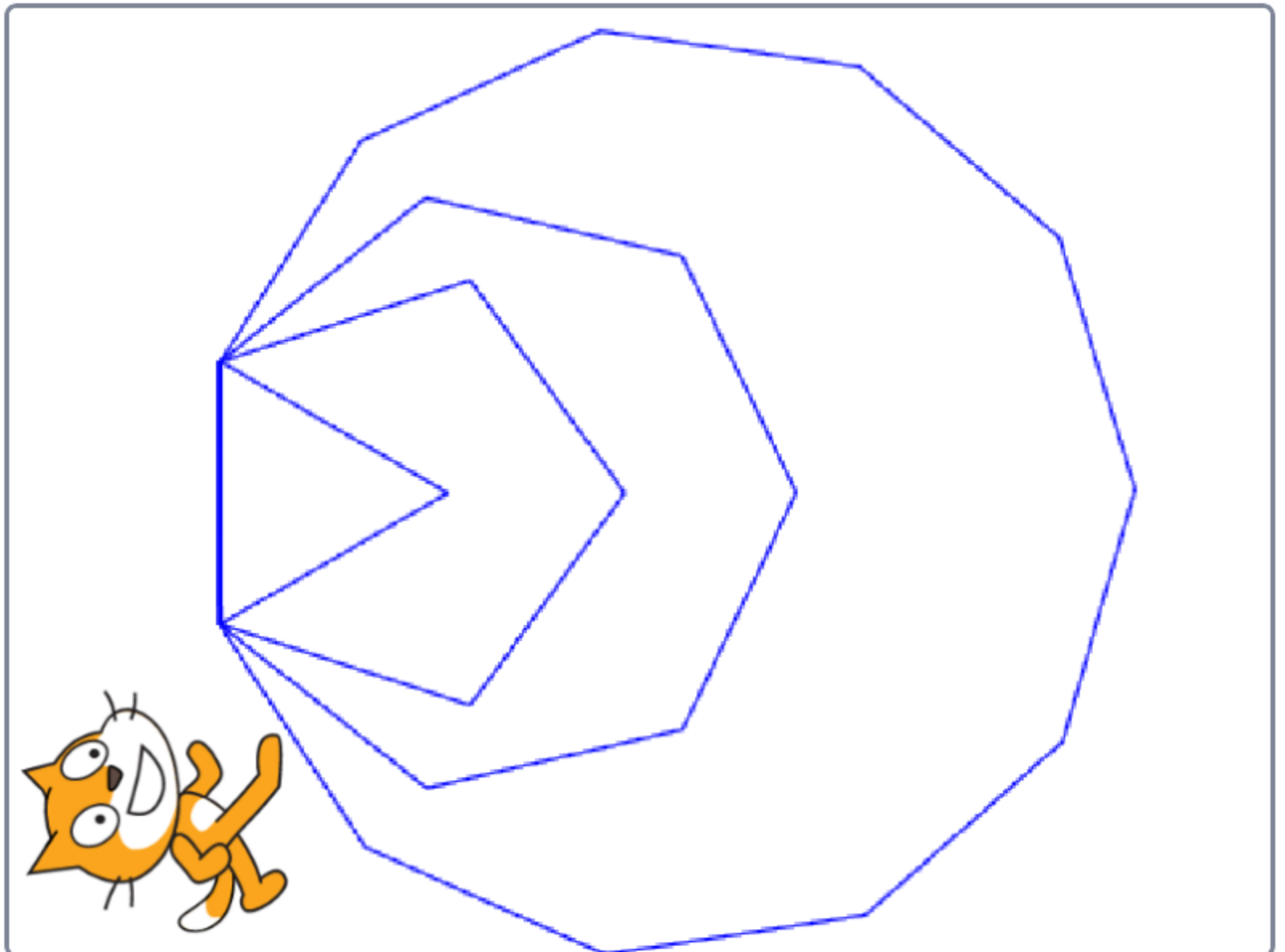
$$\begin{pmatrix} 0 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b' & a' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 1 \end{pmatrix}$$

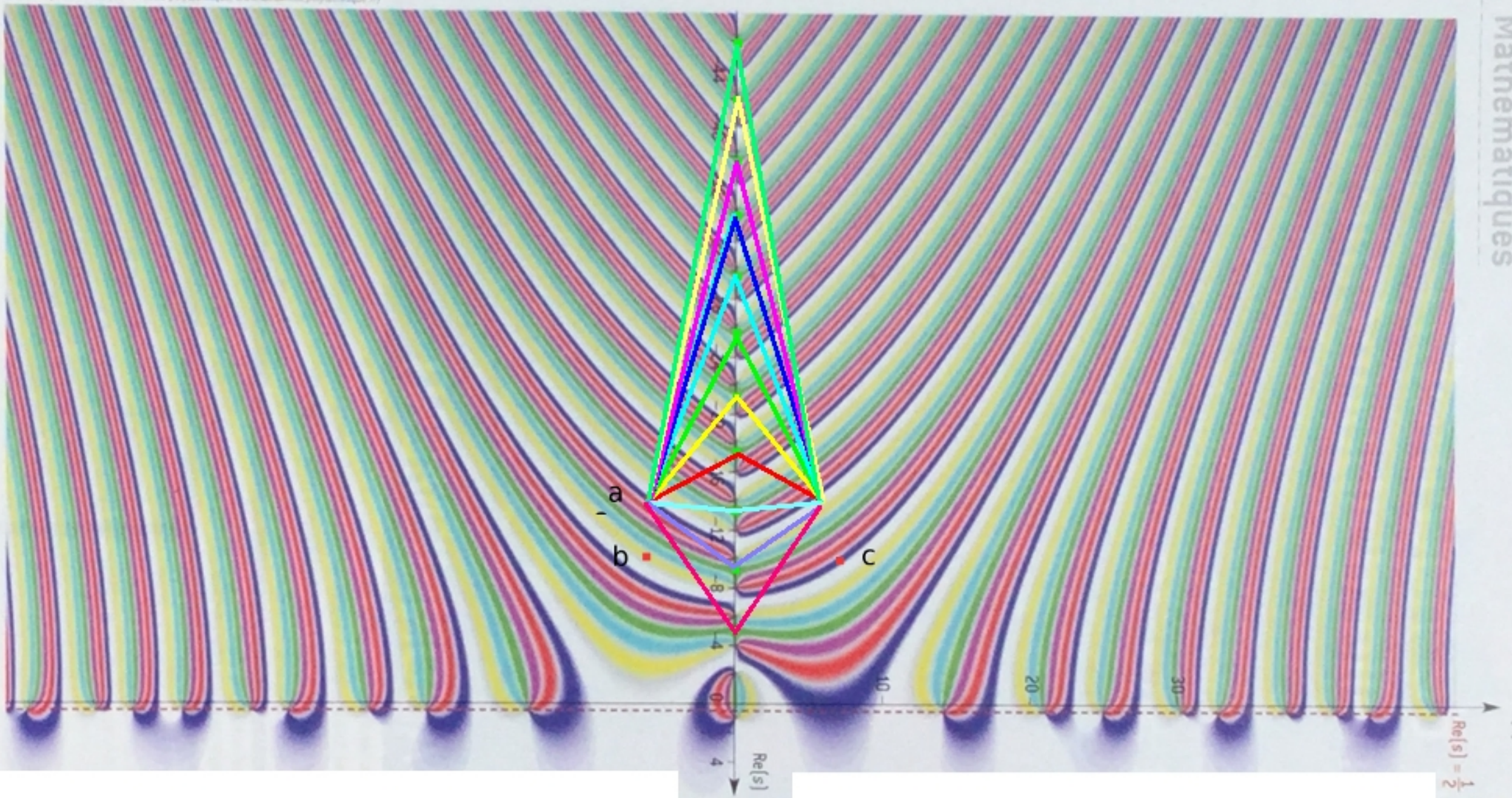
et

$$\begin{pmatrix} b' & a' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & b'a + a' \\ 0 & 1 \end{pmatrix}$$

2. Lors de ma scolarité élémentaire "maths modernes", on nous faisait utiliser des "moulinettes", par exemple la moulinette $f(x) = 3x + 2$ et la moulinette $g(x) = 8x + 4$ et l'on attirait notre attention sur le fait que l'application de 2 moulinettes successives faisait qu'on n'obtenait pas obligatoirement le même résultat suivant l'ordre d'application : la composition de deux fonctions affines est non-commutative. $f \circ g(x) \neq g \circ f(x)$. Par exemple, pour $x = 6$, $8 \times (3 \times 6 + 2) + 4 = 164$ est différent de $3 \times (8 \times 6 + 4) + 2 = 158$. Il faut pour que les matrices commutent que leurs coefficients vérifient : $ab' + b = a'b + b'$.

n	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	Π	n	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	Π	n	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Z}/7\mathbb{Z}$	Π
3	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$			$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	37	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$		$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	71	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	$\begin{pmatrix}1&4\\0&1\end{pmatrix}$	$\begin{pmatrix}1&3\\0&1\end{pmatrix}$	$\begin{pmatrix}2&16\\0&1\end{pmatrix}$
5	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$			$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	39	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	$\begin{pmatrix}4&2\\0&1\end{pmatrix}$		$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	73	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}3&4\\0&1\end{pmatrix}$	$\begin{pmatrix}3&3\\0&1\end{pmatrix}$	$\begin{pmatrix}9&13\\0&1\end{pmatrix}$
7	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$			$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	41	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&3\\0&1\end{pmatrix}$		$\begin{pmatrix}2&7\\0&1\end{pmatrix}$	75	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}5&3\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$
9	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$			$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	43	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}3&3\\0&1\end{pmatrix}$		$\begin{pmatrix}3&5\\0&1\end{pmatrix}$	77	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&4\\0&1\end{pmatrix}$	$\begin{pmatrix}0&17\\0&1\end{pmatrix}$
11	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$			$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	45	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&4\\0&1\end{pmatrix}$		$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	79	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}4&0\\0&1\end{pmatrix}$	$\begin{pmatrix}2&4\\0&1\end{pmatrix}$	$\begin{pmatrix}8&18\\0&1\end{pmatrix}$
13	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$			$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	47	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	$\begin{pmatrix}2&4\\0&1\end{pmatrix}$		$\begin{pmatrix}4&8\\0&1\end{pmatrix}$	81	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}4&4\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$
15	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$			$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	49	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}4&4\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&5\\0&1\end{pmatrix}$	83	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	$\begin{pmatrix}3&1\\0&1\end{pmatrix}$	$\begin{pmatrix}6&4\\0&1\end{pmatrix}$	$\begin{pmatrix}36&26\\0&1\end{pmatrix}$
17	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$			$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	51	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	85	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	$\begin{pmatrix}1&5\\0&1\end{pmatrix}$	$\begin{pmatrix}0&3\\0&1\end{pmatrix}$
19	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$			$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	53	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	$\begin{pmatrix}3&0\\0&1\end{pmatrix}$	$\begin{pmatrix}4&0\\0&1\end{pmatrix}$	$\begin{pmatrix}24&2\\0&1\end{pmatrix}$	87	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	$\begin{pmatrix}3&5\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$
21	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$			$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	55	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	$\begin{pmatrix}6&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	89	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	$\begin{pmatrix}4&2\\0&1\end{pmatrix}$	$\begin{pmatrix}5&5\\0&1\end{pmatrix}$	$\begin{pmatrix}40&46\\0&1\end{pmatrix}$
23	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$			$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	57	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	91	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&3\\0&1\end{pmatrix}$	$\begin{pmatrix}0&6\\0&1\end{pmatrix}$	$\begin{pmatrix}0&9\\0&1\end{pmatrix}$
25	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$		$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	59	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	$\begin{pmatrix}4&1\\0&1\end{pmatrix}$	$\begin{pmatrix}3&1\\0&1\end{pmatrix}$	$\begin{pmatrix}24&11\\0&1\end{pmatrix}$	93	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$	$\begin{pmatrix}3&3\\0&1\end{pmatrix}$	$\begin{pmatrix}2&6\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\0&1\end{pmatrix}$
27	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$		$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	61	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}5&1\\0&1\end{pmatrix}$	$\begin{pmatrix}5&5\\0&1\end{pmatrix}$	95	$\begin{pmatrix}2&1\\0&1\end{pmatrix}$	$\begin{pmatrix}0&4\\0&1\end{pmatrix}$	$\begin{pmatrix}4&6\\0&1\end{pmatrix}$	$\begin{pmatrix}0&9\\0&1\end{pmatrix}$
29	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	$\begin{pmatrix}4&0\\0&1\end{pmatrix}$		$\begin{pmatrix}8&0\\0&1\end{pmatrix}$	63	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}3&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	97	$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	$\begin{pmatrix}2&4\\0&1\end{pmatrix}$	$\begin{pmatrix}6&6\\0&1\end{pmatrix}$	$\begin{pmatrix}12&18\\0&1\end{pmatrix}$
31	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$		$\begin{pmatrix}1&2\\0&1\end{pmatrix}$	65	$\begin{pmatrix}2&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&3\\0&1\end{pmatrix}$	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&6\\0&1\end{pmatrix}$	99	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$	$\begin{pmatrix}4&4\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&0\\0&1\end{pmatrix}$
33	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	$\begin{pmatrix}3&1\\0&1\end{pmatrix}$		$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	67	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}2&3\\0&1\end{pmatrix}$	$\begin{pmatrix}4&2\\0&1\end{pmatrix}$	$\begin{pmatrix}8&8\\0&1\end{pmatrix}$					
35	$\begin{pmatrix}2&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$		$\begin{pmatrix}0&6\\0&1\end{pmatrix}$	69	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	$\begin{pmatrix}4&3\\0&1\end{pmatrix}$	$\begin{pmatrix}6&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$					





Théorème de Morley dans le corps des quaternions (Denise Vella-Chemla, 15.2.2019)

Dans une conférence au Collège de France [1] *"Langage et mathématique"*, Alain Connes évoque le fait que le théorème de Morley s'applique à tout corps possédant une racine cubique de l'unité. C'est le cas en particulier du corps des quaternions.

On cherche 3 quaternions Q, R et S qui vérifient $QRS = r$ avec r une racine cubique de l'unité dans le corps des quaternions, et $Q^3R^3S^3 = 1$.

On peut trouver de nombreuses solutions par programme : pour cibler les solutions, on pose :

- $Q = a + bi + cj + dk$,
- $R = a' + b'i + c'j + d'k$
- $S = a'' + b''i + c''j + d''k$.

On développe le produit $QRS = (a + bi + cj + dk)(a' + b'i + c'j + d'k)(a'' + b''i + c''j + d''k)$ et on utilise le fait que dans le corps des quaternions, on a $i^2 = j^2 = k^2 = -1$ et $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$ et $ik = -j$ pour obtenir la valeur suivante pour QRS :

$$\begin{array}{cccc}
 & a''(aa' - bb' - cc' - dd') & -b''(a'b + ab' - c'd + cd') & -c''(a'c + b'd + ac' - bd') & -d''(a'd - b'c + bc' + ad') \\
+ & a''i(a'b + ab' - c'd + cd') & +b''i(aa' - bb' - cc' - dd') & -c''i(a'd - b'c + bc' + ad') & +d''i(a'c + b'd + ac' - bd') \\
+ & a''j(a'c + b'd + ac' - bd') & +b''j(a'd - b'c + bc' + ad') & +c''j(aa' - bb' - cc' - dd') & -d''j(a'b + ab' - c'd + cd') \\
+ & a''k(a'd - b'c + bc' + ad') & -b''k(a'c + b'd + ac' - bd') & +c''k(a'b + ab' - c'd + cd') & +d''k(aa' - bb' - cc' - dd')
\end{array}$$

qui est de la forme :

$$\begin{array}{cccc}
 & a''A & -b''B & -c''D & -d''C \\
+ & a''B & +b''A & -c''C & +d''D \\
+ & a''D & +b''C & +c''A & -d''B \\
+ & a''C & -b''D & +c''B & +d''A
\end{array}$$

On trouve quelques racines cubiques de l'unité possibles, telles que $(-1, 1, 1, 1)$ ou bien $(-1, -1, -1, -1)$ ou encore $(-0.5, 0.5, 0.5, 0.5)$.

Et on obtient par exemple par programme la solution suivante, qui vérifie bien les contraintes souhaitées.

Si

- $Q = -1 - i - j + k$,
- $R = -1 + i + j - k$,
- $S = -1 + i + j + k$,

alors

- $QRS = r = -0.5 + 0.5i + 0.5j + 0.5j$
- avec $r^3 = 1$
- et $\mathrm{Q^3R^3S^3} = 1$.

1. https://www.college-de-france.fr/site/colloque-2018/symposium-2018-10-18-10h00.htm

Nombres et sphère quantique (Denise Vella-Chemla, 16.2.2019)

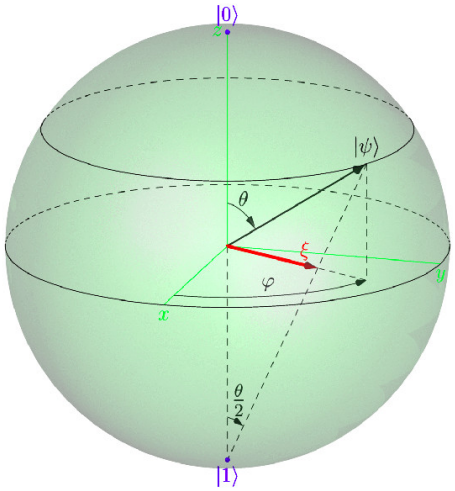
Ayant touché du doigt à l'été 2018 tout l'aléa qui semble gouverner le fait d'être ou de ne pas être premier pour un entier naturel donné, on souhaiterait ici modéliser les entiers naturels en utilisant des qubits sur la sphère quantique.

Un bit d'information ne peut prendre que 2 valeurs, 0 ou 1.
Un qubit, ou bit quantique, peut être vu comme une superposition de multiples états possibles entre 0 et 1, chacun de ces états étant caractérisé par les probabilités de $|0\rangle$ et de $|1\rangle$ qu'il "contient".

$$|\Psi\rangle = cos\frac{\theta}{2}e^{-i\frac{\varphi}{2}}|0\rangle + sin\frac{\theta}{2}e^{i\frac{\varphi}{2}}|1\rangle.$$

On représente les qubits sur la sphère quantique ainsi, on lira à profit la page

http://stla.github.io/stlapblog/posts/BlochSphere.html [1].



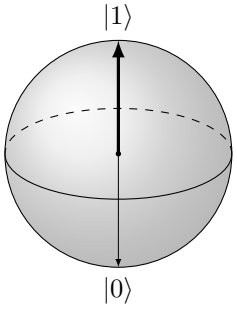
On rappelle qu'un nombre n étant donné, on a les définitions suivantes :

- n est un nombre premier si une division euclidienne de n par n'importe quel autre nombre que lui-même a un reste non-nul ;
- n est un nombre composé si l'une au moins des divisions euclidiennes de n par un autre nombre que lui-même (l'un de ses diviseurs notamment) a un reste nul.

Pour ne pas se perdre dans l'espace de Hilbert, on va imaginer qu'à un nombre n sont associés, non pas une infinité de qubits, mais seulement $n-2$ qubits, correspondant chacun aux divisions de n par les entiers de 3 à n.

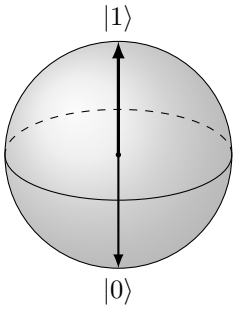
Le résultat de la division de n par d est aléatoire dans la mesure où on ne connaît pas n : quand d divisera n, le qubit fixera sa valeur sur $|0\rangle$ tandis qu'il fixera sa valeur sur $|1\rangle$ si d ne divise pas n.

De cette manière, un nombre premier aura tous ses qubits qui se fixeront sur $|1\rangle$ sauf un qui se fixera sur $|0\rangle$, ce qu'on a symbolisé ci-dessous par l'épaisseur relative des flèches vers $|1\rangle$ et $|0\rangle$.

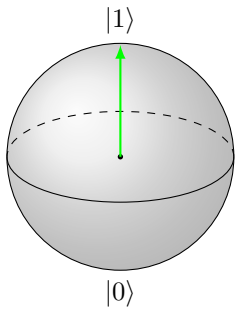


1. page dont on n'a pas trouvé le nom de l'auteur.

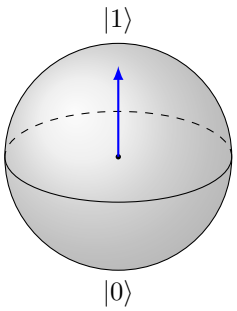
Un nombre composé, lui, aura un certain nombre de ses qubits qui se fixeront sur $|1\rangle$ et un certain nombre [2], strictement supérieur à 1, d'autres qubits qui se fixeront sur $|0\rangle$. On a symbolisé par l'épaisseur relative des flèches le fait qu'un nombre a cependant moins de diviseurs que de non-diviseurs.



Imaginons maintenant qu'on ajoute les qubits associés à un nombre ; suivant le nombre de qubits positionnés sur $|0\rangle$, le vecteur global obtenu, qui sera sur l'axe reliant les pôles de la sphère, aura son extrémité qui s'éloignera plus ou moins de la surface de la sphère et on peut dire que les nombres premiers, du fait qu'ils n'ont qu'un seul qubit sur $|0\rangle$, resteront les plus proches de la surface de la sphère.



Vecteur global associé à un nombre premier

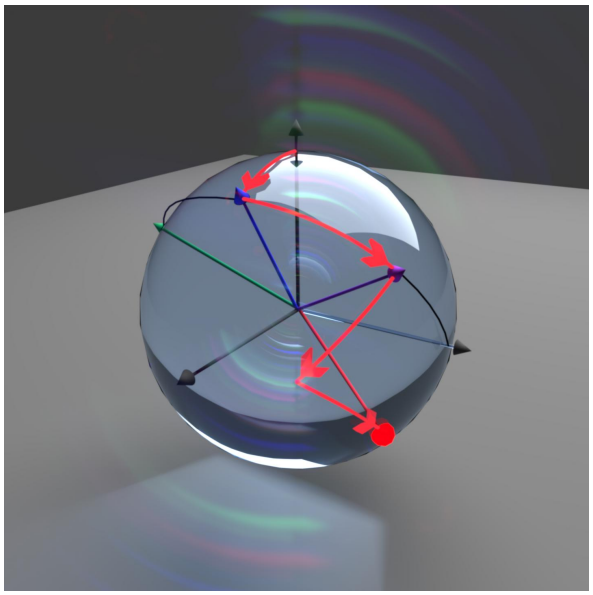


Vecteur global associé à un nombre composé

La superbe illustration suivante, trouvée à la page

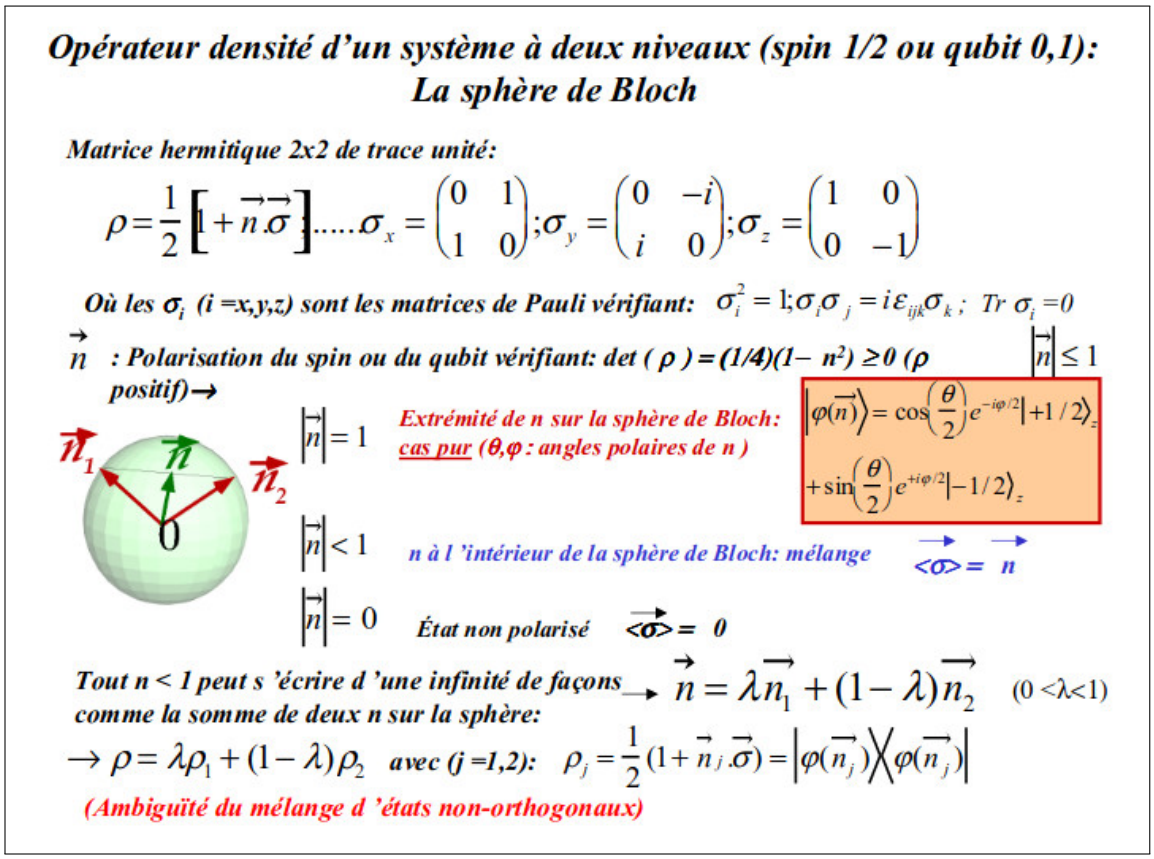
https://www.eurekalert.org/multimedia/pub/120313.php,

explicite la façon dont les vecteurs s'additionnent sur la sphère quantique.



2. son nombre de diviseurs.

Enfin, l'image ci-dessous est le dernier transparent du premier cours de Serge Haroche au Collège de France pour l'année 2001-2002 [3].
On retrouve l'idée du vecteur à l'intérieur (de norme <1) ou sur la sphère de Bloch [4] (de norme =1).



Pour le problème qui motive notre recherche depuis septembre 2005 et qui est la conjecture de Goldbach, il faudrait trouver la manière de "coder" l'intrication entre la divisibilité par p de x un décomposant de Goldbach potentiel de n et la divisibilité par p de $n-x$ son complémentaire à n.

3. Cours du 8.1.2002 dont l'intégralité du diaporama est trouvable à l'adresse https://www.college-de-france.fr/media/serge-haroche/UPL54964_SHaroche_080102.pdf
4. dite aussi sphère quantique.

Probabiliste ou quantique ? (Denise Vella-Chemla, 17.2.2019)

On revient sur les règles de combinaisons de lettres qu'on avait mis au jour en février 2014 pour les étudier en termes probabilistes ou quantiques.

On avait pris l'habitude de coder les passages du mot associé à n au mot associé à $n+2$ avec des lettres a, b, c, d mais elles n'étaient pas très parlantes, on va plutôt utiliser ici la lettre p pour premier et la lettre c pour composé.

On a 16 règles qui lient les décompositions $n = x + y$, $n = (x + 2) + (y - 2)$ et $n + 2 = (x + 2) + y$ selon le caractère premier (p) ou composé (c) des quatre nombres $x, y, x + 2$ et $y - 2$. On note ces 16 règles par des transitions d'états codées ainsi : $état_x, état_y, état_{x+2}, état_{y-2} \longrightarrow$état$_{x+2}, état_y$.

$r_1)\ \ p,p,p,p \longrightarrow p,p$	$r_5)\ \ c,p,p,p \longrightarrow p,p$	$r_9)\ \ p,c,p,p \longrightarrow p,c$	$r_{13})\ \ c,c,p,p \longrightarrow p,c$
$r_2)\ \ p,p,c,p \longrightarrow c,p$	$r_6)\ \ c,p,c,p \longrightarrow c,p$	$r_{10})\ \ p,c,c,p \longrightarrow c,c$	$r_{14})\ \ c,c,c,p \longrightarrow c,c$
$r_3)\ \ p,p,p,c \longrightarrow p,p$	$r_7)\ \ c,p,p,c \longrightarrow p,p$	$r_{11})\ \ p,c,p,c \longrightarrow p,c$	$r_{15})\ \ c,c,p,c \longrightarrow p,c$
$r_4)\ \ p,p,c,c \longrightarrow c,p$	$r_8)\ \ c,p,c,c \longrightarrow c,p$	$r_{12})\ \ p,c,c,c \longrightarrow c,c$	$r_{16})\ \ c,c,c,c \longrightarrow c,c$

Prenons un exemple pour fixer les idées : la règle r_{10}, appliquée aux nombres $13, 25, 15, 23$, qui décomposent $n = 38$ qui sont bien (dans l'ordre) p, c, c, p (premier, composé, composé, premier) permettront d'obtenir la décomposition c, c de $n + 2 = 40 = 15 + 25$.

Considérons que les probabilités de $x, y, x+2, y-2$ sont complètement indépendantes les unes des autres ; on aura alors les probabilités suivantes, associées aux règles :

r_1	p,p,p,p	$\left(\frac{1}{ln\ x}\right)^4$	X^4	r_5	c,p,p,p	$\left(\frac{1}{ln\ x}\right)^3\left(1-\frac{1}{ln\ x}\right)$	$X^3(1-X)$
r_2	p,p,c,p	$\left(\frac{1}{ln\ x}\right)^3\left(1-\frac{1}{ln\ x}\right)$	$X^3(1-X)$	r_6	c,p,c,p	$\left(\frac{1}{ln\ x}\right)^2\left(1-\frac{1}{ln\ x}\right)^2$	$X^2(1-X)^2$
r_3	p,p,p,c	$\left(\frac{1}{ln\ x}\right)^3\left(1-\frac{1}{ln\ x}\right)$	$X^3(1-X)$	r_7	c,p,p,c	$\left(\frac{1}{ln\ x}\right)^2\left(1-\frac{1}{ln\ x}\right)^2$	$X^2(1-X)^2$
r_4	p,p,c,c	$\left(\frac{1}{ln\ x}\right)^2\left(1-\frac{1}{ln\ x}\right)^2$	$X^2(1-X)^2$	r_8	c,p,c,c	$\left(\frac{1}{ln\ x}\right)\left(1-\frac{1}{ln\ x}\right)^3$	$X(1-X)^3$
r_9	p,c,p,p	$\left(\frac{1}{ln\ x}\right)^3\left(1-\frac{1}{ln\ x}\right)$	$X^3(1-X)$	r_{13}	c,c,p,p	$\left(\frac{1}{ln\ x}\right)^2\left(1-\frac{1}{ln\ x}\right)^2$	$X^2(1-X)^2$
r_{10}	p,c,c,p	$\left(\frac{1}{ln\ x}\right)^2\left(1-\frac{1}{ln\ x}\right)^2$	$X^2(1-X)^2$	r_{14}	c,c,c,p	$\left(\frac{1}{ln\ x}\right)\left(1-\frac{1}{ln\ x}\right)^3$	$X(1-X)^3$
r_{11}	p,c,p,c	$\left(\frac{1}{ln\ x}\right)^2\left(1-\frac{1}{ln\ x}\right)^2$	$X^2(1-X)^2$	r_{15}	c,c,p,c	$\left(\frac{1}{ln\ x}\right)\left(1-\frac{1}{ln\ x}\right)^3$	$X(1-X)^3$
r_{12}	p,c,c,c	$\left(\frac{1}{ln\ x}\right)\left(1-\frac{1}{ln\ x}\right)^3$	$X(1-X)^3$	r_{16}	c,c,c,c	$\left(1-\frac{1}{ln\ x}\right)^4$	$(1-X)^4$

On obtient comme somme totale des probabilités le polynôme $X^4 + 4X^3(1-X) + 6X^2(1-X)^2 + 4X(1-X)^3 + (1-X)^4$ qui développé vaut bien 1.

Si on raisonne maintenant quantiquement plutôt que probabilistiquement, on aura les probabilités suivantes, présentées selon le tableau utilisé dans la littérature pour faire la différence entre bit, pbit (ou bit probabiliste) et enfin qubit (ou bit quantique).

variable décrivant l'état	*bit*	*bit probabiliste*	*bit quantique*
type	*bit*	*pbit*	*qubit*
représentation	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}p\\1-p\end{pmatrix}$	$\begin{pmatrix}\alpha\\\beta\end{pmatrix}$
caractéristique del'observation	*certitude sur la valeur* à *prendre*	p% *de chances de valoir* 0 $(1-p)$% *de chances de valoir* 1 $p \in \mathbb{R}$	$\lvert\alpha\rvert^2$% *de chances de valoir* 0 $\lvert\beta\rvert^2$% *de chances de valoir* 1 $\alpha, \beta \in \mathbb{C}$
matrice de transition	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1-q&q\\r&1-r\end{pmatrix}$	$\begin{pmatrix}u&v\\w&x\end{pmatrix}$
type de la matrice	*déterministe*	*stochastique*	*unitaire*

Concernant la matrice stochastique de la modélisation probabiliste par des pbits (colonne au milieu du tableau), il y a 2 états et 2 transitions possibles pour chaque état et la somme des nombres sur chacune des deux lignes de la matrice vaut 1 (cela correspond aux probabilités de transition de l'un des 2 états vers lui-même ou bien vers l'autre). Imaginons quelles peuvent être les valeurs des éléments d'une matrice stochastique (probabiliste) pour la divisibilité par p : on a les 2 états possibles d'un nombre "être divisible par p" et "ne pas être divisible par p". La matrice prend la forme suivante :

$$\begin{pmatrix} 0 & 1 \\ \frac{1}{p-1} & \frac{p-2}{p-1} \end{pmatrix}$$

En effet, prenons la divisibilité par 5 des nombres de 10 à 15 : après un nombre divisible par 5 (comme 10) il y a forcément un nombre non divisible par 5 (comme 11), d'où le 0 et le 1 de la première ligne de la matrice correspondant aux 2 transitions à partir d'un nombre divisible par 5.

Pour la deuxième ligne, on part d'un nombre non-divisible par 5, comme 11, 12, 13 et 14. Parmi eux, au nombre de 4 (soit $p-1$), l'un fournit une transition vers un nombre divisible par 5 (ici 14 qui devient 15) et les 3 autres (soit $p-2$) fournissent une transition vers un nombre non-divisible par 5 ; on a expliqué les nombres de la deuxième ligne de la matrice stochastique, dont la somme vaut bien 1.

Concernant la modélisation quantique par qubits (dernière colonne du tableau) des nombres premiers, il faut alors imaginer les nombres premiers comme "polarisant" les autres nombres, dans le sens où, selon chaque nombre premier, tout autre nombre a une certaine probabilité qui varie de façon continue sur l'intervalle $[0,1]$ d'être "touché", "affecté" [1] par lui en quelque sorte, et non plus d'être divisible par lui : même si la divisibilité est une notion tout ce qu'il y a de plus binaire (un nombre étant soit divisible soit non divisible par un autre), cette notion de polarisation modéliserait le fait qu'un nombre est à une certaine distance d'être divisible ou pas par un autre. C'est la réduction du paquet d'onde qui fixe les valeurs de divisibilité d'un nombre donné par les autres. Cette notion peut permettre d'intriquer les divisibilités de x et $n-x$ par p si on connaît la divisibilité de n par p.

Comme la matrice, dans le cas quantique, doit être unitaire, il semblerait que ses éléments doivent prendre les valeurs $\frac{1}{\sqrt{p-1}}$ et $\sqrt{\frac{p-2}{p-1}}$ pour qu'on ait bien $\left(\frac{1}{\sqrt{p-1}}\right)^2 + \left(\sqrt{\frac{p-2}{p-1}}\right)^2 = \frac{1}{p-1} + \frac{p-2}{p-1} = 1$.

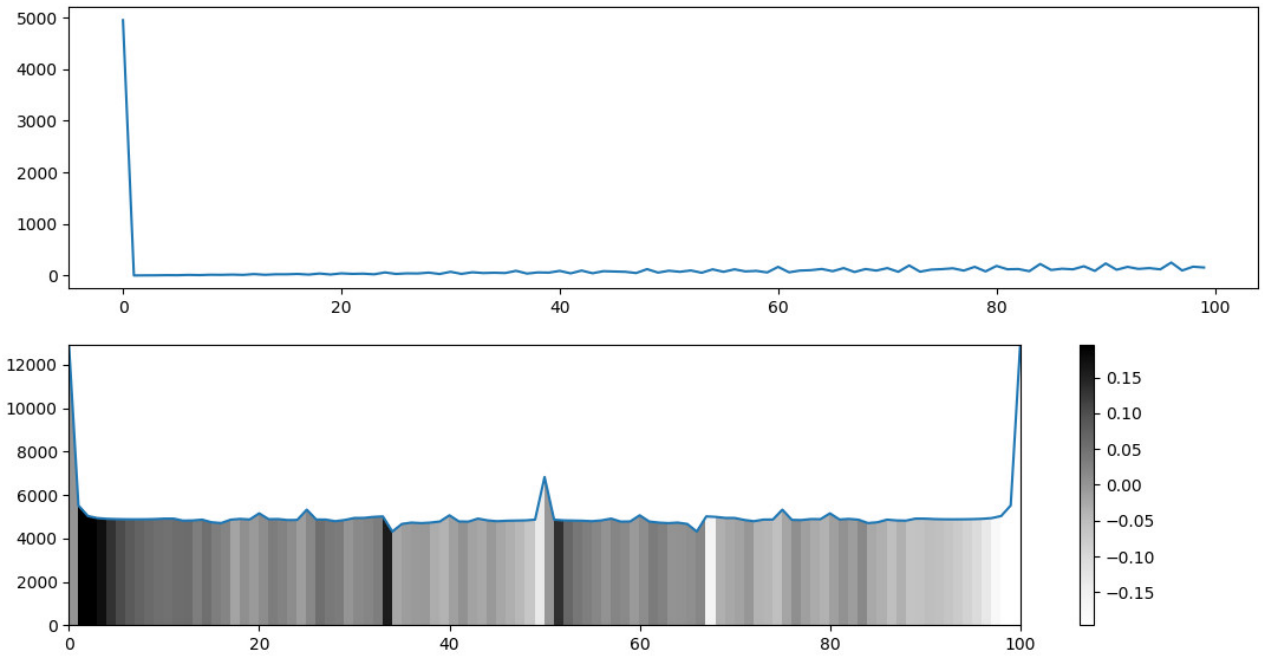
On s'est appuyé pour nos propositions sur l'exemple d'un fichier de Philippe Grangier [2] des personnes "plus ou moins blondes" ; on noterait notre "divisibilité polarisée" par les superpositions linéaires d'états $|0_p\rangle \left(\frac{1}{\sqrt{p-1}}\right) + |1_p\rangle \left(\sqrt{\frac{p-2}{p-1}}\right)$ par la superposition d'état $(|0_p\rangle + |1_p\rangle)/\sqrt{p-1}$.

On n'a cependant pas les moyens de mettre en oeuvre ce dispositif d'une quelconque manière.

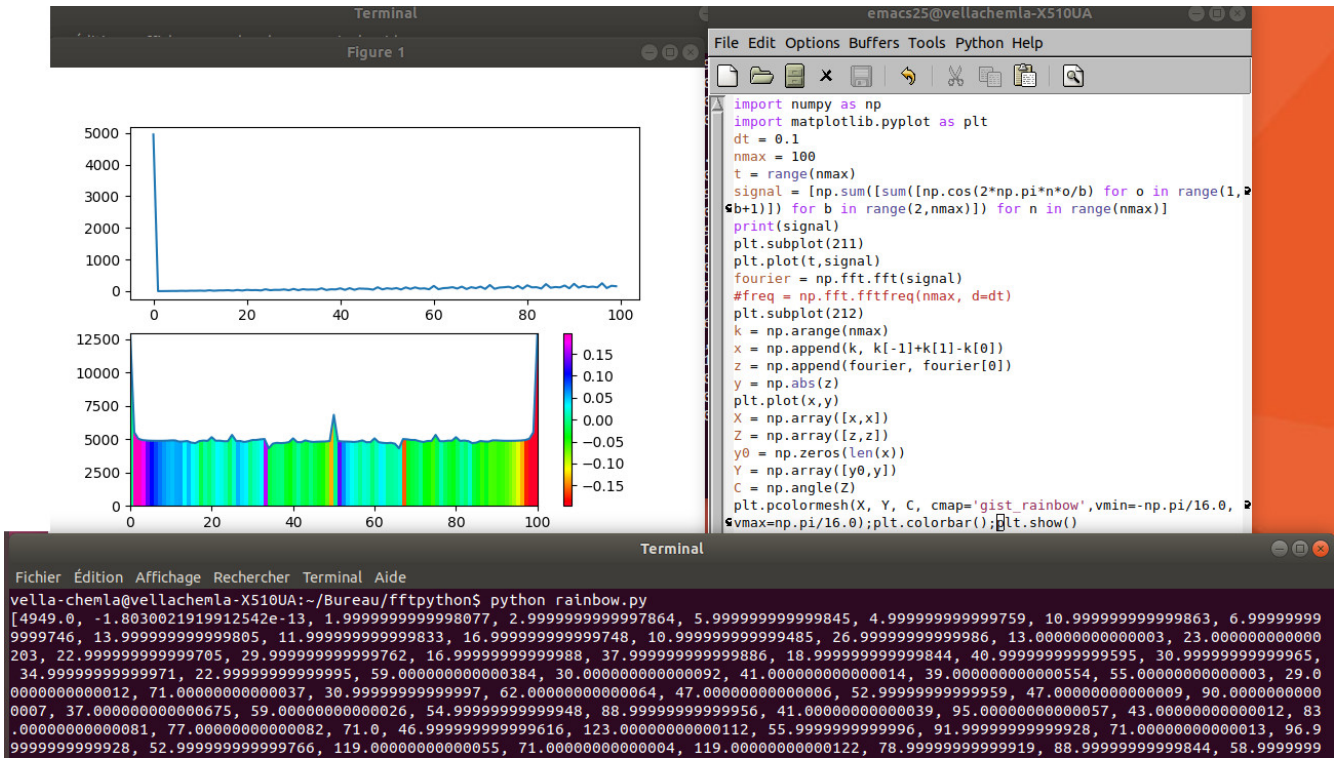
1. comme un filtre polarisant affecte la lumière.

2. consultable ici http://www.cmls.polytechnique.fr/perso/paul/SoireesPoincare/transgrangier.pdf, transparents d'une conférence "De la sphère de Poincaré aux bits quantiques : le contrôle de la polarisation de la lumière" de Philippe Grangier (soirée Poincaré du 16 octobre 2012)

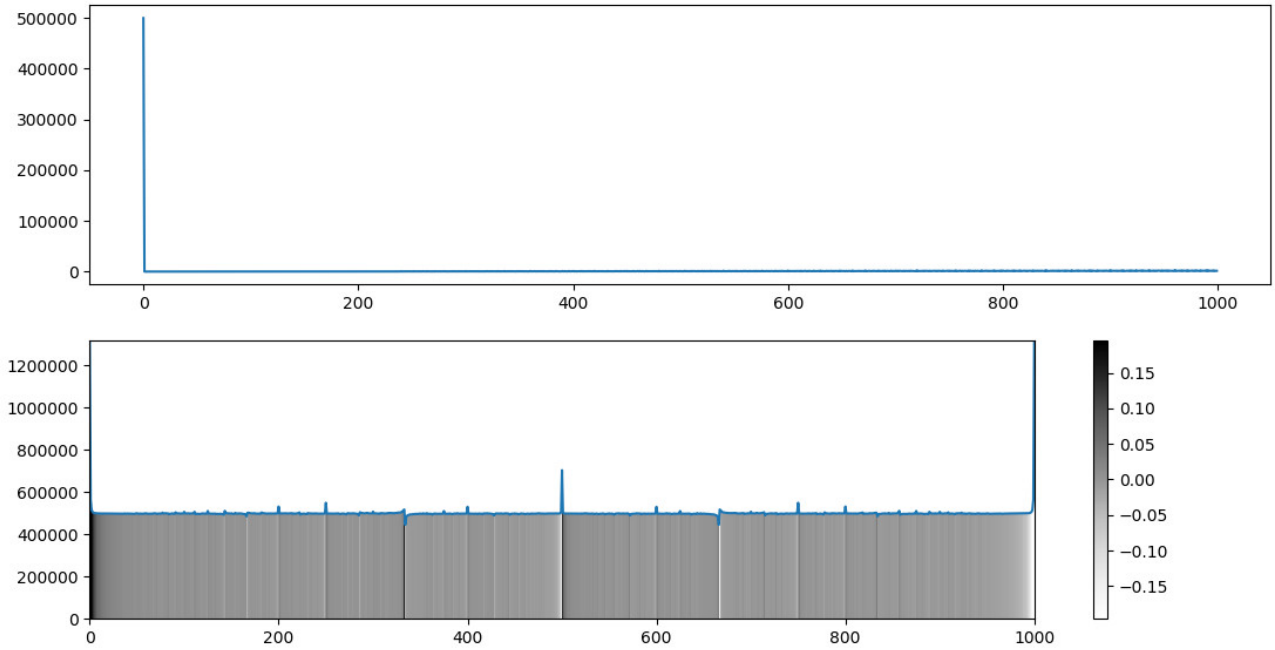
Spectres de la somme de somme de cosinus (Denise Vella-Chemla, 4.3.2019)



Couleurs arc-en-ciel

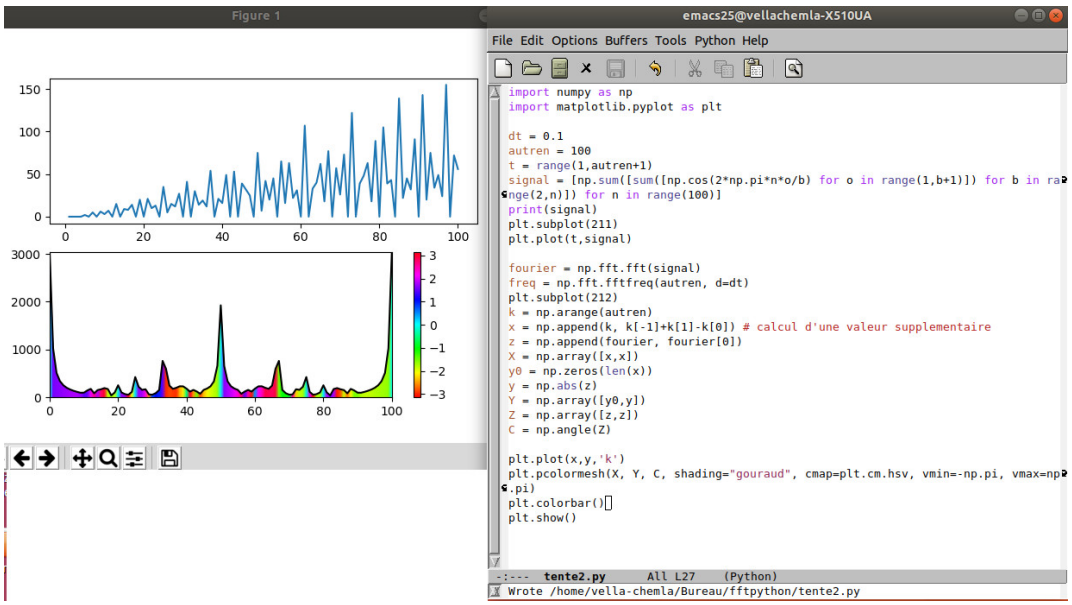


Idem jusqu'à 1000



On distingue très bien des raies noires en 501, 601, 801, 250, 333 et leur "correspondante", soit juste à côté, soit sur la moitié opposée du spectre.

Premières tentatives jusqu'à 100



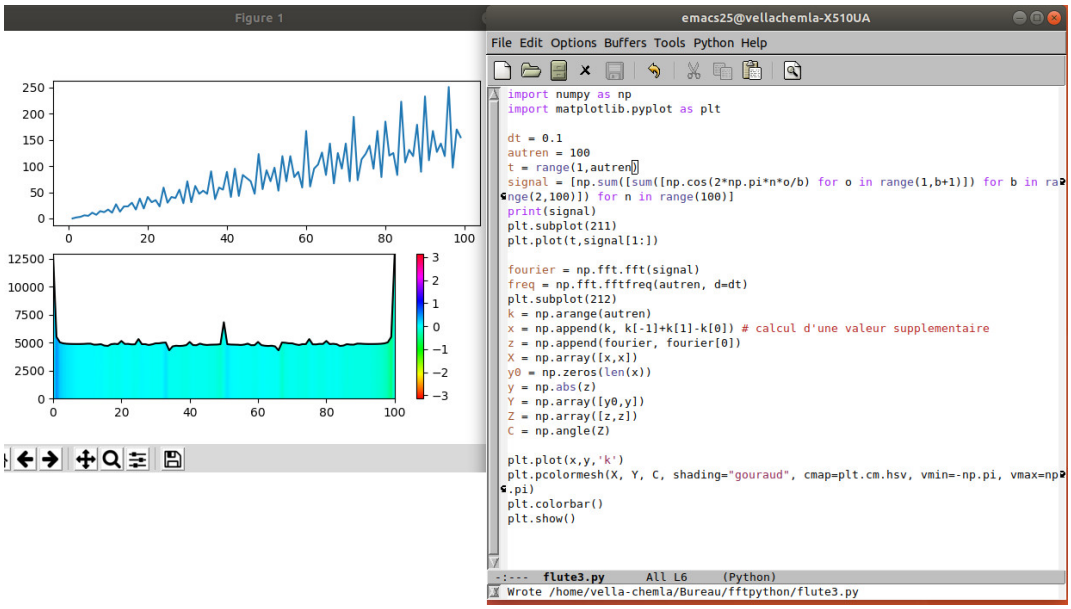


Figure 1
emacs25@vellachemla-X510UA
File Edit Options Buffers Tools Python Help
import numpy as np
import matplotlib.pyplot as plt
dt = 0.1
autren = 100
t = range(1,autren)
signal = [np.sum([sum([np.cos(2*np.pi*n*o/b) for o in range(1,b+1)]) for b in range(2,100)]) for n in range(100)]
print(signal)
plt.subplot(211)
plt.plot(t,signal[1:])
fourier = np.fft.fft(signal)
freq = np.fft.fftfreq(autren, d=dt)
plt.subplot(212)
k = np.arange(autren)
x = np.append(k, k[-1]+k[1]-k[0]) # calcul d'une valeur supplementaire
z = np.append(fourier, fourier[0])
X = np.array([x,x])
y0 = np.zeros(len(x))
y = np.abs(z)
Y = np.array([y0,y])
Z = np.array([z,z])
C = np.angle(Z)
plt.plot(x,y,'k')
plt.pcolormesh(X, Y, C, shading="gouraud", cmap=plt.cm.hsv, vmin=-np.pi, vmax=np.pi)
plt.colorbar()
plt.show()
-:--- flute3.py All L6 (Python)
Wrote /home/vella-chemla/Bureau/fftpython/flute3.py

---

jusqu'à 300

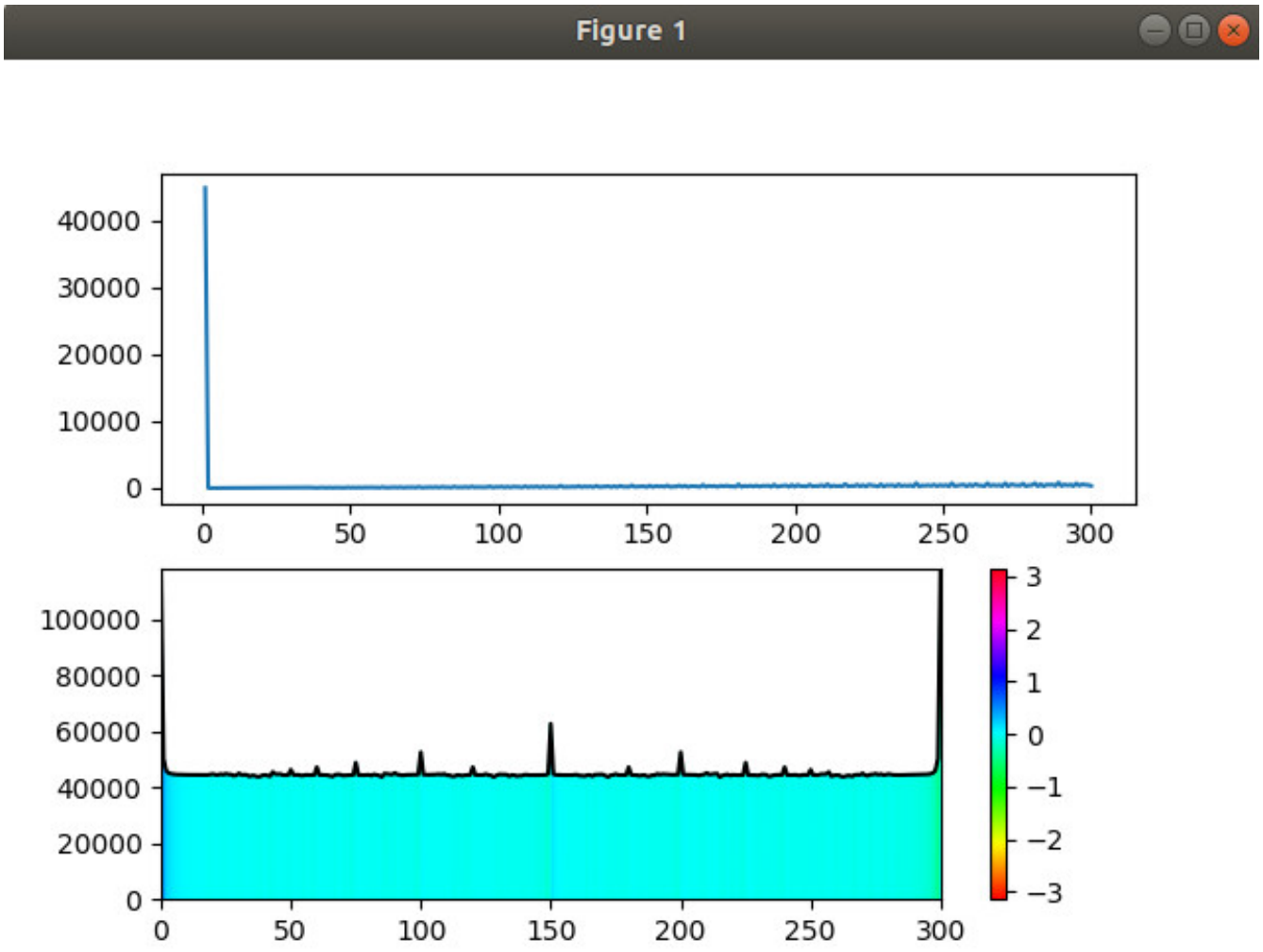
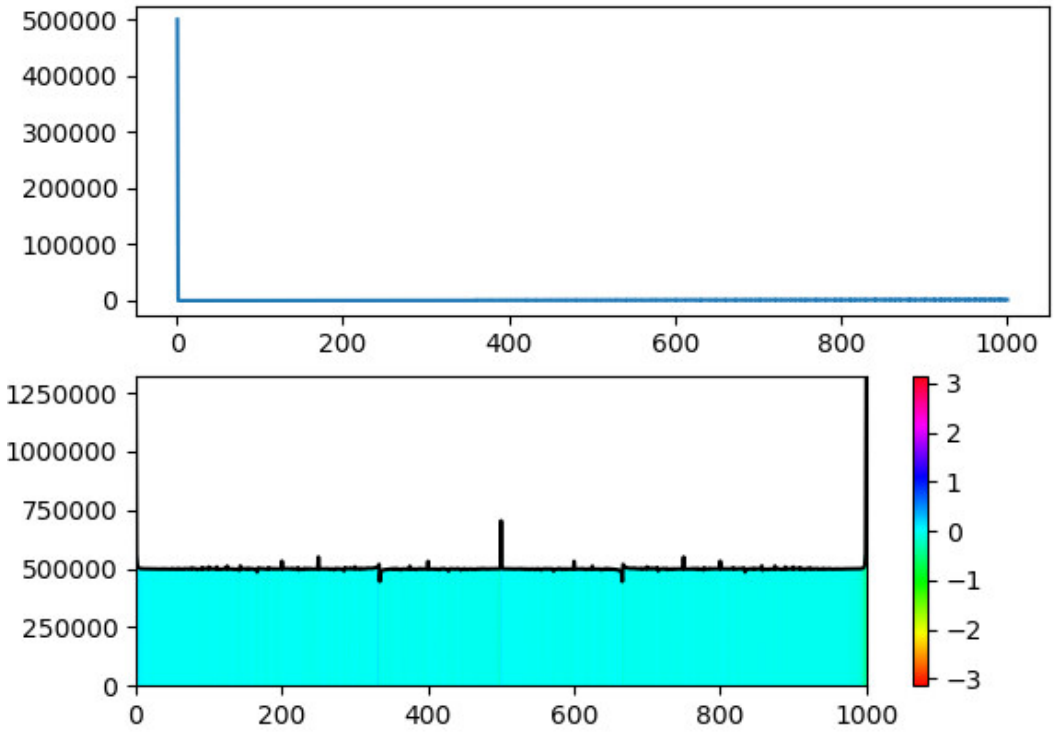


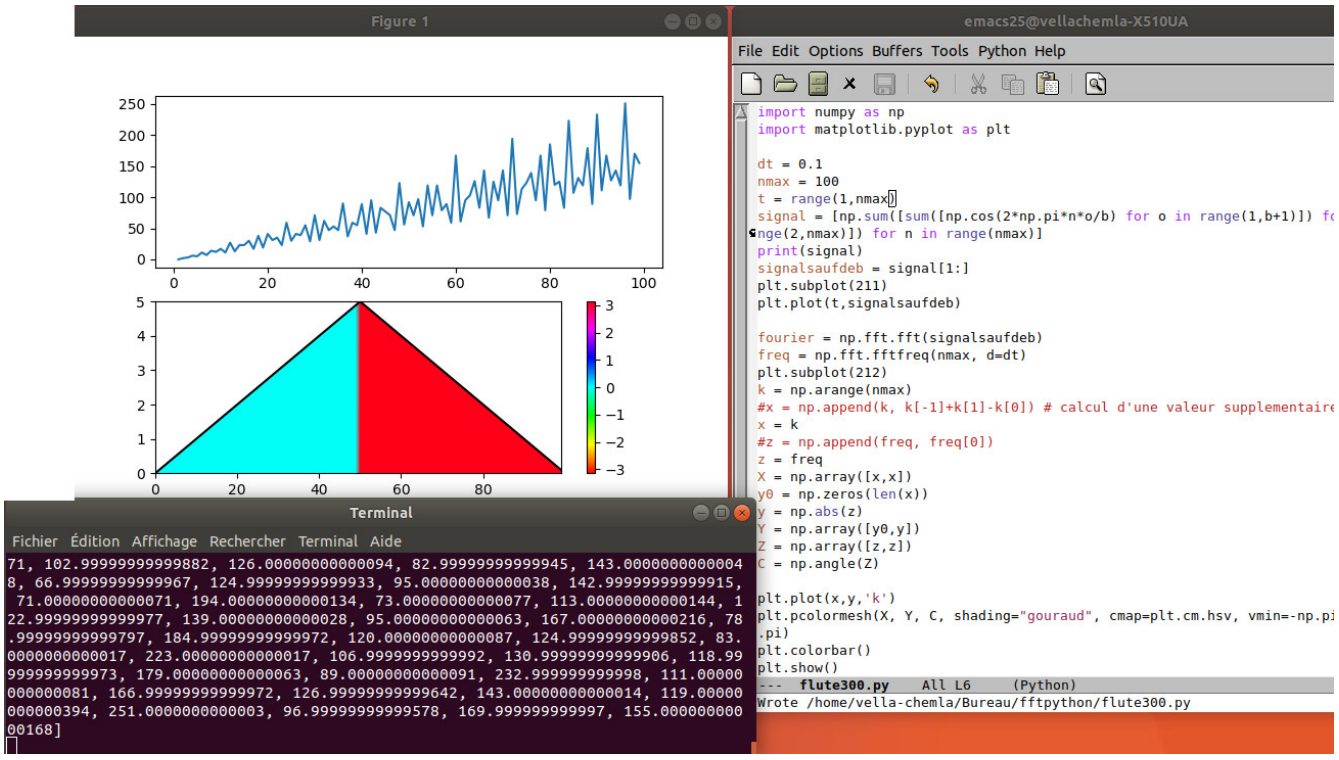
Figure 1
40000
30000
20000
10000
0
0
50
100
150
200
250
300
100000
80000
60000
40000
20000
0
3
2
1
0
−1
−2
−3

jusqu'à 1000



---

spectre en fréquences



Spectre lumineux (Denise Vella-Chemla, 5.3.2019)

On utilise des pages très didactiques ici :

https://www.courspython.com/fft-introduction.html

ou là

http://www.f-legrand.fr/scidoc/docmml/numerique/tfd/tfdimage/tfdimage.html

pour essayer de comprendre un peu la notion de transformée de Fourier puis pour dessiner le spectre de la fonction somme de sommes de cosinus, qui coïncide avec l'identité pour les nombres premiers et pour eux-seuls, fonction qu'on a définie ainsi (par exemple pour connaître les nombres premiers jusqu'à t) :

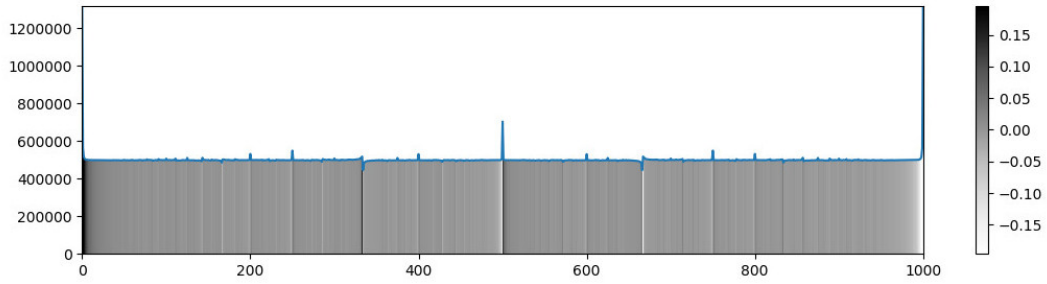
$$signal(t) = \sum_{b=2}^{t} \sum_{o=1}^{b} \cos \frac{2\pi\ t\ o}{b}$$

Voici le programme en python qui permet de calculer le spectre de la fonction $signal$ [1] :

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

dt = 0.1
nmax = 1000
t = range(nmax)
signal = [np.sum([sum([np.cos(2*np.pi*n*o/b)
      for o in range(1,b+1)]) for b in range(2,nmax)])
      for n in range(nmax)]
print(signal)
plt.subplot(211)
plt.plot(t,signal)
fourier = np.fft.fft(signal)
freq = np.fft.fftfreq(nmax, d=dt)
plt.subplot(212)
k = np.arange(nmax)
print(str(k[-1])+"␣␣"+str(k[1])+"␣␣"+str(k[0]))
x = np.append(k, k[-1]+k[1]-k[0])
z = np.append(fourier, fourier[0])
y = np.abs(z)
plt.plot(x,y)
X = np.array([x,x])
Z = np.array([z,z])
y0 = np.zeros(len(x))
print(y0)
Y = np.array([y0,y])
C = np.angle(Z)
plt.pcolormesh(X, Y, C, cmap=Greys,
                vmin=-np.pi/16.0, vmax=np.pi/16.0)
plt.colorbar()
plt.show()
```

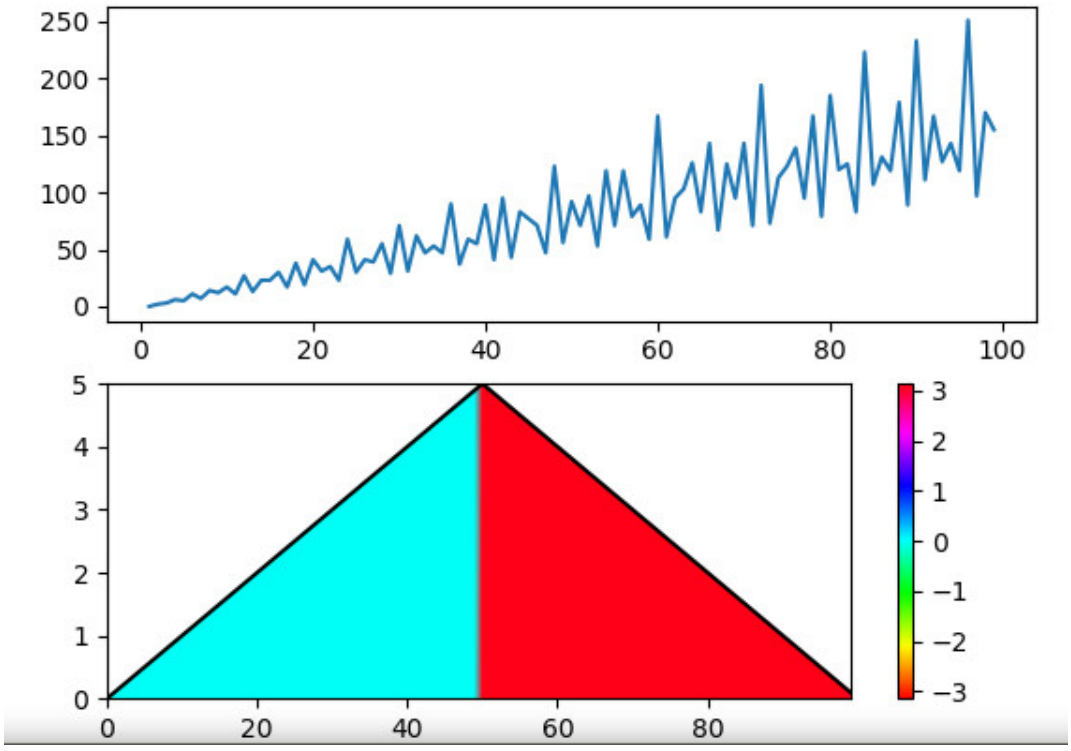
1. jusqu'à 1000.

Voici le spectre en question :



Les raies de ce spectre apparaissent très clairement aux positions 500, 333, 666, 200, 400, 600, 800, etc., c'est à dire aux positions $\frac{1}{k}$ pour k compris entre 2 et $p-1$ avec p premier si l'on considère 1000 comme l'unité.

On peut également calculer le spectre en fréquence de la fonction en question :



Notre problème, récurrent, est qu'on ne sait toujours pas si, en "découvrant" cette propriété du spectre, on a découvert un diamant ou de la simple verroterie mathématique.

Décompositions de matrices en valeurs singulières (Denise Vella-Chemla, 7.3.2019)

On présente ici quelques résultats obtenus en décomposant certaines matrices en valeurs singulières [1].

On a testé plusieurs matrices A, pour lesquelles les tests n'ont pas été probants (l'algorithme de décomposition en valeurs singulières renvoie pour une matrice A qui lui est fournie en entrée 3 matrices U, Σ et V^* telles que $A = U\Sigma V^*$) :

1) la matrice booléenne de divisibilité contenait en $A[i,j]$ le booléen 1 si i divise j et 0 sinon ;
2) la matrice booléenne "premier à" contenait en $A[i,j]$ le booléen 0 si i et j étaient premiers entre eux ($pgcd(i,j) = 1$) et 1 sinon ;
3) la matrice booléenne "décomposants de Goldbach" contenait en $A[i,j]$ le booléen 1 si i et $j-i$ étaient premiers et 0 sinon (elle ne contenait que les lignes correspondant aux nombres pairs n et les colonnes correspondant aux nombres impairs qui peuvent potentiellement décomposer additivement les nombres pairs indices des lignes) ;
4) la dernière matrice testée contenait la fraction $1/j$ en $A[i,j]$ lorsque $pgcd(i,j)$ est différent de 1 et 0 sinon.

Voici l'apparence de la dernière matrice tronquée à 10×10.

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0.5 & 0 & 0.25 & 0 & 0.166667 & 0 & 0.125 & 0 & 0.1 \\
0 & 0 & 0.333333 & 0 & 0 & 0.166667 & 0 & 0 & 0.111111 & 0 \\
0 & 0.5 & 0 & 0.25 & 0 & 0.166667 & 0 & 0.125 & 0 & 0.1 \\
0 & 0 & 0 & 0 & 0.2 & 0 & 0 & 0 & 0 & 0.1 \\
0 & 0.5 & 0.333333 & 0.25 & 0 & 0.166667 & 0 & 0.125 & 0.111111 & 0.1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0.142857 & 0 & 0 & 0 \\
0 & 0.5 & 0 & 0.25 & 0 & 0.166667 & 0 & 0.125 & 0 & 0.1 \\
0 & 0 & 0.333333 & 0 & 0 & 0.166667 & 0 & 0 & 0.111111 & 0
\end{pmatrix}$$

Notre but serait d'obtenir des valeurs singulières dans le "style" du logarithme, c'est-à-dire que les parties entières des petites valeurs se répèteraient peu et augmenteraient assez rapidement tandis que celles des grandes valeurs se répèteraient davantage et l'écart entre 2 valeurs successives serait de plus en plus faible.

1. On a utilisé le programme fourni dans cette page https://machinelearningmastery.com/singular-value-decomposition-for-machine-learning/ . Le livre de référence où trouver une présentation de la SVD (abréviation anglaise) est *Matrix computations*, Johns Hopkins éditions, 4ème édition, G.H. Golub et C.F. Van Loan (1983). Le but de la décomposition en valeurs singulières est d'extraire les caractères dominants de l'information codée par une matrice M, c'est-à-dire d'obtenir une autre matrice qui contient en quelque sorte l'essence de l'information contenue dans M. La SVD est notamment utilisée pour débruiter des spectres (cf *Performance du SVD pour débruiter les spectres RMN et Raman*, Guillaume Laurent, William Woelffel, Virgile Barret-Vivin, Emmanuelle Gouillart, Christian Bonhomme, c2i-2016 : 7ème Colloque Interdisciplinaire en Instrumentation, Jan 2016, Saint-Nazaire, France.).

Voici les programmes [2] : le programme en C++ écrit la matrice.

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

int pgcd(int m, int n) {
  while (m  != 0) {
      int r ;

      r = n % m ; n = m ; m = r ;
  }
  return(n) ;
}

int main (int argc, char* argv[])
{
  int n, x, nmax ;
  float mat[140][140] ;

  nmax = 100 ;
  for (n = 1 ; n <= nmax ; ++n)
    for (x = 1 ; x <= nmax ; ++x)
      mat[n][x] = 0 ;
  for (n = 1 ; n <= nmax ; ++n)
    for (x = 1 ; x <= nmax ; ++x)
      if (pgcd(n,x) == 1) mat[n][x] = 0.0 ;
      else mat[n][x] = 1.0/(float)x ;
  for (n = 1 ; n <= nmax ; ++n)
    {
      std::cout << "[" ;
      for (x = 1 ; x <= nmax ; ++x)
        std::cout << mat[n][x] << "," ;
      std::cout << "]," ;
      std::cout << "\n" ;
    }
}
```

Le programme python ci-dessous décompose la matrice obtenue par le programme ci-dessus en valeurs singulières (Σ est remplacé par s dans le programme) :

```python
from numpy import array
from numpy import diag
from numpy import dot
from numpy import zeros
from scipy.linalg import svd

A = array( ##ici il faut coller la matrice ##
           ## obtenue par le programme C++ ## )
print("A")
print(A)
U, s, V* = svd(A)
print("\nU") ; print(U)
print("\ns") ; print(s)
print("\nV*") ; print(V*)
print("\nA=UsV*")
for i in range(100):
   print(s[i]**2)
```

2. à réécrire, le but est de rapidement satisfaire le souhait de “voir ce que ça donne”.

Voici les résultats de quelques programmes.

```
A
[[0.        0.        0.        ... 0.        0.        0.       ]
 [0.        0.5       0.        ... 0.0102041 0.        0.01     ]
 [0.        0.        0.333333  ... 0.        0.010101  0.       ]
 ...
 [0.        0.5       0.        ... 0.0102041 0.        0.01     ]
 [0.        0.        0.333333  ... 0.        0.010101  0.       ]
 [0.        0.5       0.        ... 0.0102041 0.        0.01     ]]

U
[[ 0.00000000e+00  0.00000000e+00  0.00000000e+00 ...  0.00000000e+00
   0.00000000e+00  0.00000000e+00]
 [-1.32089477e-01  8.04762777e-02  3.68366580e-02 ... -4.60212122e-03
   5.52844163e-04  6.40499527e-04]
 [-3.49658245e-02 -1.96487394e-01  3.35452247e-02 ... -3.23711970e-03
  -1.21452459e-05  6.46622254e-03]
 ...
 [-1.33690720e-01  7.59852504e-02  2.81185431e-02 ...  1.73062952e-02
  -8.25613042e-02  8.36641413e-02]
 [-3.61404533e-02 -1.96628928e-01  3.16888927e-02 ...  3.19719470e-02
  -1.76012510e-01  2.03879401e-02]
 [-1.36344738e-01  6.87864238e-02 -1.82705303e-01 ...  6.34874962e-02
  -1.34902218e-01  5.25652046e-02]]

s
[4.65611391e+00 1.94936677e+00 9.33790933e-01 5.71790070e-01
 4.81439410e-01 2.93927295e-01 2.43090394e-01 2.13429409e-01
 1.44860809e-01 1.40061142e-01 1.35108704e-01 1.18800440e-01
 9.02263084e-02 8.02390309e-02 7.17259919e-02 6.34123028e-02
 5.86410266e-02 5.30018321e-02 4.31607748e-02 3.92038692e-02
 3.58469368e-02 3.51075312e-02 3.39330107e-02 3.32686737e-02
 3.25243339e-02 3.07325421e-02 2.93690945e-02 2.84151560e-02
 2.25946666e-02 1.93762024e-02 1.88679000e-02 1.69492000e-02
 1.63934000e-02 1.59040990e-02 1.52578836e-02 1.49254000e-02
 1.44892874e-02 1.40845000e-02 1.38715120e-02 1.36986000e-02
 1.26582000e-02 1.23193040e-02 1.20482000e-02 1.12360000e-02
 1.05183231e-02 1.03093000e-02 1.01818389e-02 9.07762826e-03
 8.89885398e-03 8.30783062e-03 8.11130666e-03 7.60308069e-03
 7.36229665e-03 7.07033010e-03 6.93997657e-03 6.67738363e-03
 6.49705085e-03 6.03641202e-03 5.71822874e-03 5.00493168e-03
 7.16854622e-16 5.20003341e-16 3.53270803e-16 3.53270803e-16
 3.53270803e-16 3.53270803e-16 3.53270803e-16 3.53270803e-16
 3.53270803e-16 3.53270803e-16 3.53270803e-16 3.53270803e-16
 3.53270803e-16 3.53270803e-16 3.53270803e-16 3.53270803e-16
 3.53270803e-16 3.53270803e-16 3.53270803e-16 3.53270803e-16
 3.53270803e-16 3.53270803e-16 3.53270803e-16 3.53270803e-16
 3.53270803e-16 3.53270803e-16 3.53270803e-16 3.53270803e-16
 3.53270803e-16 3.53270803e-16 1.88615847e-16 1.24449645e-16
 9.30644727e-17 4.19372065e-17 2.97735936e-17 1.56921106e-17
 1.45903823e-17 1.39463671e-17 1.10132647e-17 1.04494666e-17]

V*
[[ 0.00000000e+00 -7.48461738e-01 -2.19634386e-01 ... -1.55138572e-02
  -7.55676328e-03 -1.54023185e-02]
 [ 0.00000000e+00  2.95566924e-01 -8.24432046e-01 ...  3.81076411e-03
  -2.38595787e-02  2.40336935e-03]
 [ 0.00000000e+00  1.05568221e-01  1.27979748e-01 ... -6.85256944e-04
   2.07862919e-03 -2.39656320e-02]
 ...
 [ 0.00000000e+00  0.00000000e+00 -1.49050665e-01 ...  3.29510795e-02
  -9.49321653e-02 -1.40688520e-01]
 [ 0.00000000e+00  0.00000000e+00  4.65274363e-03 ... -2.63724869e-02
   2.37148263e-01  1.40517023e-01]
 [ 0.00000000e+00  0.00000000e+00 -2.41910608e-02 ...  1.47993123e-03
  -7.57626842e-02 -3.77435695e-02]]

A=UsV*
```

Voyons les carrés des éléments diagonaux de Σ dans un tableau (à lire par colonnes) :

21.6793967164	0.00128500287704	0.00016023002724	$5.13880549673e-31$	$1.24800260396e-31$
3.8000308122	0.00123253874694	0.000151765251357	$2.70403474271e-31$	$1.24800260396e-31$
0.871965506593	0.00115144921495	0.00014515912324	$1.24800260396e-31$	$1.24800260396e-31$
0.32694388399	0.00110680465294	0.000126247696	$1.24800260396e-31$	$1.24800260396e-31$
0.231783905087	0.00105783229614	0.000110635121457	$1.24800260396e-31$	$1.24800260396e-31$
0.0863932544963	0.000944489142309	0.00010628166649	$1.24800260396e-31$	$1.24800260396e-31$
0.059092939799	0.000862543711767	0.000103669843365	$1.24800260396e-31$	$1.24800260396e-31$
0.0455521125966	0.000807421088811	$8.24033347536e-05$	$1.24800260396e-31$	$1.24800260396e-31$
0.0209846541007	0.000510518956639	$7.91896020941e-05$	$1.24800260396e-31$	$1.24800260396e-31$
0.0196171235262	0.000375437221318	$6.90200496897e-05$	$1.24800260396e-31$	$1.24800260396e-31$
0.0182543619638	0.00035599765041	$6.57932956662e-05$	$1.24800260396e-31$	$3.55759375824e-32$
0.0141135446318	0.00028727538064	$5.7806836049e-05$	$1.24800260396e-31$	$1.54877142586e-32$
0.00814078671969	0.00026874356356	$5.42034119737e-05$	$1.24800260396e-31$	$8.66099608286e-33$
0.00643830208238	0.000252940365325	$4.99895677871e-05$	$1.24800260396e-31$	$1.75872929239e-33$
0.00514461791193	0.000232803011583	$4.8163274861e-05$	$1.24800260396e-31$	$8.86466876797e-34$
0.00402112014764	0.00022276756516	$4.45874520913e-05$	$1.24800260396e-31$	$2.46242336274e-34$
0.00343876999992	0.00020993944904	$4.2211669715e-05$	$1.24800260396e-31$	$2.128792558e-34$
0.0028091942088	0.00019837314025	$3.64382701353e-05$	$1.24800260396e-31$	$1.94501154613e-34$
0.00186285247845	0.000192418844822	$3.50493411279e-05$	$1.24800260396e-31$	$1.21292000214e-34$
0.00153694336395	0.00018765164196	$2.26981399349e-05$	$1.24800260396e-31$	$1.09191351983e-34$

Ce résultat ne correspondant pas à ce qu'on souhaite (écarts de plus en plus faibles mais valeurs décroissantes), on remplace les carrés des éléments diagonaux de la matrice Σ (correspondant à l'écriture des $s[i]^2$ dans le programme en python) par $25 - s[i]^2$) pour que les petits éléments soient moins répétés que les grands éléments. Il se trouve qu'on a utilisé une matrice finie de taille 100×100 et que 25 est approximativement la valeur de $100/ln\ 100$ [3].

Les images des valeurs singulières par cette modification sont :

3.32060328361	24.9987149971	24.99983977	25.0	25.0
21.1999691878	24.9987674613	24.9998482347	25.0	25.0
24.1280344934	24.9988485508	24.9998548409	25.0	25.0
24.673056116	24.9988931953	24.9998737523	25.0	25.0
24.7682160949	24.9989421677	24.9998893649	25.0	25.0
24.9136067455	24.9990555109	24.9998937183	25.0	25.0
24.9409070602	24.9991374563	24.9998963302	25.0	25.0
24.9544478874	24.9991925789	24.9999175967	25.0	25.0
24.9790153459	24.999489481	24.9999208104	25.0	25.0
24.9803828765	24.9996245628	24.99993098	25.0	25.0
24.981745638	24.9996440023	24.9999342067	25.0	25.0
24.9858864554	24.9997127246	24.9999421932	25.0	25.0
24.9918592133	24.9997312564	24.9999457966	25.0	25.0
24.9935616979	24.9997470596	24.9999500104	25.0	25.0
24.9948553821	24.999767197	24.9999518367	25.0	25.0
24.9959788799	24.9997772324	24.9999554125	25.0	25.0
24.99656123	24.9997900606	24.9999577883	25.0	25.0
24.9971908058	24.9998016269	24.9999635617	25.0	25.0
24.9981371475	24.9998075812	24.9999673019	25.0	25.0
24.9984630566	24.9998123484	24.9999749507	25.0	25.0

3. Cela corrobore l'idée que $ln\ n$ code l'information associée au nombre n.

Si on remplit la première colonne de la matrice de 1 (après tout, 1 divise tous les nombres), le résultat est moins satisfaisant :

2885.88743285	2999.99849938	2999.99982527	2999.99999526
2991.60741185	2999.99874998	2999.99984697	3000.0
2996.87846951	2999.99877043	2999.99984829	3000.0
2999.21330917	2999.99886724	2999.99986524	3000.0
2999.7011722	2999.9989062	2999.99988532	...
2999.79145017	2999.99895047	2999.99988951	
2999.91681115	2999.99910746	2999.9998961	
2999.94540223	2999.99913746	2999.99991428	
2999.95483379	2999.99922954	2999.99991908	
2999.97993775	2999.99948977	2999.99992611	
2999.98053749	2999.99962465	2999.99993332	
2999.98208001	2999.99965615	2999.99994218	
2999.98604257	2999.99971921	2999.99994313	
2999.99211913	2999.99974383	2999.99994769	
2999.99364057	2999.99974805	2999.99995042	
2999.99485926	2999.99976723	2999.99995187	
2999.99602603	2999.99978472	2999.99995542	
2999.99676973	2999.99979009	2999.99995867	
2999.99721198	2999.99980595	2999.99996619	
2999.99814259	2999.99980808	2999.99996787	

On souhaite également tester 3 matrices auxquelles on s'est intéressé à plusieurs reprises :

5) la matrice diagonale des $\exp \frac{2\pi}{p}$ avec p premier (on code le fait pour un nombre d'être composé par un élément diagonal nul) ;
6) la matrice triangulaire basse des $\cos \frac{2\pi no}{t}$;
7) une matrice similaire à celle utilisée ci-dessus mais qui verrait ses coefficients fractionnaires $1/k$ remplacés par des $1/ln\ k$.

Voici les valeurs obtenues comme images par la fonction $f(x) = 25 - x$ des $s[i]^2$ pour la matrice dans le cas 5) (c'est une matrice diagonale qui contient des coefficients 0 pour les indices qui sont des nombres composés et qui contient des $e^{\frac{2\pi}{p}}$ pour les indices qui sont des nombres premiers) :

```
  A
[[ 0.       0.       0.      ...  0.       0.       0.     ]
 [ 0.      23.1407   0.      ...  0.       0.       0.     ]
 [ 0.       0.       8.12053 ...  0.       0.       0.     ]
 ...
 [ 0.       0.       0.      ...  0.       0.       0.     ]
 [ 0.       0.       0.      ...  0.       0.       0.     ]
 [ 0.       0.       0.      ...  0.       0.       0.     ]]

U
[[0. 0. 0. ... 0. 0. 0.]
 [1. 0. 0. ... 0. 0. 0.]
 [0. 1. 0. ... 0. 0. 0.]
 ...
 [0. 0. 0. ... 1. 0. 0.]
 [0. 0. 0. ... 0. 1. 0.]
 [0. 0. 0. ... 0. 0. 1.]]
```

```
s
[2.31407000e+01 8.12053000e+00 3.51359000e+00 2.45370000e+00
 1.77039000e+00 1.62145000e+00 1.44715000e+00 1.39193000e+00
 1.31414000e+00 1.24192000e+00 1.22468000e+00 1.18509000e+00
 1.16561000e+00 1.15734000e+00 1.14303000e+00 1.12586000e+00
 1.11237000e+00 1.10849000e+00 1.09832000e+00 1.09253000e+00
 1.08988000e+00 1.08278000e+00 1.07864000e+00 1.07315000e+00
 1.06692000e+00 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15
 2.31222042e-15 2.31222042e-15 2.31222042e-15 2.31222042e-15]

 V*
[[0. 1. 0. ... 0. 0. 0.]
 [0. 0. 1. ... 0. 0. 0.]
 [0. 0. 0. ... 0. 0. 0.]
 ...
 [0. 0. 0. ... 1. 0. 0.]
 [0. 0. 0. ... 0. 1. 0.]
 [0. 0. 0. ... 0. 0. 1.]]

A=UsV*
```

−510.49199649	23.8121615856	25.0	25.0	25.0
−40.9430074809	23.8121615856	25.0	25.0	25.0
12.6546853119	23.8275874716	25.0	25.0	25.0
18.97935631	23.8365357504	25.0	25.0	25.0
21.8657192479	23.8483490775	25.0	25.0	25.0
22.3708998975	23.8616817136	25.0	25.0	25.0
22.9057568775	25.0	25.0	25.0	25.0
23.0625308751	25.0	25.0	25.0	25.0
23.2730360604	25.0	25.0	25.0	25.0
23.4576347136	25.0	25.0	25.0	25.0
23.5001588976	25.0	25.0	25.0	25.0
23.5955616919	25.0	25.0	25.0	25.0
23.6413533279	25.0	25.0	25.0	25.0
23.6605641244	25.0	25.0	25.0	25.0
23.6934824191	25.0	25.0	25.0	25.0
23.7324392604	25.0	25.0	25.0	25.0
23.7626329831	25.0	25.0	25.0	25.0
23.7712499199	25.0	25.0	25.0	25.0
23.7936931776	25.0	25.0	25.0	25.0
23.8063781991	25.0	25.0	25.0	25.0

Les résultats sont peu probants mais on obtient l'allure générale souhaitée : croissance et écarts entre deux nombres successifs allant s'amenuisant.

Les résultats sont aussi peu probants dans le cas 6) (matrice contenant des cosinus), on ne les reporte pas ici.

Dans le cas 4) de la matrice contenant des fractions comprises entre 0 et 1 pour les coefficients-noeuds de divisibilité, on obtient cet ensemble de valeurs sur la diagonale de Σ :

On rappelle l'allure de A dans le cas 3 :

```
A
[[1.        0.        0.        ... 0.        0.        0.       ]
 [1.        0.5       0.        ... 0.        0.        0.       ]
 [1.        0.        0.333333  ... 0.        0.        0.       ]
 ...
 [1.        0.5       0.        ... 0.0102041 0.        0.       ]
 [1.        0.        0.333333  ... 0.        0.010101  0.       ]
 [1.        0.5       0.        ... 0.        0.        0.01     ]]
```

108.674196502	0.00544989557862	0.00070154742262	0.000173796294339	$5.83548107524e-05$
6.37298298289	0.00493690542223	0.000674223550113	0.000156799078991	$5.7057463612e-05$
2.6313657741	0.0045987448796	0.000516204896639	0.000152790854719	$5.56007207607e-05$
0.790103378471	0.00403496458407	0.000464568247524	0.000141107212868	$5.20215590349e-05$
0.694992900526	0.0035188383274	0.000443570230473	0.000134541456887	$5.01516458977e-05$
0.26478712676	0.00278928685558	0.000404310189158	0.000132709451977	$4.67938830844e-05$
0.156211680215	0.00266398835853	0.000377332187717	0.000122297480475	$4.23923682868e-05$
0.0997187232614	0.00234967138721	0.000343045441381	0.000114474406405	$4.13880537755e-05$
0.0961606311889	0.00213991461893	0.000283145252026	0.000109830981444	$3.71099979134e-05$
0.0732673040176	0.0017509125305	0.000279703565144	0.000100589506544	$2.9167962694e-05$
0.0431835467644	0.00147994062137	0.000258312606659	$9.62424917471e-05$	$2.83785129084e-05$
0.0384593923818	0.0014636420175	0.00025506622578	$9.15174824484e-05$	$2.59672256912e-05$
0.0189708063317	0.00140542049113	0.00025060466223	$8.47712494842e-05$	$2.39457024115e-05$
0.0173481942063	0.00122058997984	0.000232917051133	$8.20546933454e-05$	$2.23150556148e-05$
0.0158902951871	0.00113845425252	0.000230384857779	$7.6353894481e-05$	$1.96574180229e-05$
0.0150803889736	0.00106674760612	0.000214903368888	$7.50016919415e-05$	$1.85404122388e-05$
0.0124047888128	0.00103596646136	0.000213529253679	$6.69506935326e-05$	$1.56248441348e-05$
0.0110721870025	0.000902278713479	0.000193575428772	$6.66349532198e-05$	$9.66809601276e-06$
0.00742389179676	0.000816317993325	0.000188458582255	$6.25382901749e-05$	$8.30007852048e-06$
0.0065713832573	0.000747999183379	0.000176250380598	$6.07565020569e-05$	$3.74036676728e-06$

On teste enfin l'utilisation de logarithmes dans les matrices (choix 7) ci-dessus) et les résultats sont plus conformes à nos attentes, même si les valeurs ne croissent pas assez rapidement.

Si on remplit la matrice par ces instructions :

```
for (n = 1 ; n <= nmax ; ++n)
    for (x = 1 ; x <= nmax ; ++x)
      if (pgcd(n,x) == 1) mat[n][x] = 0.0 ;
      else mat[n][x] = 1.0/log((float)x) ;
```

on obtient les valeurs suivantes :

−340.242100729	24.8262430882	24.9487864996	25.0	25.0
−32.9246718823	24.8316836653	24.9503668438	25.0	25.0
6.86863939688	24.8344723583	24.9522171004	25.0	25.0
16.2046556135	24.8407229417	24.9572008064	25.0	25.0
19.1024435697	24.8566646035	24.9678820754	25.0	25.0
21.6454659163	24.8775942229	24.9779736917	25.0	25.0
22.7153080672	24.8943091605	24.9789149881	25.0	25.0
22.9549748887	24.9032099609	24.9796843567	25.0	25.0
23.7751969843	24.9208201266	24.98076991	25.0	25.0
23.9021021233	24.9365609994	24.9829513981	25.0	25.0
23.9586122828	24.9398543995	24.9855631096	25.0	25.0
24.1157845746	24.940826032	24.9866367966	25.0	25.0
24.3776181934	24.9434368911	24.988599772	25.0	25.0
24.5212135021	24.9442507526	24.9890129852	25.0	25.0
24.5846452856	24.9446520334	24.9900005896	25.0	25.0
24.588005638	24.9449656552	24.9907539043	25.0	25.0
24.6322843577	24.9455846086	24.9911241054	25.0	25.0
24.7257218098	24.9456760444	24.9924839875	25.0	25.0
24.7691421779	24.947622185	24.9929701764	25.0	25.0
24.8168690809	24.9486198275	24.995261237	25.0	25.0

Si on remplit la matrice par ces instructions :

```
for (n = 1 ; n <= nmax ; ++n)
  for (x = 1 ; x <= nmax ; ++x)
    if ((n%x) == 0) mat[n][x] = 1.0/log((float)x) ;
```

on obtient les valeurs suivantes :

−10000000043.8	24.6753930433	24.9088639774	24.9566688735	24.9831513577
−32.6859009407	24.7011864118	24.9171041991	24.9605319801	24.9838171359
3.67895525934	24.7096788938	24.9224975527	24.9638082774	24.9843949814
17.326865157	24.7262349709	24.9307607898	24.966603928	24.9856747293
17.6319034623	24.7742597573	24.937243029	24.9679254797	24.9865216083
21.0390946697	24.780618833	24.9399367996	24.9713034216	24.9871382626
22.9342403634	24.8088764612	24.9402832193	24.9724298888	24.9878668791
23.1459963855	24.8180603728	24.9418196297	24.9728342474	24.9890896505
23.2631881628	24.820230044	24.9424042863	24.9738779192	24.9908592712
23.3207372372	24.8268940873	24.9439873005	24.9754361531	24.9920328012
23.8179791045	24.8338485077	24.9440982491	24.9760992002	24.9923586381
24.0875149449	24.8475764374	24.9446956735	24.9771711954	24.9925642087
24.2908156796	24.8520231185	24.9451496545	24.9776185429	24.9927293587
24.3359412848	24.8561925801	24.9453422072	24.978048135	24.9933533639
24.4043345131	24.8644732539	24.945506709	24.9789155519	24.9948330173
24.4917013581	24.8764346086	24.9467976191	24.979027889	24.9952422296
24.5188030564	24.8810703698	24.9482855416	24.9797029738	24.9958943006
24.5370699049	24.8947195631	24.949828304	24.981319458	24.9973388302
24.5912772705	24.9009438149	24.9517075316	24.9816265066	24.9979935231
24.6353758213	24.9049357469	24.9521417396	24.9821938674	24.9991433106

Si on remplit la matrice par ces instructions :

```
for (n = 1 ; n <= nmax ; ++n)
   for (x = 2 ; x <= nmax ; ++x)
      if (((n%x) == 0) && (pow(x,vp(n,x)) == n)) // puissance "pure"
        mat[n][x] = 1.0/log((float)x) ;
```

avec la fonction $vp(n, p)$ (pour valuation p-adique) définie ainsi :

```
int vp(int m, int p)
{
  if ((m%p) != 0) return 0 ;
  else return vp(m/p, p)+1 ;
}
```

on obtient les valeurs suivantes :

11.4782557783	24.898284293	24.9317803063	24.943833844	24.9503668438
21.4307171924	24.900990343	24.9325403271	24.9442204247	24.9506129382
24.176624281	24.9057952028	24.9332718109	24.9445976679	24.950854874
24.2215022649	24.9099387896	24.9346573931	24.9449656552	24.9510922352
24.3356643273	24.9118064433	24.9353137078	24.9453249341	24.9513250506
24.4367510818	24.9135557678	24.9359479828	24.9456760444	24.951553789
24.5977332191	24.9151984832	24.9365609994	24.9460190538	24.9517789144
24.652418068	24.918204	24.9371545239	24.9463540285	24.9520000101
24.7610588334	24.9195835179	24.9377282912	24.9466814955	24.9522171004
24.826084311	24.9208894372	24.9382850194	24.9470019746	24.9524306452
24.8380500951	24.9226826697	24.9388239138	24.94731552	24.9526406651
24.8480006034	24.9233053442	24.9393466542	24.947622185	24.9542476861
24.8564173601	24.9244255915	24.9398543995	24.947922478	24.9547473696
24.8636404056	24.9254939302	24.9403473109	24.9485045905	24.95988736
24.8754220621	24.9265129228	24.940826032	24.9487864996	24.963488203
24.8803006074	24.9274866659	24.9412911946	24.9490631211	24.9690438208
24.8846562179	24.9284191379	24.9417439022	24.9493340417	24.9760850348
24.8885722191	24.9293115479	24.9426129229	24.94959975	24.9778914044
24.8921146853	24.930168238	24.9430304255	24.9498602814	24.9878829985
24.8953380448	24.9309902862	24.9434368911	24.9501161176	25.0

La première de ces trois propositions d'utilisation du logarithme népérien (noté *log* en C++) semble la plus intéressante, la croissance des valeurs étant plus progressive que dans les deux derniers cas.

Décomposition en valeurs singulières d'une matrice diagonale de nombres premiers (Denise Vella-Chemla, 10.3.2019)

On peut se reporter à http://denise.vella.chemla.free.fr/decovalesing.pdf pour lire ce que l'on tente de faire en ce moment : calculer la décomposition en valeurs singulières d'une matière A choisie de façon un peu hasardeuse et étudier l'allure de la matrice intermédiaire Σ obtenue par la décomposition $A = U\Sigma V^*$.

On est complètement surprise par le fait d'obtenir le spectre suivant lorsqu'on initialise la matrice A à une matrice diagonale définie par :

- $A[i,j] = 0 \iff i \neq j$;
- $A[i,i] = 0 \iff i$ est un nombre composé;
- $A[i,i] = i \iff i$ est un nombre premier.

Voici les programmes : le programme en C++ écrit la matrice.

```
#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 main (int argc, char* argv[]) {
  int n, x, nmax ;
  float mat[140][140] ;

  nmax = 100 ;
  for (n = 1 ; n <= nmax ; ++n)
     for (x = 1 ; x <= nmax ; ++x)
        mat[n][x] = 0 ;
  for (n = 1 ; n <= nmax ; ++n)
     if (prime(n)) mat[n][n] = (float)n ;
  }
}
```

Le programme python ci-dessous décompose la matrice obtenue par le programme ci-dessus en valeurs singulières (Σ est remplacé par s dans le programme) :

```
# Reconstruct SVD
from numpy import array
from numpy import diag
from numpy import dot
from numpy import zeros
from scipy.linalg import svd

A = array( ## ici coller la matrice diagonale obtenue par le programme en C++ ## )
print("A")
print(A)
U, s, V = svd(A)
print("\nU")
print(U)
print("\ns")
print(s)
print("\nV")
print(V)
print("\nA=UsV")
#Sigma = zeros((A.shape[0], A.shape[1]))
#Sigma[:A.shape[1], :A.shape[1]] = diag(s)
#print("\n On controle quon revient bien a la matrice initiale.")
#B = U.dot(Sigma.dot(V))
#print(B)
for i in range(100):
    print(float(i)-s[i]**2)
```

Voici le résultat de ce programme.

```
A
[[0 0 0 ... 0 0 0]
 [0 2 0 ... 0 0 0]
 [0 0 3 ... 0 0 0]
 ...
 [0 0 0 ... 0 0 0]
 [0 0 0 ... 0 0 0]
 [0 0 0 ... 0 0 0]]

U
[[0. 0. 0. ... 0. 0. 0.]
 [0. 0. 0. ... 0. 0. 0.]
 [0. 0. 0. ... 0. 0. 0.]
 ...
 [0. 0. 0. ... 1. 0. 0.]
 [0. 0. 0. ... 0. 1. 0.]
 [0. 0. 0. ... 0. 0. 1.]]

s
[9.700000e+01 8.900000e+01 8.300000e+01 7.900000e+01 7.300000e+01
 7.100000e+01 6.700000e+01 6.100000e+01 5.900000e+01 5.300000e+01
 4.700000e+01 4.300000e+01 4.100000e+01 3.700000e+01 3.100000e+01
 2.900000e+01 2.300000e+01 1.900000e+01 1.700000e+01 1.300000e+01
 1.100000e+01 7.000000e+00 5.000000e+00 3.000000e+00 2.000000e+00
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15
 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15 9.692247e-15]
```

```
V
[[0. 0. 0. ... 0. 0. 0.]
 [0. 0. 0. ... 0. 0. 0.]
 [0. 0. 0. ... 0. 0. 0.]
 ...
 [0. 0. 0. ... 1. 0. 0.]
 [0. 0. 0. ... 0. 1. 0.]
 [0. 0. 0. ... 0. 0. 1.]]

A=UsV
```

Les images par $f(x) = x - \Sigma[x]^2$ des nombres de 1 à 100 sont (lire le tableau par colonnes) :

−9409.0	−101.0	40.0	60.0	80.0
−7920.0	−28.0	41.0	61.0	81.0
−6887.0	−3.0	42.0	62.0	82.0
−6238.0	14.0	43.0	63.0	83.0
−5325.0	20.0	44.0	64.0	84.0
−5036.0	25.0	45.0	65.0	85.0
−4483.0	26.0	46.0	66.0	86.0
−3714.0	27.0	47.0	67.0	87.0
−3473.0	28.0	48.0	68.0	88.0
−2800.0	29.0	49.0	69.0	89.0
−2199.0	30.0	50.0	70.0	90.0
−1838.0	31.0	51.0	71.0	91.0
−1669.0	32.0	52.0	72.0	92.0
−1356.0	33.0	53.0	73.0	93.0
−947.0	34.0	54.0	74.0	94.0
−826.0	35.0	55.0	75.0	95.0
−513.0	36.0	56.0	76.0	96.0
−344.0	37.0	57.0	77.0	97.0
−271.0	38.0	58.0	78.0	98.0
−150.0	39.0	59.0	79.0	99.0

On obtient comme images des nombres négatifs pour les nombres inférieurs à 25 qui se trouve être égal à $100/ln\ 100$ puis les images deviennent $f(x) = x - 1$ pour les nombres compris entre 25 et 100.

Décomposition en valeurs singulières d'une matrice diagonale particulière (Denise Vella-Chemla, 10.3.2019)

On peut se reporter à cette première note ou à cette seconde note pour avoir une idée de ce que l'on tente de faire en ce moment : il s'agit de calculer la décomposition en valeurs singulières d'une matière A choisie de façon un peu hasardeuse et d'étudier l'allure de la matrice intermédiaire Σ obtenue par la décomposition $A = U\Sigma V^*$.

La matrice A est une matrice triangulaire basse définie par :

$$A[n,x] \ = \ \begin{cases} \dfrac{ln\ n}{2\pi} \text{ pour } x \text{ de 1 à } n \text{ inclus si } x|n \ ; \\ \\ 0 \text{ sinon.} \end{cases}$$

Voici les programmes : le programme en C++ écrit la matrice.

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

int prime(int atester)
{
  unsigned long diviseur=2;
  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, x, nmax ;
  float mat[1441][1441] ;

  nmax = 1420 ;
  for (n = 1 ; n <= nmax ; ++n)
    for (x = 1 ; x <= nmax ; ++x)
      mat[n][x] = 0 ;
  for (n = 1 ; n <= nmax ; ++n)
    for (x = 1 ; x <= n ; ++x)
      if ((n%x) == 0) mat[n][x] = log(float(n))/(2.0*M_PI) ;
  for (n = 1 ; n <= nmax ; ++n)
    {
      std::cout << "[" ;
      for (x = 1 ; x <= nmax ; ++x)
        std::cout << mat[n][x] << "," ;
      std::cout << "]," ;
      std::cout << "\n" ;
    }
}
```

Des contraintes d'occupation mémoire obligent à utiliser une matrice de taille 1420×1420.

On rappelle que la matrice Σ contient sur sa diagonale les valeurs singulières de A, i.e. les racines carrées positives des valeurs propres de AA^* ou de A^*A (qui sont égales même si AA^* et A^*A ne le sont pas forcément).

Les carrés des $\Sigma[x]$ sont les valeurs propres de AA^* ou de A^*A.

Le programme python ci-dessous décompose la matrice, obtenue par le programme C++, en valeurs singulières (Σ est remplacé par s dans le programme python) puis il calcule les valeurs $561 - Sigma[i]^2$ (561 est la valeur approximative de la plus grande valeur propre, augmentée de 14, au hasard) :

```
# Reconstruct SVD
from numpy import array
from numpy import diag
from numpy import dot
from numpy import zeros
from scipy.linalg import svd

A = array( ## ici coller la matrice obtenue par le programme en C++ ci-dessus ##)
print("A")
print(A)
U, s, V = svd(A)
print("\nU")
print(U)
print("\ns")
print(s)
print("\nV")
print(V)
print("\nA=UsV")
#Sigma = zeros((A.shape[0], A.shape[1]))
#Sigma[:A.shape[1], :A.shape[1]] = diag(s)
#print("\n On controle quon revient bien a la matrice initiale.")
#B = U.dot(Sigma.dot(V))
#print(B)
for i in range(1420):
    print(561.0-s[i]**2)
```

Voici le résultat de ce programme.

```
[[0.       0.       0.       ... 0.       0.       0.      ]
 [0.110318 0.110318 0.       ... 0.       0.       0.      ]
 [0.17485  0.       0.17485  ... 0.       0.       0.      ]
 ...
 [1.15499  1.15499  0.       ... 1.15499  0.       0.      ]
 [1.1551   0.       1.1551   ... 0.       1.1551   0.      ]
 [1.15521  1.15521  0.       ... 0.       0.       1.15521 ]]

U
[[-1.11022302e-16 -2.22044605e-16 -8.32667268e-16 ... -3.74640945e-14
  -6.55399315e-14 -1.00000000e+00]
 [-2.37741008e-03 -2.20525478e-04  2.39321467e-03 ... -2.98632712e-02
  -9.63851830e-01  8.56161866e-14]
 [-3.24211617e-03 -5.43586719e-03 -1.32043909e-03 ...  9.53958320e-01
  -7.86474610e-03 -2.08945830e-14]
 ...
 [-2.49213541e-02 -2.36216548e-03  2.52226092e-02 ...  1.68724033e-04
   1.67998280e-04 -5.89805982e-17]
 [-2.40657814e-02 -4.10170863e-02 -9.30135671e-03 ...  4.28189685e-04
   8.55092204e-05  1.52655666e-16]
 [-3.82290192e-02  2.60573330e-02  3.63728214e-02 ...  3.22972602e-05
   2.90778634e-04 -1.52655666e-16]]

s
[5.19519165e+01 2.33923756e+01 2.29849024e+01 ... 1.09106584e-02
 5.80333762e-03 4.39334124e-15]
```

```
V
[[-6.76167566e-01 -4.43423166e-01 -2.87138977e-01 ... -5.54049143e-04
  -5.35079087e-04 -8.50065758e-04]
 [-4.23779456e-01  3.77018141e-01 -3.03460160e-01 ... -1.16631058e-04
  -2.02539653e-03  1.28681636e-03]
 [ 3.74925019e-01  1.23704447e-01 -5.48503307e-01 ...  1.26743463e-03
  -4.67437144e-04  1.82808029e-03]
 ...
 [ 1.49022340e-02 -1.78557679e-02  4.46248656e-02 ...  1.78609360e-02
   4.53319943e-02  3.41960279e-03]
 [-1.72699861e-02 -3.34339569e-02  1.70089522e-02 ...  3.34352999e-02
   1.70198095e-02  5.78822753e-02]
 [-3.39422117e-02  3.39422117e-02  3.39422117e-02 ... -3.39422117e-02
   3.39422117e-02 -9.54297405e-14]]

A=UsV
```

Les images par $f(x) = 561 - \Sigma[x]^2$ des nombres de 1 à 100 sont (lire le tableau par colonnes) :

−2138.00163247	494.352578525	526.030438578	538.735890534	544.586861925
13.7967646102	496.423846665	526.962704161	538.906093642	544.639440943
32.6942613319	500.887531138	528.449732725	539.041910525	544.916130435
149.91021977	502.006046786	529.444517937	539.120948115	545.267733941
240.926080288	502.707132998	530.321019491	539.270944879	545.633447427
326.689323827	504.732573721	531.265305219	540.233068476	545.932498456
341.547037108	506.744921471	531.898239776	540.582091414	546.010740386
373.437083444	509.938685426	532.348022699	541.056424656	546.090943439
388.848448189	513.795276939	532.772537589	541.41614529	546.190883682
417.15295015	514.926930875	533.047292939	541.697715318	546.212261214
430.24116732	515.221874876	533.901683211	542.211203976	546.340190077
443.507958568	516.353247519	534.573267235	542.319979404	546.409623531
452.738552489	517.564578917	534.962065599	542.57018078	546.5786899
453.488661267	518.94473361	535.460457317	543.216188088	546.827693581
473.073059951	521.647161951	536.065685687	543.334098616	546.96084195
476.230907792	522.407058441	536.345286542	543.522994082	546.972997394
478.300876214	522.767562886	536.808390947	543.531950249	547.085008873
479.612324772	523.947602098	537.503330118	543.889064808	547.15630978
483.374316104	524.564302067	538.255446817	543.984084876	547.225608769
493.069420209	525.186869247	538.559008719	544.067879807	547.298583047

Les 100 dernières valeurs (pour x allant de 1410 à 1420) obtenues par le programme sont :

560.994042303
560.994228392
560.995469467
560.995857567
560.996124514
560.996425799
560.996510886
560.996835094
560.997738359
560.998028077
560.998281736
560.998537424
560.99868932
560.999219922
560.999231672
560.999605627
560.999714664
560.999880958
560.999966321
561.0

On est satisfait du fait que les valeurs croissent bien comme un logarithme.

Décomposition en valeurs singulières d'une matrice un peu creuse mais particulière (Denise Vella-Chemla, 13.3.2019)

On peut se reporter à cette première note ou à cette seconde note pour avoir une idée de ce que l'on tente de faire en ce moment : il s'agit de calculer la décomposition en valeurs singulières d'une matière A choisie de façon un peu hasardeuse et d'étudier l'allure de la matrice intermédiaire Σ obtenue par la décomposition $A = U\Sigma V^*$.

La matrice A est une matrice triangulaire basse contenant des nombres complexes et définie par :

$$A[n,x] \ = \ \begin{cases} e^{\frac{2ix\pi}{n}} \text{ si } x \text{ et } n \text{ sont premiers}, 1 \leqslant x \leqslant n \ ; \\ \\ 0 \text{ sinon.} \end{cases}$$

Voici les programmes : le programme en C++ écrit la matrice.

```
#include <iostream>
#include <stdio.h>
#include <cmath>
#include <complex>
using namespace std ;
#define M_PI 3.14159265358979323846
typedef std::complex<double> dcomplex ;
const dcomplex di = dcomplex(0.0,1.0) ;

int prime(int atester) {
  unsigned long diviseur=2;
  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, x, nmax ;
  dcomplex mat[421][421] ;

  nmax = 100 ;
  for (n = 1 ; n <= nmax ; ++n)
    for (x = 1 ; x <= nmax ; ++x)
      mat[n][x] = 0 ;
  for (n = 1 ; n <= nmax ; ++n)
    if (prime(n))
      for (x = 1 ; x <= n ; ++x)
        if (prime(x))
          mat[n][x] = exp((dcomplex((float)x,0)*2.0*di*M_PI)/dcomplex((float)n,0.0)) ;
  for (n = 1 ; n <= nmax ; ++n) {
      std::cout << "[" ;
      for (x = 1 ; x <= nmax ; ++x)
        std::cout << mat[n][x] << "," ;
      std::cout << "]," ;
      std::cout << "\n" ;
  }
}
```

Des contraintes d'occupation mémoire font qu'on expérimente seulement sur une matrice de taille 100×100.

On rappelle que la matrice Σ contient sur sa diagonale les valeurs singulières de A, i.e. les racines carrées positives des valeurs propres de AA^* ou de A^*A (qui sont égales même si les produits matriciels AA^* et A^*A ne le sont pas forcément).

Les carrés des $\Sigma[x]$ sont les valeurs propres de AA^* ou de A^*A.

Le programme python ci-dessous décompose la matrice, obtenue par le programme C++, en valeurs singulières (Σ est remplacé par s dans le programme python) puis il calcule les valeurs des carrés des $Sigma[i]$:

```
# Reconstruct SVD
import numpy as np
from numpy import array
from numpy import diag
from numpy import dot
from numpy import zeros
from numpy.linalg import svd

A = array( # ici coller la matrice obtenue par le programme en C++ # )
print("A")
print(A)
U, s, V = np.linalg.svd(A)
print("\nU")
print(U)
print("\ns")
print(s)
print("\nV")
print(V)
print("\nA=UsV")
#Sigma = zeros((A.shape[0], A.shape[1]))
#Sigma[:A.shape[1], :A.shape[1]] = diag(s)
#print("\n On controle quon revient bien a la matrice initiale.")
#B = U.dot(Sigma.dot(V))
#print(B)
for i in range(100):
    print(s[i]**2)
    print( )
```

Voici le résultat de ce programme. On ne fournit que V et Σ, avec, en regard pour V, les indices entiers auxquels sont associés ces complexes.

```
V
[ [[ 1.00000000e+00  0.00000000e+00]..........................1
   [ 0.00000000e+00  1.00000000e+00]]
  [[-1.00000000e+00  2.44929000e-16]..........................2
   [ 2.44929000e-16  1.00000000e+00]]
  [[-8.66025606e-01 -4.99999650e-01]..........................3
   [-4.99999650e-01  8.66025606e-01]]
  [[ 1.00000000e+00  0.00000000e+00]..........................4
   [ 0.00000000e+00  1.00000000e+00]]
  [[-1.00000000e+00 -0.00000000e+00]..........................5
   [-0.00000000e+00 -1.00000000e+00]]
  [[ 1.00000000e+00  0.00000000e+00]..........................6
   [ 0.00000000e+00  1.00000000e+00]]
  [[ 6.23489736e-01 -7.81831535e-01]..........................7
   [ 7.81831535e-01  6.23489736e-01]]
  [[ 1.00000000e+00  0.00000000e+00]..........................8
   [ 0.00000000e+00  1.00000000e+00]]
  [[ 1.00000000e+00  0.00000000e+00]..........................9
   [ 0.00000000e+00  1.00000000e+00]]
  [[ 1.00000000e+00  0.00000000e+00]..........................10
   [ 0.00000000e+00  1.00000000e+00]]
```

```
[[-7.38660966e-01 -6.74077130e-01].....11
  [ 6.74077130e-01 -7.38660966e-01]]
[[ 1.00000000e+00  0.00000000e+00].....12
  [ 0.00000000e+00  1.00000000e+00]]
[[-9.35016434e-01  3.54604382e-01].....13
  [-3.54604382e-01 -9.35016434e-01]]
[[ 1.00000000e+00  0.00000000e+00].....14
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....15
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....16
  [ 0.00000000e+00  1.00000000e+00]]
[[-3.78451830e-01 -9.25620988e-01].....17
  [ 9.25620988e-01 -3.78451830e-01]]
[[ 1.00000000e+00  0.00000000e+00].....18
  [ 0.00000000e+00  1.00000000e+00]]
[[-6.77282597e-01 -7.35722967e-01].....19
  [ 7.35722967e-01 -6.77282597e-01]]
[[ 1.00000000e+00  0.00000000e+00].....20
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....21
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....22
  [ 0.00000000e+00  1.00000000e+00]]
[[-6.50478929e-01 -7.59524300e-01].....23
  [ 7.59524300e-01 -6.50478929e-01]]
[[ 1.00000000e+00  0.00000000e+00].....24
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....25
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....26
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....27
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....28
  [ 0.00000000e+00  1.00000000e+00]]
[[-7.70779716e-01 -6.37101742e-01].....29
  [ 6.37101742e-01 -7.70779716e-01]]
[[ 1.00000000e+00  0.00000000e+00].....30
  [ 0.00000000e+00  1.00000000e+00]]
[[-9.01507120e-01 -4.32764270e-01].....31
  [ 4.32764270e-01 -9.01507120e-01]]
[[ 1.00000000e+00  0.00000000e+00].....32
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....33
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....34
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....35
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....36
  [ 0.00000000e+00  1.00000000e+00]]
[[-9.07897613e-01 -4.19191990e-01].....37
  [ 4.19191990e-01 -9.07897613e-01]]
[[ 1.00000000e+00  0.00000000e+00].....38
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....39
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....40
  [ 0.00000000e+00  1.00000000e+00]]
[[-8.98389049e-01 -4.39200544e-01].....41
  [ 4.39200544e-01 -8.98389049e-01]]
[[ 1.00000000e+00  0.00000000e+00].....42
  [ 0.00000000e+00  1.00000000e+00]]
[[-9.55128668e-01 -2.96191201e-01].....43
  [ 2.96191201e-01 -9.55128668e-01]]
[[ 1.00000000e+00  0.00000000e+00].....44
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....45
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....46
  [ 0.00000000e+00  1.00000000e+00]]
```

```
[[-9.67768909e-01 -2.51839908e-01].....47
  [ 2.51839908e-01 -9.67768909e-01]]
[[ 1.00000000e+00  0.00000000e+00].....48
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....49
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....50
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....51
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....52
  [ 0.00000000e+00  1.00000000e+00]]
[[-6.77877621e-01 -7.35174762e-01].....53
  [ 7.35174762e-01 -6.77877621e-01]]
[[ 1.00000000e+00  0.00000000e+00].....54
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....55
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....56
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....57
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....58
  [ 0.00000000e+00  1.00000000e+00]]
[[-7.02084591e-01 -7.12093552e-01].....59
  [ 7.12093552e-01 -7.02084591e-01]]
[[ 1.00000000e+00  0.00000000e+00].....60
  [ 0.00000000e+00  1.00000000e+00]]
[[-8.14806979e-01 -5.79732341e-01].....61
  [ 5.79732341e-01 -8.14806979e-01]]
[[ 1.00000000e+00  0.00000000e+00].....62
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....63
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....64
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....65
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....66
  [ 0.00000000e+00  1.00000000e+00]]
[[-8.51828819e-01 -5.23820259e-01].....67
  [ 5.23820259e-01 -8.51828819e-01]]
[[ 1.00000000e+00  0.00000000e+00].....68
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....69
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....70
  [ 0.00000000e+00  1.00000000e+00]]
[[-8.90461902e-01 -4.55057800e-01].....71
  [ 4.55057800e-01 -8.90461902e-01]]
[[ 1.00000000e+00  0.00000000e+00].....72
  [ 0.00000000e+00  1.00000000e+00]]
[[-9.33934364e-01 -3.57444546e-01].....73
  [ 3.57444546e-01 -9.33934364e-01]]
[[ 1.00000000e+00  0.00000000e+00].....74
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....75
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....76
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....77
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....78
  [ 0.00000000e+00  1.00000000e+00]]
[[-9.40182654e-01 -3.40670776e-01].....79
  [ 3.40670776e-01 -9.40182654e-01]]
[[ 1.00000000e+00  0.00000000e+00].....80
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....81
  [ 0.00000000e+00  1.00000000e+00]]
[[ 1.00000000e+00  0.00000000e+00].....82
  [ 0.00000000e+00  1.00000000e+00]]
[[-9.42395225e-01 -3.34501481e-01].....83
  [ 3.34501481e-01 -9.42395225e-01]]
```

```
      [[ 1.00000000e+00  0.00000000e+00]..........................84
        [ 0.00000000e+00  1.00000000e+00]]
      [[ 1.00000000e+00  0.00000000e+00]..........................85
        [ 0.00000000e+00  1.00000000e+00]]
      [[ 1.00000000e+00  0.00000000e+00]..........................86
        [ 0.00000000e+00  1.00000000e+00]]
      [[ 1.00000000e+00  0.00000000e+00]..........................87
        [ 0.00000000e+00  1.00000000e+00]]
      [[ 1.00000000e+00  0.00000000e+00]..........................88
        [ 0.00000000e+00  1.00000000e+00]]
      [[-8.98788033e-01 -4.38383476e-01]..........................89
        [ 4.38383476e-01 -8.98788033e-01]]
      [[ 1.00000000e+00  0.00000000e+00]..........................90
        [ 0.00000000e+00  1.00000000e+00]]
      [[ 1.00000000e+00  0.00000000e+00]..........................91
        [ 0.00000000e+00  1.00000000e+00]]
      [[ 1.00000000e+00  0.00000000e+00]..........................92
        [ 0.00000000e+00  1.00000000e+00]]
      [[ 1.00000000e+00  0.00000000e+00]..........................93
        [ 0.00000000e+00  1.00000000e+00]]
      [[ 1.00000000e+00  0.00000000e+00]..........................94
        [ 0.00000000e+00  1.00000000e+00]]
      [[ 1.00000000e+00  0.00000000e+00]..........................95
        [ 0.00000000e+00  1.00000000e+00]]
      [[ 1.00000000e+00  0.00000000e+00]..........................96
        [ 0.00000000e+00  1.00000000e+00]]
      [[-8.07036946e-01 -5.90500946e-01]..........................97
        [ 5.90500946e-01 -8.07036946e-01]]
      [[ 1.00000000e+00  0.00000000e+00]..........................98
        [ 0.00000000e+00  1.00000000e+00]]
      [[ 1.00000000e+00  0.00000000e+00]..........................99
        [ 0.00000000e+00  1.00000000e+00]]
      [[ 1.00000000e+00  0.00000000e+00]........................100
        [ 0.00000000e+00  1.00000000e+00]]]

A=UsV
```

On est étonné par l'image du nombre premier 5, qui vaut $-1-i$.

La matrice Σ contient les nombres complexes suivants pour les indices de 1 à 100. Seuls les nombres premiers ont une image puisque c'est ce qui avait été choisi dans l'opérateur A initial :

0	0	0	0	2.6826396	2.40903408	3.21129004	2.7726549	0	0
1	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0
1.22474473	0.70710653	2.28586372	1.94289118	2.79906634	2.48298778	0	0	3.55554093	3.2184044
0	0	0	0	0	0	0	0	0	0
1.519545	0.83125352	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
1.54950625	1.26452807	0	0	2.83967352	2.63367708	3.29123225	2.85793428	0	0
0	0	0	0	0	0	0	0	0	0
0	0	2.48973762	1.94966722	0	0	0	0	3.60924318	3.31260671
0	0	0	0	0	0	0	0	0	0
1.72149134	1.42704872	2.60157616	2.05713421	0	0	3.3744563	2.93479958	0	0
0	0	0	0	0	0	0	0	0	0
1.79378393	1.66803534	0	0	2.93039612	2.72264253	3.46912883	2.99418543	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
2.07867357	1.63680052	2.58302332	2.30824337	0	0	0	0	3.71177469	3.35003389
0	0	0	0	0	0	0	0	0	0
2.1600962	1.82592019	0	0	3.10887717	2.70829899	3.4907486	3.13283731	0	0
0	0	0	0	0	0	0	0	0	0

Les images par $f(x) = \Sigma[x]^2$ des nombres de 1 à 100 sont les nombres complexes suivants (lire le tableau par colonnes) :

0	0	0	0	7.19655524	5.80344518	10.3123837	7.6876152	0	0
1	0	0	0	0	0	0	0	0	0
1.49999965	0.49999965	5.22517294	3.77482612	7.83477236	6.16522832	0	0	12.64187133	10.35812691
0	0	0	0	0	0	0	0	0	0
2.30901701	0.69098241	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
2.40096962	1.59903125	0	0	8.0637457	6.93625495	10.83220972	8.16778837	0	0
0	0	0	0	0	0	0	0	0	0
0	0	6.19879343	3.80120228	0	0	0	0	13.02663633	10.9733632
0	0	0	0	0	0	0	0	0	0
2.96353242	2.03646804	6.76819854	4.23180114	0	0	11.3869553	8.61304856	0	0
0	0	0	0	0	0	0	0	0	0
3.2176608	2.78234189	0	0	8.58722143	7.41278233	12.03485482	8.96514636	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
4.32088383	2.67911596	6.67200946	5.32798744	0	0	0	0	13.77727135	11.22272707
0	0	0	0	0	0	0	0	0	0
4.66601558	3.33398455	0	0	9.66511729	7.33488344	12.1853258	9.81466959	0	0
0	0	0	0	0	0	0	0	0	0

Décomposition en valeurs singulières de matrices particulières (Denise Vella-Chemla, 16.3.2019)

On peut se reporter à cette première note ou à cette seconde note ou enfin à cette troisième note pour avoir une idée de ce que l'on tente de faire en ce moment : il s'agit de calculer la décomposition en valeurs singulières d'une matière A choisie de façon un peu hasardeuse et d'étudier l'allure de la matrice intermédiaire Σ obtenue par la décomposition $A = U\Sigma V^*$.

On a pensé qu'on n'avait pas à être étonné de n'obtenir dans les notes précédentes que des images non nulles par Σ pour les nombres premiers puisqu'on avait fourni en entrée dans la matrice A le caractère de primalité des nombres (en particulier, la diagonale contenait la fonction caractéristique de la primalité des entiers).

La matrice A est une matrice de taille $nmax \times nmax$ telle que :

$$A[n, x] \ = \ \exp^{\frac{2i\pi x}{n}} \ \text{pour } n \textit{ et } x \text{ de 1 à } nmax$$

On est surpris d'obtenir comme images par $f(x) = \Sigma(x)^2$ des nombres complexes de la forme

$$x + i(nmax - x).$$

$1.0000e+02$	$4.09680341e-26$	51.71946136	48.28056313	50.99241648	49.00757786	55.54479049	44.45517579
$1.00000e+02$	$1.02420072e-26$	52.0770335	47.92298378	51.92773788	48.07228729	55.8493131	44.15069444
50.49996468	49.49998846	50.97493075	49.02507433	52.75980697	47.24019891	56.08817752	43.91180768
50.	50.	50.74266197	49.25731949	53.45466721	46.54534907	56.26216941	43.7378124
50.00002494	50.0000005	52.08268658	47.91732933	53.98991974	46.01008996	56.37274824	43.62725715
50.49996468	49.49998846	52.45522828	47.5447676	54.35372903	45.64625469	56.42193999	43.57806703
50.62348038	49.37652373	51.8122622	48.18775192	54.54337738	45.45660478	56.41226319	43.5877271
50.00001547	50.00001547	50.50000775	49.50000089	54.56360078	45.43638159	56.34664051	43.65336783
50.5000012	49.50000221	50.98297507	49.01701991	54.42501822	45.57499231	56.2282475	43.77176835
50.00002494	50.0000005	52.18931756	47.81070298	54.14254195	45.85747342	56.06047706	43.93952407
50.50001771	49.50000928	52.83564252	47.16436149	53.7340621	46.26593254	55.84689278	44.15309886
50.86600157	49.13395157	52.82887293	47.17111154	53.21924622	46.7807493	55.59114372	44.40884805
51.00600502	48.99401998	52.23495185	47.76501902	52.61850001	47.38150608	55.29688729	44.70313292
50.90097402	49.09903035	51.22174315	48.77824031	51.95212119	48.047871	54.96774453	45.03225131
51.06461084	48.93540466	50.00000521	50.00000521	51.23980141	48.76021007	54.60737619	45.39264337
51.3065839	48.69345822	51.22442366	48.77556618	50.50000758	49.5000007	54.21927527	45.78072479
50.93247391	49.06752123	52.28181236	47.71820333	50.25027925	49.74971985	53.80688996	46.19309324
50.50000056	49.50000364	53.05403951	46.94595496	50.99573165	49.00426365	53.37354928	46.6264451
51.53460282	48.46536501	53.47759145	46.52243373	51.72291063	48.27710378	52.92240023	47.07760766
50.00001272	50.00001272	53.53807779	46.46194223	52.42017597	47.57984453	52.45647392	47.54352274
51.69158482	48.30843165	53.26027481	46.73970698	53.07773615	46.92227771	51.97864504	48.0213566
50.50002084	49.50000546	52.69652891	47.30347872	53.68758634	46.31242446	51.49162079	48.50838052
51.51404839	48.48593489	51.91532163	48.08467263	54.24335596	45.75664101	50.99795155	49.00205637
51.67303109	48.32696596	50.9917972	49.00821198	54.74021129	45.25977205	50.50000501	49.49999517
50.0000066	50.00000286	50.0000066	50.00000286	55.17477148	44.82523736	50.00000473	50.00000473

Si la matrice est triangulaire basse plutôt que complète (c'est-à-dire que les éléments de la diagonale de Σ soient nuls ou pas, ou, pour préciser davantage, que l'on oblige x à être inférieur ou égal, ou bien strictement inférieur à n, n étant compris entre 1 et $nmax$) alors tous les éléments ont des images très semblables, de l'ordre de $\frac{x}{2} + i\frac{x}{2}$, par exemple pour une matrice de taille 100×100.

1.	0.	13.00000452	13.00000188	25.49999966	25.49999796	37.99998808	37.99998808
$2.00000e+00$	$7.49871565e-33$	13.50000301	13.50000153	26.00000641	26.00000641	38.50000853	38.49999811
1.5	1.4999986	14.00000063	14.00000063	26.50000354	26.50000001	38.99999586	38.9999914
2.	2.	14.49999954	14.49999519	27.00000602	27.00000307	39.49999247	39.49999155
2.50000125	2.50000003	15.00000324	15.00000155	27.50000272	27.50000214	40.00000215	40.00000215
3.	2.9999972	15.50000062	15.49999841	27.99999544	27.99999544	40.50000425	40.50000177
3.50000103	3.49999929	16.00000221	16.00000221	28.50000339	28.49998673	40.9999976	40.99999411
4.00000124	4.00000124	16.5000025	16.50000021	28.99999907	28.99999038	41.50000609	41.50000049
4.50000038	4.49999994	17.00000071	16.99999761	29.50000364	29.50000268	42.0000068	42.0000068
5.00000249	5.00000005	17.50000388	17.50000328	30.00000479	30.00000479	42.50000579	42.49999631
5.50000244	5.50000045	18.00000065	18.00000065	30.50000105	30.49999552	43.00000784	42.99998618
5.9999972	5.9999972	18.49999796	18.499996	31.00000124	30.99999683	43.49999849	43.49999388
6.50000226	6.50000094	18.9999999	18.99998817	31.50000604	31.49999752	44.00000841	44.00000841
7.00000206	6.99999857	19.49999793	19.4999957	31.99999742	31.99999742	44.49999782	44.4999971
7.50000162	7.50000077	20.00000209	20.00000209	32.50000576	32.50000239	45.00001303	45.0000052
8.00000337	8.00000337	20.4999988	20.49999706	33.000005	33.00000043	45.50000135	45.50000084
8.50000036	8.4999988	21.00000709	20.9999997	33.50000274	33.49999666	45.99999221	45.99999221
9.00000076	8.99999989	21.50000392	21.49999309	33.99999832	33.99999832	46.50000021	46.49999253
9.49999995	9.49999409	22.00000578	22.00000578	34.50000519	34.50000476	47.00000557	47.00000309
10.00000254	10.00000254	22.50000651	22.5000026	35.00000776	35.00000656	47.50000102	47.49999558
10.50000355	10.49999985	23.00000218	22.99999004	35.50000757	35.50000258	48.00000081	48.00000081
11.00000488	11.0000009	23.50000278	23.50000155	36.00000388	36.00000388	48.50000084	48.50000056
11.50000109	11.49999502	23.99999847	23.99999847	36.50000518	36.49999273	49.00000705	49.00000173
11.99999969	11.99999969	24.50000352	24.50000086	36.99999593	36.999992	49.50000441	49.49999513
12.50000165	12.50000072	25.0000033	25.00000143	37.50000858	37.49999738	50.00000473	50.00000473

Probabilités de transition (Denise Vella-Chemla, 17.2.2019)

On doit reprendre ici une idée de modélisation qu'on a eue pour la conjecture de Goldbach et utilisant des matrices stochastiques, en essayant d'être un peu plus précise quant aux probabilités des différentes transitions possibles entre les décompositions des nombres entiers pairs comme sommes de deux impairs qui partagent certains composants (en l'occurrence, le premier ou le second sommant des décompositions).

On revient sur les règles de combinaisons de lettres qu'on avait mis au jour en février 2014 pour les étudier en termes probabilistes.

On avait pris l'habitude de coder ces transitions dans le domaine de la théorie des langages, par des mots associés à n ou $n+2$ avec des lettres a, b, c, d mais ces lettres n'étaient pas très parlantes, ce qui gênait la compréhension des processus à l'œuvre ; on va plutôt utiliser ici les lettres p pour premier et c pour composé.

On a 16 règles possibles qui lient les décompositions de n et $n+2$ en sommes de deux impairs, la première décomposition étant de la forme $n = x + y$, la seconde dénotant $n = (x+2) + (y-2)$ et la troisième étant la décomposition de $n+2$ suivante : $n + 2 = (x+2) + y$.

On identifie ces 16 règles selon le caractère premier (p) ou composé (c) des quatre nombres $x,\ y,\ x+2$ et $y-2$. Il y a 16 règles parce qu'on considère l'état *premier* ou *composé* des 4 variables qui "passent" de **2** décompositions de n à **1** décomposition de $n+2$ et que ces 4 variables peuvent prendre 2 états chacune.

On note ces 16 règles par des transitions d'états :

$$état_x,\ état_y,\ état_{x+2},\ état_{y-2} \longrightarrow état_{x+2},\ état_y.$$

$r_1)\ \ p,p,p,p \longrightarrow p,p$	$r_5)\ \ c,p,p,p \longrightarrow p,p$	$r_9)\ \ p,c,p,p \longrightarrow p,c$	$r_{13})\ \ c,c,p,p \longrightarrow p,c$
$r_2)\ \ p,p,c,p \longrightarrow c,p$	$r_6)\ \ c,p,c,p \longrightarrow c,p$	$r_{10})\ \ p,c,c,p \longrightarrow c,c$	$r_{14})\ \ c,c,c,p \longrightarrow c,c$
$r_3)\ \ p,p,p,c \longrightarrow p,p$	$r_7)\ \ c,p,p,c \longrightarrow p,p$	$r_{11})\ \ p,c,p,c \longrightarrow p,c$	$r_{15})\ \ c,c,p,c \longrightarrow p,c$
$r_4)\ \ p,p,c,c \longrightarrow c,p$	$r_8)\ \ c,p,c,c \longrightarrow c,p$	$r_{12})\ \ p,c,c,c \longrightarrow c,c$	$r_{16})\ \ c,c,c,c \longrightarrow c,c$

Prenons un exemple pour fixer les idées : l'application de la règle r_{10}, appliquée aux nombres $13, 25, 15, 23$, qui décomposent $n = 38$ qui sont bien (dans l'ordre) p, c, c, p (premier, composé, composé, premier) permet d'obtenir la décomposition c, c de $n + 2 = 40 = 15 + 25$.

Les transitions qui lient deux décompositions de n à une décomposition de $n+2$ s'effectuent bien sûr d'une manière complètement déterministe : lorsqu'on imagine le passage de la décomposition $98 = 19 + 79$ à la décomposition $100 = 21 + 79$ comme étiquetable par la transition $G \rightarrow \neg G$ qui signifie que la décomposition de 98 en $19+79$ est une décomposition de Goldbach (notée G, elle additionne deux nombres premiers) tandis que la décomposition de 100 en $21 + 79$ n'est pas une décomposition de Goldbach (notée $\neg G$ car 21 est composé), cette transition s'effectue avec la probabilité 1, elle est effective, on dirait "instanciée" en termes informatiques, comme peut être instanciée une variable.

Mais lorsqu'on imagine l'espace infini de toutes les additions de nombres entiers impairs, et qu'on ne sait pas de quoi sont composées ces additions, si elles contiennent 0, 1, 2, 3 ou 4 nombres premiers, on peut associer aux transitions entre additions des probabilités de passage, qui font penser aux transitions entre états du domaine de la physique, et qui peuvent être visualisées selon le petit automate ci-dessous, codable par la matrice :

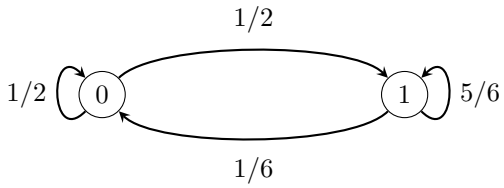
$$M = \begin{array}{c} \\ G \\ \neg\, G \end{array} \begin{array}{c} \begin{array}{cc} G & \neg\, G \end{array} \\ \begin{pmatrix} 1/2 & 1/2 \\ 1/6 & 5/6 \end{pmatrix} \end{array}$$

On fixe ces valeurs pour les probabilités car en comptant le nombre de règles parmi les 4 qui présentent 2 lettres p en $3^{\text{ème}}$ et $4^{\text{ème}}$ variables de la partie gauche de la règle (les règles $r_1,\ r_5,\ r_9,\ r_{13}$), 2 permettent d'obtenir également deux lettres p en partie droite de la règle (les règles $r_1,\ r_5$) et 2 règles ne le permettent pas (les règles $r_9,\ r_{13}$) : ceci explique les deux valeurs $1/2$ de la première ligne de la matrice de transition.

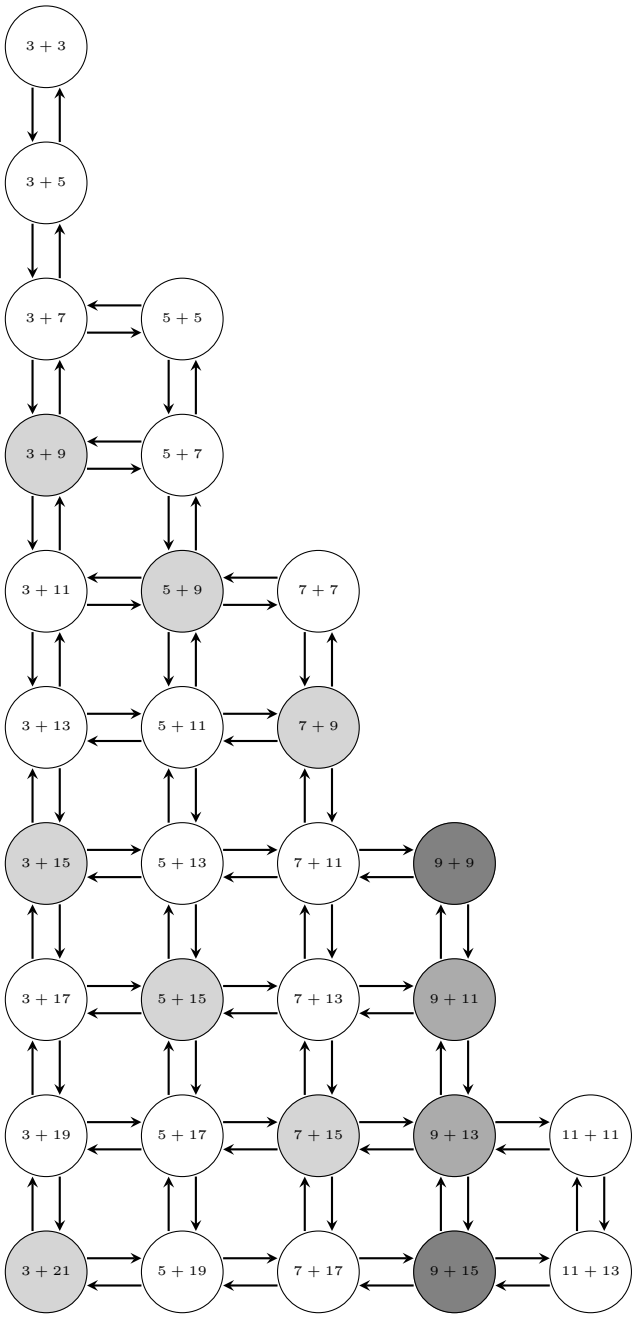
Les valeurs $1/6$ et $5/6$ de la seconde ligne se justifient par le fait que 10 règles parmi les 12 règles restantes (règles des seconde, troisième et quatrième lignes), qui présentent au moins une lettre c en $3^{\text{ème}}$ ou $4^{\text{ème}}$

variables de la partie gauche de la règle, 2 seulement permettent d'obtenir deux lettres p en partie droite de la règle (les règles r_3, r_7) et 10 règles ne le permettent pas : ceci explique les deux valeurs $2/12 = 1/6$ et $10/12 = 5/6$ de la seconde ligne de la matrice de transition.

Mais comme on ne sait pas quel est précisément le "ratio" de nombres premiers que contient un état, on doit simplement voir toutes les transitions entre états comme respectant toutes ce petit graphe simple à deux états.



Pour ne pas surcharger la représentation du graphe d'états ci-dessous, on ne note ni les transitions d'un état vers lui-même, ni les probabilités associées aux transitions. Il faut aussi imaginer toutes les flèches entrantes et sortantes vers d'autres états que l'on ne considère pas lorsqu'on cherche les décompositions de Goldbach d'un nombre.



Le problème maintenant est qu'en élevant la petite matrice M à une certaine puissance pour essayer de comprendre ce qui a lieu ligne par ligne (et être assuré qu'il y a toujours une décomposition au moins de couleur blanche (ou G par ligne ou décomposition de chaque pair en une somme de deux nombres premiers), on obtient une tendance générale vers la matrice suivante :

$$M^{1000} = \begin{array}{c} \\ G \\ \neg\, G \end{array} \begin{array}{c} \begin{array}{cc} G & \neg\, G \end{array} \\ \begin{pmatrix} 1/4 & 3/4 \\ 1/4 & 3/4 \end{pmatrix} \end{array}$$

ce qui semble indiquer que chaque état a une chance sur 2 d'être une décomposition de Goldbach (en additionnant les deux quarts de la colonne G) mais on ne sait pas combiner les différents états et $1/2$ n'est pas 1.

On trouve cependant dans cette page

http://villemin.gerard.free.fr/Wwwgvmm/Probabil/ProbCalc.htmdeuxde

l'énoncé d'un problème posé par le Chevalier de Méré au milieu du XVII$^{\text{ème}}$ dont l'énoncé est : *"qu'est-ce qui est le plus probable, obtenir un 6 en 4 jets d'un dé ou obtenir un double-6 en 24 jets de deux dés (chacune de ces probabilités globales étant proche de* 50%*) ?"*.

La page explique que Pascal fonde le calcul des probabilités en fournissant comme réponse à ce problème qu'augmenter le nombre de lancers diminue la probabilité globale :

$$1 - \left(\frac{35}{36}\right)^{24} = 0.49\ldots \text{ est inférieur à } 1 - \left(\frac{5}{6}\right)^{4} = 0.51\ldots.$$

Concernant la conjecture de Godlbach, le fait que les lignes contiennent de plus en plus de nombres, potentiellement premiers, ne semble pas augmenter la probabilité d'obtenir une décomposition d'un nombre pair n en somme de deux nombres premiers pour n de plus en plus grand.

Extrait d'une conférence du 15 juin 2011 de Pierre Boulez et Alain Connes à l'IRCAM au sujet de la créativité en musique et mathématiques (DC 30/12/13)

Pierre Boulez explique [1] : "Quand je regarde la musique, je commence par essayer d'en comprendre la forme".

[puis, à propos de non-experts s'exprimant au sujet d'une musique entendue] "Il n'y avait *(de leur part)* aucune conception de la forme mais il y avait une conception des évènements et des évènements qui n'étaient pas liés par une forme, mais des évènements séparés.
C'est très difficile d'approcher une forme même car une forme est vraiment disons... ce que... comment la personne la regarde.
Quand on voit le détail *(d'une partition musicale)*, on voit comment le discours se construit, s'il se construit plus horizontalement que verticalement ou plus verticalement qu'horizontalement, par cassure ou continuité".

Notes (!)
J'applique la méthode préconisée par Francis Brown : je regarde intensément mes grilles de divisibilité, et j'attends qu'un miracle se produise...
Pourquoi une colonne vide (qui dénote une décomposition de Goldbach) n'est pas perdue d'une grille à la suivante ; il y a quelque-chose qui ne bouge pas, au fur et à mesure du processus, un invariant qui fait qu'une condition est conservée et cette condition garantit la non-perte de l'existence d'un décomposant de Goldbach. On voit bien ce qui ne varie pas d'une grille à l'autre : c'est la forme (au sens de Pierre Boulez) des configurations bleues ou grises ; pour décrire mathématiquement une forme, il faut utiliser les distances entre les sommets de la forme et dans le cas qui nous intéresse, les sommets en question correspondent aux restes des différents entiers dans les différents corps premiers, les coordonnées de points qu'on a définies dans d'autres notes. On a le sentiment de s'approcher un peu du but, mais il semble tout de même encore très loin...

1. entre les minutes 19 et 21

Ci-dessous un extrait des Leçons de solfège et de piano de Pascal Quignard (p.27, aux éditions Arléa, 2013) (DV, 18/1/2014)

L'étude est à l'homme adulte ce que le jeu est à l'enfant. C'est la plus concentrée des passions. C'est la moins décevante des habitudes, ou des attentions, ou des accoutumances, ou des drogues. L'âme s'évade. Les maux du corps s'oublient. L'identité personnelle se dissout. On ne voit pas le temps passer. On s'envole dans le ciel du temps. Seule la faim fait lever la tête et ramène au monde.
Il est midi.
Il est déjà sept heures du soir.

[...]

Primo Levi s'en prit à Paul Celan avec violence : "Ecrire, c'est transmettre, dit-il. Ce n'est pas chiffrer le message et jeter la clé dans les buissons." Mais Primo Levi se trompait. Ecrire, ce n'est pas transmettre. C'est appeler. Jeter la clé est encore appeler une main après soi qui cherche.

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

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

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

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

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

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

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

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

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

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

1. du 9 janvier 2019.

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

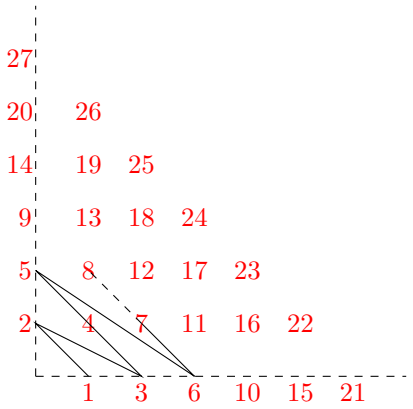
```
from math import *

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

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

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

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

Picorer l'aléa (Denise Vella-Chemla, 22.4.2019)

On voudrait montrer ici, de façon imagée ainsi que par programme, l'aléa qui gouverne le fait d'être premier ou pas pour les nombres. On utilise une bijection de $\mathbb{N}^2$ dans $\mathbb{N}$, utilisée par Cantor, qu'on illustre ainsi :



Voici le programme qui permet d'obtenir une telle numérotation [1] :

```
#include <iostream>
#include <stdio.h>
#define GREEN    "\033[0;32m"
#define WHITE     "\033[1;37m"

int main (int argc, char* argv[])
{ int x, y, res, nmax, nbprime, nbprimedanscarreCantor ;

  nmax = 17 ;
  nbprime = 1 ;
  for (x = 3 ; x <= nmax*nmax ; x = x+2)
    if (prime(x)) nbprime = nbprime+1 ;
  nbprimedanscarreCantor = 0 ;
  for (y = 0 ; y <= nmax ; ++y) {
      for (x = 0 ; x <= nmax ; ++x) {
          res = y+((x+y)*(x+y+1))/2 ;
          if (prime(res)) {
              std::cout << "\033[0;32m" ;
              nbprimedanscarreCantor = nbprimedanscarreCantor+1 ;
          }
          else std::cout << "\033[1;37m" ;
            printf("%5d␣␣␣",res) ;
      }
      std::cout << "\n\n" ;
  }
  std::cout << "vrai␣nombre␣de␣premiers␣" << nbprime ;
  std::cout << "␣nb␣premiers␣dans␣carre␣Cantor␣" ;
  std::cout << nbprimedanscarreCantor << "\n" ;
}
```

1. pour gagner en lisibilité, on a supprimé du programme la fonction booléenne *prime* qui est à ajouter.

et son résultat pour $n = 17$:

0	1	3	6	10	15	21	28	36	45	55	66	78	91	105	120	136	153
2	4	7	11	16	22	29	37	46	56	67	79	92	106	121	137	154	172
5	8	12	17	23	30	38	47	57	68	80	93	107	122	138	155	173	192
9	13	18	24	31	39	48	58	69	81	94	108	123	139	156	174	193	213
14	19	25	32	40	49	59	70	82	95	109	124	140	157	175	194	214	235
20	26	33	41	50	60	71	83	96	110	125	141	158	176	195	215	236	258
27	34	42	51	61	72	84	97	111	126	142	159	177	196	216	237	259	282
35	43	52	62	73	85	98	112	127	143	160	178	197	217	238	260	283	307
44	53	63	74	86	99	113	128	144	161	179	198	218	239	261	284	308	333
54	64	75	87	100	114	129	145	162	180	199	219	240	262	285	309	334	360
65	76	88	101	115	130	146	163	181	200	220	241	263	286	310	335	361	388
77	89	102	116	131	147	164	182	201	221	242	264	287	311	336	362	389	417
90	103	117	132	148	165	183	202	222	243	265	288	312	337	363	390	418	447
104	118	133	149	166	184	203	223	244	266	289	313	338	364	391	419	448	478
119	134	150	167	185	204	224	245	267	290	314	339	365	392	420	449	479	510
135	151	168	186	205	225	246	268	291	315	340	366	393	421	450	480	511	543
152	169	187	206	226	247	269	292	316	341	367	394	422	451	481	512	544	577
170	188	207	227	248	270	293	317	342	368	395	423	452	482	513	545	578	612

On voit qu'"il manque" des nombres de la suite séquentielle des entiers et qui sont compris entre 1 et n^2 si on prend n la longueur du côté du carré considéré (par exemple, ici, 153, 171, n'apparaissent pas) tandis que des nombres sont présents qui sont supérieurs à n^2 (par exemple 334).

Pour avoir une image en tête, c'est un peu comme si on avait pris pour une bonne part le début de la suite séquentielle des entiers mais qu'à partir d'un certain rang [2], au lieu de poursuivre la séquence, on avait décidé d'aller picorer un peu au hasard des nombres au-delà de n^2.

L'idée est alors de comparer le nombre de nombres premiers contenus dans ce qu'on appellera le "carré de Cantor" avec $\pi(n^2)$ (le nombre de nombres premiers inférieurs à n^2).

n	*nb premiers dans le carré de Cantor*	*nb premiers*	*ratio*
10^4	1236	1229	0.00566343042
10^6	78094	78498	0.00514662793
10^8	5739288	5761455	0.00384746561

Il semblerait que picorer au hasard dans la suite des entiers à partir d'un certain rang ne modifie pas sensiblement le comptage des nombres premiers, ce qui est déjà connu : deux nombres assez proches ont à peu près la même "chance" d'être premiers.

On peut peut-être "abaisser l'aléa" en utilisant certaines suites de nombres. Par exemple, si on s'intéresse à la suite diagonale de nombres commençant par 3, 11, etc. et définie par

$$\begin{cases} U_0 = 3 \\ \Delta_0 = 8 \\ \Delta_{n+1} = \Delta_n + 4 \\ U_{n+1} = U_n + \Delta_n \end{cases}$$

et qu'on compte le nombre de nombres premiers que cette suite contient, on en trouve environ 16 % alors que la proportion fournie par le théorème des nombres premiers $\frac{10000}{ln\ 10000}$ est d'environ 10 %.

2. Ici, à partir de 152 alors que $17^2 = 289$.

Entre deux (Denise Vella-Chemla, 25.4.2019)

On fournit ici un programme dont le but est de mesurer la manière dont un nombre premier est de plus en plus moyenne des 2 nombres premiers qui le précède et le suive.

Ce programme consiste à agréger les écarts, pour 3 nombres premiers consécutifs $pprec, pmilieu, psuiv$, entre le nombre premier $pmilieu$ et la moyenne $(pprec + psuiv)/2$ des nombres premiers $pprec$ et $psuiv$ qui le précède et le suive. Cet écart est normalisé selon la longueur de l'intervalle considéré (qui est égale à $psuiv - pprec$). Le tableau fournit la limite de 0.5 vers laquelle le processus semble tendre, que l'on exprime en disant qu'"un nombre premier est de plus en plus moyenne des 2 nombres premiers qui le précède et le suive".

```
def prime(atester):
  ...

pprec = 2
pmilieu = 3
psuiv = 5
nbprime = 3
sommecarresecartsmoyenne = 0.0
moyenne = (2.0+5.0)/2.0
if (moyenne > 3.0):
  ecartmoyenne = (moyenne-3.0)/3.0
else:
  ecartmoyenne = (3.0-moyenne)/3.0
sommecarresecartsmoyenne = sommecarresecartsmoyenne+ecartmoyenne
for x in range(7, 10000000, 2):
  if (prime(x)):
    nbprime = nbprime+1
    pprec = pmilieu
    pmilieu = psuiv
    psuiv = x
    moyenne = (float(pprec)+float(psuiv))/2.0
    if (float(pmilieu) > moyenne):
      ecartmoyenne = (float(pmilieu)-moyenne)/(float(psuiv)-float(pprec))
      ecartmoyenne = 0.5+ecartmoyenne
    else:
      ecartmoyenne = (moyenne-float(pmilieu))/(float(psuiv)-float(pprec))
      ecartmoyenne = 0.5-ecartmoyenne
    sommecarresecartsmoyenne = sommecarresecartsmoyenne+ecartmoyenne
print("dersomme␣"+str(sommecarresecartsmoyenne))
print("nb␣premiers␣"+str(nbprime))
print("␣moyenne␣des␣ecarts␣finale␣"+str(sommecarresecartsmoyenne / float(nbprime)))
```

n	$\pi(n)$	Σ *ecarts*	*Moyenne des positions*
10^2	25	10.8452380952	0.43380952381
10^3	168	82.5222222222	0.491203703704
10^4	1229	612.779005588	0.498599679079
10^5	9592	4791.04363013	0.499483280873
10^6	78498	39247.5993047	0.499982156293
10^7	664579	332250.932257	0.499941966654
10^9	5761455	2880703.44203	0.499995824324

Des premiers comme s'il en pleuvait (Denise Vella-Chemla, 26.4.2019)

En essayant de placer les nombres entiers successifs non pas sur la droite linéaire et séquentielle traditionnelle mais sur un plan cartésien, selon la numérotation de Cantor, on a découvert des sortes de "gisements de premiers" qui apparaissent comme des travées de nombres de la couleur choisie pour distinguer les nombres premiers des autres nombres au sein du carré.

On a testé cette chaîne-ci :

$$3 \xrightarrow{+8} 11 \xrightarrow{+12} 23 \xrightarrow{+16} 39 \xrightarrow{+20} 59\ldots$$

définie par :

$$\begin{cases} U_0 = 3 \\ \Delta_0 = 8 \\ U_{n+1} = U_n + \Delta_n \\ \Delta_{n+1} = \Delta_n + 4 \end{cases}$$

Pour $n = 10000$, on trouve une proportion de 16.4 % de nombres premiers dans la séquence considérée alors que ce ratio est de 12.29 % pour l'ensemble des entiers de 1 à 10000 ; pour $n = 100000$, le ratio passe à 12.81 % alors qu'il est de 9.59 % dans la séquence complète des entiers jusqu'à 100000.

En décidant de se promener par légers zig-zags, on trouve également la séquence :

$$1 \xrightarrow{+2} 3 \xrightarrow{+4} 7 \xrightarrow{+4} 11 \xrightarrow{+6} 17 \xrightarrow{+6} 23 \xrightarrow{+8} 31 \xrightarrow{+8} 39\ldots$$

définie par :

$$\begin{cases} U_0 = 1 \\ \Delta_0 = 2 \\ U_{n+1} = U_n + \Delta_n \\ \Delta_{n+1} = \Delta_n + 2 \text{ si } n \text{ est pair, } \Delta_{n+1} = \Delta_n \text{ sinon.} \end{cases}$$

Pour $n = 10000$, on trouve une proportion de 20.97 % de nombres premiers dans la séquence considérée alors que ce ratio est de 12.29 % pour l'ensemble des entiers de 1 à 10000 ; pour $n = 100000$, le ratio passe à 15.99 % alors qu'il est de 9.59 % dans la séquence complète des entiers jusqu'à 100000.

En faisant une dernière étude visuelle du résultat du programme qui écrivait les nombres à la manière de Cantor, on trouve un ultime gisement ; il correspond à la séquence de nombres :

$$29 \xrightarrow{+2} 31 \xrightarrow{+6} 37 \xrightarrow{+10} 47 \xrightarrow{+14} 61 \xrightarrow{+18} 79 \xrightarrow{+22} 91 \xrightarrow{+26} 117\ldots$$

définie par :

$$\begin{cases} U_0 = 29 \\ \Delta_0 = 2 \\ U_{n+1} = U_n + \Delta_n \\ \Delta_{n+1} = \Delta_n + 4 \end{cases}$$

On note dans le tableau ci-dessous la proportion de nombres premiers trouvés selon le nombre de nombres de la séquence définie ci-dessus testés, c'est assez impressionnant :

nb de nbs testés	dernier nombre testé	pourcentage de nombres premiers
50	5029	86.27 %
100	20029	75 %
200	80029	66.66 %
500	500029	54.5 %
800	1280029	50.81 %
1000	2000029	49.65 %
2019	8152751	44.75 %
5000	50000029	38.39 %
50000	5000000029	29.69 %
500000	500000000029	23.95 %

Il vaut mieux penser que le k−ième nombre de la la séquence qui semble prolifique s'obtient par l'opération matricielle :

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^k \begin{pmatrix} 29 \\ 2 \\ 4 \end{pmatrix}$$

avec

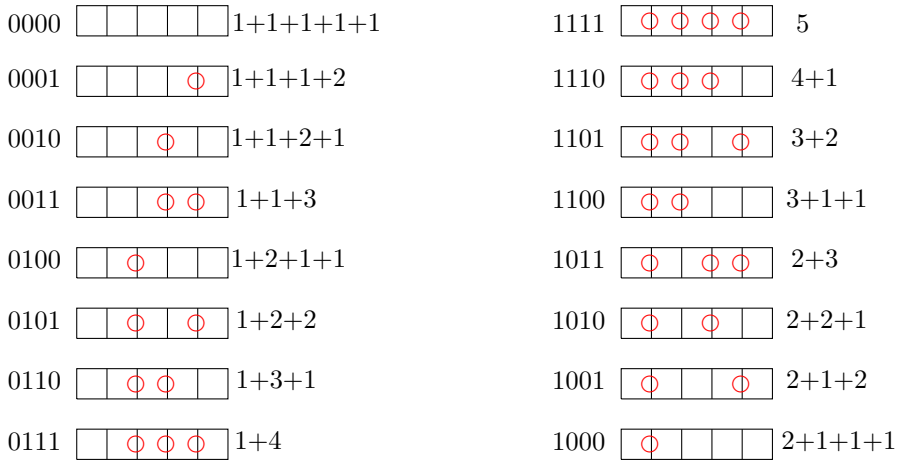
$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^k = \frac{1}{2} \begin{pmatrix} 2 & 2k & k^2 - k \\ 0 & 2 & 2k \\ 0 & 0 & 2 \end{pmatrix}$$

On lit que la matrice 3×3 est une matrice de Toeplitz et on obtient une formule simple pour les nombres dont on teste la primalité : ils sont de la forme $2k^2 + 29$.

Compositions palindromiques (Denise Vella-Chemla, 29.4.2019)

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

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



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

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

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

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

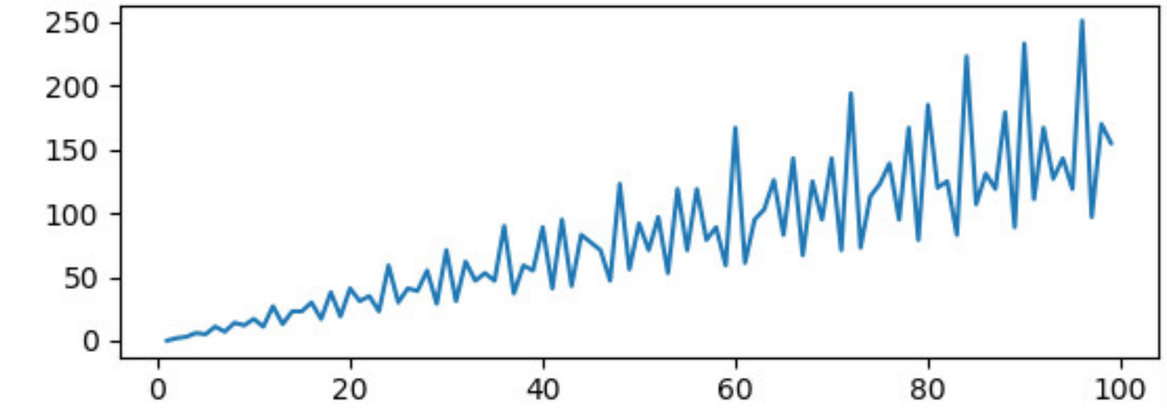
Un nombre n est alors composé si l'un de ses mots (non triviaux) associés m_k, auquel on concatène un 0 (noté en rouge pour le distinguer du mot initial) est une puissance au moins carrée de l'un des sous-mots propres de m_k. Inversement, un nombre n est premier si aucun de ses mots associés m_k ne vérifie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

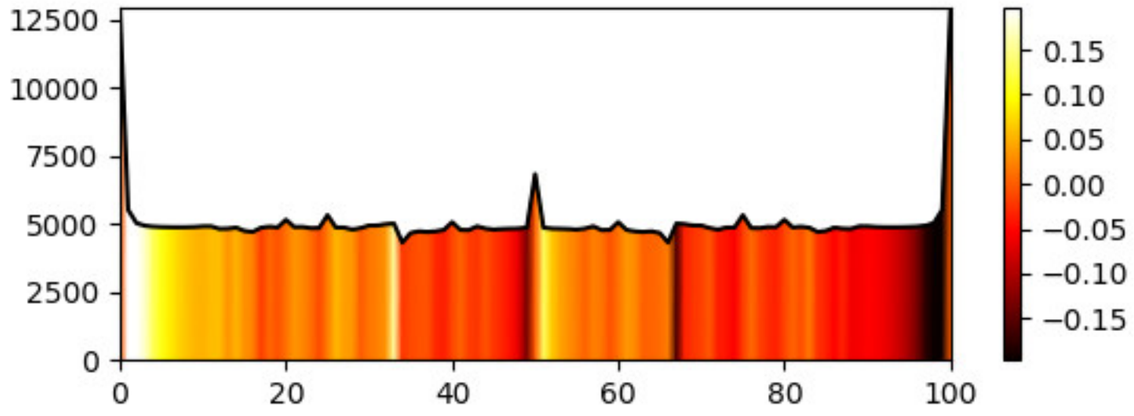
Par exemple, aucun des mots palindromiques associés à 7 et auxquels on concatène un 0 n'est puissance de l'un de ses sous-mots propres : $0011000, 0100100, 0111100, 1000010, 1100110, 1011010$.
9 est composé : son mot associé 11011011 auquel on concatène 0 est puissance cubique de 110.

$$110110110 = (110)^3$$

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

Figure 1





emacs25@vellachemla-X510UA

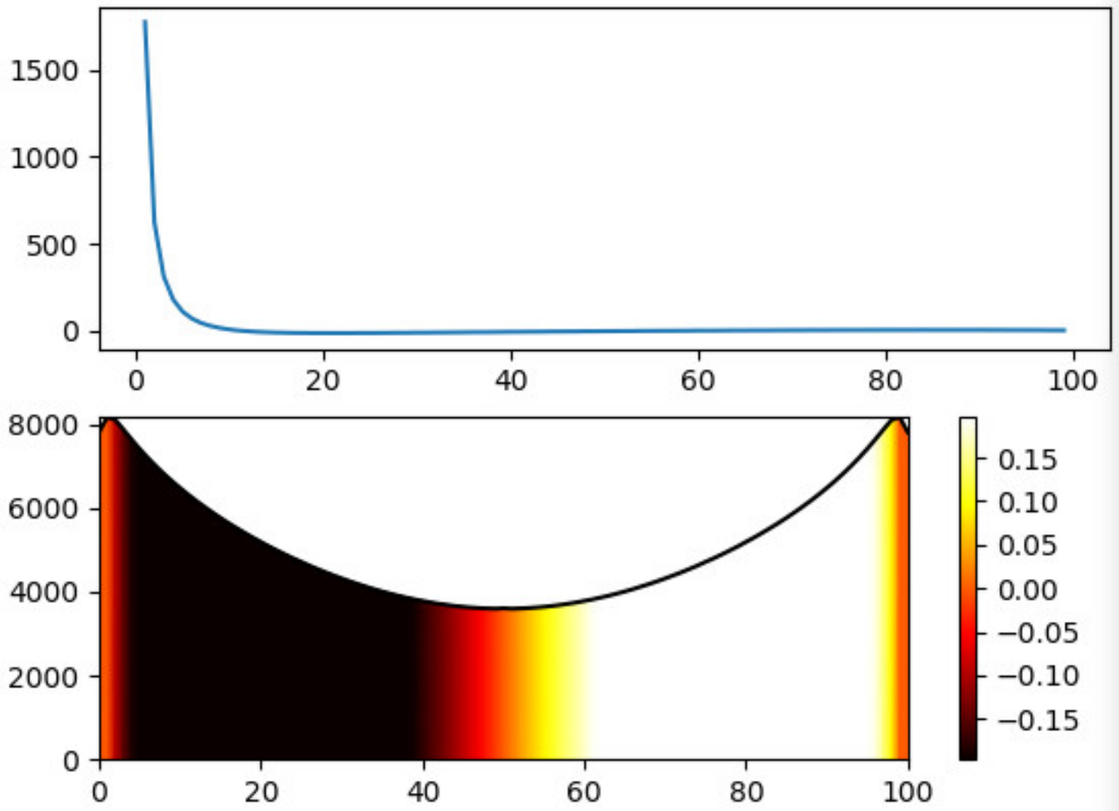
File Edit Options Buffers Tools Python Help

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

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

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

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

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

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

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

Figure 1



emacs25@vellachemla-X510UA

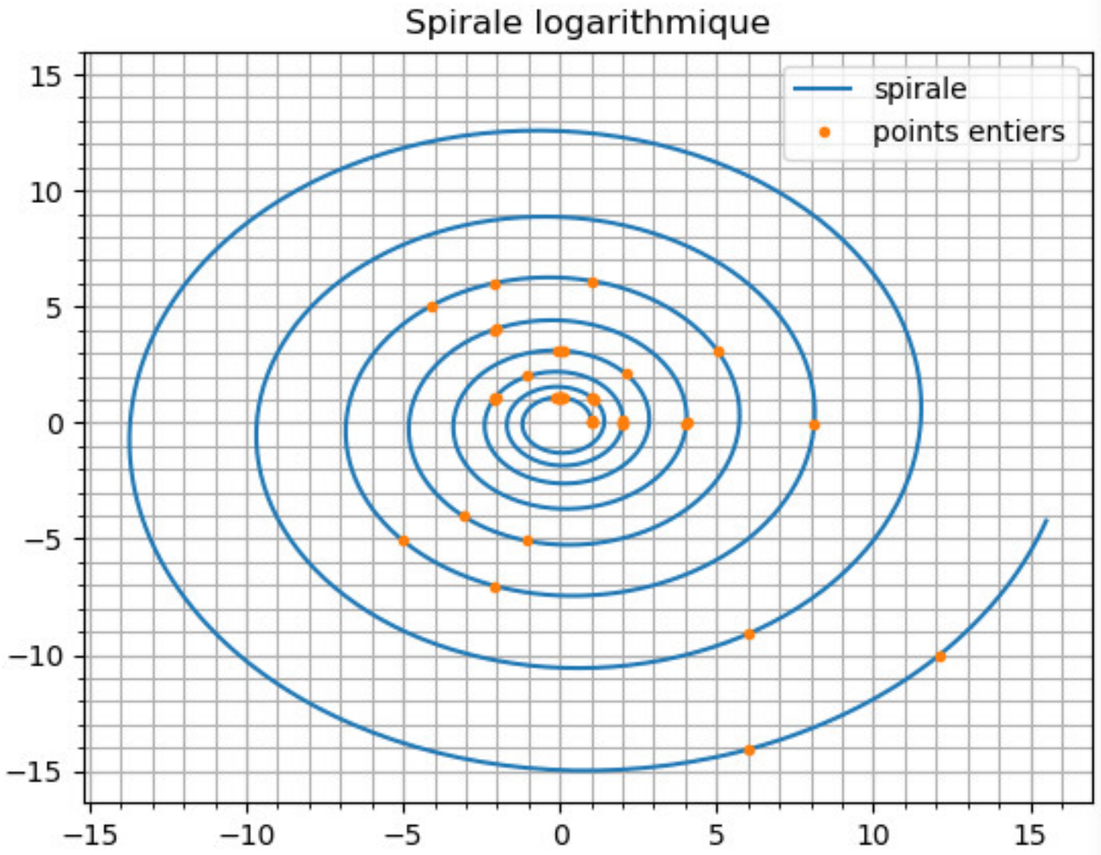
File Edit Options Buffers Tools Python Help

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

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

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

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

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

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

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

Figure 1



emacs25@vellachemla-X510UA

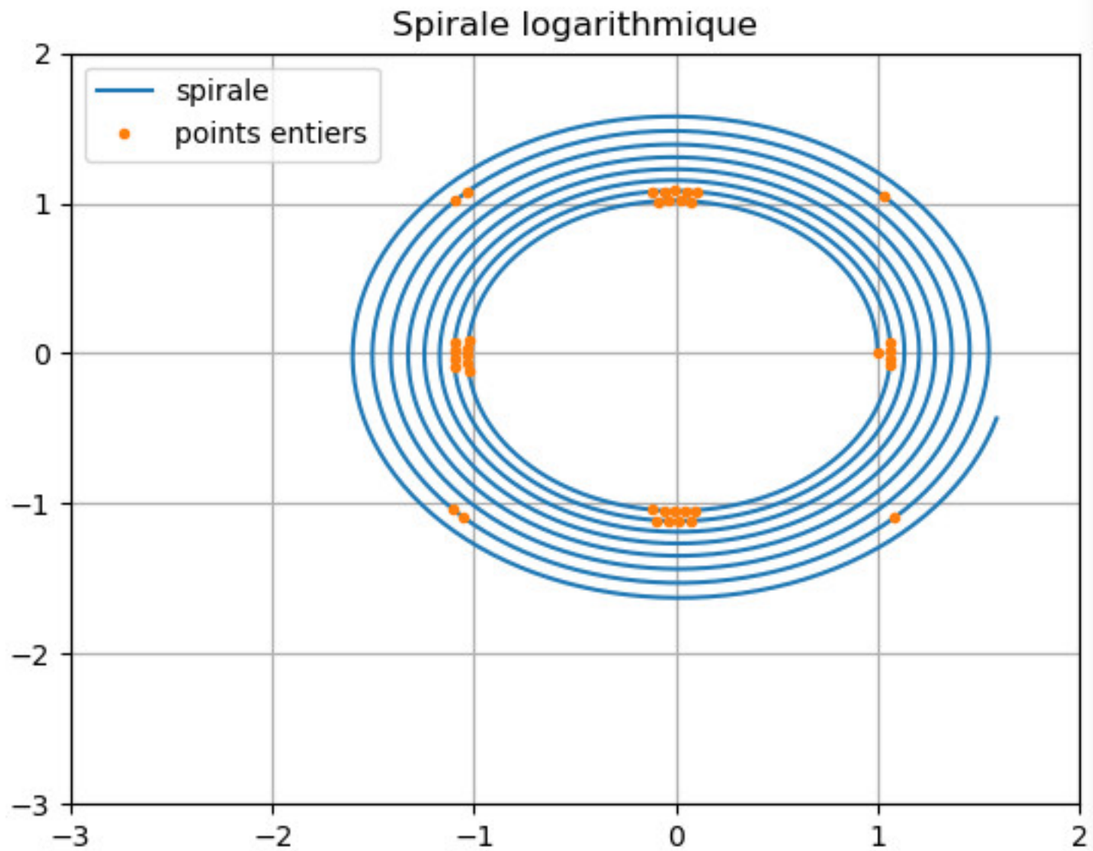
File Edit Options Buffers Tools Python Help

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

a, b = 1.0, 0.05555

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

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

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

plt.show()
```

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

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

Figure 1



emacs25@vellachemla-X510UA

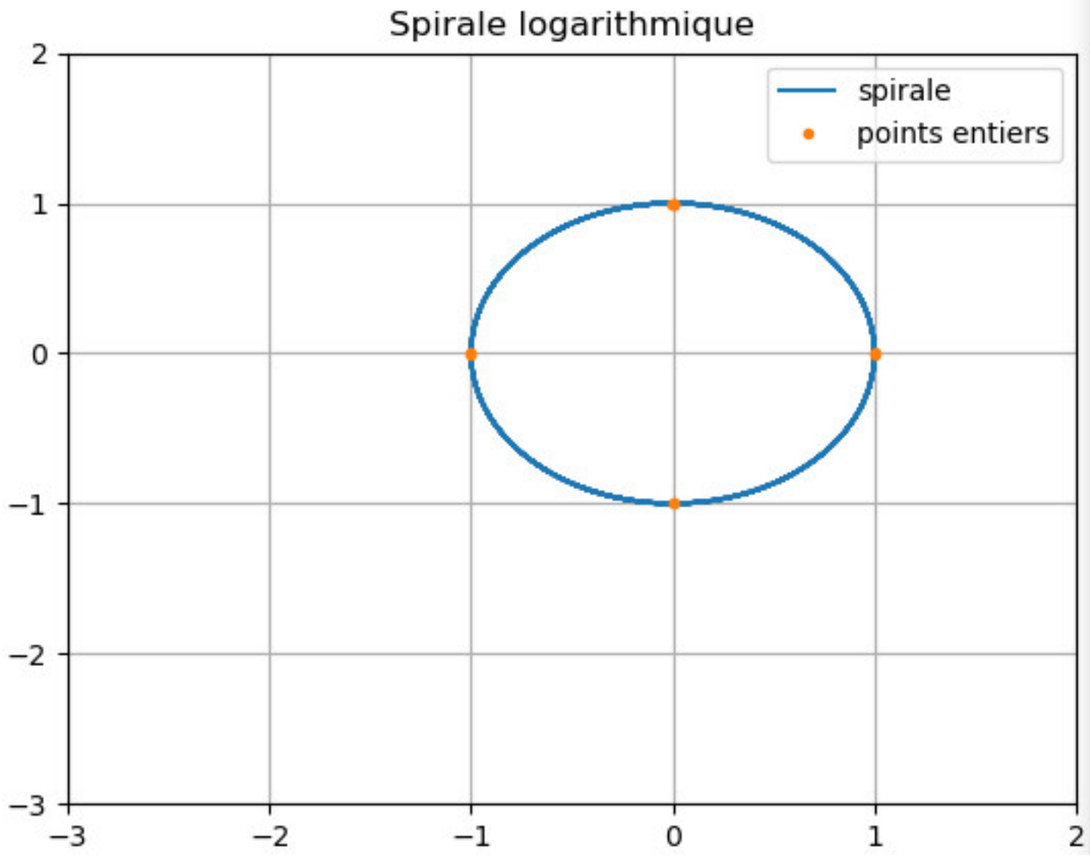
File Edit Options Buffers Tools Python Help

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

a, b = 1.0, 0.01

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

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

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

plt.show()
```

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

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

Figure 1



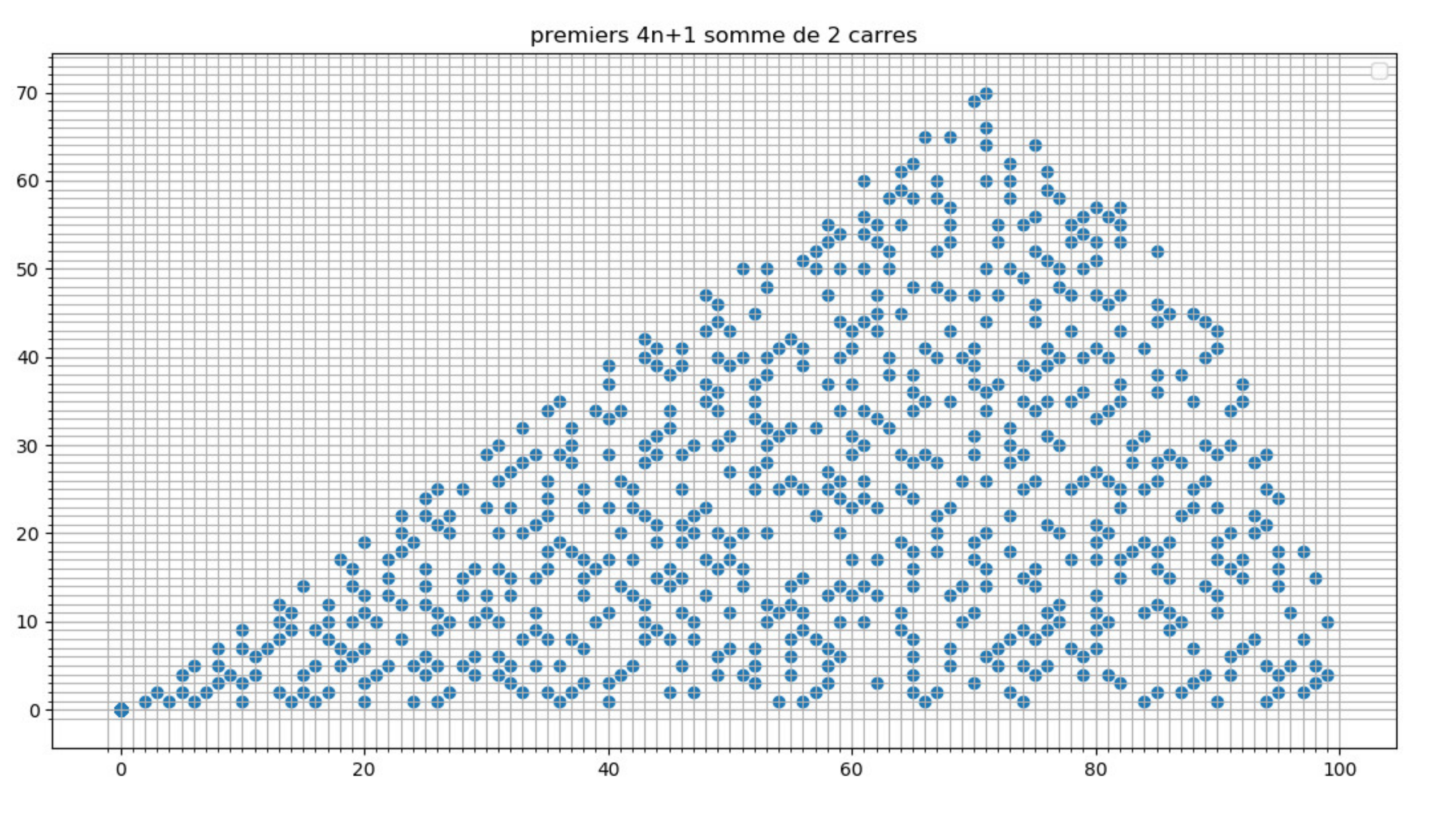
emacs25@vellachemla-X510UA

File Edit Options Buffers Tools Python Help

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

a, b = 1.0, 0.000001

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

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

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

plt.show()
```

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

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


premiers 4n+1 somme de 2 carres
70
60
50
40
30
20
10
0
0
20
40
60
80
100

Section 182 des Recherches arithmétiques de Gauss[*]

182. Descendons maintenant à quelques cas particuliers remarquables autant à cause de leur élégance, que par l'assiduité avec laquelle *Euler* s'en est occupé.

1°. Aucun nombre, à moins que son résidu quadratique ne soit -1, ne peut être représenté par la forme $x^2 + y^2$, dans laquelle x et y sont premiers entre eux, ou sont décomposables en deux nombres quarrés premiers entre eux ; mais tous les nombres qui jouiront de cette propriété pourront se décomposer en deux quarrés. Soit M un de ces nombres et $\pm N$, $\pm N'$, $\pm N''$, etc. les valeurs de l'expression $\sqrt{-1}$ $(mod\ M)$; alors par le n° 176, la forme $\left(M, N, \frac{N^2+1}{M}\right)$ sera proprement équivalente à la forme $(1, 0, 1)$; soit $x = \alpha x' + \beta y', y = \gamma x' + \delta y'$ une transformation propre de la forme $(1, 0, 1)$ en la forme $\left(M, N, \frac{N^2+1}{2}\right)$; on aura les quatre représentations suivantes du nombre M par la forme $x^2 + y^2$, savoir, $x = \pm\alpha, y = \pm\gamma; x = \mp\gamma, y = \pm\alpha$.[†] (2°. -n°180).

Comme la forme $(1, 0, 1)$ est ambiguë, il est évident que la forme $\left(M, -N, \frac{N^2+1}{M}\right)$ lui est aussi proprement équivalente, et que la première se change en la seconde par la transformation propre $x = \alpha x' - \beta y'$, $y = -\gamma x' + \delta y'$, d'où naissent quatre représentations de M appartenantes à $-N$, $x = \pm\alpha, y = \mp\gamma; x = \pm\gamma, y = \mp\alpha$. Il suit de là qu'il y a huit représentations du nombre M, dont quatre appartiennent à la valeur N, et quatre à la valeur $-N$. Mais toutes ces représentations donnent la même décomposition du nombre M en deux quarrés, $M = \alpha^2 + \gamma^2$, tant qu'on ne considère que les quarrés et non l'ordre et les signes des racines.

∗. (mise au format LaTex D.Vella-Chemla, 7.5.2019)

†. $\mp$ plutôt que $\pm$ pour le second y ?

Si donc il n'y a pas d'autres valeurs que N et $-N$ pour l'expression $\sqrt{-1}$ $(mod\ M)$, ce qui arrive, par exemple, toutes les fois que M est un nombre premier, M ne pourra être décomposé que d'une manière en deux quarrés. Or comme -1 est résidu de tous les nombres premiers de la forme $4n+1$ (n°108), et qu'un nombre premier ne peut évidemment se partager en deux quarrés non premiers entre eux, nous aurons le théorème suivant.

Tout nombre premier de la forme $4n+1$ *peut être décomposé en deux quarrés, et ne peut l'être que d'une seule manière.*

Ainsi :

$1 = 0 + 1$	$5 = 1 + 4$	$13 = 4 + 9$	$17 = 1 + 16$
$29 = 4 + 25$	$37 = 1 + 36$	$41 = 16 + 25$	$53 = 4 + 49$
$61 = 25 + 36$	$73 = 9 + 64$	$89 = 25 + 64$	$97 = 16 + 81$

etc.

Ce théorème élégant a été donné par *Fermat*, mais *Euler* est le premier qui l'ait démontré, *Comm. nov. Petr. T. V. ann. 1754 et 1755. p. 3.* Dans le *T. IV*, il existe une dissertation sur le même sujet, *p. 8* ; mais alors il n'était pas parvenu à son but.

Si donc un nombre de la forme $4n+1$ ne peut pas être décomposé en deux quarrés, ou peut l'être de plusieurs manières, on sera sûr que ce n'est pas un nombre premier.

Mais réciproquement, si l'expression $\sqrt{-1}$ $(mod\ M)$ a encore d'autres valeurs que N et $-N$, il y aura d'autres représentations de M. Ainsi, dans ce cas, M peut se décomposer en deux quarrés de plusieurs manières ; par exemple : $65 = 1 + 64 = 16 + 49, 221 = 25 + 196 = 100 + 121$.

Les autres représentations dans lesquelles x et y prennent des valeurs non premières entre elles, se trouvent facilement par notre méthode. Observons seulement que si le nombre M renferme des facteurs de la forme $4n + 3$, dont on ne puisse pas le délivrer en le divisant par un quarré, ce qui arrivera toutes les fois que le nombre M renfermera des puissances impaires de ces facteurs, il ne pourra en aucune manière être décomposé en deux quarrés (**).

(**) Soit le nombre $M = 2^{\mu}.S.a^{\alpha}b^{\beta}c^{\gamma}$, etc., ensorte que a, b, c, etc. soient des facteurs premiers inégaux de la forme $4m + 1$, et S le produit de tous les facteurs premiers de la forme $4n + 3$; cette forme donnée au nombre M convient dans tous les cas ; pour M impair, il suffit de faire $\mu = 0$; si M ne renferme aucun facteur de la forme $4n+3$, on fera $S = 1$: si S n'est pas un quarré, M ne pourra en aucune manière être décomposé en deux quarrés ; mais si S est un quarré, il y aura $\frac{1}{2}(\alpha+1)(\beta+1)(\gamma+1)$, etc. décompositions de M, lorsque quelqu'un des nombres α, β, γ, etc. sont impairs, et il y en aura $\frac{1}{2}(\alpha + 1)(\beta + 1)(\gamma + 1)$, etc.$+\frac{1}{2}$, quand tous les nombres α, β, γ, etc. seront pairs, tant qu'on ne fait attention qu'aux carrés eux-mêmes. Ceux qui ont quelque habitude du calcul des combinaisons, déduiront sans peine de notre théorie générale la démonstration de ce théorème, auquel nous ne pouvons nous arrêter, non plus qu'à d'autres particuliers (Voyez n° 105).

Retour aux polynômes de Tchebychev ainsi que d'autre part aux indices de la section 53 des Recherches arithmétiques de Gauss (Denise Vella-Chemla, 9.5.2019)

1) Cosinus, divisibilité, symbole de Kronecker

On voudrait revenir ici sur la possibilité de calculer les cosinus d'un multiple entier d'un angle en utilisant le polynôme de Tchebychev $T_2(x)$ de première espèce et de degré 2, ce qui permet, en utilisant un symbole de Kronecker, de calculer les booléens de divisibilité qu'on a utilisés à plusieurs reprises.

On rappelle que les polynômes de Tchebychev sont définis par la récurrence suivante :

$$\begin{cases} T_0(x) = 1 \\ T_1(x) = x \\ T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \end{cases}$$

En particulier, le polynôme de Tchebychev de degré 2 est égal à $T_2(x) = 2x^2 - 1$.

On a utilisé pour modéliser la divisibilité de x par y le nombre $\cos\left(\frac{2\pi x}{y}\right)$ qu'on réécrit, pour le considérer comme un multiple entier d'angle comme $\cos\left(2\left(\frac{\pi x}{y}\right)\right)$ et l'on peut obtenir la valeur de ce cosinus par le polynôme $T_2(x)$ en la variable $\cos\left(\frac{\pi x}{y}\right)$.

Si on se place dans le plan complexe, on utilisera plutôt la représentation du cosinus comme moyenne de deux complexes :

$$\cos\left(\frac{\pi x}{y}\right) = \frac{e^{\frac{i\pi x}{y}} + e^{-\frac{i\pi x}{y}}}{2}$$

Ci-dessous, on fournit un programme de calcul en python des cosinus par cette méthode.

```
#include <iostream>
#include <stdio.h>
#include <math.h>
#include <complex.h>

typedef std::complex<double> dcomp;
const double PI = acos(-1.0);

double T_rec(int n, double x) {
  if (n == 0) return 1.0;
  if (n == 1) return x;
  return 2.0 * x * T_rec(n-1, x) - T_rec(n-2, x);
}

int main (int argc, char* argv[])
{
  double err = 1.e-8;
  int n = 10;

  for (int y = 1; y <= n; ++y) {
    for (int x = 1; x <= n; ++x) {
      double z = cos(PI*(double)x/(double)y);
      double t = T_rec(2, z);
      std::cout << x << ", " << y << " --> " << t << "\n" ;
    }
    std::cout << "\n" ;
  }
}
```

Le résultat de ce programme pour x et y variant de 1 à 10 est fourni plus loin.

Le cosinus pour x et y vaut bien sûr 1 lorsque x divise y et un nombre différent de 1 dans les autres cas. Pour obtenir à la place du cosinus un booléen de divisibilité d'un nombre x par un nombre y, on pourra utiliser le symbole de Kronecker $\delta_1^i(T_2(cos(\pi x/y)))$ qui vaut 1 si $T_2(cos(\pi x/y)) = 1$ et 0 sinon.

La définition de cette fonction de divisibilité permet de caractériser les nombres premiers (leur somme de cosinus sur tous les nombres qui leur sont strictement inférieurs vaut 1).

Cette fonction prend les valeurs suivantes :

x | y	1	2	3	4	5	6	7	8	9	10
1	1	0	0	0	0	0	0	0	0	0
2	1	1	0	0	0	0	0	0	0	0
3	1	0	1	0	0	0	0	0	0	0
4	1	1	0	1	0	0	0	0	0	0
5	1	0	0	0	1	0	0	0	0	0
6	1	1	1	0	0	1	0	0	0	0
7	1	0	0	0	0	0	1	0	0	0
8	1	1	0	1	0	0	0	1	0	0
9	1	0	1	0	0	0	0	0	1	0
10	1	1	0	0	1	0	0	0	0	1

Cosinus calculés par le programme utilisant le polynôme de Tchebychev

Voici le résultat du programme pour x et y variant de 1 à 4.

```
1 , 1 --> 1
2 , 1 --> 1
3 , 1 --> 1
4 , 1 --> 1
5 , 1 --> 1
6 , 1 --> 1
7 , 1 --> 1
8 , 1 --> 1
9 , 1 --> 1
10 , 1 --> 1

1 , 2 --> -1
2 , 2 --> 1
3 , 2 --> -1
4 , 2 --> 1
5 , 2 --> -1
6 , 2 --> 1
7 , 2 --> -1
8 , 2 --> 1
9 , 2 --> -1
10 , 2 --> 1

1 , 3 --> -0.5
2 , 3 --> -0.5
3 , 3 --> 1
4 , 3 --> -0.5
5 , 3 --> -0.5
6 , 3 --> 1
7 , 3 --> -0.5
8 , 3 --> -0.5
9 , 3 --> 1
10 , 3 --> -0.5

1 , 4 --> -1.03412e-13
2 , 4 --> -1
3 , 4 --> 3.10679e-13
4 , 4 --> 1
5 , 4 --> -5.16614e-13
6 , 4 --> -1
7 , 4 --> 7.24325e-13
8 , 4 --> 1
9 , 4 --> -9.3026e-13
10 , 4 --> -1
```

2) Indices de Gauss, cardinaux d'ensembles de nombres qui sont racines d'équations identiques

On cherche une caractérisation claire des nombres premiers de la forme $4k+3$: on a du mal à en trouver une dans la littérature alors que tous connaissent le fait qu'un nombre premier de la forme $4k+1$ se décompose de manière unique en une somme de deux carrés [1].
On calcule les indices associés à chaque nombre modulo un certain entier n. Les indices en question sont expliqués dans l'article 53 des recherches arithmétiques.

53. Pour nous faire entendre plus facilement, nous présenterons d'abord un exemple. Soit $p=19$, les nombres $1, 2, 3 \ldots 18$ peuvent se distribuer de la manière suivante relativement aux diviseurs de 18 :

$$1\{1,\quad 2\{18,\quad 3\left\{\begin{matrix}7\\11\end{matrix}\right.,\quad 6\left\{\begin{matrix}8\\12\end{matrix}\right.,\quad 9\left\{\begin{matrix}4,\ 5,\ 6\\9,\ 16,\ 17\end{matrix}\right.,\quad 18\left\{\begin{matrix}2,\ 3,\ 10\\13,\ 14,\ 15\end{matrix}\right.$$

Ainsi dans ce cas $\downarrow 1=1$, $\downarrow 2=1$, $\downarrow 3=2$, $\downarrow 6=2$, $\downarrow 9=6$, $\downarrow 18=6$. Avec une légère attention on voit qu'il y en a, relativement à chaque exposant, autant qu'il y a de nombres premiers avec cet exposant et non plus grands que lui, ou bien, en reprenant le signe du n° 40, que $\downarrow d=\phi d$. Mais on peut démontrer généralement cette observation de la manière suivante :

L'analyse des données fait comprendre cet article ainsi : l'ensemble des nombres premiers à n est constitué d'un certain nombre de parties disjointes. Chaque partie contient des nombres dont la même puissance est congrue à l'unité modulo n (on mettra par exemple dans un même ensemble les nombres dont la puissance 7ème vaut 1). La somme des cardinaux des différentes parties est égale à $\varphi(n)$ l'indicateur d'Euler de n.
L'analyse de ce résultat fournit la caractérisation suivante pour les nombres premiers :

- *un nombre premier p de la forme $4k+3$ est tel que les ensembles de nombres qui sont premiers à p et dont une même puissance vaut 1 sont appariables par leur cardinalité ;*

- *il en est de même pour une puissance d'un nombre premier p de la forme $4k+3$ (on peut apparier les ensembles de nombres de même puissance égale à l'unité dans le corps premier $\mathbb{Z}/p\mathbb{Z}$ par bijection (i.e. ils sont 2 par 2 de même cardinal) ;*

- *un nombre premier p de la forme $4k+1$ est tel que l'un de ses ensembles de nombres qui sont premiers à p et dont une même puissance vaut 1 n'est appariable à aucun autre par sa cardinalité.*

Cardinalité des ensembles de mêmes puissances égales à l'unité, pour les nombres impairs entre 10 et 20

Le premier exemple est à lire ainsi : 2^{10} et 6^{10} sont égaux à 1 modulo 10, ou encore 3^5. Ces nombres dont une même puissance vaut 1 sont à imaginer comme étant placés dans un même ensemble et les

1. Théorème démontré par Fermat, Euler, Gauss (cf. http://denisevellachemla.eu/Gauss-4k+1-RA182.pdf et Don Zagier "A one-sentence proof that every prime $p \equiv 1$ (*mod* 4) is a sum of two squares", *Amer. Math. Monthly*, 97 (2) :144, 1990.)

cardinaux de ces ensembles valent ici 4, 4, 1 et 1 (indiqués après la flèche à droite de 10).

```
11  →  4,  4,  1,  1
10  :  2  6  7  8
 5  :  3  4  5  9
 2  :  10
 1  :  1

13  →  4,  2,  2,  2,  1,  1
12  :  2  6  7  11
 6  :  4  10
 4  :  5  8
 3  :  3  9
 2  :  12
 1  :  1

15  →  4,  3,  1
 4  :  2  7  8  13
 2  :  4  11  14
 1  :  1

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

19  →  6,  6,  2,  2,  1,  1
18  :  2,  3,  10,  13,  14,  15
 9  :  4,  5,  6,  9,  16,  17
 6  :  8,  12
 3  :  7,  11
 2  :  18
 1  :  1
```

Si maintenant on se contente de reporter les cardinaux des ensembles (à droite des flèches ci-dessus) pour les impairs de 3 à 99, on voit apparaître cette propriété d'appariement des ensembles de même cardinaux pour les premiers de la forme $4k+3$ ainsi que pour leurs puissances. Ces appariements sont symbolisés par des points-virgules et les nombres de forme $4k+3$ ou leurs puissances colorés en bleu.

3 : 1/1	23 : 10/10, 1/1	43 : 12/12, 6/6, 2/2, 1/1	63 : 24, 8, 3, 1	83 : 40/40, 1/1
5 : 2, 1, 1	25 : 8, 4, 4, 2, 1, 1	45 : 8, 6, 4, 3, 2, 1	65 : 24, 12, 6, 3, 2, 1	85 : 32, 16, 12, 3, 1
7 : 2/2, 1/1	27 : 6/6, 2/2, 1/1	47 : 22/22, 1/1	67 : 20/20, 10/10, 2/2, 1/1	87 : 24, 18, 6, 4, 3, 1
9 : 2/2, 1/1	29 : 12, 6, 6, 2, 1, 1	49 : 12, 12, 6, 6, 2, 2, 1, 1	69 : 30, 10, 3, 1	89 : 40, 20, 10, 10, 4, 2, 1, 1
11 : 4/4, 1/1	31 : 8/8, 4/4, 2/2, 1/1	51 : 16, 8, 4, 3, 1	71 : 24/24, 6/6, 4/4, 1/1	91 : 32, 24, 8, 4, 3, 1
13 : 4, 2, 2, 2, 1, 1	33 : 12, 4, 3, 1	53 : 24, 12, 12, 2, 1, 1	73 : 24, 12, 8, 6, 6, 4, 4, 2, 2, 2, 1, 1	93 : 24, 12, 8, 6, 4, 3, 2, 1
15 : 4, 3, 1	35 : 8, 6, 4, 3, 2, 1	55 : 16, 12, 4, 4, 3, 1	75 : 16, 12, 4, 4, 3, 1	95 : 24, 18, 8, 6, 6, 4, 3, 2, 1
17 : 8, 4, 2, 1, 1	37 : 12, 6, 6, 4, 2, 2, 2, 1, 1	57 : 18, 6, 6, 3, 2, 1	77 : 24, 12, 8, 6, 4, 3, 2, 1	97 : 32, 16, 16, 8, 8, 4, 4, 2, 2, 2, 1, 1
19 : 6/6, 2/2, 1/1	39 : 8, 6, 4, 3, 2, 1	59 : 28/28, 1/1	79 : 24/24, 12/12, 2/2, 1/1	99 : 24, 12, 8, 6, 4, 3, 2, 1
21 : 6, 3, 2, 1	41 : 16, 8, 4, 4, 4, 2, 1, 1	61 : 16, 8, 8, 8, 4, 4, 4, 2, 2, 2, 1, 1	81 : 18/18, 6/6, 2/2, 1/1	

Caractérisation topologique des nombres premiers (Denise Vella-Chemla, 11.5.2019)

Après être revenue à l'article 53 des Recherches arithmétiques de Gauss et au résultat d'un programme de calcul d'indices [1] des nombres qui appartiennent au groupe des unités [2] d'un corps premier, il semblerait qu'on puisse caractériser, d'un point de vue arithmétique puis d'un point de vue topologique, les nombres premiers de la forme $4k+3$, même si cette caractérisation ne permet pas pour l'instant de les distinguer de leurs puissances.

Présentons 4 exemples pour fixer les idées : on travaille dans les corps premiers $\mathbb{Z}/p\mathbb{Z}$ et on indique pour les différentes puissances (avant les signes :) les nombres dont cette puissance est égale à l'unité. Par exemple, dans le tableau ci-dessous, fournissant les puissances associées aux unités dans $\mathbb{Z}/p\mathbb{Z}$ pour $p = 7, 13, 29$ ou 31, les 3 nombres colorés en rouge sont à lire comme $8^4 \equiv 1$ $(mod\ 13)$ (effectivement, $8^4 = 4096 = 315 \times 13 + 1$).

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

On va appeler "puissances appariées" (ou leur ensemble associé "ensembles appariés") les puissances dont les ensembles de nombres ont même cardinal. Par exemple, pour le module $p = 31$, on dira que la puissance 10 et la puissance 5 sont appariées car leur ensemble associé de nombres sont tous les deux de cardinalité 4.

On effectue les constatations suivantes [3].

Pour les nombres premiers $4k+3$, les ensembles associés aux différentes puissances sont appariés 2 à 2. Ce n'est pas le cas pour les nombres premiers $4k+1$ ou pour leurs puissances, pour lesquels par exemple la plus grande puissance a systématiquement un ensemble de nombres associé qui n'est "apparié à aucun autre ensemble".

Pour les nombres premiers p de la forme $4k+1$, il semblerait que les propriétés suivantes soient systématiquement vérifiées :

- il y a deux fois plus de nombres dont la puissance $p-1$ est égale à l'unité que de nombres dont la puissance $\frac{p-1}{2}$ est égale à l'unité ; il y a autant de nombres dont la puissance $\frac{p-1}{2}$ est égale à l'unité que de nombres dont la puissance $\frac{p-1}{4}$ est égale à l'unité ;

1. i.e. puissances égales à l'unité, cf. http://denise.vella.chemla.free.fr/polyetindices.pdf
2. Les résultats du programme de calcul avait été fournis ici en septembre 2016 : http://denise.vella.chemla.free.fr/indices-RA53.
3. Je ne sais pas si ces constatations découlent de théorèmes voire ont déjà été démontrées.

- pour les ensembles appariés dont les éléments x sont toujours tels que x et $p-x$ sont systématiquement dans des ensembles différents, on a les congruences suivantes (à échange de x et $p-x$ près) :

$$\begin{cases} x^k \equiv 1 \ (mod\ p) \\ (p-x)^{\frac{k}{2}} \equiv 1 \ (mod\ p) \end{cases}$$

- pour les ensembles non appariés avec x et $p-x$ systématiquement dans le même ensemble :

$$\begin{cases} x^k \equiv 1 \ (mod\ p) \\ (p-x)^k \equiv 1 \ (mod\ p). \end{cases}$$

Pour les nombres premiers p de la forme $4k+3$ ou leurs puissances, il semblerait que les propriétés suivantes soient systématiquement vérifiées :

- il y a autant de nombres dont la puissance $p-1$ est égale à l'unité que de nombres dont la puissance $\frac{p-1}{2}$ est égale à l'unité ;
- pour tous les ensembles qui sont tous appariés avec x et $p-x$ systématiquement dans des ensembles différents (à échange de x et $p-x$ près) :

$$\begin{cases} x^k \equiv 1 \ (mod\ p) \\ (p-x)^{\frac{k}{2}} \equiv 1 \ (mod\ p) \end{cases}$$

Ce qui semblerait au premier abord permettre de distinguer les nombres premiers de la forme $4k+1$ (ou leurs puissances) des nombres composés impairs (on ne peut, que ce soit pour les uns ou pour les autres, apparier leurs unités qu'on "quotiente par la puissance les amenant à 1", pour le dire rapidement), c'est le fait que pour les nombres premiers $4k+1$, il y ait exactement moitié moins de nombres associés à la puissance $\frac{p-1}{2}$ qu'à la puissance $p-1$, ce qui n'est pas le cas pour les nombres composés.

On visualise cela dans le tableau des cardinaux d'ensembles d'unités par des couleurs permettant d'observer cette propriété de "exactement moitié moins". Les premiers $4k+1$ sont colorés en bleus, les impairs composés en rouge. Malheureusement, ce qui semblait une caractérisation n'en est pas une : tous les $4k+1$ vérifient cette condition, sauf les $4k+1$ qui sont puissances d'un $4k+3$ (comme 9, 27, etc.). Il semblerait qu'on ait cependant obtenu une condition nécessaire : le fait que la deuxième classe ait un cardinal différent de la moitié du cardinal de la première classe semble impliquer que n est un nombre composé même si l'implication dans l'autre sens n'est pas vraie.

3 : 1/1	29 : 12, 6, 6, 2, 1, 1	55 : 16, 12, 4, 4, 3, 1	81 : 18/18, 6/6, 2/2, 1/1
5 : 2, 1, 1	31 : 8/8, 4/4, 2/2, 1/1	57 : 18, 6, 6, 3, 2, 1	83 : 40/40, 1/1
7 : 2/2, 1/1	33 : 12, 4, 3, 1	59 : 28/28, 1/1	85 : 32, 16, 12, 3, 1
9 : 2/2, 1/1	35 : 8, 6, 4, 3, 2, 1	61 : 16, 8, 8, 8, 4, 4, 4, 2, 2, 2, 1, 1	87 : 24, 18, 6, 4, 3, 1
11 : 4/4, 1/1	37 : 12, 6, 6, 4, 2, 2, 2, 1, 1	63 : 24, 8, 3, 1	89 : 40, 20, 10, 10, 4, 2, 1, 1
13 : 4, 2, 2, 2, 1, 1	39 : 8, 6, 4, 3, 2, 1	65 : 24, 12, 6, 3, 2, 1	91 : 32, 24, 8, 4, 3, 1
15 : 4, 3, 1	41 : 16, 8, 4, 4, 4, 2, 1, 1	67 : 20/20, 10/10, 2/2, 1/1	93 : 24, 12, 8, 6, 4, 3, 2, 1
17 : 8, 4, 2, 1, 1	43 : 12/12, 6/6, 2/2, 1/1	69 : 30, 10, 3, 1	95 : 24, 18, 8, 6, 6, 4, 3, 2, 1
19 : 6/6, 2/2, 1/1	45 : 8, 6, 4, 3, 2, 1	71 : 24/24, 6/6, 4/4, 1/1	97 : 32, 16, 16, 8, 8, 4, 4, 2, 2, 2, 1, 1
21 : 6, 3, 2, 1	47 : 22/22, 1/1	73 : 24, 12, 8, 6, 6, 4, 4, 2, 2, 2, 1, 1	99 : 24, 12, 8, 6, 4, 3, 2, 1
23 : 10/10, 1/1	49 : 12, 12, 6, 6, 2, 2, 1, 1	75 : 16, 12, 4, 4, 3, 1	
25 : 8, 4, 4, 2, 1, 1	51 : 16, 8, 4, 3, 1	77 : 24, 12, 8, 6, 4, 3, 2, 1	
27 : 6/6, 2/2, 1/1	53 : 24, 12, 12, 2, 1, 1	79 : 24/24, 12/12, 2/2, 1/1	

Pour les nombres premiers de la forme $4k+1$, la meilleure caractérisation les concernant semble être le fait qu'ils sont de manière unique somme de 2 carrés d'entiers [4].

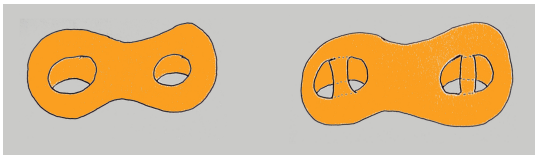
On fournit en annexe une représentation imagée obtenue par programme en python des nombres premiers $4k+1$ sommes de 2 carrés.

Dans tous les cas, la meilleure caractérisation des nombres premiers reste le petit théorème de Fermat : ce sont les seuls nombres pour lesquels tout nombre premier à p est solution pour la puissance $p-1$: $x^{p-1} \equiv 1 \ (mod\ p)$.

4. Ce théorème a été démontré par Fermat, Euler, Gauss et Zagier notamment, cf. la démonstration transcrite des Recherches arithmétiques de Gauss ici : http://denisevellachemla.eu/Gauss-4k+1-RA182.pdf.

Voyons maintenant deux manières de lier les résultats présentés ci-desus concernant les nombres premiers de la forme $4k+3$ à la topologie :

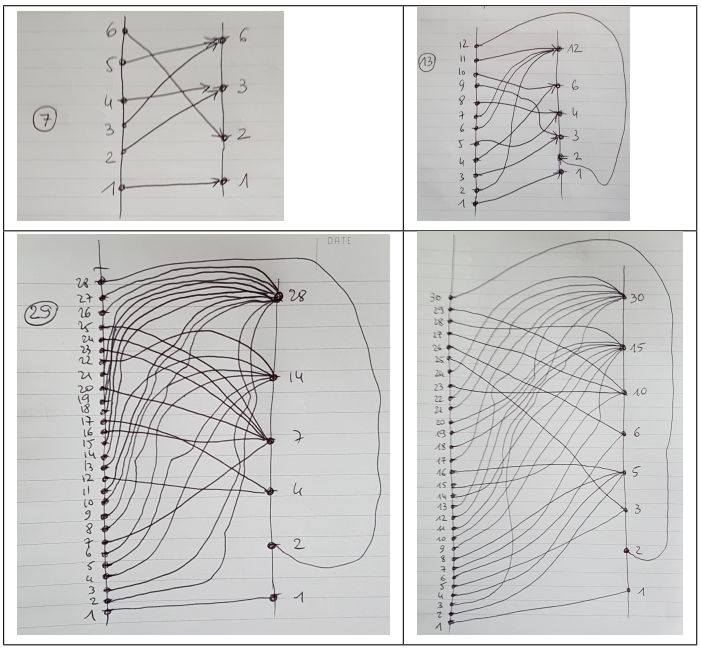
1) *première méthode envisagée* : on trouve dans la littérature qu'il est possible de compter le nombre de solutions d'une équation de la forme $x^p \equiv 1\ (mod\ k)$ sur un tore à p trous. Peut-être peut-on envisager de "dupliquer chaque trou" en comblant une sorte de tunnel de matière au milieu du trou ainsi :



2) *seconde méthode envisagée* : on a l'idée de représenter les nombres et les puissances correspondantes dans les corps premiers par les dessins ci-après (les nombres sur la ligne verticale à gauche sont les unités [5] du corps premier $\mathbb{Z}/p\mathbb{Z}$ considéré et les nombres sur la ligne verticale à droite sont les exposants qui permettent d'amener les nombres de la ligne gauche jusqu'à 1 par élévation à la puissance.

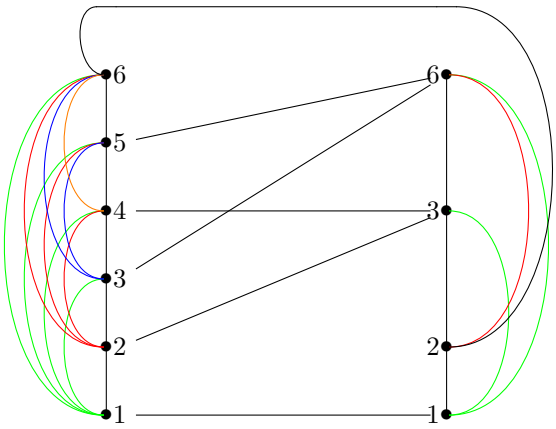
Le fait que 1 soit systématiquement d'indice 1 et $p-1$ d'indice 2 va nous permettre de transformer la représentation de la fonction "puissance qui permet d'atteindre l'unité" en une courbe fermée qui se croisera plusieurs fois elle-même ; les points de croisement seront vus comme des sommets, les éléments de courbe entre sommets seront les arêtes, on aura alors un graphe dans lequel il s'agira de trouver une chaîne eulérienne (dans un graphe connexe - i.e. tel que tout sommet est atteignable par un chemin depuis tout autre-, une chaîne eulérienne existe forcément si seuls deux sommets sont de degré impair ; cette chaîne passe par toutes les arêtes une fois et une seule et permet d'aller de l'un des deux sommets de degré impair à l'autre).

Voici les représentations imagées des fonctions "indices de Gauss".



5. C'est ainsi qu'on appelle les nombres premiers à p, ceux qui n'ont aucun diviseur commun avec p, i.e. les nombres tels que $PGCD(x,p) = 1$; le plus grand diviseur commun de x et y est habituellement simplement noté par le couple (x,y).

Présentons l'ajout d'arêtes sur la représentation associée à $p = 7$. On ajoute autant d'arêtes que nécessaire de façon à ce que tout nombre, qu'il soit sur la ligne verticale à gauche ou sur la ligne verticale à droite, puisse atteindre tout autre nombre sur la ligne en question. On symbolise ces arêtes supplémentaires en rouge, vert, bleu et orange pour améliorer la lisibilité.
Comptons les degrés des sommets (on appelle g_1 à g_6 les sommets à gauche (les indices de Gauss) de bas en haut et d_1 à d_4 les sommets de droite (les éléments du groupe des unités).
Les sommets g_1 à g_6 sont de degrés 6, les sommets d_1 et d_2 sont de degré 4 et les sommets d_3 et d_4 sont de degré 5. Le nombre d'arêtes est la moitié de la somme des degrés, ici 27.
Comme seuls deux sommets sont de degré impair (d_3 et d_4) dans le graphe, la propriété d'Euler est vérifiée, qui permet de parcourir toutes les arêtes une fois et une seule. Comme un tel circuit est difficile à faire apparaître sur le graphe "chargé" en arêtes, on le note par une succession possible de sommets : $d_4\ d_1\ d_3\ d_4\ d_2\ d_1\ g_1\ g_2\ d_3\ g_4\ g_5\ d_4\ g_3\ g_2\ g_4\ g_3\ g_5\ g_6\ g_4\ g_1\ g_3\ g_6\ g_2\ g_5\ g_1\ g_6\ d_2\ d_3$.



Malheureusement, ce qui marchait pour 7 ne marche pas pour 11, 13 : leur graphe contiennent chacun 4 sommets de degré impair, ce qui empêche d'y trouver une chaîne eulérienne. Ce n'est pas une bonne idée que de poursuivre dans cette voie-là.

Annexe 1 : Transcription des articles 53 et 54 des Recherches arithmétiques de Gauss

53. Pour nous faire entendre plus facilement, nous présenterons d'abord un exemple. Soit $p = 19$, les nombres $1, 2, 3 \ldots 18$ peuvent se distribuer de la manière suivante relativement aux diviseurs de 18 :

$$1 \left\{ 1, \quad 2 \right\{ 18, \quad 3 \left\{ \begin{matrix} 7 \\ 11 \end{matrix} \right. , \quad 6 \left\{ \begin{matrix} 8 \\ 12 \end{matrix} \right. , \quad 9 \left\{ \begin{matrix} 4,\ 5,\ 6 \\ 9,\ 16,\ 17 \end{matrix} \right. , \quad 18 \left\{ \begin{matrix} 2,\ 3,\ 10 \\ 13,\ 14,\ 15 \end{matrix} \right. .$$

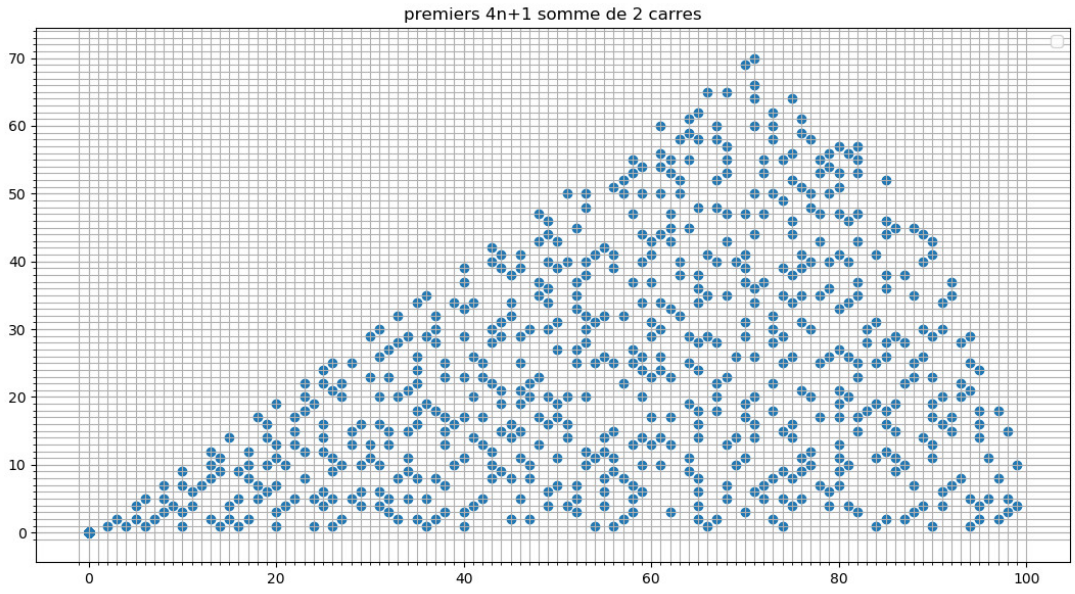
Ainsi dans cas $\psi\ 1 = \ 1, \psi\ 2 = \ 1, \psi\ 3 = \ 2, \psi\ 6 = \ 2, \psi\ 9 = \ 6, \psi\ 18 = \ 6$. Avec une légère attention on voit qu'il y en a, relativement à chaque exposant, autant qu'il y a de nombres premiers avec cet exposant et non plus grands que lui, ou bien, en reprenant le signe du n° 40, que $\psi d = \varphi d$. Mais on peut démontrer généralement cette observation de la manière suivante :

1°. S'il y a un nombre a appartenant à l'exposant d, c'est-à-dire dont la puissance d soit congrue à l'unité, et les puissances inférieures incongrues, toutes les puissances de ce nombre, savoir $a, a^2, a^3, a^4 \ldots a^d$, ou leurs résidus *minima*, auront leur puissance d congrue avec l'unité ; et comme cela peut s'exprimer en disant que les résidus *minima* des nombres $a, a^2, a^3, a^4 \ldots a^d$ qui sont tous différents sont les racines de la congruence $x^d \equiv 1$, qui ne peut avoir plus de d racines différentes, il est évident qu'il

n'y a pas de nombres autres que les résidus *minima* de $a, a^2, a^3, a^4 \ldots a^d$ dont les puissances d soient congrues à l'unité ; d'où il suit que les nombres appartenans à l'exposant d se trouvent tous entre les résidus *minima* des nombres $a, a^2, a^3, a^4 \ldots a^d$. On déterminera comme il suit quels ils sont et quel est leur nombre. Si k est un nombre premier avec d, toutes les puissances de a^k, dont les exposans sont $< d$, ne seront pas congrues à l'unité. Soit en effet $\frac{1}{k}$ $(mod.\ d) = m$ (voyez n°31), on aura $a^{km} \equiv a$; donc si la puissance e de a^k était congrue à l'unité, et que l'on eût $e < d$, on aurait aussi $a^{kme} \equiv 1$, et par conséquent $a^e \equiv 1$; ce qui est contre l'hypothèse. Il est évident, d'après cela, que le résidu *minimum* de a^k appartiendra à d ; mais si k a un commun diviseur δ avec d, le résidu *minimum* de a^k n'appartiendra pas à l'exposant d. Car $\frac{kd}{\delta}$ est divisible par d, ou bien $\frac{kd}{\delta} \equiv 0$ $(mod.\ d)$; parconséquent $a^{\frac{kd}{\delta}} \equiv 1$; c'est-à-dire $(a^k)^{\frac{d}{\delta}} \equiv 1$. Nous conclurons de là qu'il y a autant de nombres appartenans à l'exposant d, qu'il y a de nombres premiers avec d dans la série $1, 2, 3 \ldots d$. Mais il faut se souvenir que cette conclusion suppose qu'il existe déjà un nombre a appartenant à l'exposant d ; parconséquent il reste douteux s'il ne pourrait pas se faire qu'aucun nombre n'appartînt à un exposant donné, et la conclusion se réduit à $\psi d = 0$, ou $= \varphi d$.

54. 2°. Soient d, d', d'', etc. les diviseurs de $p-1$; comme tous les nombres $1, 2, 3 \ldots p-1$ doivent être distribués entre ces diviseurs, on aura $\psi d + \psi d' + \psi d'' + etc. = p-1$. Mais (n°40) nous avons démontré que $\varphi d + \varphi d' + \varphi d'' + etc. = p-1$, et du n° précédent il suit que $\psi d = 0$ ou $= \varphi d$; et parconséquent que ψd ne peut pas être $> \varphi d$; ce qui s'étend à $\psi d'$ et $\varphi d'$, etc. Si donc un ou plusieurs des nombres $\psi d, \psi d'$, etc. étaient plus petit que son correspondant parmi les nombres $\varphi d, \varphi d'$, etc., la somme des premiers ne pourrait être égale à la somme des derniers. D'où nous concluons enfin que dans tous les cas, $\psi d = \varphi d$, et que parconséquent ψd ne dépend point de la grandeur de $p-1$.

Annexe 2 : Premiers $4k+1$ sommes de deux carrés



Grouper par quatre (Denise Vella-Chemla, 16.5.2019)

On présente ici une caractérisation des nombres premiers particulière, basée sur des regroupements des nombres 4 par 4 et qui permet de distinguer les nombres premiers de la forme $4k+3$ de ceux de la forme $4k+1$ et les distinguer également de leurs puissances, ce qu'on n'était pas parvenue à trouver jusque-là.

On regroupe dans chaque corps premier $\mathbb{Z}/p\mathbb{Z}$ pour p premier ou dans chaque anneau $\mathbb{Z}/n\mathbb{Z}$ pour n impair les nombres 4 par 4 : chaque groupement contient un nombre, son opposé, son inverse (s'il existe, i.e. si p est premier) et l'opposé de son inverse.

Ensuite, on choisit de passer d'un groupement à l'autre en multipliant par deux l'un des éléments d'un groupement : les résultats d'un programme semble indiquer que pour les nombres premiers, un tel procédé permet de "passer par" chaque groupement une fois et une seule (ce qu'on appelle en théorie des graphes parcourir un chemin Hamiltonien), tandis que cela ne semble pas possible dans le cas des anneaux, i.e. quand n n'est pas premier. Voici le programme de calcul des regroupements des nombres 4 par 4.

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

int main (int argc, char* argv[])
{
  int n, numdugroupe, nmin, nmax, k, m ;
  bool marque[200] ;
  int tab[200][4] ;

  nmin = 3 ;
  nmax = 100 ;

  for (n = nmin ; n <= nmax ; n=n+2)
    {
      std::cout << "\n" << n << "␣-->␣\n" ;
      for (k = 1 ; k <= n ; ++k)
        {
          marque[k] = false ;
          tab[k][1] = 0 ;
          tab[k][2] = 0 ;
          tab[k][3] = 0 ;
          tab[k][4] = 0 ;
        }
      tab[1][1] = 2 ; marque[2] = true ;
      tab[1][2] = (n+1)/2 ; marque[(n+1)/2] = true ;
      tab[1][3] = n-2 ; marque[n-1] = true ;
      tab[1][4] = n-(n+1)/2 ; marque[n-(n+1)/2] = true ;
      std::cout << "groupe␣" << "1␣(" ;
      std::cout << tab[1][1] << "," ;
      std::cout << tab[1][2] << "," ;
      std::cout << tab[1][3] << "," ;
      std::cout << tab[1][4] << ").\n" ;
      numdugroupe = 2 ;

      for (k = 3 ; k <= n/2 ; ++k)
        {
          if (marque[k] == false)
            {
              tab[numdugroupe][1] = k ;
              marque[k] = true ;
              tab[numdugroupe][4] = n-k ;
              marque[n-k] = true ;
              for (m = k+1 ; m <= n/2 ; ++m)
                {
                  if (((k*m) % n == 1) || ((k*m) % n == n-1))
                    {
                      tab[numdugroupe][2] = m ;
                      marque[m] = true ;
                      tab[numdugroupe][3] = n-m ;
                      marque[n-m] = true ;
                    }
                }
```

```
            std::cout << "groupe␣" << numdugroupe ;
            std::cout << "␣(" << tab[numdugroupe][1] << "," ;
            std::cout << tab[numdugroupe][2] << "," ;
            std::cout << tab[numdugroupe][3] << "," ;
            std::cout << tab[numdugroupe][4] << ").\n" ;
            numdugroupe = numdugroupe+1 ;
          }
        }
    }
}
```

Voici son résultat pour les nombres impairs de 7 à 25.

```
7 -->
groupe 1 (2,4,5,3).

9 -->
groupe 1 (2,5,7,4).
groupe 2 (3,0,0,6).

11 -->
groupe 1 (2,6,9,5).
groupe 2 (3,4,7,8).

13 -->
groupe 1 (2,7,11,6).
groupe 2 (3,4,9,10).
groupe 3 (5,0,0,8).

15 -->
groupe 1 (2,8,13,7).
groupe 2 (3,0,0,12).
groupe 3 (4,0,0,11).
groupe 4 (5,0,0,10).
groupe 5 (6,0,0,9).

17 -->
groupe 1 (2,9,15,8).
groupe 2 (3,6,11,14).
groupe 3 (4,0,0,13).
groupe 4 (5,7,10,12).

19 -->
groupe 1 (2,10,17,9).
groupe 2 (3,6,13,16).
groupe 3 (4,5,14,15).
groupe 4 (7,8,11,12).

21 -->
groupe 1 (2,11,19,10).
groupe 2 (3,0,0,18).
groupe 3 (4,5,16,17).
groupe 4 (6,0,0,15).
groupe 5 (7,0,0,14).
groupe 6 (8,0,0,13).
groupe 7 (9,0,0,12).

23 -->
groupe 1 (2,12,21,11).
groupe 2 (3,8,15,20).
groupe 3 (4,6,17,19).
groupe 4 (5,9,14,18).
groupe 5 (7,10,13,16).

25 -->
groupe 1 (2,13,23,12).
groupe 2 (3,8,17,22).
groupe 3 (4,6,19,21).
groupe 4 (5,0,0,20).
groupe 5 (7,0,0,18).
groupe 6 (9,11,14,16).
groupe 7 (10,0,0,15).
```

On retrouve le fait connu que les nombres non premiers à n (i.e. tels que $(n, x) \neq 1$) ne sont pas inversibles (les quadruplets des nombres non inversibles contiennent des zéros parce que le programme

n'a pu leur trouver d'inverse).

Les nombres premiers de la forme $4k+1$ semblent distinguables des nombres premiers de la forme $4k+3$ car un seul de leur quadruplets contient 2 zéros. Aux nombres composés impairs sont associés plusieurs groupements de nombres contenant 2 zéros (pour tous les nombres non-inversibles).
Mais le fait qui est peut-être plus intéressant est qu'il semblerait que l'on puisse parcourir tous les groupes de 4 nombres, une fois et une seule chacun, dans les corps premiers $\mathbb{Z}/p\mathbb{Z}$ (quelle que soit leur forme $4k+1$ ou $4k+3$) en passant simplement d'un élément d'un groupe à un élément d'un autre groupe par une multiplication modulaire par 2 par exemple.

Voici alors les chemins Hamiltoniens pour les nombres premiers 23 et 29 et les chemins qui n'en sont pas pour les nombres composés 25 et 27.

Pour 23, en multipliant par 2, on parcourt les groupements ainsi :

$$G_1 \rightarrow G_3 \rightarrow G_2 \rightarrow G_5 \rightarrow G_4$$

Pour 29, en multipliant par 2, on parcourt les groupements ainsi :

$$G_1 \rightarrow G_3 \rightarrow G_5 \rightarrow G_6 \rightarrow G_2 \rightarrow G_4 \rightarrow G_7$$

Pour 25, en multipliant par 2, on parcourt les groupements ainsi :

$$G_1 \rightarrow G_3 \rightarrow G_2 \rightarrow G_6 \rightarrow G_5 \rightarrow G_6 \ (cycle\ sur\ G_6)$$

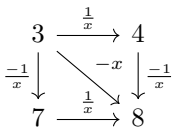
Pour 27, en multipliant par 2, on parcourt les groupements ainsi :

$$G_1 \rightarrow G_3 \rightarrow G_6 \rightarrow G_4 \rightarrow G_4 (cycle\ sur\ G_4)$$

Ces propriétés juste découvertes nous font penser aux nombres premiers comme à des sortes d'empilement de carrés (un peu comme les étages d'un immeuble) entre lesquels on se déplace. Au sommet d'un carré donné se trouvent un nombre, son opposé, son inverse et l'opposé de son inverse ; ainsi à chaque carré correspond un petit diagramme qui commute dans la mesure où l'inverse de l'opposé d'un nombre est l'opposé de son inverse. Il faudrait être capable de démontrer que les nombres premiers ont pour propriété que l'application réitérée d'une même opération permet de parcourir tous leurs groupes de nombres associés une fois et une seule (selon un chemin Hamiltonien).

Tout ça a déjà été démontré par Gauss : on vient seulement de comprendre un peu mieux les puissances, et le fait qu'une *racine primitive* de Gauss permet de parcourir toutes les classes modulaires dans $\mathbb{Z}/p\mathbb{Z}$.

Ci-dessous, un des petits carrés de l'immeuble dans $\mathbb{Z}/11\mathbb{Z}$ entre lesquels on monte ou descend par l'élévation à la puissance, en ayant démarré sur une racine primitive pour passer une fois et une seule par chaque coin de chaque étage.



Des puissances et des palindromes (Denise Vella-Chemla, 18.5.2019)

On présente ici une découverte de propriétés palindromiques des puissances des nombres dans les corps premiers.

On se place dans un corps premier $\mathbb{Z}/p\mathbb{Z}$ et on regroupe les nombres 4 par 4 : chaque quadruplet q_n contient un nombre n, son opposé $-n$, son inverse $1/n$ et l'opposé de son inverse $-1/n$. On considère également la fonction qui, inversement [1], associe aux nombres n, $-n$, $1/n$ et $-1/n$ l'indice q_n du quadruplet auquel ils appartiennent.

Pour avoir une image en tête, on peut visualiser les nombres de 1 à $p-1$ aux 4 coins de carrés qu'on aurait empilés comme les étages d'un immeuble et les q_n sont les numéros des étages.

Un nombre premier p a comme propriété que tout nombre de 1 à $p-1$ est égal à une puissance d'une racine primitive de p. En étudiant les puissances en question, ou plutôt leur étage associé, on va voir que les étages ne sont pas parcourus aléatoirement, mais selon un ordre doublement palindromique.

Expliquons ces idées sur un exemple. Ci-dessous, on fournit les (plus petites) racines primitives des nombres premiers de 11 à 100 qu'on a utilisées.

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

Voici les différents quadruplets de nombres associés à 97 et les puissances de 7 prise comme racine primitive de 97 dans le corps premier $\mathbb{Z}/97\mathbb{Z}$.

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

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

1. au sens fonctionnel cette fois.

Si maintenant on écrit, dans l'ordre des puissances successives ci-dessus, les indices des quadruplets correspondant, on obtient l'ordre suivant de parcours des "étages" de l'immeuble des petits carrés (ou quadruplets) :

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

On repère bien l'identité des images entre la première et la troisième colonne ou bien entre la seconde et la quatrième colonne ainsi que l'ordre inversé des nombres de la première à la seconde colonne par exemple. Ces propriétés de palindromie des images s'observent pour tous les nombres premiers inférieurs à 100 et doivent donc être démontrable. La palindromie ayant lieu à la fois sur la séquence totale de quadruplets ainsi que sur chacune des moitiés de la séquence prises séparément, on a du coup une périodicité sur la séquence globale, de longueur la moitié de la longueur totale. Cette longueur vaut $p - 1$ pour les nombres premiers, elle est moindre pour les nombres composés.

Concernant maintenant les modules composés, du fait que certains nombres inférieurs à eux partagent avec eux certains diviseurs, on perd cette possibilité qu'une racine primitive permette d'obtenir tous les nombres du corps premier par élévation à toutes les puissances. Outre ce fait que certains indices de groupes ne puissent jamais être atteints par les puissances, on constate parfois de minuscules "défauts de palindromie", notamment pour des puissances de nombres premiers, dont on donne simplement quelques exemples ci-dessous.

En prenant comme racine primitive 3 pour le module 25, on obtient les puissances et les indices du tableau ci-dessous. 19 nombres sont atteints. Le centre du mot palindrome est coloré en bleu, le défaut de palindromie en rouge.

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

En prenant comme racine primitive 5 pour le module 27, on obtient les puissances et les indices du tableau ci-dessous. Les palindromies, à gauche du milieu, à droite, ainsi que globale, sont toutes respectées ; du coup, il y a périodicité puisque moitié gauche et droite de la séquence sont égales. Cependant, seulement 17 quadruplets sont atteints (17 n'est pas égal à $27 - 1$).

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

En prenant comme racine primitive 3 ou 11 pour le module 49, les palindromies sont respectées mais ce n'est pas le cas pour la racine primitive 5 pour laquelle on a :

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

On essaie deux exemples de modules supplémentaires, qui sont deux puissances de nombres premiers : $81 = 3^4$ et $121 = 11^2$.

Pour 81 avec 5 comme racine primitive, 5^{20} est dans le quadruplet (étage) 27 quand 5^{34} est dans le quadruplet 1, la palindromie globale n'est pas respectée à une puissance près. Pour 121 de racine primitive 7, c'est 7^8 qui se retrouve dans le quadruplet 33 quand 7^{55} est dans le quadruplet 1.

Programme de recherche des premiers par les propriétés quadratiques (Denise Vella-Chemla, 18.5.2019)

Le programme ci-dessous trouve, de façon très inefficace, les nombres premiers en testant la condition fournie par Gauss dans les Recherches arithmétiques.

Un nombre est premier si et seulement si son nombre de résidus quadratiques est égal à $\frac{p-1}{2}$.

```
#include <iostream>
#include <stdio.h>
#include <math.h>
#include <time.h>

int main (int argc, char* argv[])
{
  int x, y, z, p, nbsol, k ;
  bool marque[1000], trouve, condition ;
  float tps1, tps2 ;

  tps1 = clock() ;
  for (p = 7 ; p <= 1000 ; p=p+2)
    {
      nbsol = 0 ;
      for (k = 1 ; k <= p-1 ; ++k) marque[k] = false ;
      for (x = 1 ; x <= p-1 ; ++x)
        {
          for (y = 0 ; y <= p-1 ; ++y)
            for (z = 0 ; z <= p-1 ; ++z)
                if (x*x-p*y-z == 0)
                    marque[x*x-p*y] = true ;
        }
      for (k = 1 ; k <= p-1 ; ++k)
        if (marque[k])
          nbsol = nbsol+1 ;
      if (nbsol == (p-1)/2)
        condition = true ;
      else
        condition = false ;
      if (condition)
        std::cout << p << "␣␣␣" ;
    }
  tps2 = clock() ;
  std::cout << (float)(tps2-tps1)/CLOCKS_PER_SEC << "\n" ;
}
```

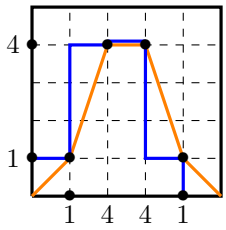
Voici le résultat de ce programme :

```
7   11   13   17   19   23   29   31   37   41   43   47   53   59
61   67   71   73   79   83   89   97   101   103   107   109   113
127   131   137   139   149   151   157   163   167   173   179   181
191   193   197   199   211   223   227   229   233   239   241   251
257   263   269   271   277   281   283   293   307   311   313   317
331   337   347   349   353   359   367   373   379   383   389   397
401   409   419   421   431   433   439   443   449   457   461   463
467   479   487   491   499   503   509   521   523   541   547   557
563   569   571   577   587   593   599   601   607   613   617   619
631   641   643   647   653   659   661   673   677   683   691   701
709   719   727   733   739   743   751   757   761   769   773   787
797   809   811   821   823   827   829   839   853   857   859   863
877   881   883   887   907   911   919   929   937   941   947   953
967   971   977   983   991   997
289.332
```

Nombres premiers et aires dans un carré (Denise Vella-Chemla, 20.5.2019)

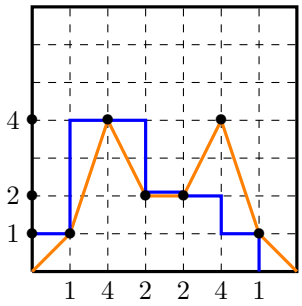
Dans les dessins ci-dessous, on représente sur un carré les résidus modulaires quadratiques de Gauss.

Résidus quadratiques modulo 5



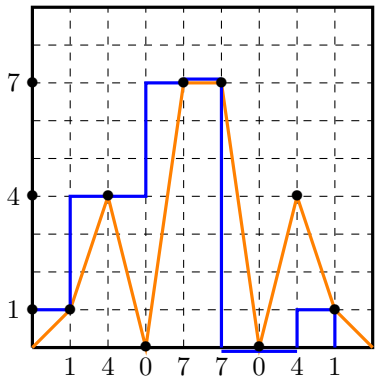
$$Aire = 10 = p\left(\frac{p-1}{2}\right)$$

Résidus quadratiques modulo 7



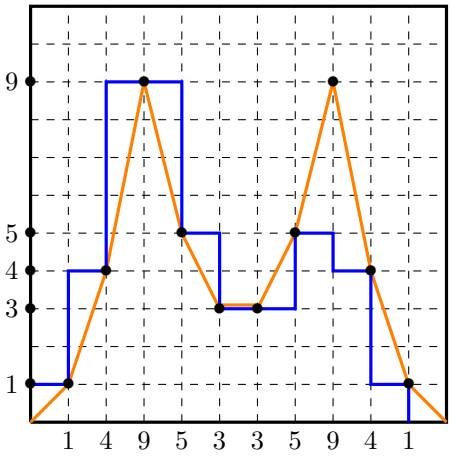
$$Aire = 14 = p\left(\frac{p-3}{2}\right)$$

Résidus quadratiques modulo 9



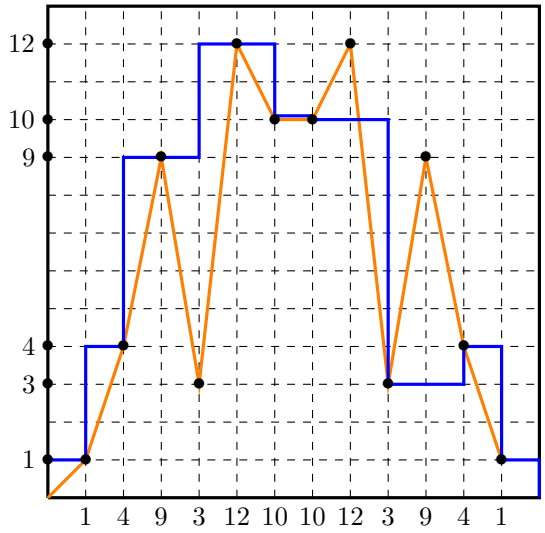
$$Aire = 24 < p\left(\frac{p-1}{2}\right)$$

Résidus quadratiques modulo 11



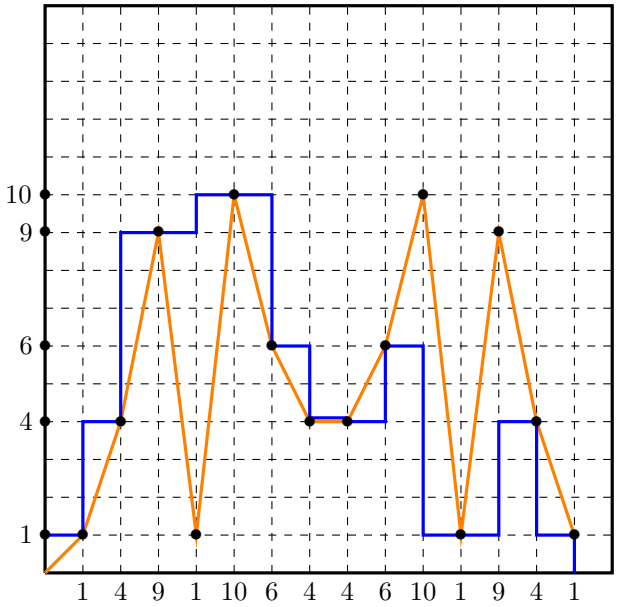
$$Aire = 44 = p\left(\frac{p-3}{2}\right)$$

Résidus quadratiques modulo 13



$$Aire = 78 = p\left(\frac{p-1}{2}\right)$$

Résidus quadratiques modulo 15



$$Aire = 70 < p\left(\frac{p-3}{2}\right)$$

Les dessins semblent indiquer que si un nombre de la forme $4k+1$ a sa somme des carrés inférieure à $p\left(\frac{p-1}{2}\right)$ alors il est composé tandis qu'il est premier si elle est égale à la valeur en question.

De même, si un nombre de la forme $4k+3$ a sa somme des carrés inférieure à $p\left(\frac{p-3}{2}\right)$ alors il est composé tandis qu'il est premier si elle est égale à la valeur en question.

Cela pourrait s'expliquer par le fait que lorsque n est composé, certains nombres qui ne sont pas premiers à n ont leur carré qui peut s'annuler (cf. le dessin associé à 9). Ce n'est pas le cas pour l'exemple du nombre composé 15, il faudrait trouver comment préciser l'explication.

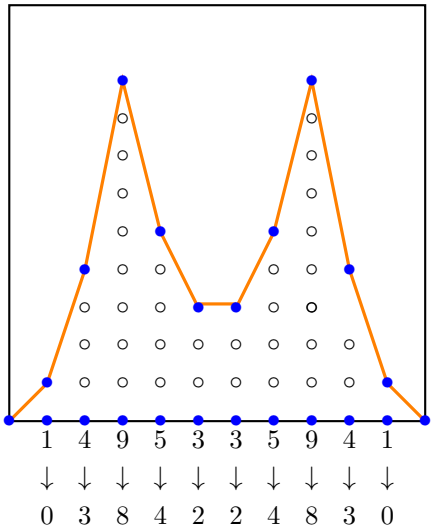
On essaie de trouver une formule qui permettrait de calculer l'aire plus rapidement, les dessins aident visuellement à la trouver.

On a le théorème de Pick qui fournit l'aire d'une surface en fonction du nombre de ses points intérieurs et du nombre de ses points sur le bord de la forme, ces points appartenant tous à un réseau de points équidistants. Mais il faut

que la forme n'ait pas de trous. La formule est $Aire = Int + \frac{1}{2}Bord - 1$. Si la forme comporte des trous (ici dans le cas de 9 où la forme est coupée en 3), il faut soustraire $\chi(F)$, la caractéristique d'Euler de la forme, au lieu de 1 (dans le cas de 9, il y a 2 coupures de la forme, qui la coupent en 3 morceaux). *Note :* dans le cas de coupures, les points du bord appartenant à deux morceaux différents doivent être comptés en double.

Le nombre de points du bord du polygone associé à m vaut clairement $2m$. Le nombre de points intérieurs, en le comptant une verticale après l'autre, est nul pour un carré nul, et vaut $c-1$ dans le cas d'un carré égal à c.

Explicitons sur le dessin de 11.



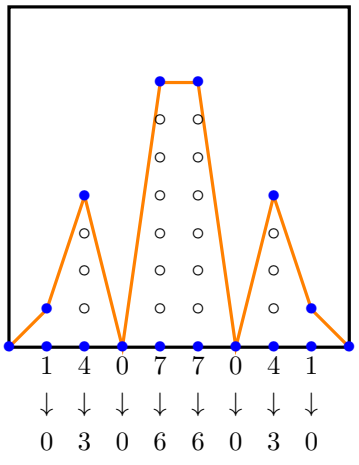
$$Bord = 22$$
$$Int = 34$$
$$Aire = 0.5 \times 22 + 34 - 1 = 44$$

On obtient ainsi l'aire directement en ajoutant $2n-1$ à la somme des résidus quadratiques auxquels on a soustrait 1 s'ils sont non nuls.

Tableau des nombres de points pour appliquer la formule de Pick aux dessins présentés

5	10	6	10	
7	14	8	14	
9	18	18	26	au lieu de 24
11	22	34	44	
13	26	66	78	
15	30	56	70	

Illustration des coupures par l'exemple du module 9

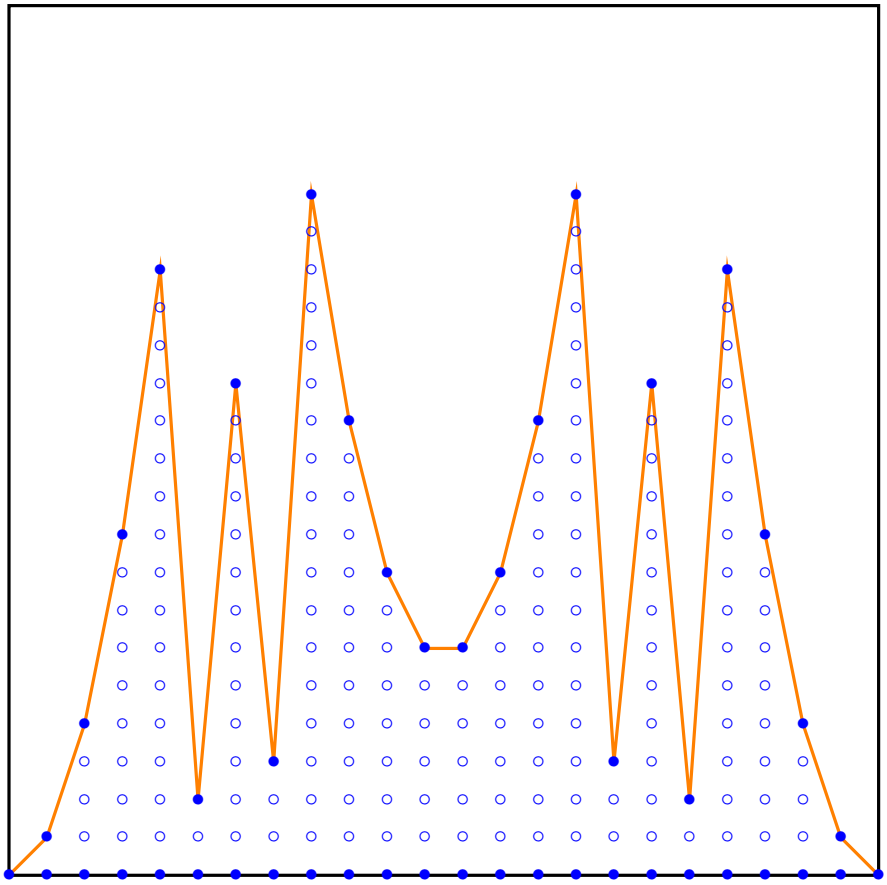


$$Aire = 5 + 14 + 5 = Int + \frac{1}{2}Bord - 3$$

Malheureusement, nos conjectures tombent dès $p = 23$, pour lequel l'aire vaut 207, inférieure à $230 = p\left(\frac{p-3}{2}\right)$.

Elles sont aussi invalidées par de nombreux autres petits nombres premiers (31, 47, etc.) et les formules sont de plus vérifiées par des nombres composés (comme 65 ou 85).

Résidus quadratiques modulo 23



emacs25@vellachemla-X510UA

File Edit Options Buffers Tools C++ Help

```cpp
#include <iostream>
#include <stdio.h>
#include <time.h>
#include <math.h>

int main (int argc, char* argv[]) {
  int n, d, nmax, pix ;
  bool pasdivisible ;
  float tps1, tps2 ;

  tps1 = clock() ;
  pix = 0 ;
  nmax = 1000 ;
  std::cout << nmax << "--->\n" ;
  for (n = 3 ; n <= nmax ; n=n+2) {
      pasdivisible = true ;
      d = 3 ;
      while ((pasdivisible) && (d <= sqrt(n))) {
          if ((n % d) == 0)
            pasdivisible = false ;
          d = d+2 ;
      }
      if (pasdivisible) {
          pix = pix+1 ;
          std::cout << n << "    " ;
      }
  }
  std::cout << "pix " << pix << "\n" ;
  tps2 = clock() ;
  std::cout << "\n" << (float)(tps2-tps1)/CLOCKS_PER_SEC << "\n" ;
}
```

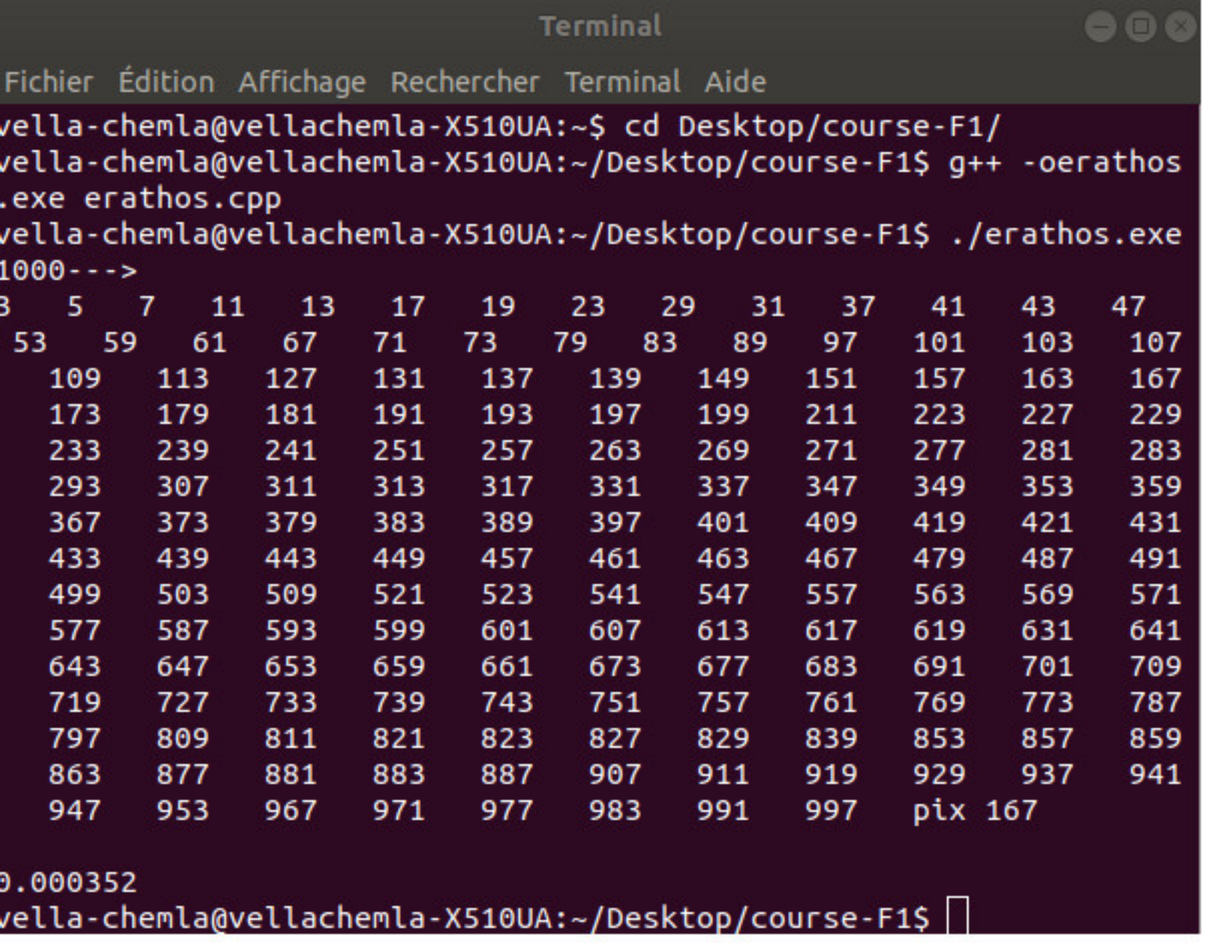
-:--- **erathos.cpp** All L7 (C++/l Abbrev)

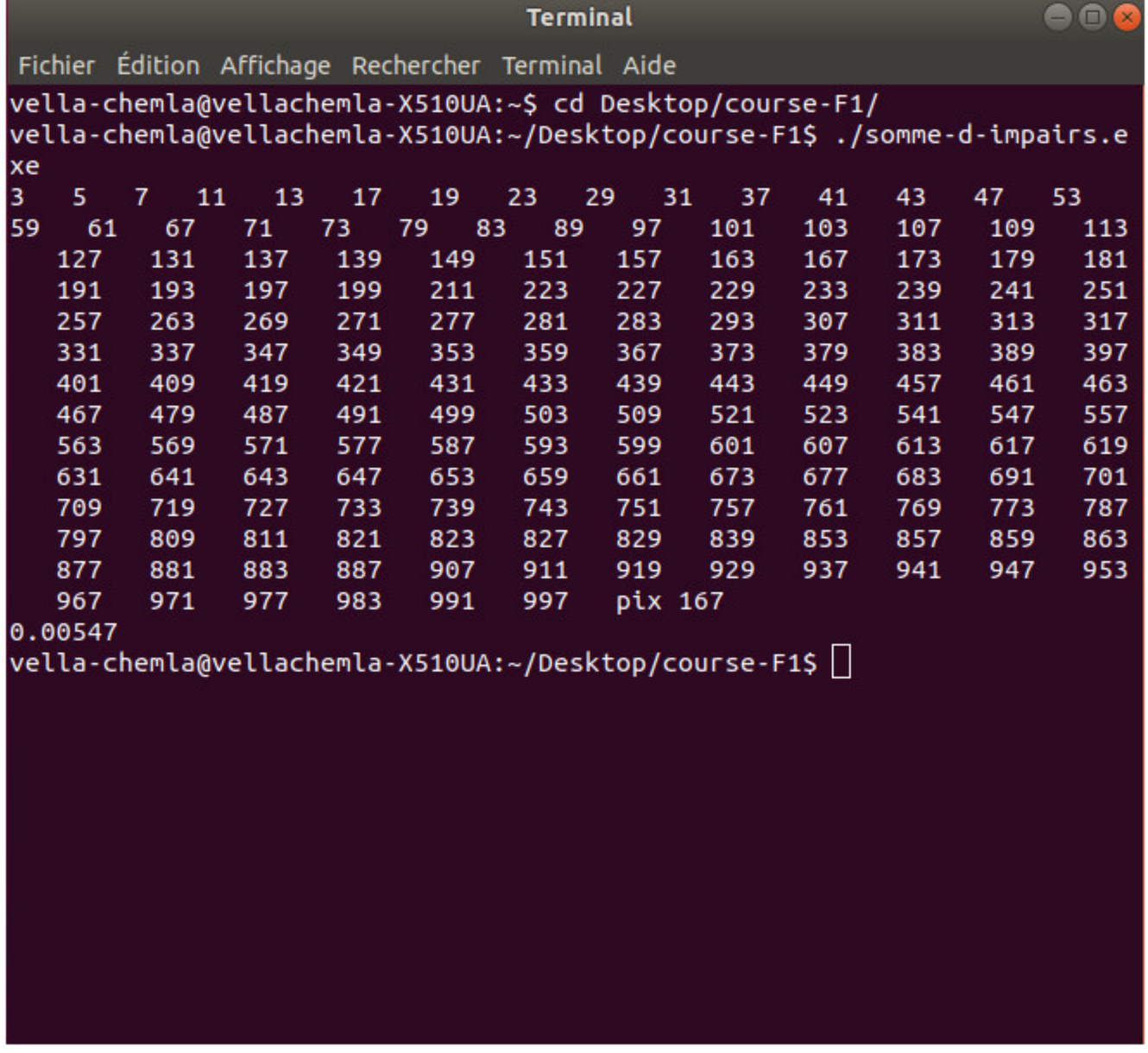
emacs25@vellachemla-X510UA

File Edit Options Buffers Tools C++ Help

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

int main (int argc, char* argv[]) {
  int x, p, nbsol, somme, pix ;
  bool marque[1000001] ;
  float tps1, tps2 ;

  pix = 0 ;
  tps1 = clock() ;
  for (p = 3 ; p <= 1000 ; p=p+2) {
      nbsol = 0 ;
      somme = 0 ;
      for (x = 1 ; x <= p-1 ; ++x) marque[x] = false ;
      for (x = 0 ; x <= (p-1)/2 ; ++x) {
          somme = (somme +(2*x+1)) % p ;
          marque[somme] = true ;
      }
      for (x = 1 ; x <= p-1 ; ++x)
        if (marque[x])
          nbsol = nbsol+1 ;
      if (nbsol == (p-1)/2) {
          std::cout << p << "    " ;
          pix = pix+1 ;
      }
  }
  std::cout << "pix " << pix << "\n" ;
  tps2 = clock() ;
  std::cout << (float)(tps2-tps1)/CLOCKS_PER_SEC << "\n" ;
}
```

-:--- **somme-d-impairs.cpp** All L6 (C++/l Abbrev)


Terminal
Fichier Édition Affichage Rechercher Terminal Aide
vella-chemla@vellachemla-X510UA:~$ cd Desktop/course-F1/
vella-chemla@vellachemla-X510UA:~/Desktop/course-F1$ g++ -oerathos
.exe erathos.cpp
vella-chemla@vellachemla-X510UA:~/Desktop/course-F1$ ./erathos.exe
1000--->
3 5 7 11 13 17 19 23 29 31 37 41 43 47
53 59 61 67 71 73 79 83 89 97 101 103 107
109 113 127 131 137 139 149 151 157 163 167
173 179 181 191 193 197 199 211 223 227 229
233 239 241 251 257 263 269 271 277 281 283
293 307 311 313 317 331 337 347 349 353 359
367 373 379 383 389 397 401 409 419 421 431
433 439 443 449 457 461 463 467 479 487 491
499 503 509 521 523 541 547 557 563 569 571
577 587 593 599 601 607 613 617 619 631 641
643 647 653 659 661 673 677 683 691 701 709
719 727 733 739 743 751 757 761 769 773 787
797 809 811 821 823 827 829 839 853 857 859
863 877 881 883 887 907 911 919 929 937 941
947 953 967 971 977 983 991 997 pix 167
0.000352
vella-chemla@vellachemla-X510UA:~/Desktop/course-F1$


Terminal
Fichier Édition Affichage Rechercher Terminal Aide
vella-chemla@vellachemla-X510UA:~$ cd Desktop/course-F1/
vella-chemla@vellachemla-X510UA:~/Desktop/course-F1$ ./somme-d-impairs.e
xe
3 5 7 11 13 17 19 23 29 31 37 41 43 47 53
59 61 67 71 73 79 83 89 97 101 103 107 109 113
127 131 137 139 149 151 157 163 167 173 179 181
191 193 197 199 211 223 227 229 233 239 241 251
257 263 269 271 277 281 283 293 307 311 313 317
331 337 347 349 353 359 367 373 379 383 389 397
401 409 419 421 431 433 439 443 449 457 461 463
467 479 487 491 499 503 509 521 523 541 547 557
563 569 571 577 587 593 599 601 607 613 617 619
631 641 643 647 653 659 661 673 677 683 691 701
709 719 727 733 739 743 751 757 761 769 773 787
797 809 811 821 823 827 829 839 853 857 859 863
877 881 883 887 907 911 919 929 937 941 947 953
967 971 977 983 991 997 pix 167
0.00547
vella-chemla@vellachemla-X510UA:~/Desktop/course-F1$

Terminal

Fichier Édition Affichage Rechercher Terminal Aide

```
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$ python chazy.py
2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103
 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 2
11 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317
 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 4
43 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571
 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 6
91 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827
 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 9
71 977 983 991 997 pix 168
Temps d execution : 1.29903316498 secondes ---
vella-chemla@vellachemla-X510UA:~/Desktop$
```

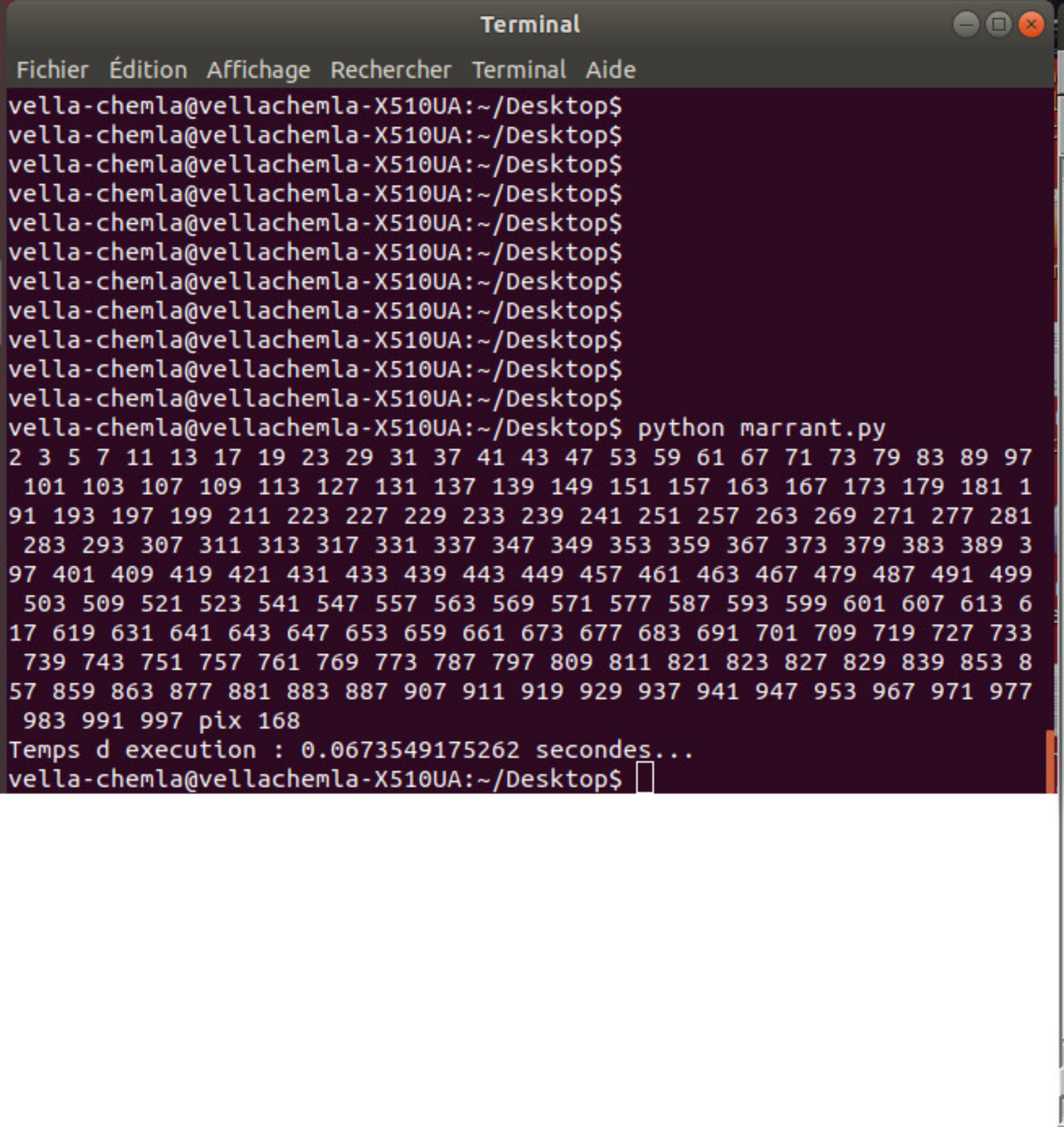
emacs25@vellachemla-X510UA

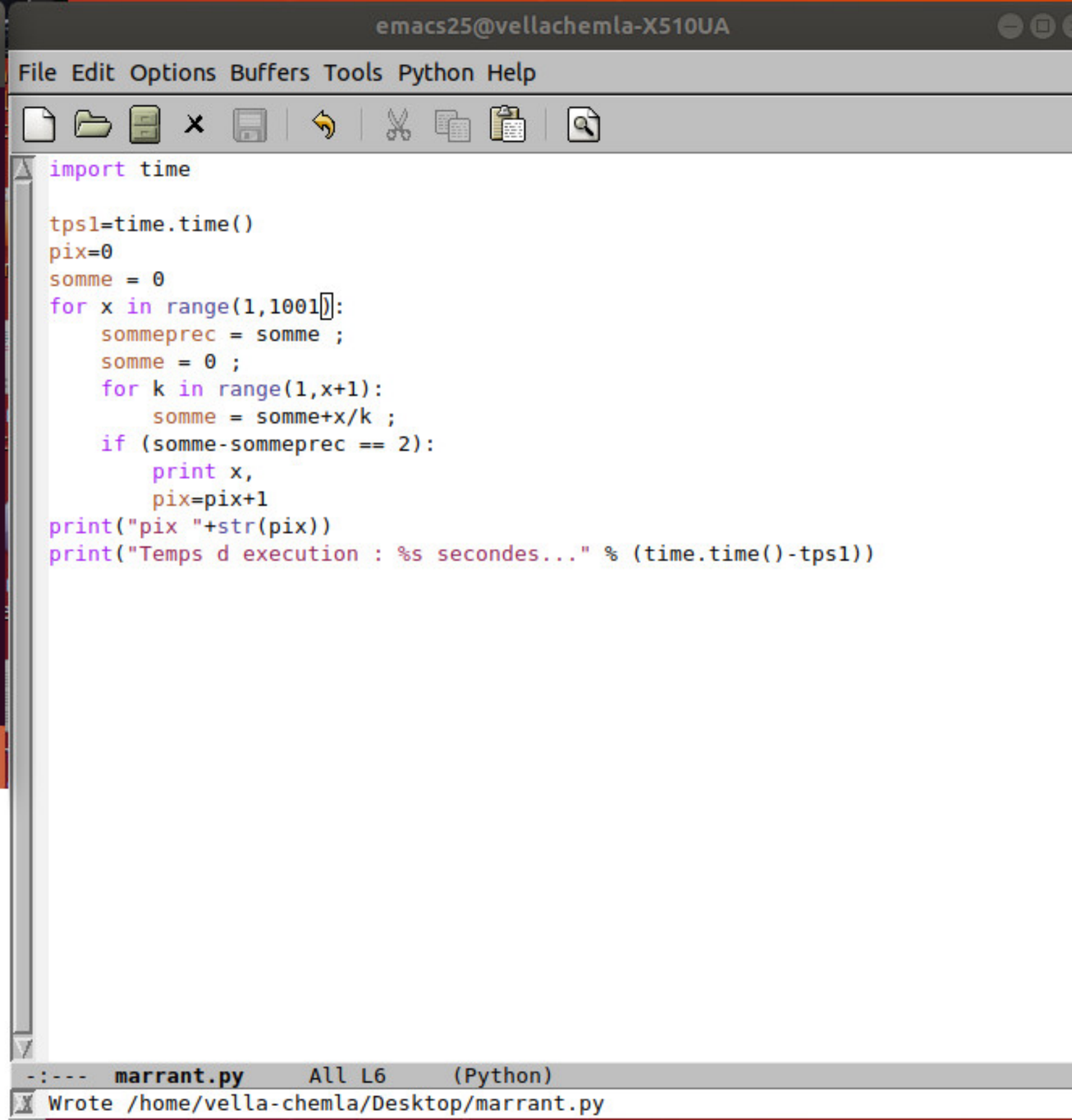
File Edit Options Buffers Tools Python Help

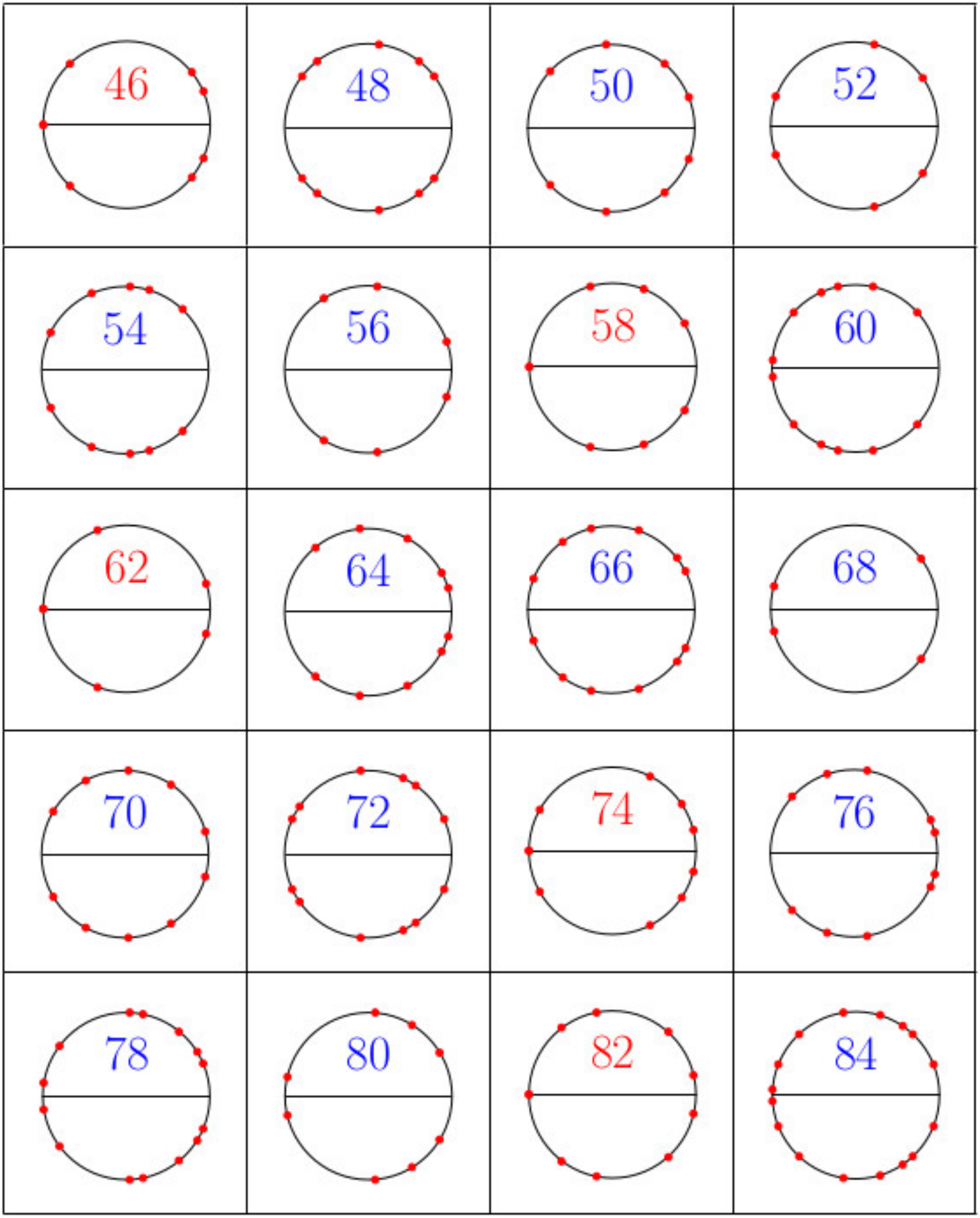
```
import numpy as np
from numpy import *
import time

tps1=time.time()
pix = 0 ;
sigma = np.zeros(1000, dtype='i')
sigma[1] = 1
for n in range(2,1000):
      somme = 0
      for k in range(1,n):
          somme = somme+(-(n*n)+5*k*n-5*k*k)*sigma[k]*sigma[n-k]
      sigma[n] = (12*somme)/(n*n*(n-1))
      if (sigma[n] == (n+1)):
          print n,
          pix = pix+1
print("pix "+str(pix))
print("Temps d execution : %s secondes ---" % (time.time()- tps1))
```

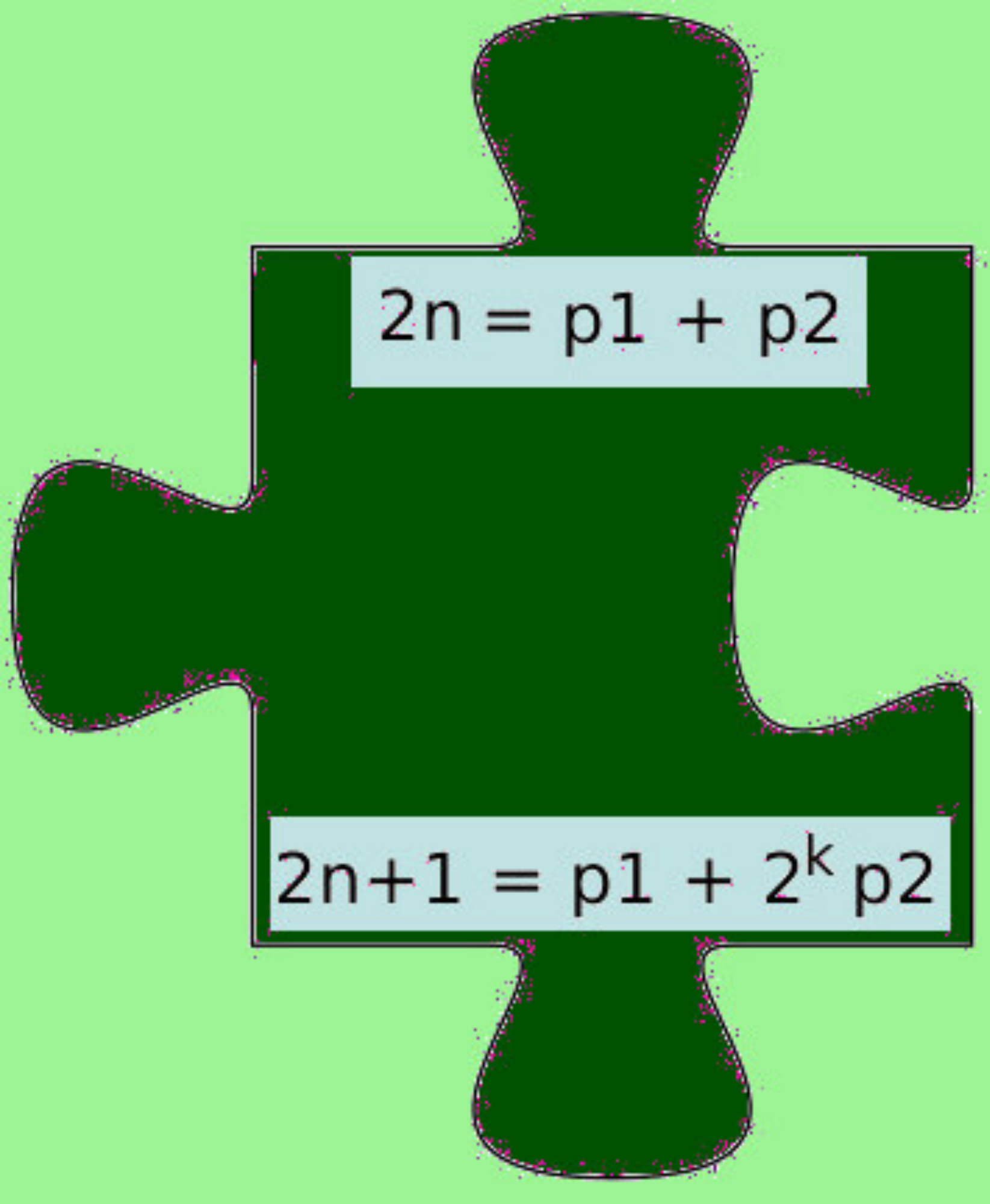
-:--- chazy.py All L1 (Python)

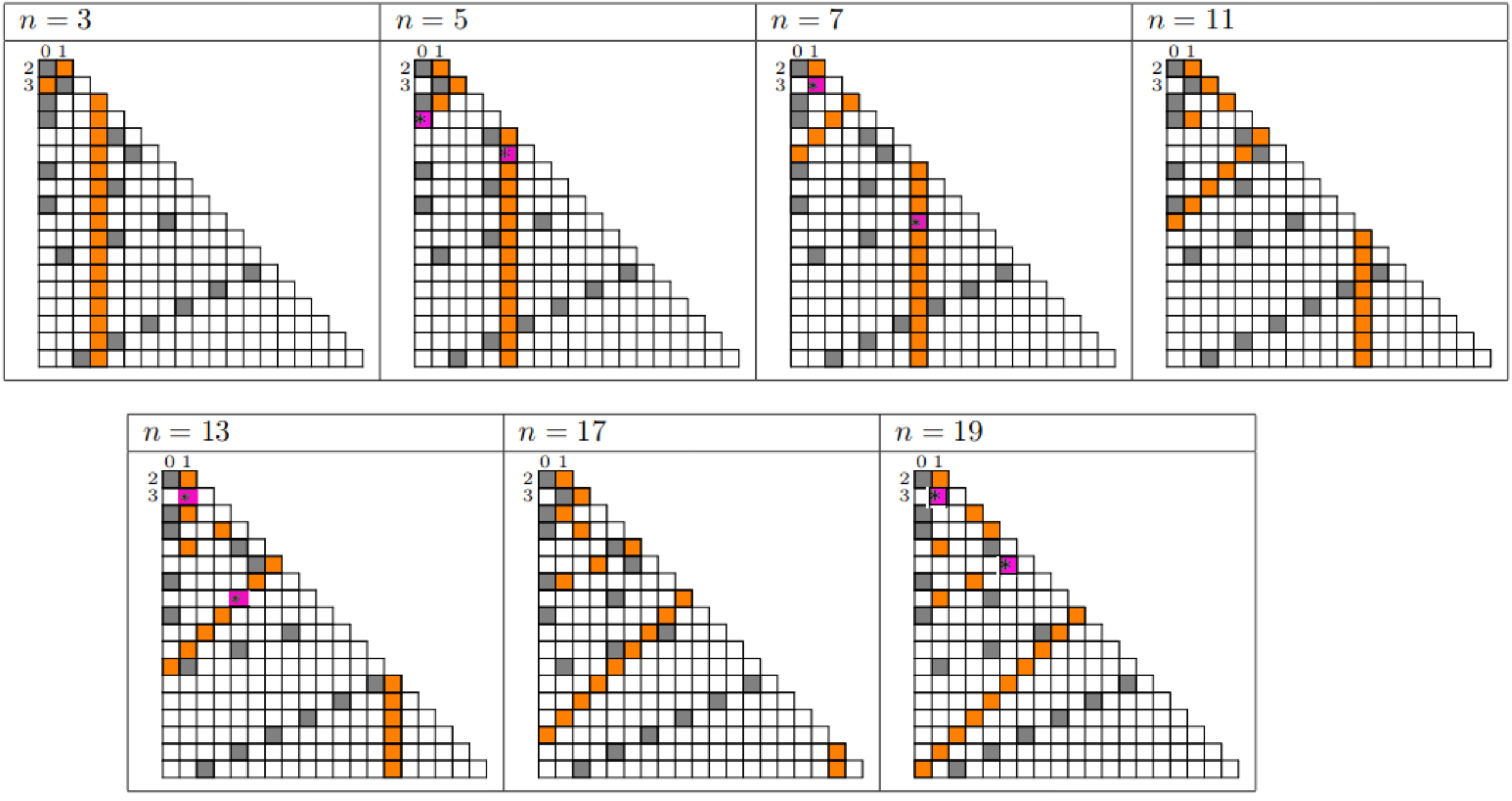
5 1


Terminal
Fichier Édition Affichage Rechercher Terminal Aide
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$ python marrant.py
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
101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 1
91 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281
283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 3
97 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499
503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 6
17 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727 733
739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 8
57 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977
983 991 997 pix 168
Temps d execution : 0.0673549175262 secondes...
vella-chemla@vellachemla-X510UA:~/Desktop$


emacs25@vellachemla-X510UA
File Edit Options Buffers Tools Python Help
import time
tps1=time.time()
pix=0
somme = 0
for x in range(1,1001):
sommeprec = somme ;
somme = 0 ;
for k in range(1,x+1):
somme = somme+x/k ;
if (somme-sommeprec == 2):
print x,
pix=pix+1
print("pix "+str(pix))
print("Temps d execution : %s secondes..." % (time.time()-tps1))
-:--- marrant.py All L6 (Python)
Wrote /home/vella-chemla/Desktop/marrant.py


46
48
50
52
54
56
58
60
62
64
66
68
70
72
74
76
78
80
82
84


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


$n = 3$
$n = 5$
$n = 7$
$n = 11$
$n = 13$
$n = 17$
$n = 19$
0 1
2
3

Voici la forme générale de la matrice G.

$$\begin{pmatrix}
0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 1 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 1 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 0 & 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 1 & 0 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 1 & 0 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 1 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 1 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 0 & 1 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 1 & 0 & 0 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}$$

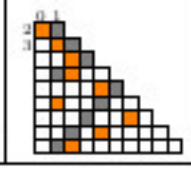
Tous les ... sont des 0.

D'un Z qui veut dire... (Denise Vella-Chemla, 15.6.2019)

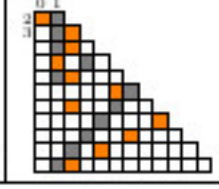
$2p = p + p$: un nombre premier vérifie trivialement la conjecture de Goldbach. On repère de belles lettres Z dans le bas des tores trapézoïdaux qu'on a choisis pour représenter les restes des nombres dans des divisions par les entiers successifs à commencer par 2.

14

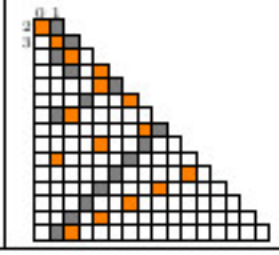
22



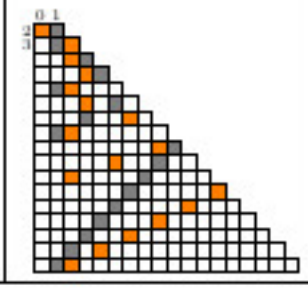
26



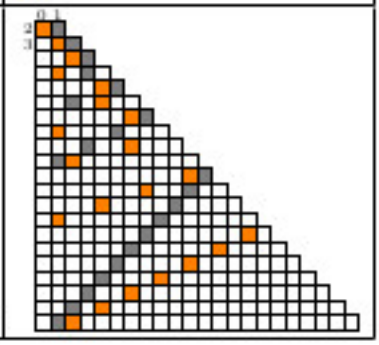
34



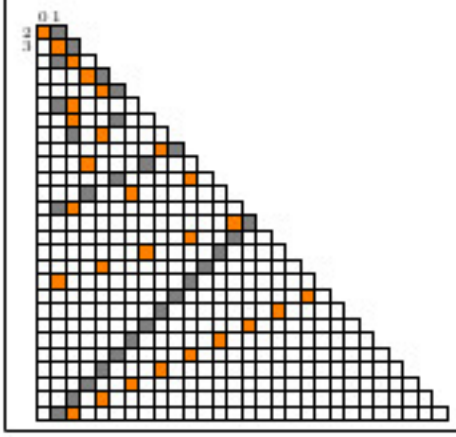
38



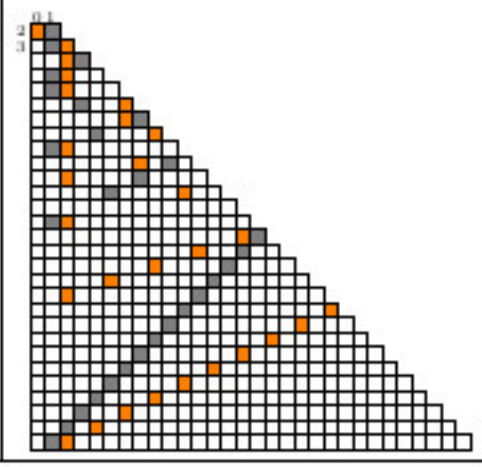
46



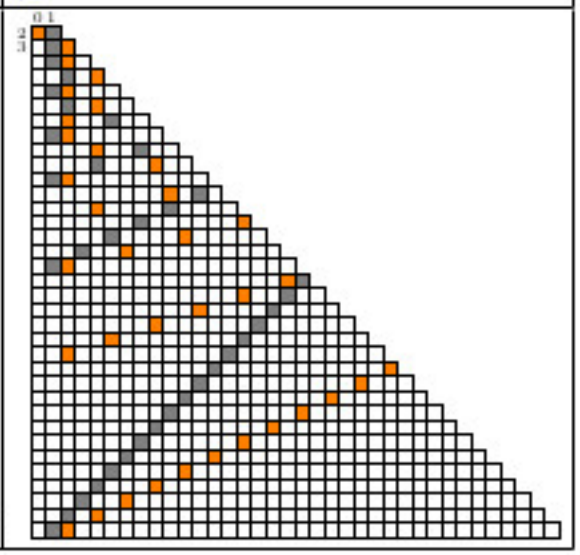
58



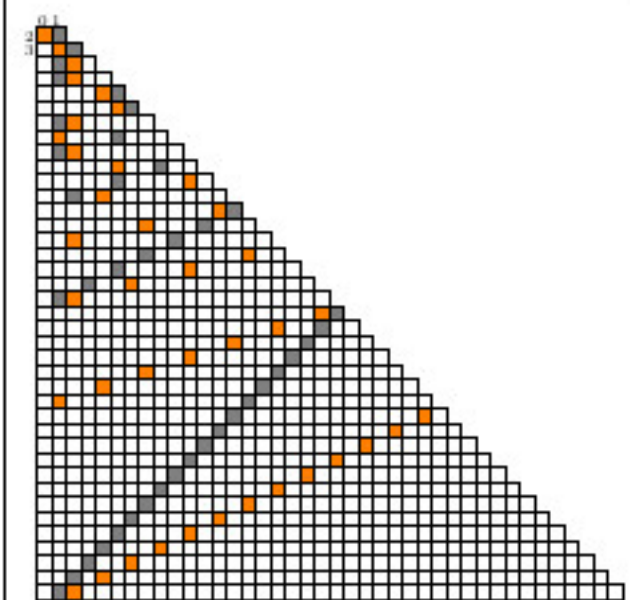
62



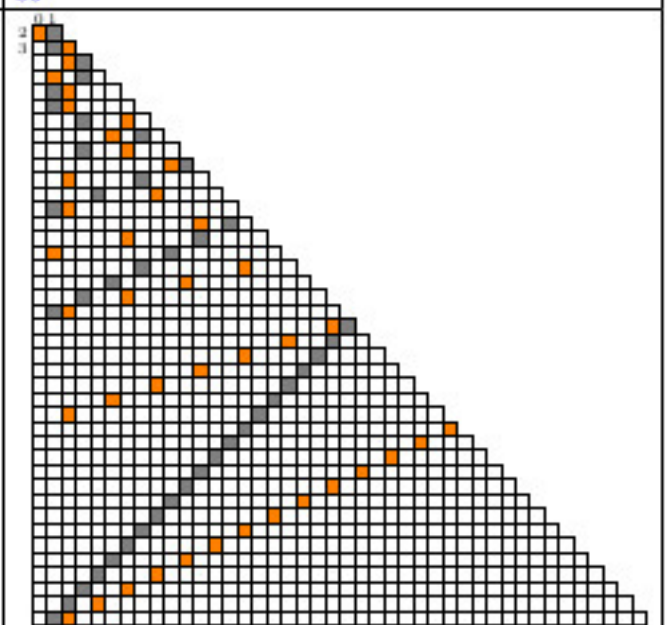
74



82



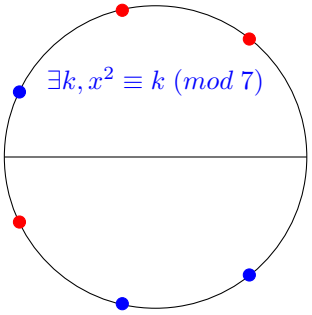
86



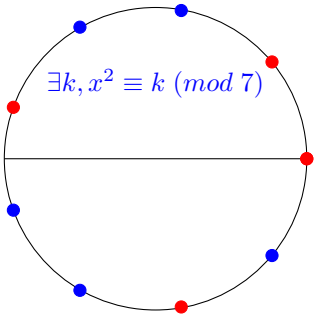
Résidus quadratiques sur colliers (Denise Vella-Chemla, 22.5.2019)

Un nombre premier p est caractérisé par le fait que dans $\mathbb{Z}/p\mathbb{Z}$, $\frac{p-1}{2}$ nombres sont résidus quadratiques et $\frac{p-1}{2}$ ne le sont pas. Dans une représentation des classes de congruences sur un cercle, les résidus quadratiques sont symétriques (x résidu de $p \iff n-x$ résidu de p) pour les nombres premiers de la forme $4k+1$ et anti-symétriques (x résidu de $p \iff n-x$ non résidu de p) pour les nombres premiers de la forme $4k+3$.

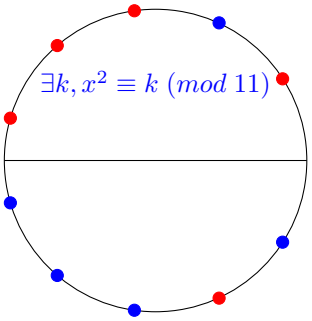
Solutions de $\exists k, x^2 \equiv k \ (mod\ 7)$: 1, 2, 4.
7 est premier.
Il y a 3 solutions.



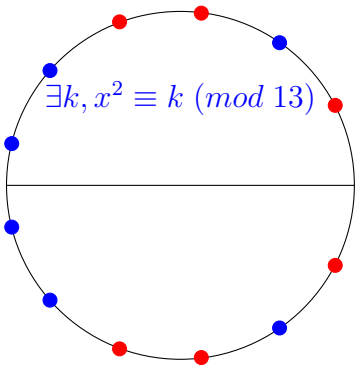
Solutions de $\exists k, x^2 \equiv k \ (mod\ 9)$: 0, 1, 4, 7.
9 est composé.
Il y a 4 solutions.



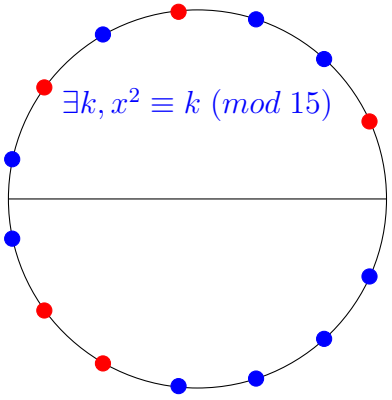
Solutions de $\exists k, x^2 \equiv k \ (mod\ 11)$: 1, 3, 4, 5, 9.
11 est premier.
Il y a 5 solutions.



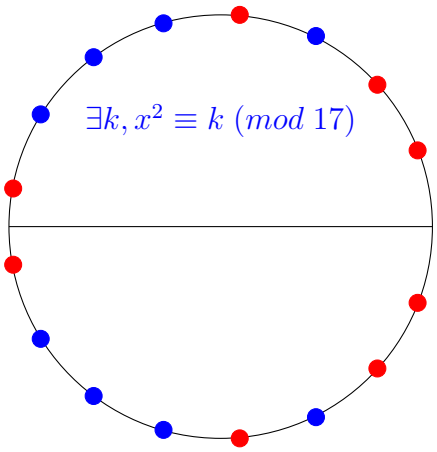
Solutions de $\exists k, x^2 \equiv k \ (mod\ 13)$: 1, 3, 4, 9, 10, 12.
13 est premier.
Il y a 6 solutions.



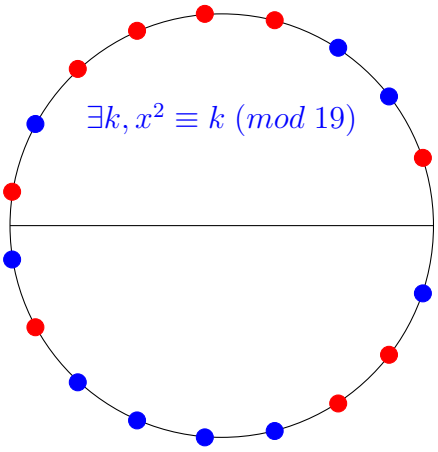
Solutions de $\exists k, x^2 \equiv k \ (mod\ 15)$: 1, 4, 6, 9, 10.
15 est composé.
Il y a 5 solutions.



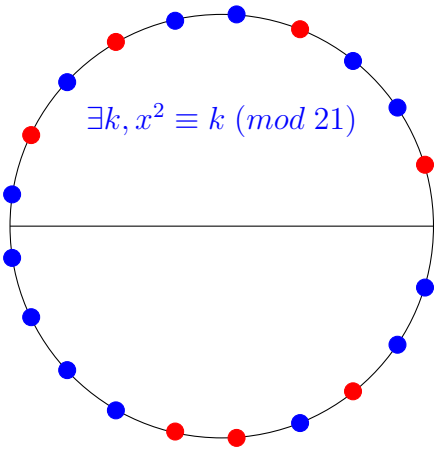
Solutions de $\exists k, x^2 \equiv k \ (mod\ 17)$: 1, 2, 4, 8, 9, 13, 15, 16.
17 est premier.
Il y a 8 solutions.



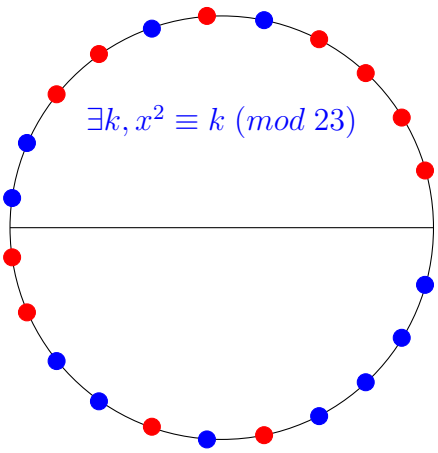
Solutions de $\exists k, x^2 \equiv k \ (mod\ 19)$: 1, 4, 5, 6, 7, 9, 11, 16, 17.
19 est premier.
Il y a 9 solutions.



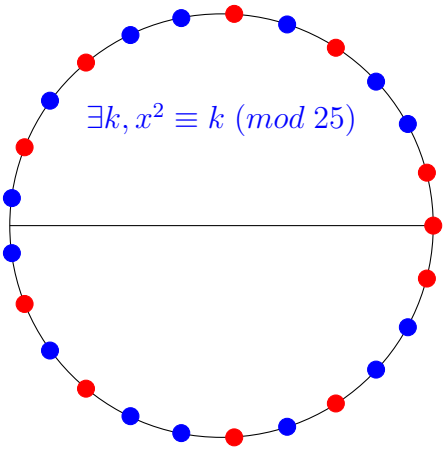
Solutions de $\exists k, x^2 \equiv k \ (mod\ 21)$: 1, 4, 7, 9, 15, 16, 18.
21 est composé.
Il y a 4 solutions.



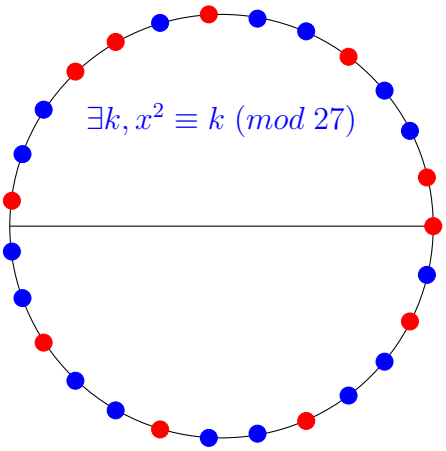
Solutions de $\exists k, x^2 \equiv k \ (mod\ 23)$: 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.
23 est premier.
Il y a 11 solutions.



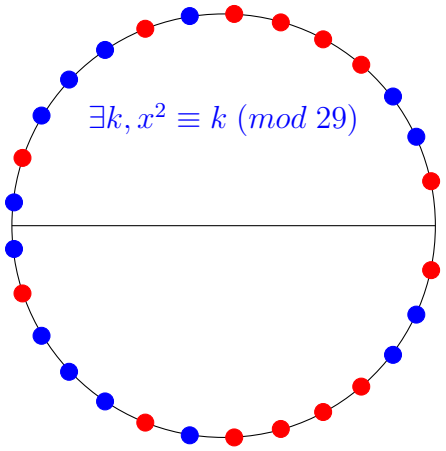
Solutions de $\exists k, x^2 \equiv k \ (mod\ 25)$: 0, 1, 4, 6, 9, 11, 14, 16, 19, 21, 24.
25 est composé.
Il y a 11 solutions.



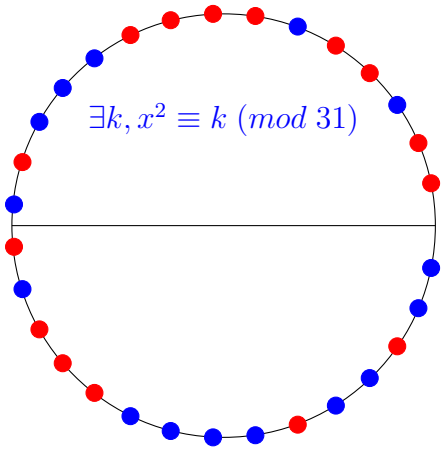
Solutions de $\exists k, x^2 \equiv k \ (mod\ 27)$: 0, 1, 4, 7, 9, 10, 13, 16, 19, 22, 25.
27 est composé.
Il y a 10 solutions.



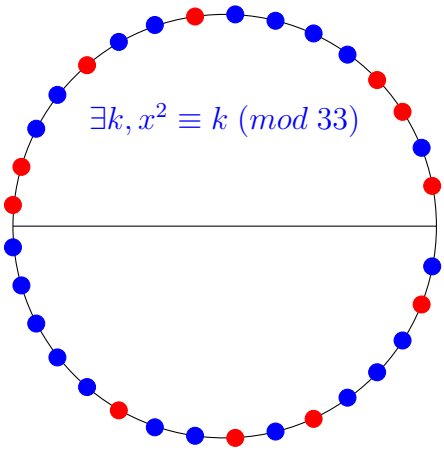
Solutions de $\exists k, x^2 \equiv k \ (mod\ 29)$: 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28.
29 est premier.
Il y a 14 solutions.



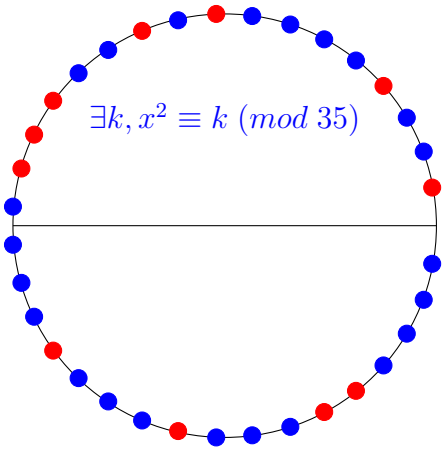
Solutions de $\exists k, x^2 \equiv k \ (mod\ 31)$: 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28.
31 est premier.
Il y a 15 solutions.



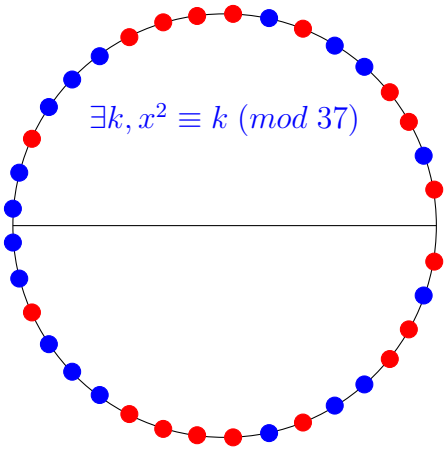
Solutions de $\exists k, x^2 \equiv k \ (mod\ 33)$: 1, 3, 4, 9, 12, 15, 16, 22, 25, 27, 31.
33 est composé.
Il y a 11 solutions.



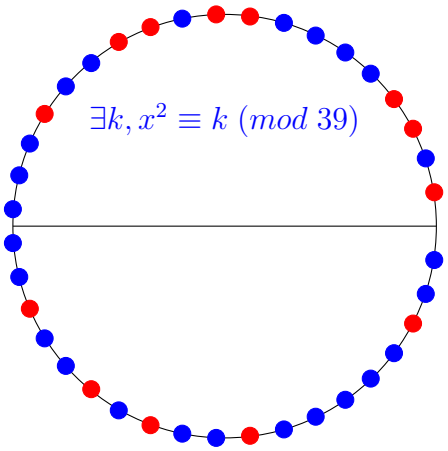
Solutions de $\exists k, x^2 \equiv k \ (mod\ 35)$: 1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30.
35 est composé.
Il y a 11 solutions.



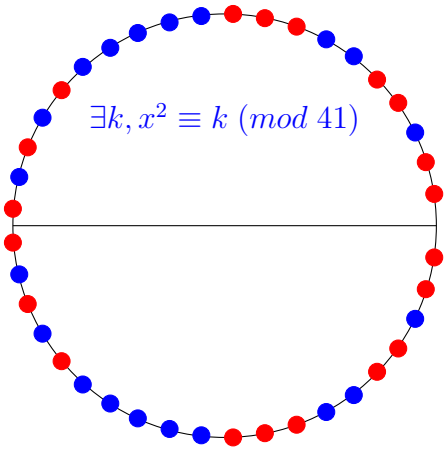
Solutions de $\exists k, x^2 \equiv k \ (mod\ 37)$: 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36.
37 est premier.
Il y a 18 solutions.



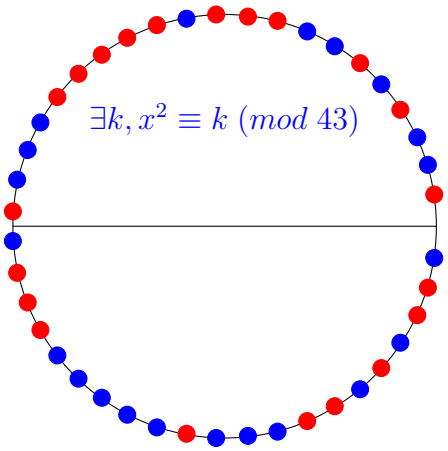
Solutions de $\exists k, x^2 \equiv k \ (mod\ 39)$: 1, 3, 4, 9, 10, 12, 13, 16, 22, 25, 27, 30, 36.
39 est composé.
Il y a 13 solutions.



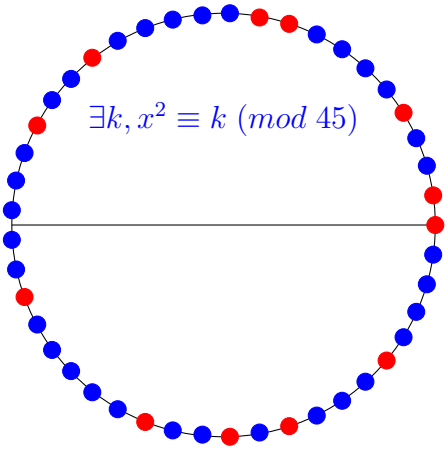
Solutions de $\exists k, x^2 \equiv k \ (mod\ 41)$: 1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40.
41 est premier.
Il y a 20 solutions.



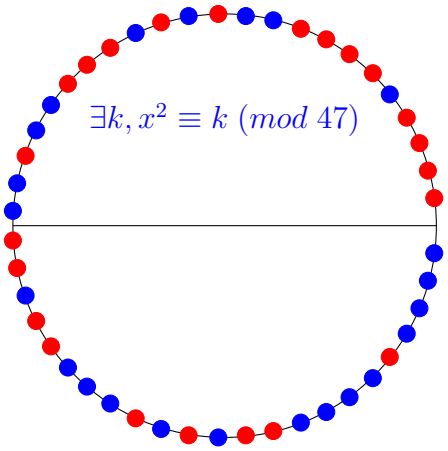
Solutions de $\exists k, x^2 \equiv k \ (mod\ 43)$: 1, 4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23, 24, 25, 31, 35, 36, 38, 40, 41.
43 est premier.
Il y a 21 solutions.



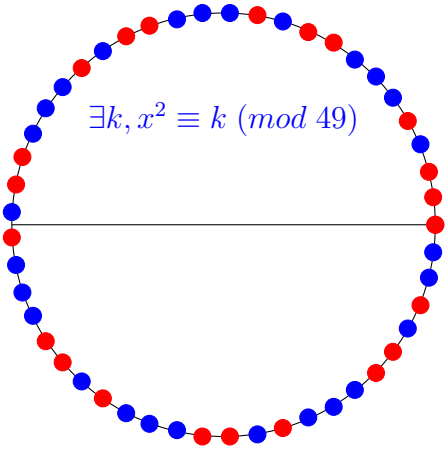
Solutions de $\exists k, x^2 \equiv k \ (mod\ 45)$: 0, 1, 4, 9, 10, 16, 19, 25, 31, 34, 36, 40.
45 est composé.
Il y a 12 solutions.



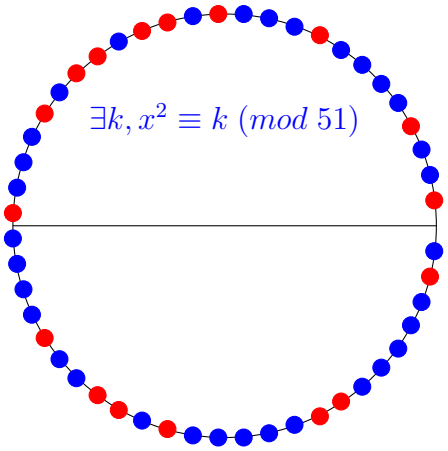
Solutions de $\exists k, x^2 \equiv k \ (mod\ 47)$: 1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42.
47 est premier.
Il y a 23 solutions.



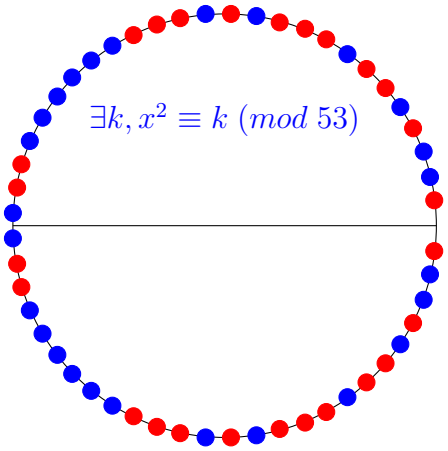
Solutions de $\exists k, x^2 \equiv k \ (mod\ 49)$: 0, 1, 2, 4, 8, 9, 11, 15, 16, 18, 22, 23, 25, 29, 30, 32, 36, 37, 39, 43, 44, 46.
49 est composé.
Il y a 22 solutions.



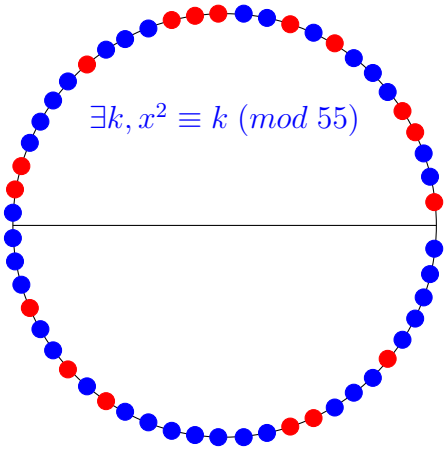
Solutions de $\exists k, x^2 \equiv k \ (mod\ 51)$: 1, 4, 9, 13, 15, 16, 18, 19, 21, 25, 30, 33, 34, 36, 42, 43, 49.
51 est composé.
Il y a 4 solutions.



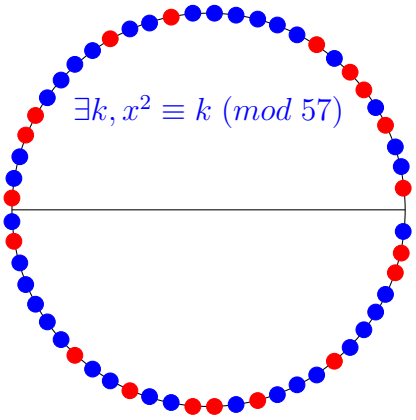
Solutions de $\exists k, x^2 \equiv k \ (mod\ 53)$: 1, 4, 6, 7, 9, 10, 11, 13, 15, 16, 17, 24, 25, 28, 29, 36, 37, 38, 40, 42, 43, 44, 46, 47, 49, 52.
53 est premier.
Il y a 4 solutions.



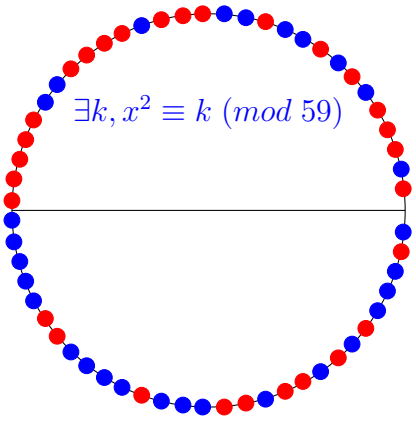
Solutions de $\exists k, x^2 \equiv k \ (mod\ 55)$: 1, 4, 5, 9, 11, 14, 15, 16, 20, 25, 26, 31, 34, 36, 44, 45, 49.
55 est composé.
Il y a 4 solutions.



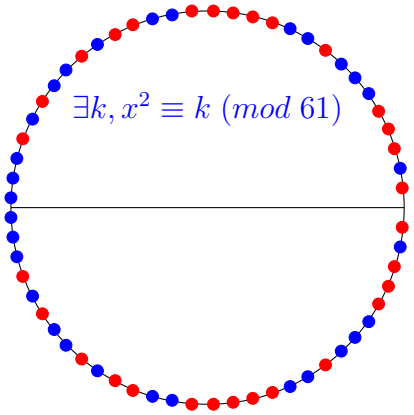
Solutions de $\exists k, x^2 \equiv k \ (mod\ 57)$: 1, 4, 6, 7, 9, 16, 19, 24, 25, 28, 30, 36, 39, 42, 43, 45, 49, 54, 55.
57 est composé.
Il y a 4 solutions.



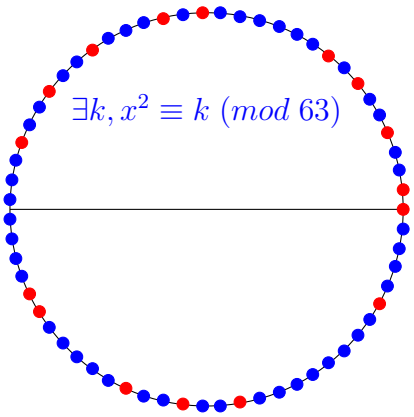
Solutions de $\exists k, x^2 \equiv k \ (mod\ 59)$: 1, 3, 4, 5, 7, 9, 12, 15, 16, 17, 19, 20, 21, 22, 25, 26, 27, 28, 29, 35, 36, 41, 45, 46, 48, 49, 51, 53, 57.
59 est premier.
Il y a 29 solutions.



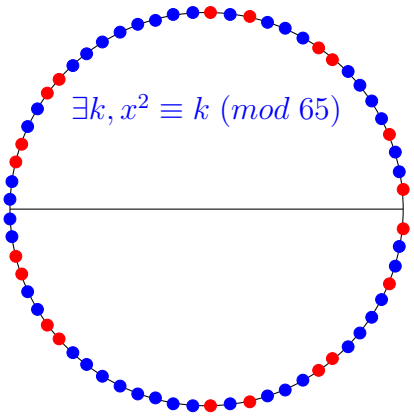
Solutions de $\exists k, x^2 \equiv k \ (mod\ 61)$: 1, 3, 4, 5, 9, 12, 13, 14, 15, 16, 19, 20, 22, 25, 27, 34, 36, 39, 41, 42, 45, 46, 47, 48, 49, 52, 56, 57, 58, 60.
61 est premier.
Il y a 30 solutions.



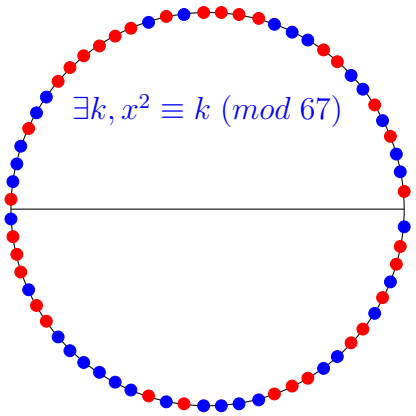
Solutions de $\exists k, x^2 \equiv k \ (mod\ 63)$: 0, 1, 4, 7, 9, 16, 18, 22, 25, 28, 36, 37, 43, 46, 49, 58.
63 est composé.
Il y a 16 solutions.



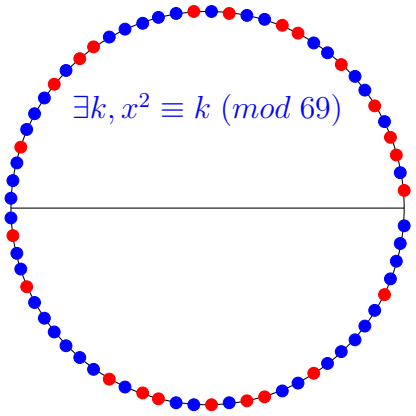
Solutions de $\exists k, x^2 \equiv k \ (mod\ 65)$: 1, 4, 9, 10, 14, 16, 25, 26, 29, 30, 35, 36, 39, 40, 49, 51, 55, 56, 61, 64.
65 est composé.
Il y a 20 solutions.



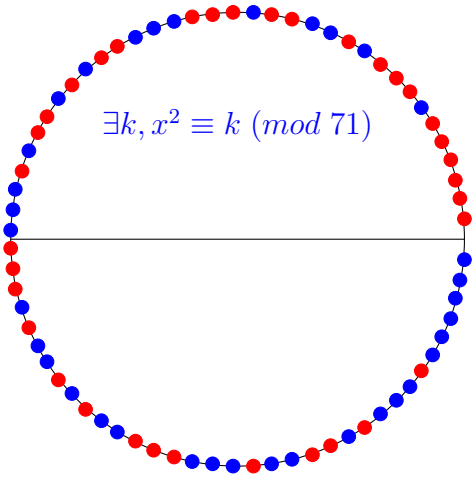
Solutions de $\exists k, x^2 \equiv k \ (mod\ 67)$: 1, 4, 6, 9, 10, 14, 15, 16, 17, 19, 21, 22, 23, 24, 25, 26, 29, 33, 35, 36, 37, 39, 40, 47, 49, 54, 55, 56, 59, 60, 62, 64, 65.
67 est premier.
Il y a 33 solutions.



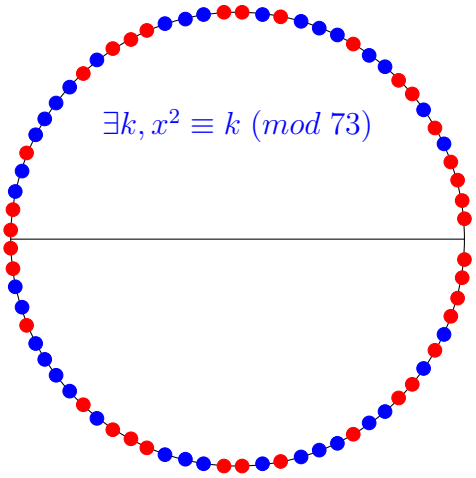
Solutions de $\exists k, x^2 \equiv k \ (mod\ 69)$: 1, 3, 4, 6, 9, 12, 13, 16, 18, 24, 25, 27, 31, 36, 39, 46, 48, 49, 52, 54, 55, 58, 64.
69 est composé.
Il y a 23 solutions.



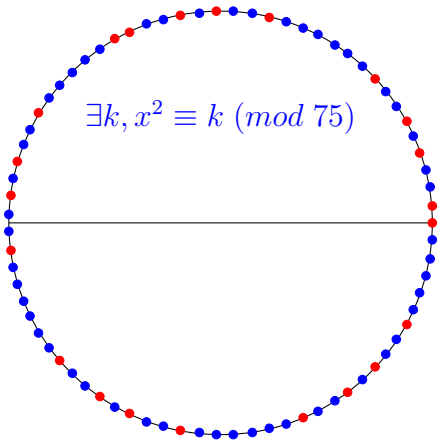
Solutions de $\exists k, x^2 \equiv k \ (mod\ 71)$: 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 19, 20, 24, 25, 27, 29, 30, 32, 36, 37, 38, 40, 43, 45, 48, 49, 50, 54, 57, 58, 60, 64.
71 est premier.
Il y a 35 solutions.



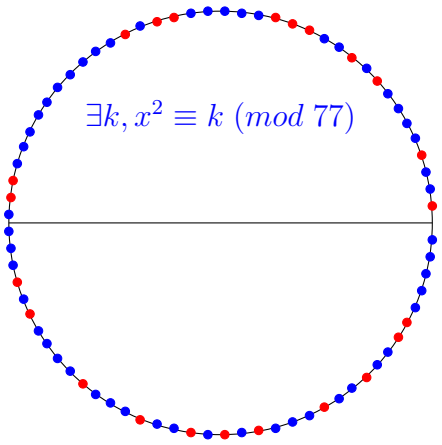
Solutions de $\exists k, x^2 \equiv k \ (mod\ 73)$: 1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 19, 23, 24, 25, 27, 32, 35, 36, 37, 38, 41, 46, 48, 49, 50, 54, 55, 57, 61, 64, 65, 67, 69, 70, 71, 72.
73 est premier.
Il y a 36 solutions.



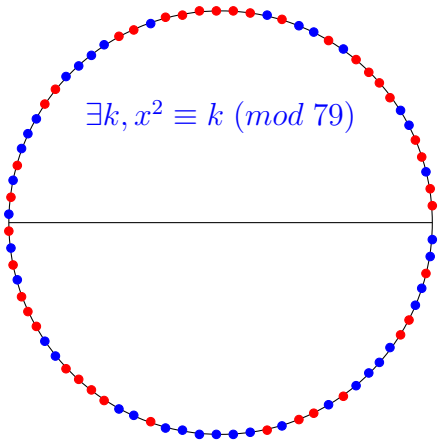
Solutions de $\exists k, x^2 \equiv k \ (mod\ 75)$: 0, 1, 4, 6, 9, 16, 19, 21, 24, 25, 31, 34, 36, 39, 46, 49, 51, 54, 61, 64, 66, 69.
75 est composé.
Il y a 22 solutions.



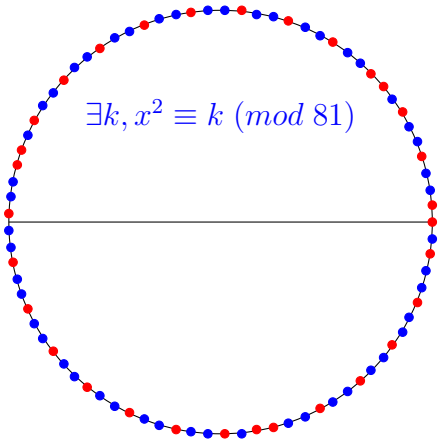
Solutions de $\exists k, x^2 \equiv k \ (mod\ 77)$: 1, 4, 9, 11, 14, 15, 16, 22, 23, 25, 36, 37, 42, 44, 49, 53, 56, 58, 60, 64, 67, 70, 71.
77 est composé.
Il y a 23 solutions.



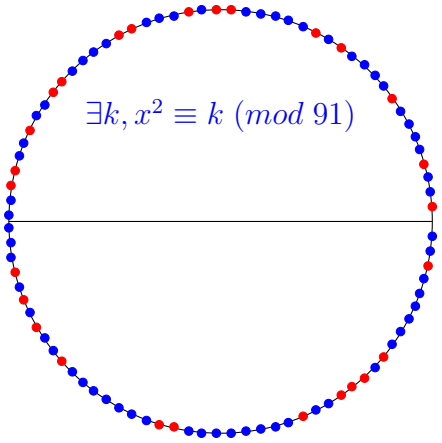
Solutions de $\exists k, x^2 \equiv k \ (mod\ 79)$: 1, 2, 4, 5, 8, 9, 10, 11, 13, 16, 18, 19, 20, 21, 22, 23, 25, 26, 31, 32, 36, 38, 40, 42, 44, 45, 46, 49, 50, 51, 52, 55, 62, 64, 65, 67, 72, 73, 76.
79 est premier.
Il y a 39 solutions.



Solutions de $\exists k, x^2 \equiv k \ (mod\ 81)$: 0, 1, 4, 7, 9, 10, 13, 16, 19, 22, 25, 28, 31, 34, 36, 37, 40, 43, 49, 52, 55, 58, 61, 63, 64, 67, 70, 73, 76, 79.
81 est composé.
Il y a 30 solutions.

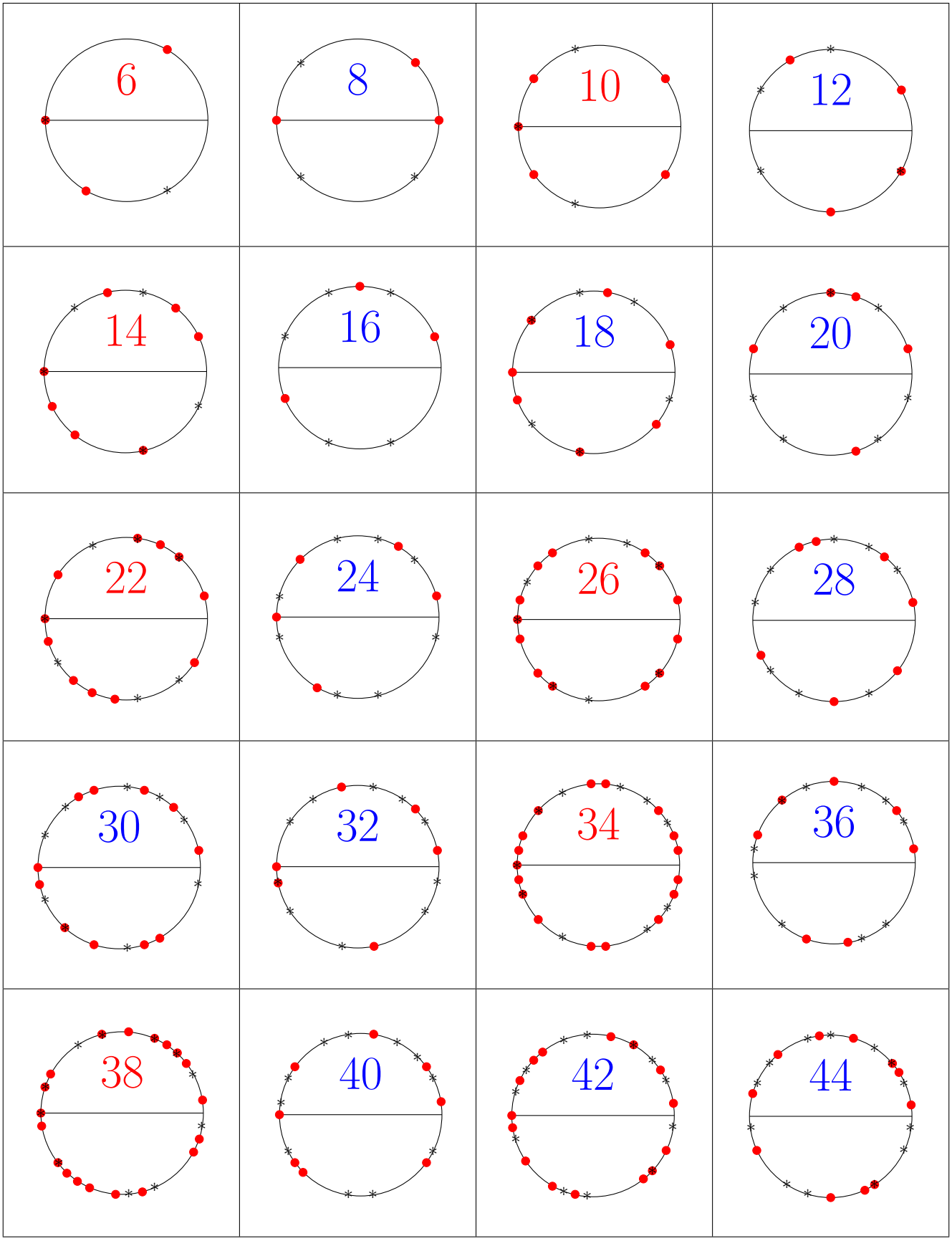


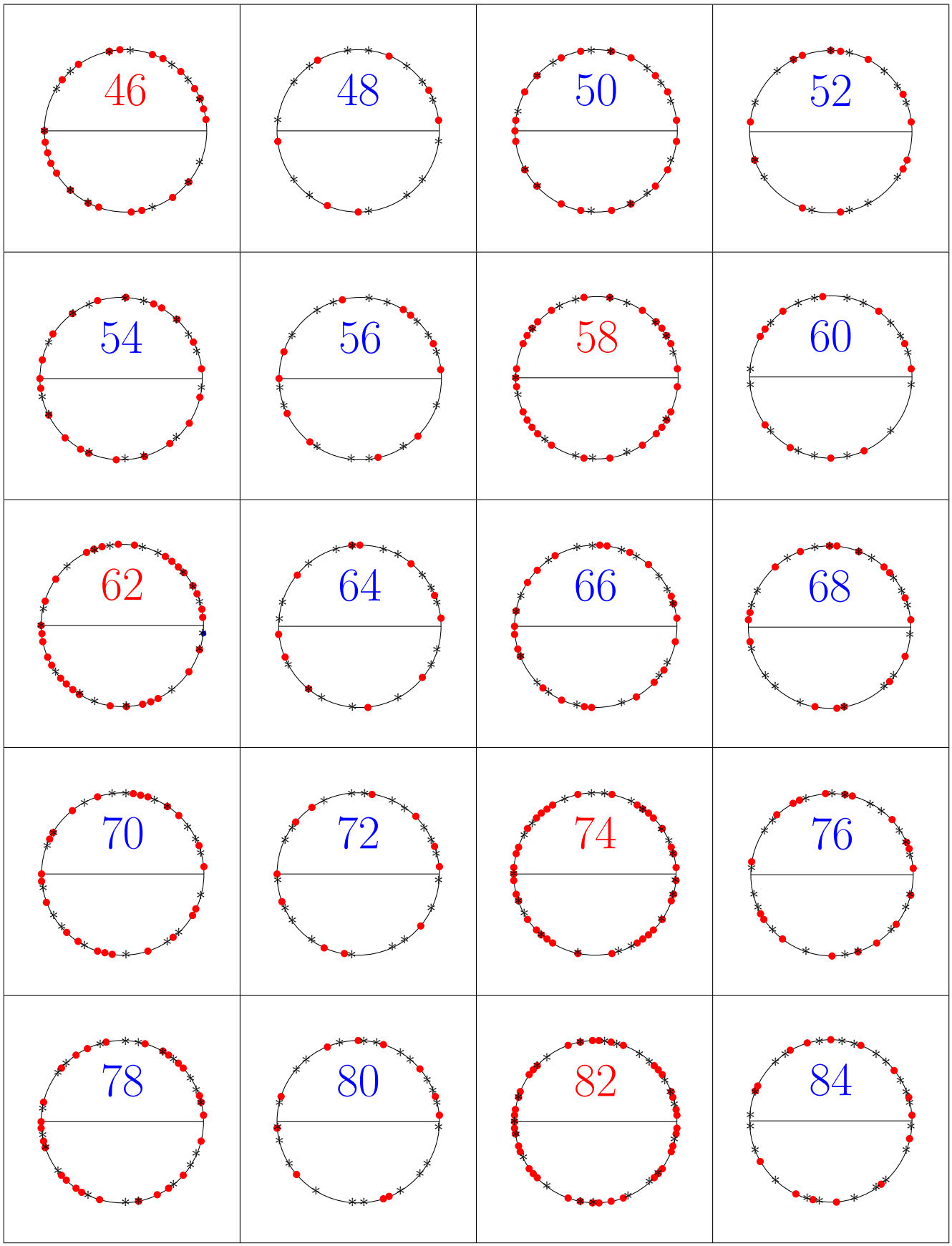
Solutions de $\exists k, x^2 \equiv k \ (mod\ 91)$: 1, 4, 9, 14, 16, 22, 23, 25, 29, 30, 35, 36, 39, 42, 43, 49, 51, 53, 56, 64, 65, 74, 77, 78, 79, 81, 88.
91 est composé.
Il y a 27 solutions.

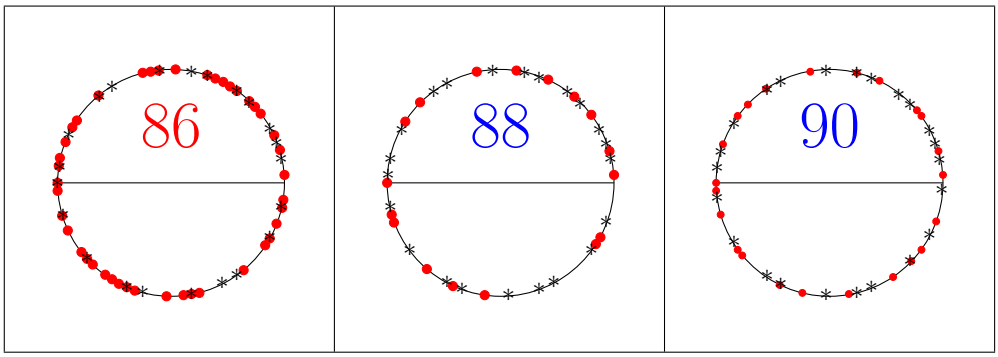


Résidus quadratiques sur colliers pour nombres pairs (Denise Vella-Chemla, 23.5.2019)

Pour chaque n pair sont fournies les résidus quadratiques de n, c'est-à-dire les solutions de l'équation $x^2 \equiv 1 \ (mod\ n)$, représentés par des points rouges ; les nombres premiers sont indiqués par des petites étoiles. Les doubles de premiers sont indiqués par leur gros nombre à l'intérieur du cercle coloré en rouge.

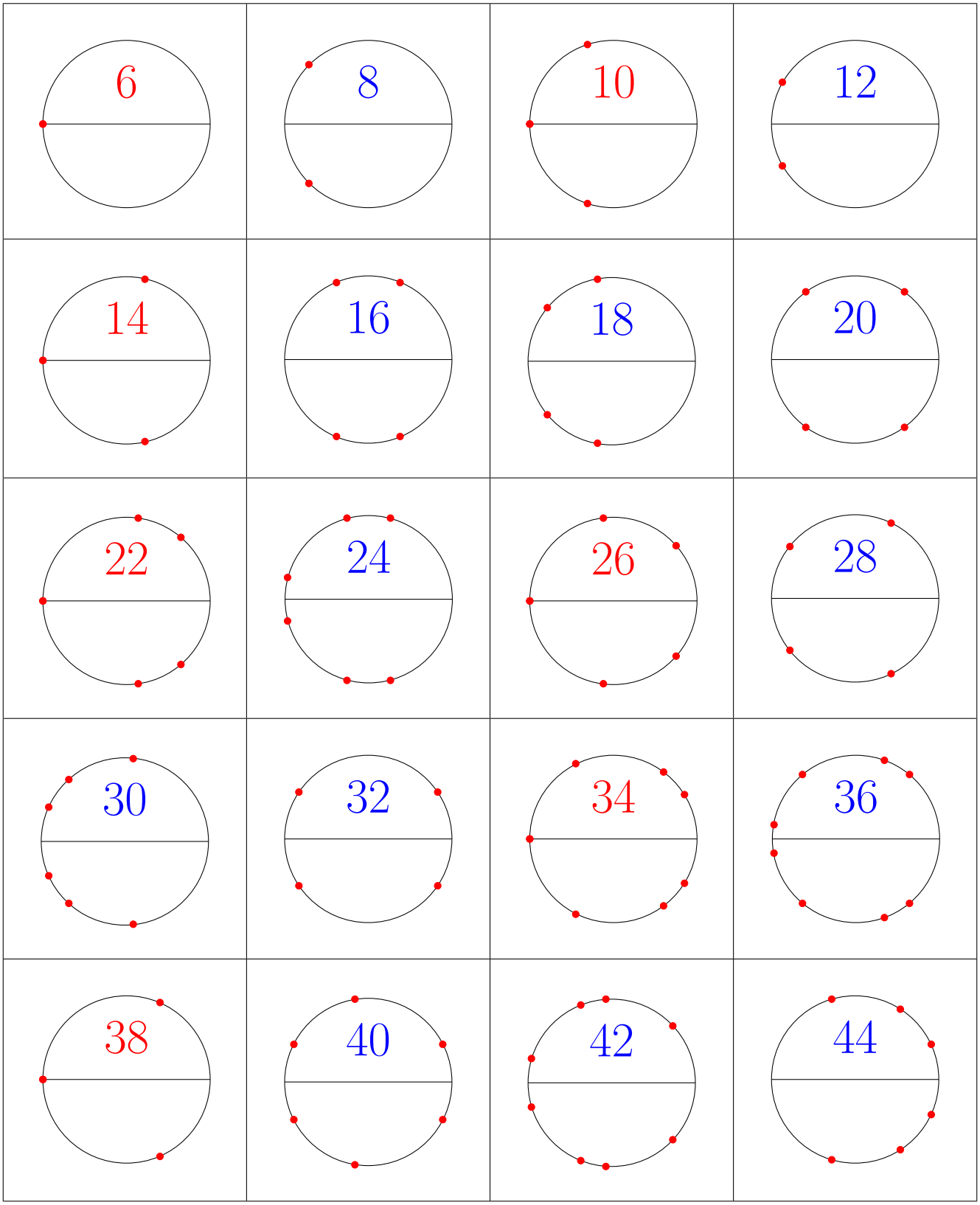


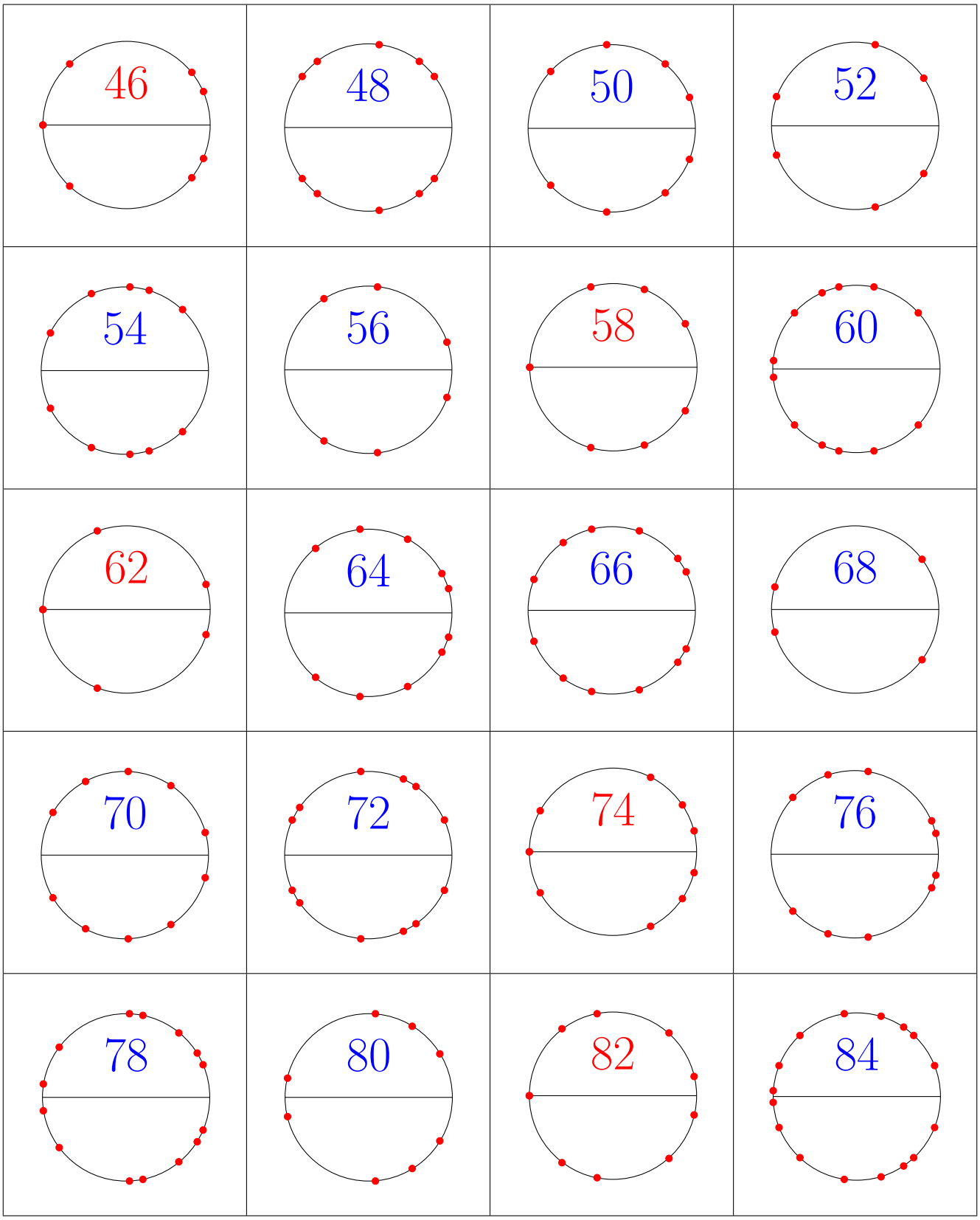

46
48
50
52
54
56
58
60
62
64
66
68
70
72
74
76
78
80
82
84

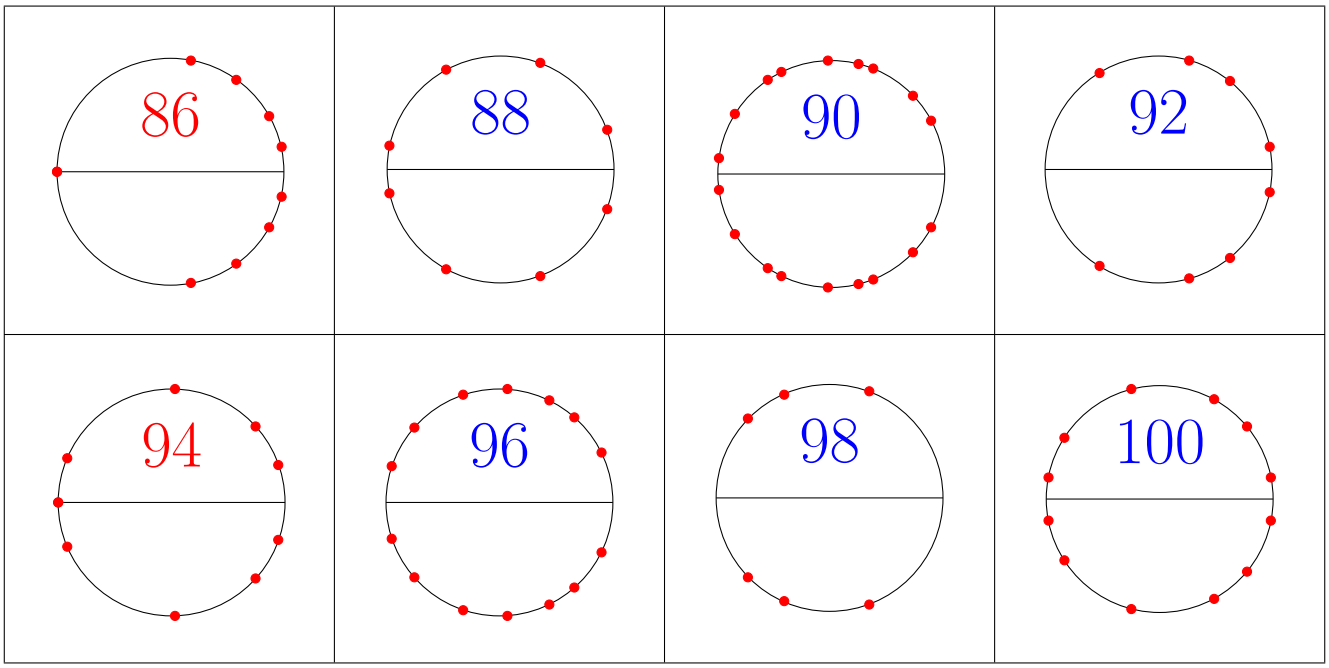

86
88
90

Décomposants de Goldbach sur colliers pour nombres pairs (Denise Vella-Chemla, 23.5.2019)

Pour chaque n pair sont fournies les décomposants de Goldbach de n, c'est-à-dire les solutions du système d'incongruences $x^2 - nx \not\equiv 0 \ (mod\ p)$, $\forall p\ premier < \sqrt{n}$. Les doubles de nombres premiers, qui vérifient trivialement la conjecture de Goldbach, sont écrits en rouge.




46
48
50
52
54
56
58
60
62
64
66
68
70
72
74
76
78
80
82
84

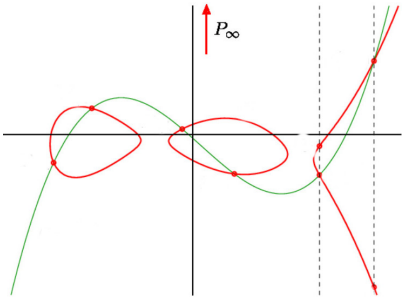

86
88
90
92
94
96
98
100

Ô stop ! (Denise Vella-Chemla, 31.5.2019)

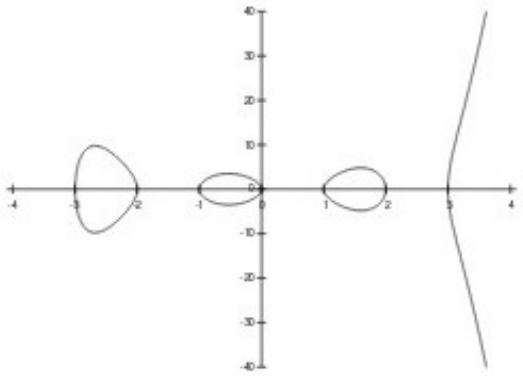
Il s'agit de garder en mémoire le fait qu'en calculant les indices de la section 53 des Recherches arithmétiques de Gauss (consultables ici http://denise.vella.chemla.free.fr/indices-RA53.pdf), on a réalisé à nouveau que la caractéristique des nombres premiers est d'avoir une solution au moins à l'équation $x^{\frac{p-1}{2}} \equiv 1 \ (mod \ p)$ (on peut réécrire cette congruence $x^{\frac{p-1}{2}} - kp - 1 = 0$), alors que cette équation n'a pas de solution pour p composé.

Cela permet d'associer à chaque nombre premier une courbe hyperelliptique de genre $\frac{p-1}{2}$ (ou une surface de Riemann à $\frac{p-1}{2}$ trous), selon les exemples ci-dessous.

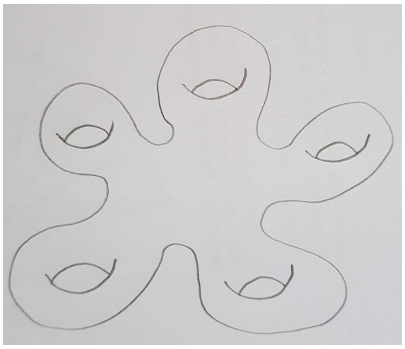
Exemple d'une courbe hyperelliptique de genre 2 associable au nombre premier 5



Exemple d'une courbe hyperelliptique de genre 3 associable au nombre premier 7



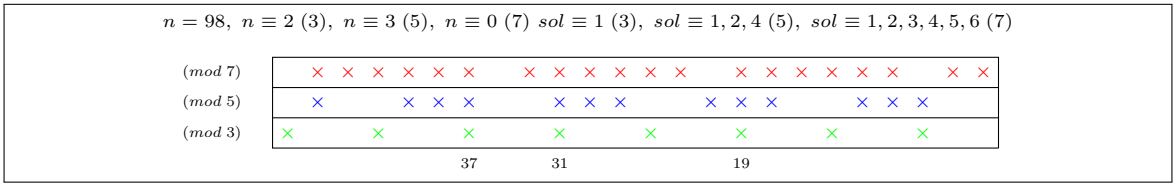
Exemple d'une surface de Riemann à 5 trous associable au nombre premier 11



Conjecture de Goldbach et les impairs (Denise Vella-Chemla, 2.6.2019)

Après avoir écouté une conférence de Timothy Gowers, présentant les leçons de Pólya pour résoudre un problème (ici https://vimeo.com/331192239), ainsi qu'un interview qu'il a donné dans le cadre des Heidelberg Laureate Forum (ici https://www.youtube.com/watch?v=7F97Q1DGOkE), on a l'idée d'appliquer des éléments de connaissance qui nous ont été utiles pour comprendre la conjecture de Goldbach forte (tout nombre pair supérieur à 6 est la somme de deux nombres premiers impairs) aux cas des nombres impairs et cela nous amène à une curieuse découverte. La conjecture de Goldbach pour les nombres impairs exprime que tout nombre impair est la somme de 3 nombres premiers. Harald Helfgott a proposé une démonstration de la conjecture de Goldbach pour les impairs en 2013. La conjecture de Goldbach pour les impairs découlerait trivialement de la conjecture de Goldbach forte (en effet, tout nombre impair étant la somme d'un nombre pair et de 3, si tout nombre pair était la somme de deux nombres premiers, alors tout nombre impair serait la somme de ces deux nombres premiers et de 3, et donc la somme de trois nombres premiers). Ce n'est pas à cela qu'on s'intéresse ici. Il s'agit plutôt d'étudier quel est le complémentaire à un nombre impair n d'un nombre premier qui n'a aucun reste commun avec n (dans les divisions par les nombres premiers inférieurs à $\sqrt{n}$).

Précisons l'idée : pour trouver les décomposants de Goldbach d'un nombre pair n, on a pris l'habitude d'utiliser un crible particulier : le crible d'élimination des restes modulaires de n ; par exemple, si on cherche les décomposants de Goldbach de 98, qui est égal à 2 modulo 3, à 3 modulo 5 et à 0 modulo 7, on va éliminer tous les nombres impairs qui sont égaux soit à 0 soit à 98, modulo 3 ou bien modulo 5 ou bien modulo 7. Ce faisant, on obtiendra tous les décomposants de Goldbach de 98 compris entre la partie entière de la racine carrée de 98 et la moitié de 98. On a symbolisé ceci par des petits dessins tels que celui ci-dessous, dans lequel les croix montrent les nombres impairs qui ne sont pas égaux à 0 ou bien à 98, modulo 3, modulo 5 et modulo 7.



On décide de réappliquer le même crible aux nombres impairs n, pour voir si le complémentaire d'un nombre premier p qui ne partagerait aucun de ses restes avec n impair aurait des propriétés particulières.

On utilise le programme suivant :

```
#include <iostream>
#include <stdio.h>
#include <math.h>

int tabfacteurs[2021], tabpuiss[2021], tabexpo[2021], residfacteurs[2021] ;

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 factorise(int i) {
  int k, p, nbdiv, tempo, expo ;
  int tab[2018] ;

  std::cout << i << "\n" ;
  tab[i] = 1 ;
  tabfacteurs[i] = 1 ;
  tabpuiss[i] = 1 ;
  tabexpo[i] = 1 ;
  tempo = i ; p = i/2 ; nbdiv = 1 ;
  if (prime(tempo)) {
      tabfacteurs[1] = tempo ;
      tabpuiss[1] = tempo ;
      tabexpo[1] = 1 ;
  }
  else while ((tempo > 1) && (p > 1)) {
           if ((prime(p)) && ((tempo%p) == 0)) {
               tabfacteurs[nbdiv] = p ;
               nbdiv = nbdiv+1 ;
               tempo = tempo/p ;
           }
           p=p-1 ;
  }
  if (not(prime(i))) nbdiv=nbdiv-1 ;
  if ((nbdiv == 1) && (prime(i))) {
      tabpuiss[1] = i ;
      tabexpo[1] = 1 ;
  }
  else if ((nbdiv == 1) && (not(prime(i)))) {
      tempo = tabfacteurs[1] ;
      tabpuiss[1] = i ;
      expo = 1 ;
      while (tempo < i) {
          tempo=tempo*tabfacteurs[1] ;
          expo = expo+1 ;
      }
      tabexpo[1] = expo ;
  }
  else if (nbdiv > 1) {
      for (k = 1 ; k <= nbdiv ; ++k) {
          tempo = tabfacteurs[k] ;
          expo = 1 ;
          while (((i % tempo) == 0) && (tempo < i)) {
              tempo=tempo*tabfacteurs[k] ;
              expo = expo+1 ;
          }
          tabpuiss[k] = tempo/tabfacteurs[k] ;
          tabexpo[k] = expo-1 ;
      }
  }
  for (k = nbdiv ; k >= 1 ; --k) {
      std::cout << tabfacteurs[k] << "^" ;
      std::cout << tabexpo[k] << "." ;
  }
}

int main (int argc, char* argv[]) {
  int x, y, module ;
  bool restesdifferents ;

  for (x = 7 ; x <= 2020 ; x = x+2) {
      std::cout << "\n\n" << x << "␣-->␣\n" ;
      for (y = sqrt(x) ; y <= x/2 ; ++y)
        if (prime(y)) {
            restesdifferents = true ;
            for (module = 3 ; module <= sqrt(x) ; module = module+2) {
                if (prime(module))
                  restesdifferents = restesdifferents && ((x % module) != (y % module)) ;
            }
            if (restesdifferents) {
                std::cout << "\n" << y << "␣+␣" ;
                factorise(x-y) ;
                std::cout << "\n" ;
            }
        }
  }
}
```

Le résultat de ce programme est consultable ici : http://denise.vella.chemla.free.fr/resetlesimpairs.pdf.

On constate avec surprise qu'il semblerait qu'un nombre impair puisse toujours s'écrire $p_1 + 2^k p_2$ avec $k \geq 1$ et p_1 et p_2 premiers. Cette constatation est peut-être aussi difficile à démontrer que la conjecture de Goldbach.

L'intérêt cependant d'une telle découverte, si elle s'avérait juste, est simplement qu'elle fournit une généralisation de la conjecture de Goldbach, la conjecture forte pour les pairs pouvant être vue comme une réécriture de la formule proposée pour les impairs, avec $k = 0$, i.e. pouvant s'écrire pour tout n pair supérieur ou égal à 6, selon une écriture de la forme $n = p_1 + 2^0 p_2$.

Tentative de démonstration du fait que s'il existe, pour un nombre impair donné n, un nombre premier $p_1 \leq \frac{n}{2}$ qui lui est incongru selon tout module inférieur à sa racine carrée, alors le complémentaire à n de p_1 est un nombre de la forme $2^k p_2$ avec p_2 premier et $k \geq 1$

Soit n un nombre impair et supposons qu'il existe une décomposition additive de n de la forme $p_1 + n'$ avec $p_1 \not\equiv n \ (mod\ m)$ pour tout m premier tel que $3 \leq m \leq \sqrt{n}$. Montrons qu'n' est alors nécessairement de la forme $2^k p_2$ avec $k \geq 1$ et p_2 premier.

n étant impair, n' est forcément pair. Voyons pourquoi, sous la condition que p_1 existe, alors n' ne contient dans sa factorisation qu'un seul nombre premier (qu'on appellera p_2), en plus d'un certain nombre d'occurrences du facteur premier 2. On a :

$$\frac{n}{2} \leq n' \leq n$$

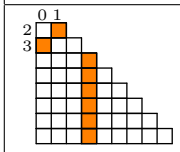
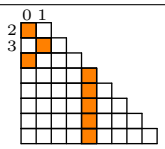
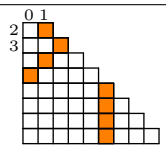
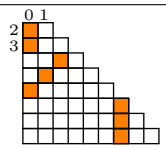
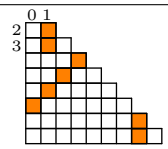
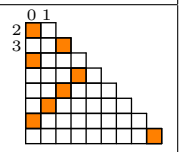
et

$$p_1 \not\equiv n \ (mod\ m) \text{ pour tout } m \text{ premier tel que } 3 \leq m \leq \sqrt{n} \qquad (1)$$

Cela a pour conséquence que les deux diviseurs premiers autres que 2 de n' devraient être supérieurs à $\sqrt{n}$ (car (1) $\iff$ $n - p_1 \not\equiv 0 \ mod\ m$ avec les mêmes conditions) ; mais si tel était le cas, i.e. si $n' = 2p'p''$ avec $p' > \sqrt{n}$ et $p'' > \sqrt{n}$ alors n' serait supérieur à $2n$, ce qui est en contradiction avec l'hypothèse $\frac{n}{2} \leq n' \leq n$. Le complémentaire de p_1 à n est alors forcément de la forme $2^k p_2$ avec $k \geq 1$ et p_2 premier impair. On n'est cependant pas assuré de l'existence obligatoire de p_1.

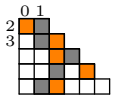
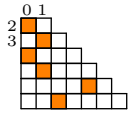
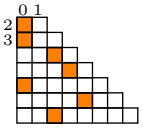
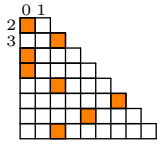
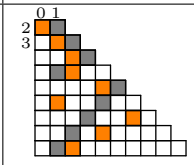
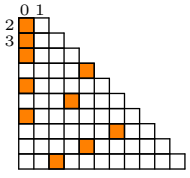
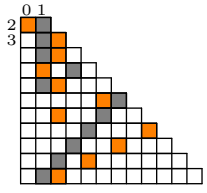
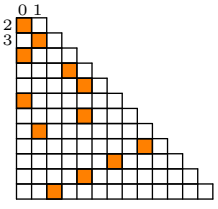
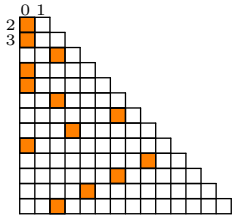
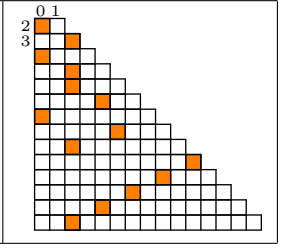
Tores trapézoïdaux (Denise Vella-Chemla, 9.6.2019)

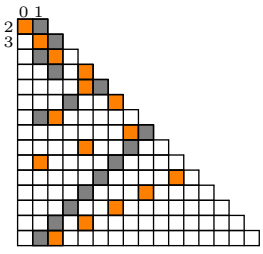
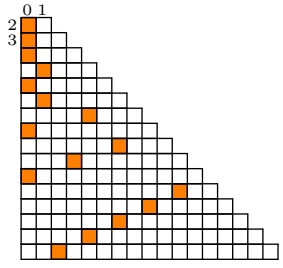
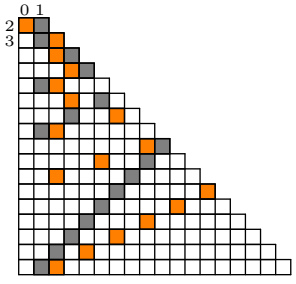
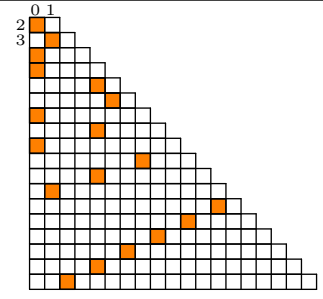
On observe d'abord des pixels qui avancent dans un tore trapézoïdal de taille donnée (utile par exemple si on cherche les décomposants de Goldbach de 20).
Les indices des colonnes de chaque tore trapézoïdal représenté par une matrice triangulaire basse de pixels sont égaux à 0, 1, 2, etc.
Les indices des lignes sont égaux à 2, 3, etc.
Le pixel $[i, j]$ de la matrice de n est orange si $n \equiv i \ (mod\ j)$.
Chaque pixel arrivant au bout d'une ligne à droite est ramené à l'extrémité gauche de la ligne et se remet à parcourir la ligne de gauche à droite.

$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
					

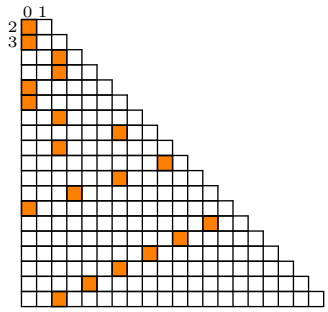
On fournit ci-dessous les tores associés aux seuls nombres pairs. Pour voir le mouvement d'un pixel d'un tore à l'autre, rappelons-nous qu'il saute une case de nombre pair en nombre pair. On montre pour les nombres pairs $2p$ (en orange) doubles d'un nombres premier p (en gris) ce dcomposant de Goldbach trivial puisque $2p = p + p$.

Sont décomposants de Goldbach d'un nombre pair n les nombres premiers dont le tore coupé à $n/2$ n'a aucun pixel commun avec celui de n. Un nombre premier est caractérisé par le fait que la colonne d'indice 0 de ses tores (quelle que soit leur taille) ne contient qu'un seul pixel à 1. Dans les trapèzes de pixels ci-dessous, on a également détaillé que 11 est décomposant de Goldbach de 54, que 47 est un décomposant trivial de 94 (pour montrer la diagonale de pixels d'un nombre premier, là 47, dans le bas du graphique).

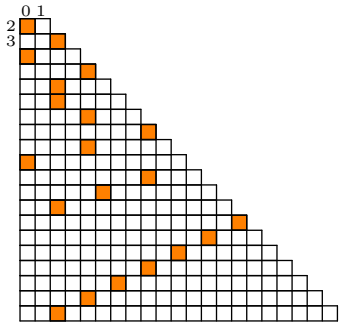
14 : 3, 7	16 : 3, 5	18 : 5, 7	20 : 3, 7	22 : 3, 5, 11
				
24 : 5, 7, 11	**26 : 3, 7, 13**	**28 : 5, 11**	**30 : 7, 11, 13**	**32 : 3, 13**
				

34 : 3, 5, 11, 17	36 : 5, 7, 13, 17	38 : 7, 19	40 : 3, 11, 17
			

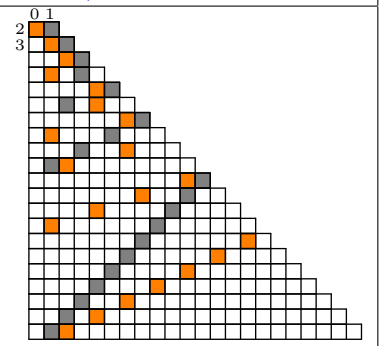
42 : 5, 11, 13, 19



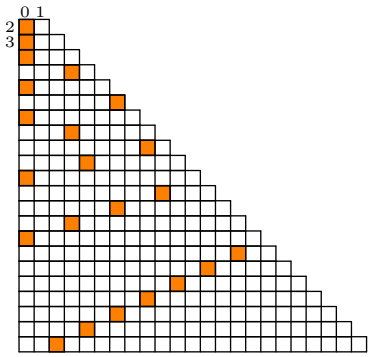
44 : 7, 13



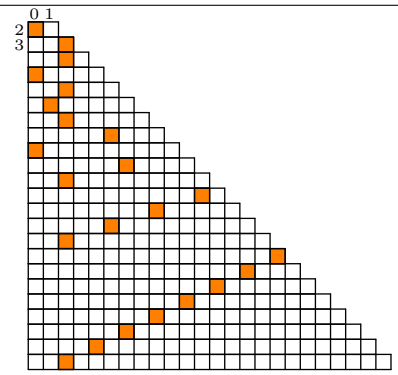
46 : 17, 23



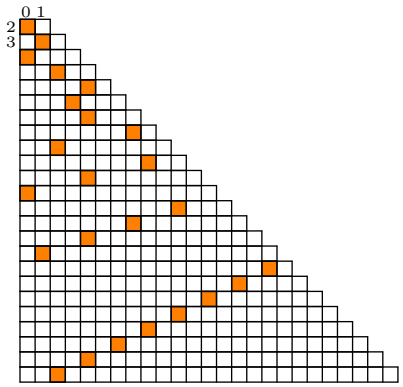
48 : 7, 11, 17, 19



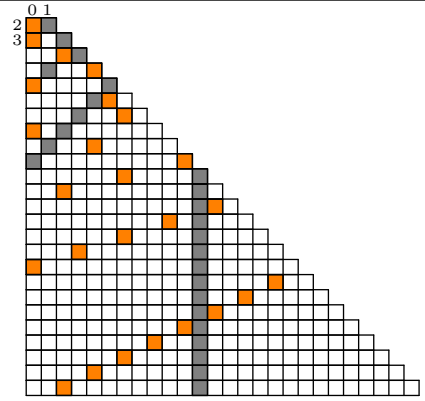
50 : 7, 13, 19



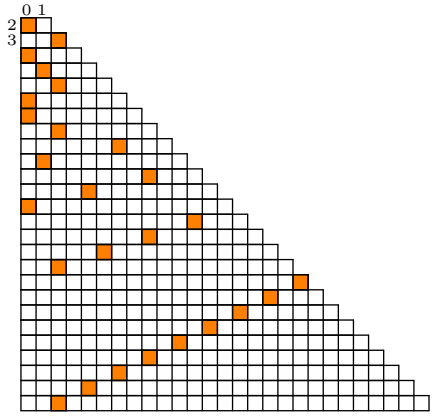
52 : 11, 23



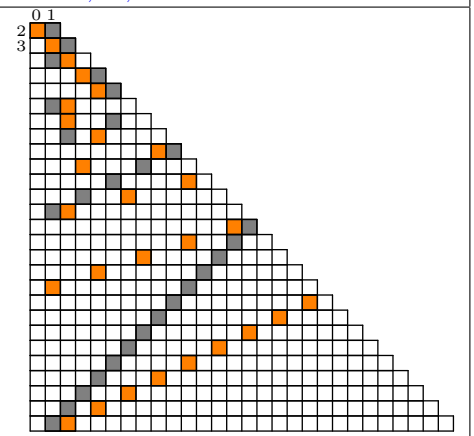
54 : 7, 11, 13, 17, 23



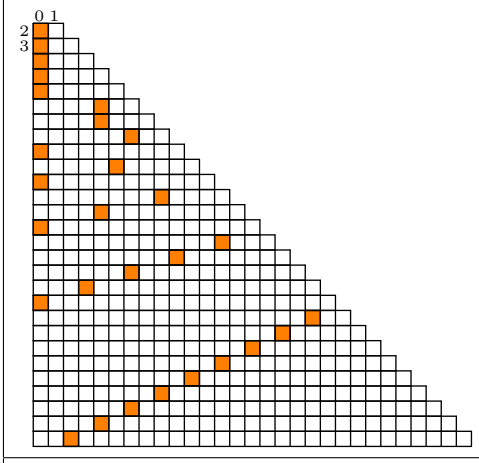
56 : 13, 19



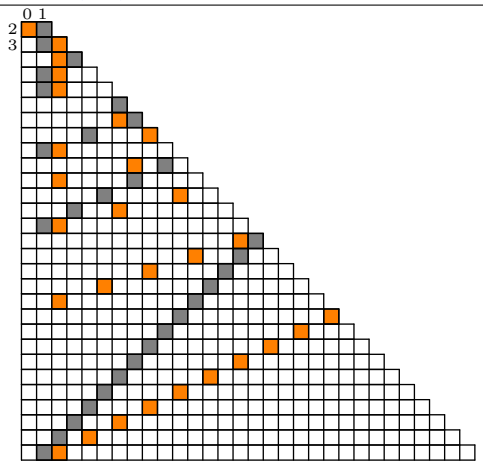
58 : 11, 17, 29



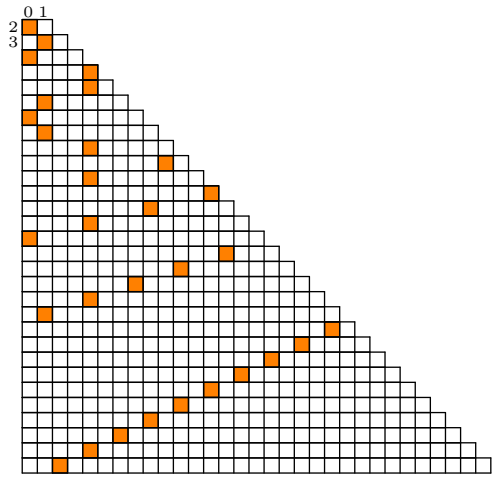
60 : 7, 11, 13, 17, 19, 23, 29



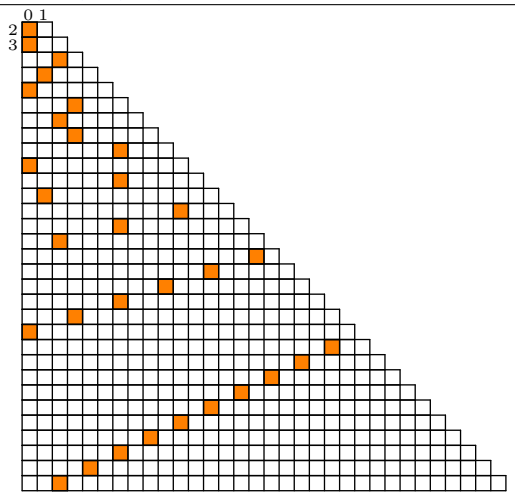
62 : 13, 19, 31



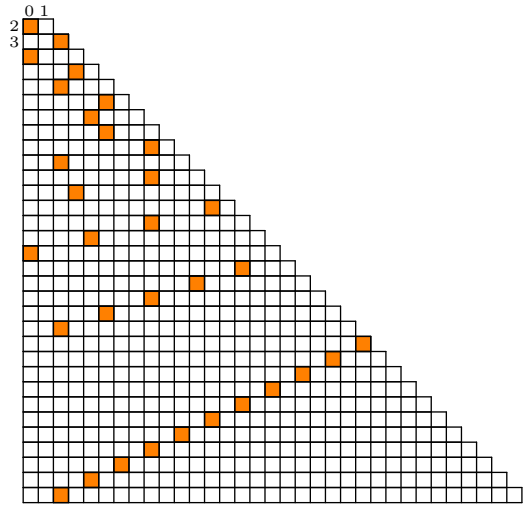
64 : 11, 17, 23



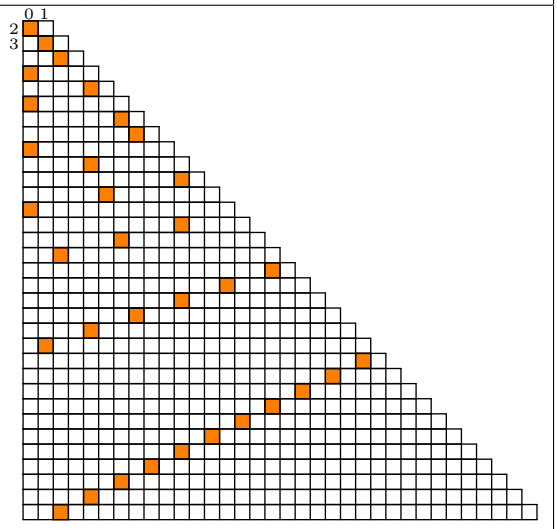
66 : 13, 19, 23, 29

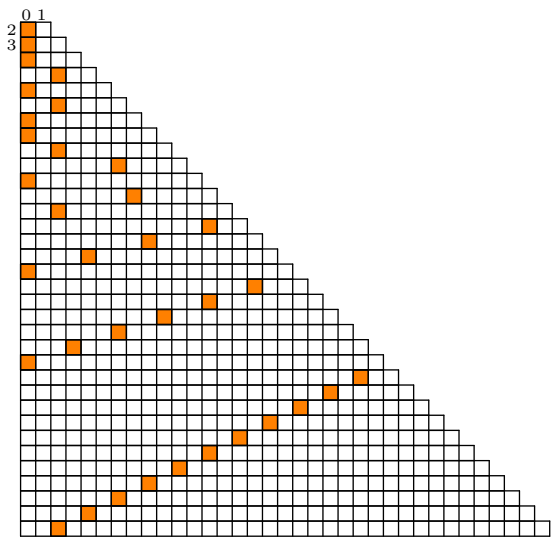
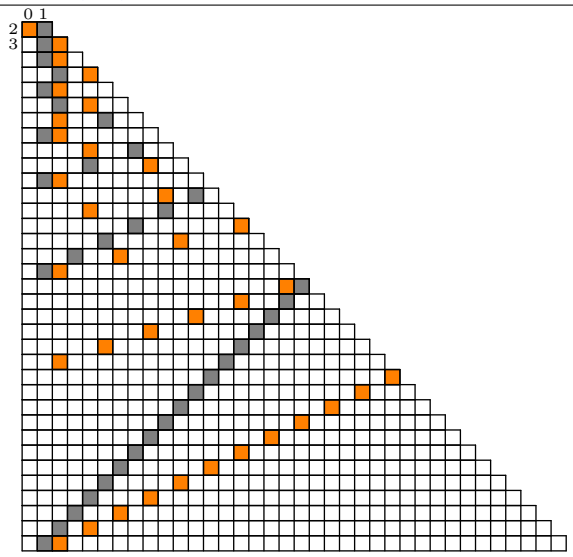
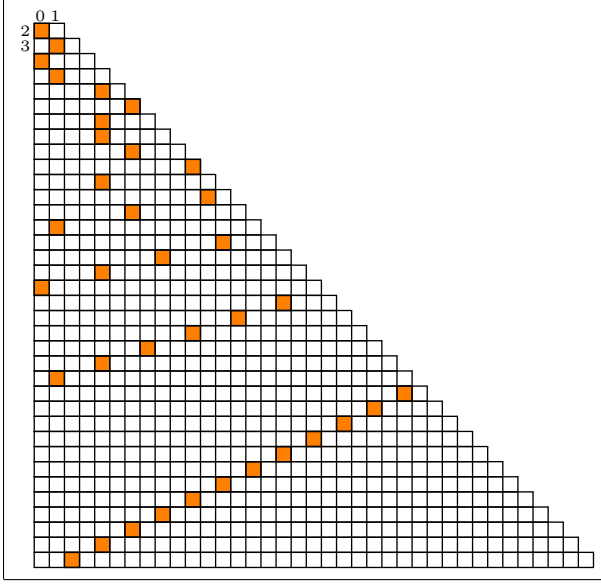
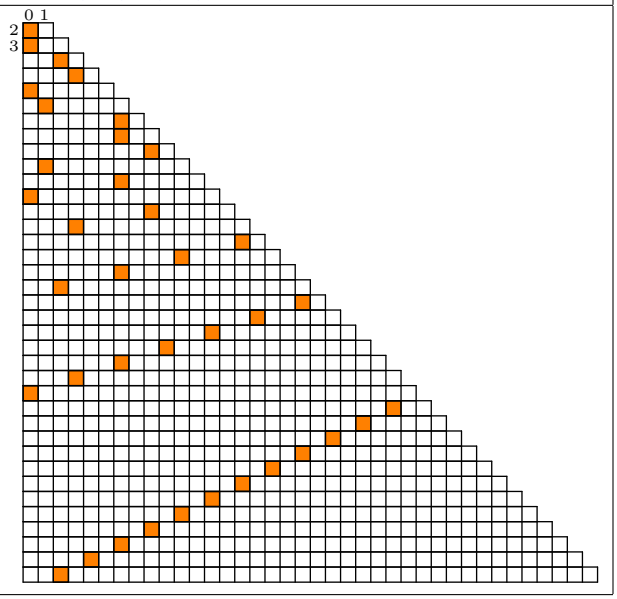


68 : 31

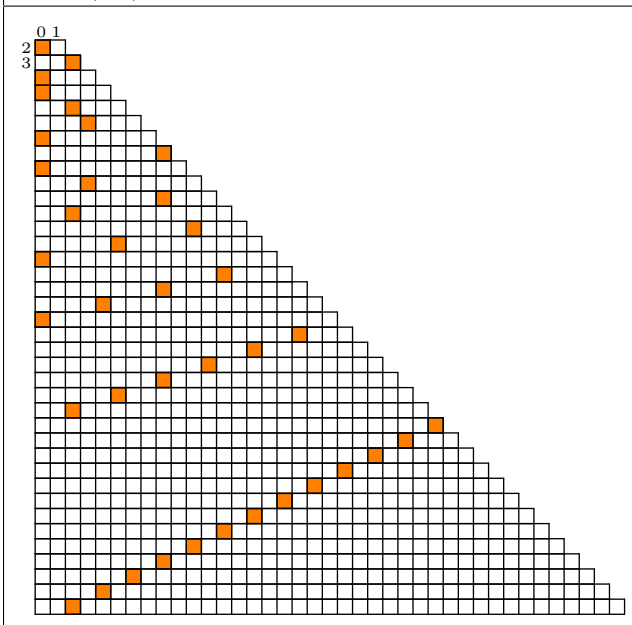


70 : 11, 17, 23, 29

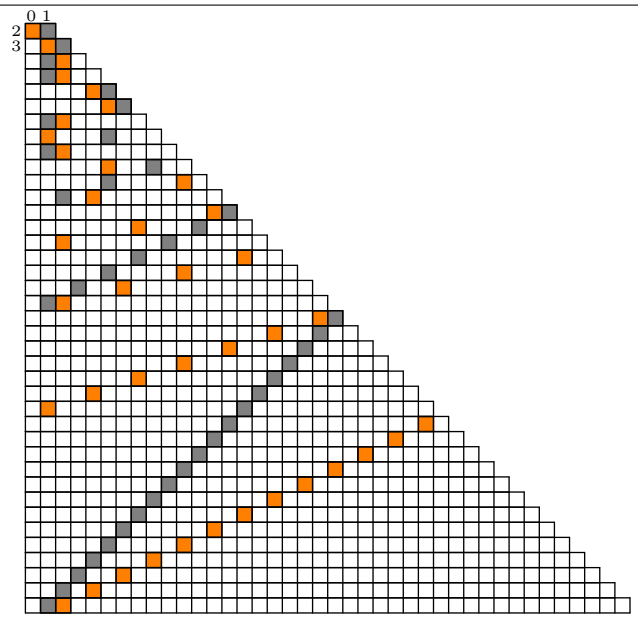


$72 : 11, 13, 19, 29, 31$	$74 : 13, 31, 37$
	
$76 : 17, 23, 29$	$78 : 11, 17, 19, 31, 37$
	

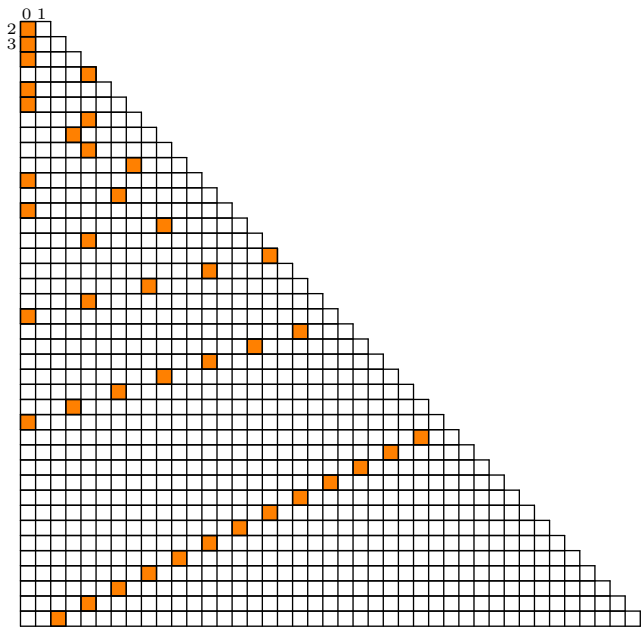
80 : 13, 19, 37



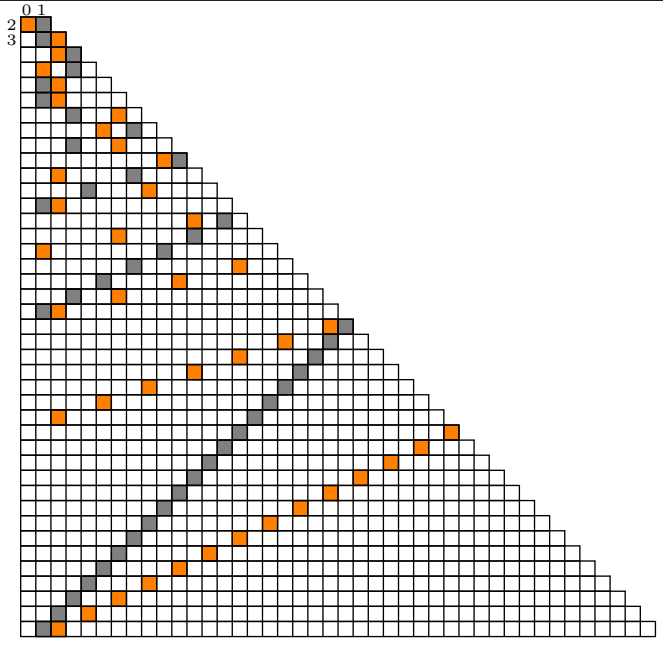
82 : 11, 23, 29, 41



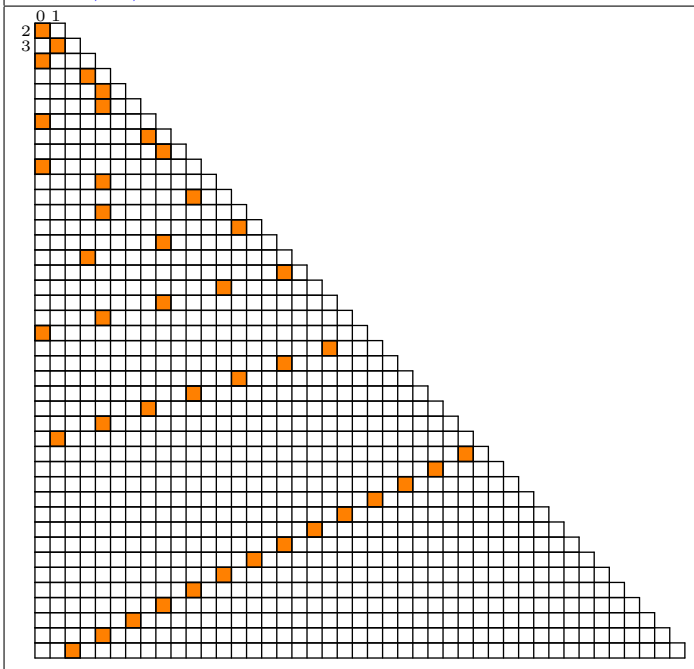
84 : 11, 13, 17, 23, 31, 37, 41



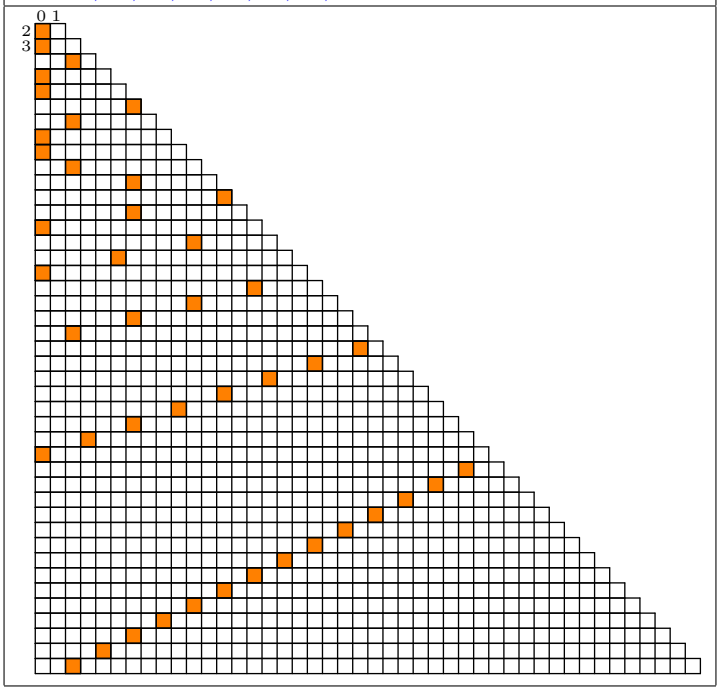
86 : 13, 19, 43



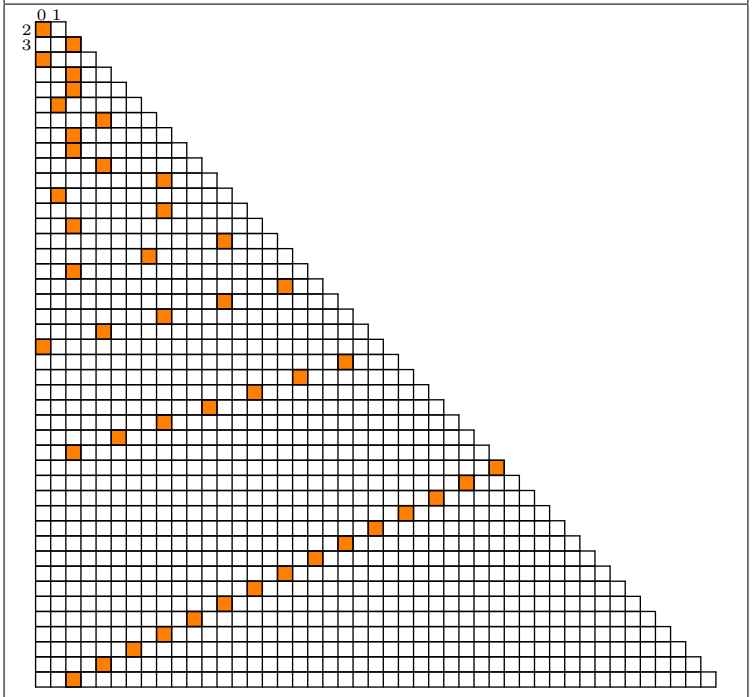
88 : 17, 29, 41



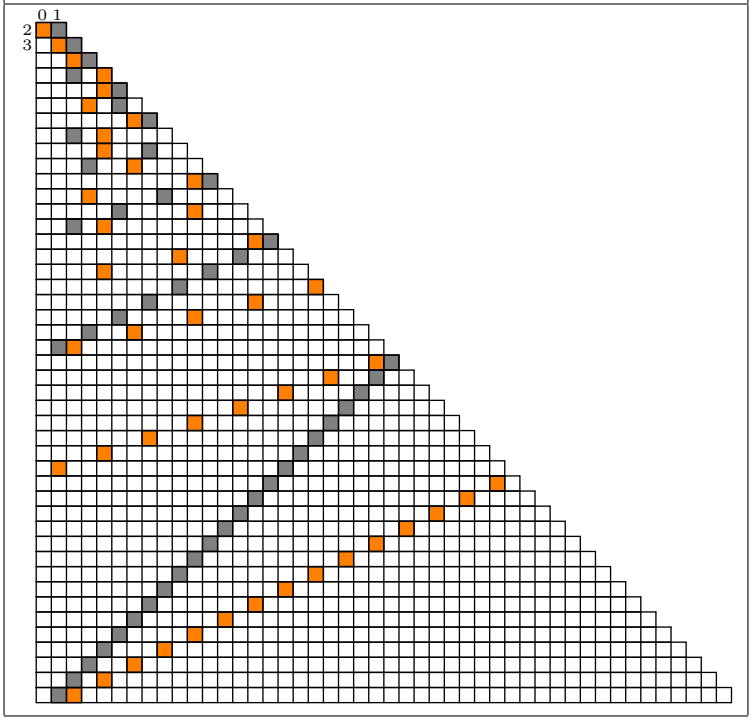
90 : 11, 17, 19, 23, 29, 31, 37, 43



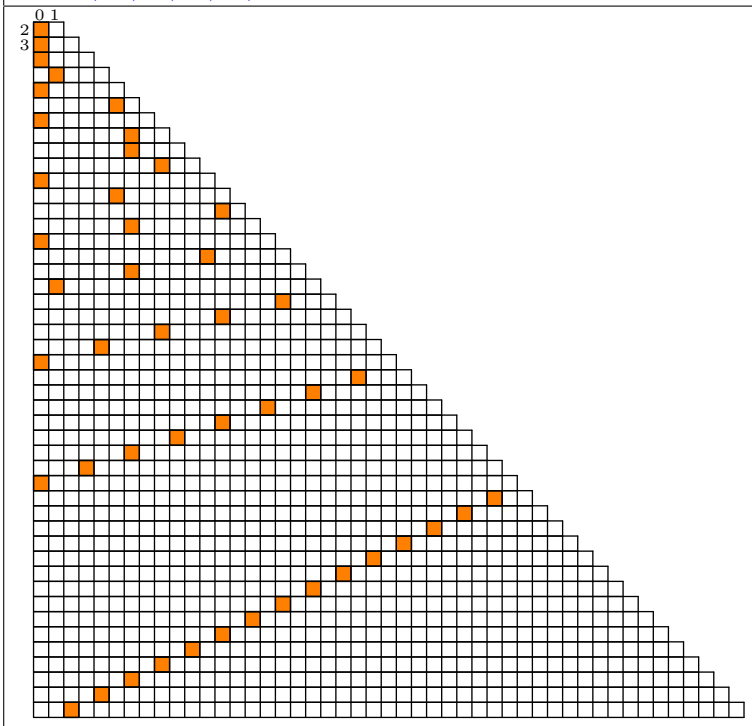
92 : 13, 19, 31



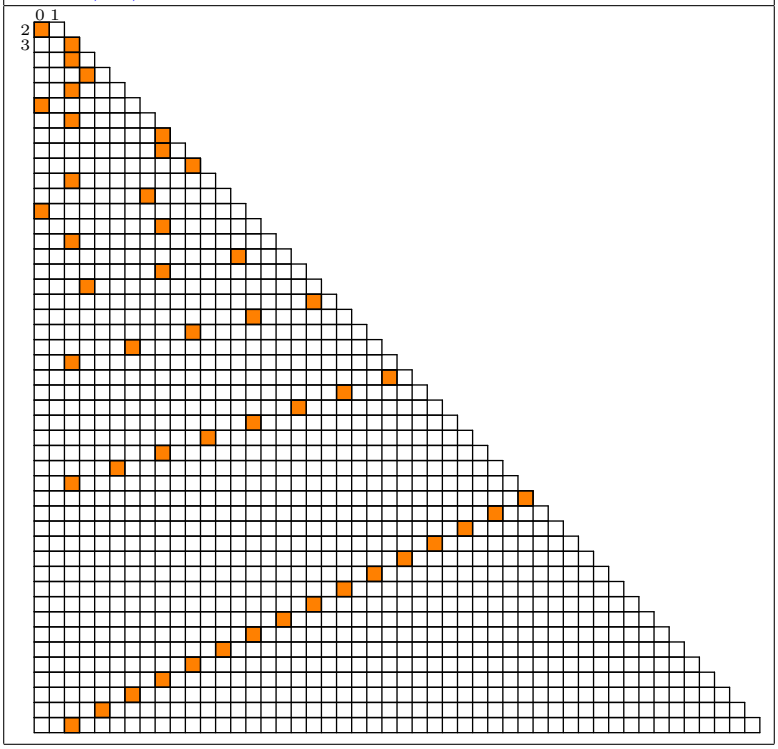
94 : 11, 23, 41, 47



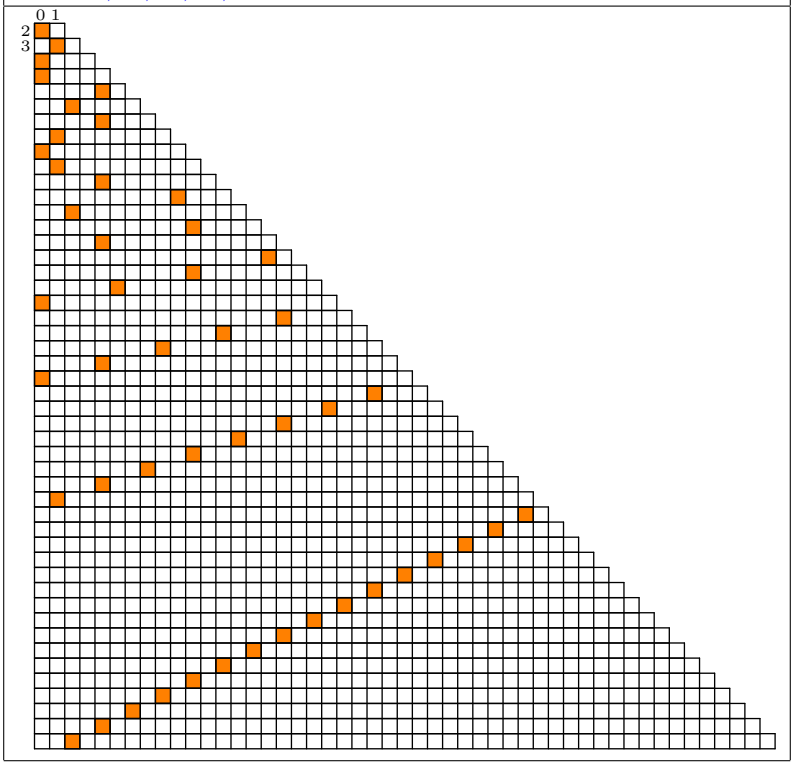
96 : 13, 17, 23, 29, 37, 43



98 : 19, 31, 37

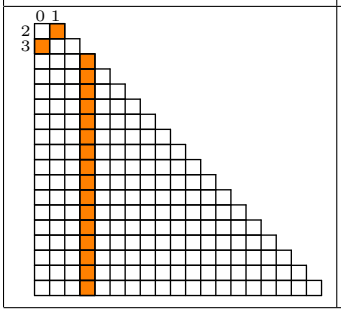


100 : 11, 17, 29, 41, 47

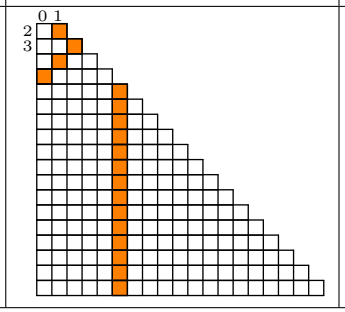


Ci-dessous, on peut observer les tores des nombres premiers 3, 5, 7, 11, 13, 17, 19 à la recherche des décomposants de Goldbach de 40.

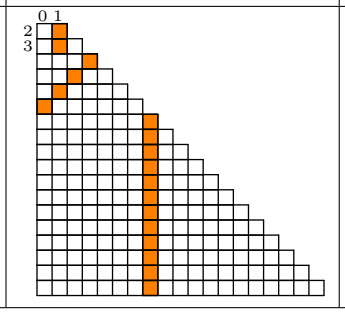
$n = 3$



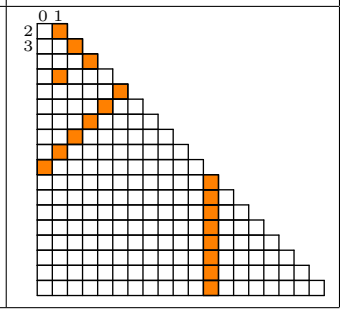
$n = 5$



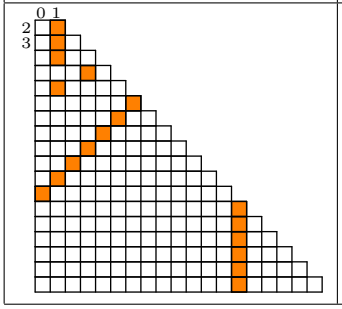
$n = 7$



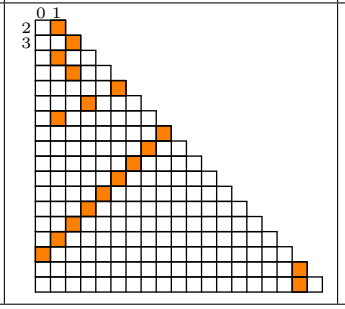
$n = 11$



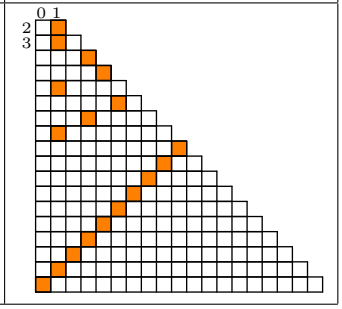
$n = 13$



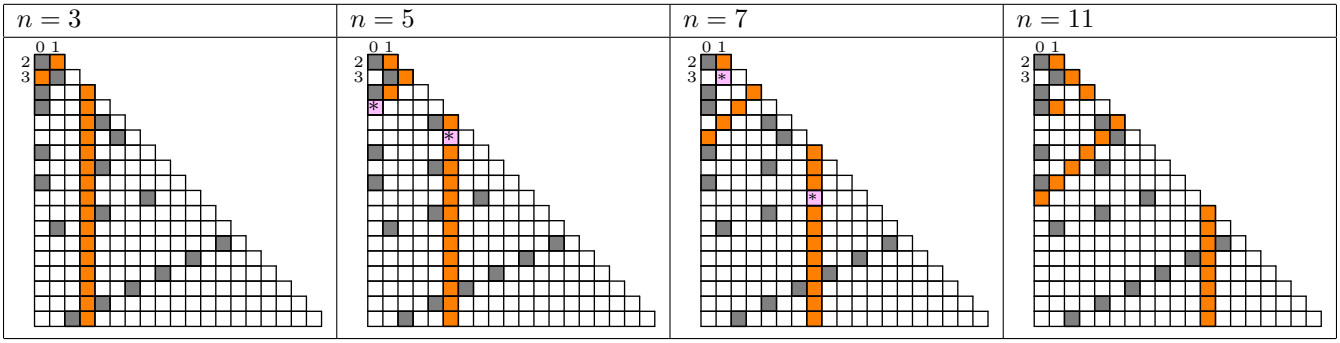
$n = 17$

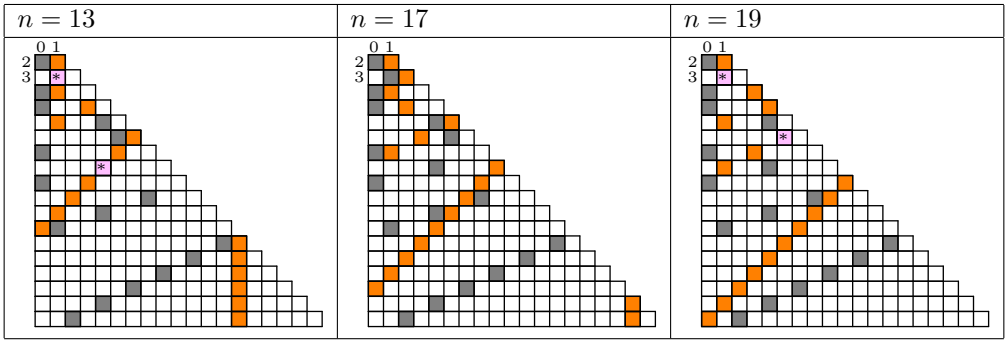


$n = 19$



Les mêmes tores des nombres premiers 3, 5, 7, 11, 13, 17, 19 avec en transparence (gris) le tore de 40 pour voir les conflits empêchant 5, 7, 13 et 19 d'être décomposants de Goldbach de 40.





Un nombre premier devant éviter les pixels colorés d'un nombre pair pour pouvoir le décomposer, on peut compter le nombre de pixels colorés à éviter : il y en a $\dfrac{n}{\dfrac{(n+1)(n+2)}{2} - 1} = \dfrac{2}{n+3}$.

Le nombre de pixels à éviter est ainsi de plus en plus petit au fur et à mesure de l'augmentation de n. Ceci est un argument supplémentaire en faveur du fait que la conjecture de Goldbach est en quelque sorte probabilistiquement de plus en plus vraie.

Cette connaissance un peu plus précise qu'on a du processus à l'œuvre, qui permet à un nombre d'être ou de ne pas être un décomposant de Goldbach d'un nombre pair, amène à des calculs différents de ceux qu'on a proposés dans http://denise.vella.chemla.free.fr/denitac.pdf.

Fournissons quelques exemples pour fixer les idées : plaçons nous dans la ligne de pixels d'un nombre premier p. On a vu que x a un reste valide pour être un décomposant de Goldbach de n si le pixel de x dans la ligne correspondant au nombre premier p est à la fois différent de 0 et différent du pixel de n.

Fixons $p = 5$. Il y a 5^2 possibilités de restes, i.e. de pixels possibles pour x et n qui sont

$$\begin{array}{c}(0,0),(0,1),(0,2),(0,3),(0,4),\\(1,0),(1,1),(1,2),(1,3),(1,4),\\(2,0),(2,1),(2,2),(2,3),(2,4),\\(3,0),(3,1),(3,2),(3,3),(3,4),\\(4,0),(4,1),(4,2),(4,3),(4,4).\end{array}$$

Là, on a le choix entre deux possibilités :

- soit on a la connaissance que x est un nombre premier, auquel cas son pixel est différent de 0 et il a 16 possibililités sur les 20 possibilités restantes d'avoir son pixel différent de celui de n, c'est-à-dire qu'il a $\dfrac{(p-1)^2}{p(p-1)} = \dfrac{p-1}{p}$ chances que ça soit le cas et il faut faire le produit de tous ces $\dfrac{p-1}{p}$ pour

avoir le nombre de chances total selon tous les nombres premiers ; on trouve une minoration du produit $\prod \frac{p-1}{p}$ dans [1]. Il faut multiplier cette minoration par la minoration de $\pi(\frac{n}{2})$, qui est $\frac{\frac{n}{2}}{ln\,\frac{n}{2}}$ (minoration fournie par la même référence).

- soit on n'a pas la connaissance que x est un nombre premier et x doit alors éviter deux pixels sur chaque ligne d'un nombre premier, et celui de n, et le pixel 0, de façon à assurer d'une part que x soit un nombre non divisible par tout nombre premier inférieur à $\sqrt{n}$, ce qui le rendra premier quant à lui ; d'autre part, pour ne pas avoir son pixel identique à celui de n, il y a toujours 16 possibilités qui conviennent pour x mais elles sont à ramener aux 25 possibilités totales, selon la formule $\frac{(p-1)^2}{p^2} = \left(\frac{p-1}{p}\right)^2$. Dans ce cas-là, on n'arrive pas à raisonner plus avant car les nombres étant inférieurs à 1, la minoration du produit des $\frac{p-1}{p}$ ne permet pas d'obtenir une minoration pour le produit de leur carré.

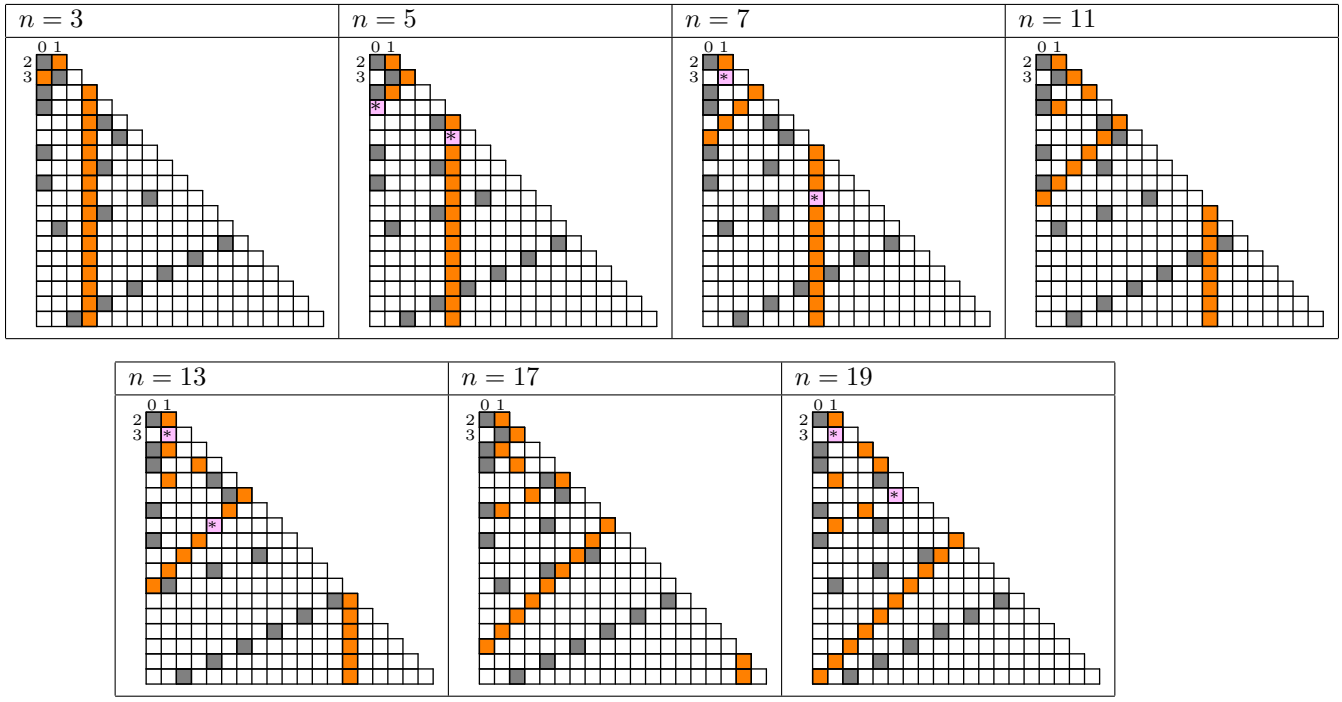
Référence

[1] J. B. Rosser et L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, dedicated to Hans Rademacher for his seventieth birthday, Illinois J. Math., Volume 6, Issue 1 (1962), 64-94.

```
import numpy as np
import math
from math import sqrt

pasdg = np.zeros((102), dtype='i')
tab=np.zeros((102,102,102),dtype='i')
for n in range(6,102,2):
    print('val de reference : '+str(n))
    for y in range(2,n/2+1):
        for z in range(0,y):
            if ((n % y) == z):
              tab[n][y][z] = 1
            print(str(tab[n][y][z])),
        print('')
    print('bzzzz')
    for x in range(3,n/2+1):
        pasdg[x] = 0
      for y in range(2,n/2):
          for z in range(0,y):
            tab[x][y][z] = 0
            if ((x % y) == z):
                tab[x][y][z] = 1
                if (tab[n][y][z] == 1):
                        pasdg[x] = 1 ;
          if (tab[x][y][0] == 1) and (x != y):
            pasdg[x] = 1
    for x in range(3,n/2+1):
        print(str(x))
        for y in range(2,n/2+1):
            for z in range(0,y):
                print(str(tab[x][y][z])),
            print('')
        print('')
    for x in range(3,n/2+1,2):
      if (pasdg[x] == 0):
        print(str(x)+" dg de "+str(n))
    print('')
```

Matrices de pixels (Denise Vella-Chemla, 13.6.2019)

On a présenté ici http://denise.vella.chemla.free.fr/pixels2.pdf une modélisation de la recherche de décomposants de Goldbach par ce qu'on a appelé les tores trapézoïdaux : il s'agit de lignes de pixels circulant (au sens donné à la notion de matrice circulante) et qui parfois, pour deux tores donnés, en l'occurrence celui d'un nombre pair et celui d'un décomposant potentiel de ce nombre pair, voient certains de leurs pixels coïncider ou pas.
Ci-dessous, on peut observer les tores des nombres premiers 3, 5, 7, 11, 13, 17, 19 à la recherche des décomposants de Goldbach de 40.
On a noté les restes de 40 en gris et les restes des nombres premiers en orange sauf lorsque les deux couleurs coïncidaient sur un même pixel qu'on a alors noté en rose pour bien voir les conflits ; de tels conflits empêchent 5, 7, 13 et 19 d'être décomposants de Goldbach de 40 et l'absence de conflits permet à 3, 11 et 17 d'être des décomposants de Goldbach de 40.



Voyons maintenant comment représenter les transformations opérées dans chaque ligne par des opérateurs matriciels :

- à la première ligne, qui correspond à la parité des nombres qui se succèdent selon le rythme pair, impair, pair, impair, etc..., on associe l'opérateur $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$;
  on a ainsi $\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{2k+1} = \begin{pmatrix} 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{2k} = \begin{pmatrix} 1 & 0 \end{pmatrix}$;
- à la seconde ligne, qui correspond à la divisibilité des nombres par 3 qui se succède au rythme oui, non, non, oui, non, non, etc..., on associe l'opérateur $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$;
  on a ainsi $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^{3k+1} = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^{3k+2} = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^{3k} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$;

- à la ligne p, on associe l'opérateur matriciel à p lignes et p colonnes qui contient un 1 en bas à gauche et une diagonale de 1 à droite de la diagonale principale, tous ses autres éléments étant nuls ; il permet de faire "circuler" le bit 1 de place en place à droite vers le bout de la ligne et de le ramener au début de la ligne lorsque le bout de la ligne est atteint ;

Pour trouver les décomposants de Goldbach du si petit nombre 40, on est amené à fabriquer une matrice plutôt grosse (de taille 190×190 puisque $\frac{19\times 20}{2} = 190$) qu'on appellera G ; cette matrice contient les différents opérateurs $M1$, $M2$, etc., M_{19} bien alignés sur sa diagonale, on l'appelle matrice diagonale par blocs.

On voit alors que selon cette modélisation, 17 est un décomposant de Goldbach de 40 pour la raison très simple suivante : appelons L_1 la longue matrice à une seule ligne contenant les bits suivants :

10100100010000100000...1000000000000000000

Cette matrice modélise le nombre 1, elle contient des bits 1 entre lesquelles sont intercalés un bit 0, puis 2, puis 3, puis 4, etc. jusqu'à 18 bits 0 sur sa dernière ligne (c'est une matrice de $n/2-2$ lignes avec $n = 40$).

La matrice associée au nombre 17 s'obtient en multipliant la matrice A par la matrice G élevée à la puissance 17, la matrice associée au nombre 40 s'obtient en multipliant la matrice A par la matrice G élevée à la puissance 40. Pour que 17 soit un décomposant de Goldbach de 40, il faut que $A.G^{17}$ et $A.G^{40}$ ne contiennent aucun bit 1 à une position commune, ce qui peut s'exprimer par le fait que leur produit est nul. On peut aussi exprimer cette condition en utilisant la distance de Hamming, qui compte les bits différents de deux chaînes de caractères, et qui en l'occurrence doit être égale à $n - 6$ lorsqu'on cherche un décomposant de Goldbach de n.

On est ainsi ramené à la théorie des langages, à l'origine de l'informatique, dans la mesure où il s'agit, pour trouver un décomposant de Goldbach d'un nombre pair, de lire des chaînes de booléens et de repérer si elles contiennent des lettres 1 à des positions identiques.

Voici la forme générale de la matrice G.

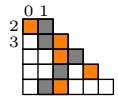
$$\begin{pmatrix}
0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 1 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 1 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 0 & 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 1 & 0 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 1 & 0 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 1 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 1 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 0 & 1 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 1 & 0 & 0 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}$$

Tous les ... sont des 0.

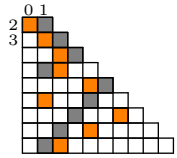
D'un Z qui veut dire... (Denise Vella-Chemla, 15.6.2019)

$2p = p + p$: un nombre premier vérifie trivialement la conjecture de Goldbach. On repère de belles lettres Z dans le bas des tores trapézoïdaux qu'on a choisis pour représenter les restes des nombres dans des divisions par les entiers successifs à commencer par 2.

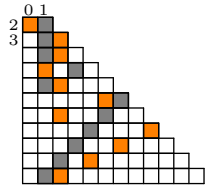
14



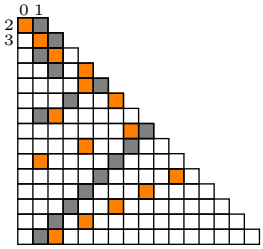
22



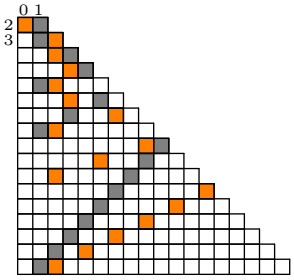
26



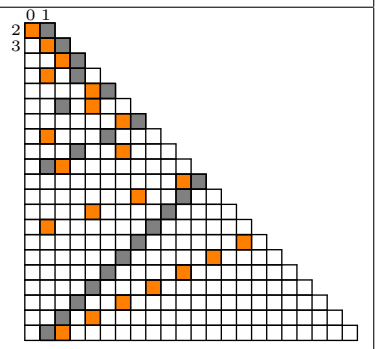
34



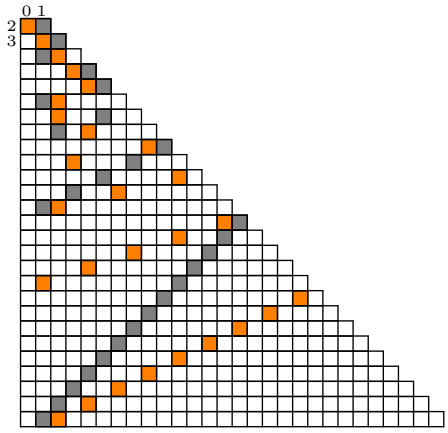
38



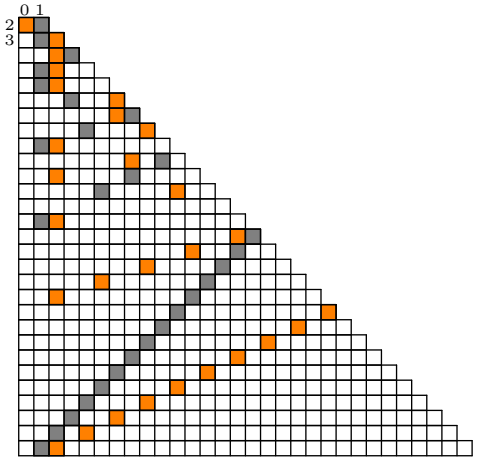
46



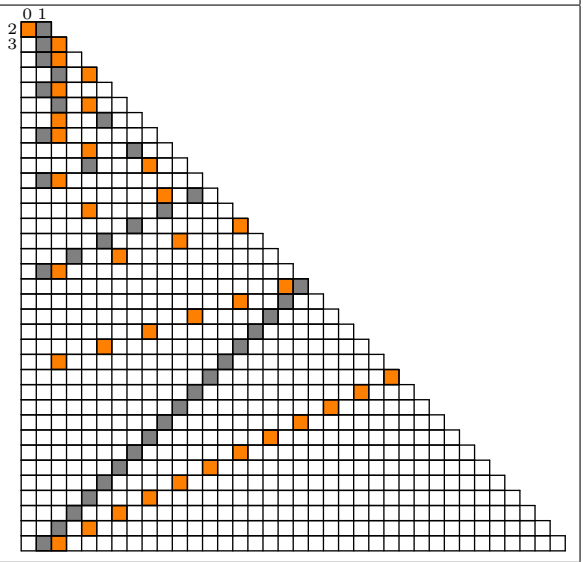
58



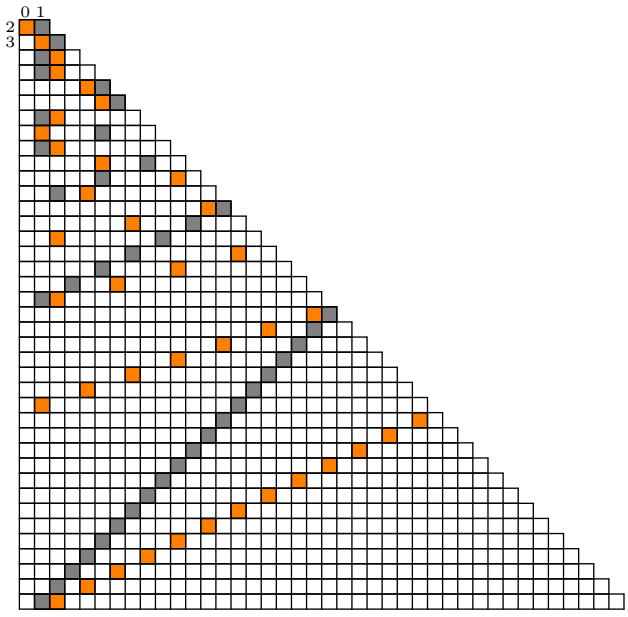
62



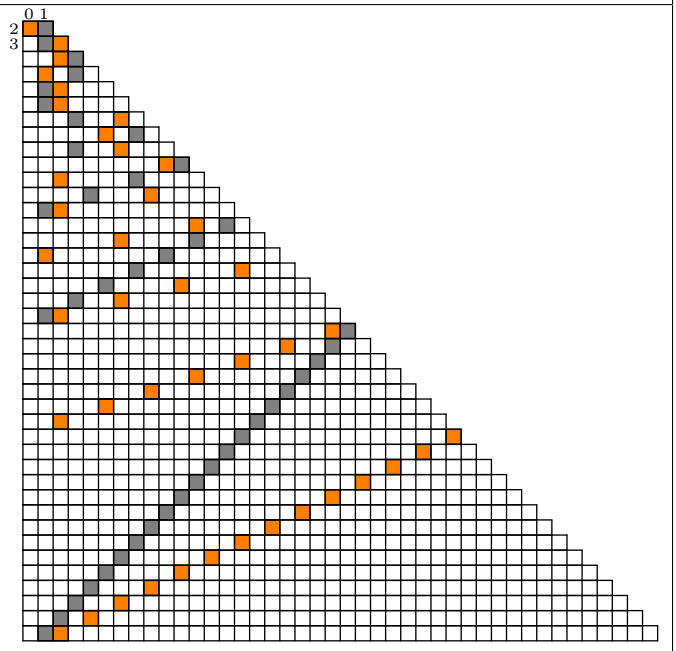
74



82



86



Conjecture de Goldbach, où l'on retrouve ζ autrement (Denise Vella-Chemla, 29.5.2019)

On s'intéresse à la conjecture de Goldbach qui stipule que tout nombre pair supérieur strictement à 2 est la somme de deux nombres premiers.

On rappelle qu'un nombre premier inférieur à $\frac{n}{2}$, qui ne partage aucun de ses restes avec n un nombre pair supérieur à 2, dans toute division par un nombre premier inférieur à $\sqrt{n}$, est un décomposant de Goldbach de n.

En effet, si x inférieur à $\frac{n}{2}$ ne partage aucun de ses restes avec n dans toute division par un nombre premier inférieur à $\sqrt{n}$, alors $n-x$ est lui aussi premier.

La probabilité asymptotique qu'un nombre x inférieur à $\frac{n}{2}$ soit premier est fournie par le théorème des nombres premiers ; elle vaut :

$$\frac{\frac{n}{2}}{ln\left(\frac{n}{2}\right)}$$

La minoration de $\pi(k)$ (le nombre de nombres premiers inférieurs à k) par $\frac{k}{ln\ k}$ est fournie dans [1], page 69, pour $x \geq 17$.

Supposons maintenant que x est premier. Etudions les probabilités d'égalité des restes de x et n quand on les divise par les nombres premiers inférieurs à $\sqrt{n}$.

Puisqu'on a supposé x premier, on sait au moins qu'il n'a aucun reste nul lorsqu'on le divise par un nombre premier inférieur à $\sqrt{n}$.

n a un certain reste, lorsqu'on le divise par un nombre premier inférieur à $\sqrt{n}$. x doit "éviter" le reste en question (ne doit pas avoir le même).

Si on considère une division de n par l'un de ses diviseurs premiers p de reste nul, x n'a que ce reste nul (0) à éviter. Or x a déjà évité 0 par le fait qu'il est premier. x a le choix entre $p-1$ restes possibles dans la division par p.

Si on considère une division de n par un nombre premier qui n'est pas l'un de ses diviseurs, n a selon ce nombre premier un reste non-nul que x doit éviter. x a alors le choix entre $p-2$ restes possibles dans sa division par p, qu'il peut avoir à égales probabilités l'un ou l'autre mais on va utiliser le fait que $\frac{1}{p-2} > \frac{1}{p-1}$ et minorer chaque probabilité selon un nombre premier p donné par $\frac{1}{p-1}$, pour homogénéiser les différents cas (considération des diviseurs ou des non-diviseurs de n).

Voyons des exemples, pour fixer les idées : dans une division par 3, on minore le nombre de possibilités par 2 possibilités de reste (1 et 2), et x a une chance sur deux (i.e. 1/2) d'obtenir l'un ou l'autre.

Dans une division par 5, il reste à x 4 possibilités de reste (1, 2, 3 ou 4), et x a une chance sur 4 (i.e. 1/4) d'obtenir l'un ou l'autre.

Dans une division par 7, il reste à x 6 possibilités de reste (1, 2, 3, 4, 5 et 6), et x a une chance sur 6 (i.e. 1/6) d'obtenir l'un ou l'autre.

Plus généralement, dans une division par p, on minore la probabilité que x et n aient le même reste ainsi : il y a $p-1$ possibilités de restes possibles au maximum pour x (qui sont 1, 2, ..., $p-1$), et x a une chance sur $p-1$ (i.e. 1/(p-1)) d'obtenir l'un ou l'autre de ces restes.

Tous ces événements ayant des probabilités indépendantes, la probabilité d'obtenir leur conjonction est le produit des probabilités de chaque événement séparé (les événements considérés étant "x et n ont même

reste dans une division par 3", "x et n ont même reste dans une division par 5", etc.).

Ce produit s'écrit :

$$\prod_{p\ premier\ <\sqrt{n}} \frac{1}{p-1}$$

On peut le réécrire :

$$\prod_{p\ premier\ <\sqrt{n}} \frac{1}{p^{-(-1)}-1}$$

puis

$$-\prod_{p\ premier\ <\sqrt{n}} \frac{1}{1-p^{-(-1)}}$$

On peut étendre ce produit à l'infinité des nombres premiers car en fait, c'est selon tout nombre premier que n et x ne peuvent être congrus, pour que le complémentaire à n de x qu'est $n-x$ soit premier. On reconnaît alors $-\zeta(-1)$ dans le produit proposé pour que x et n aient des restes différents dans un division par un nombre premier quelconque. Ramanujan a démontré que $\zeta(-1) = -\frac{1}{12}$. La note [1] fournit une démonstration simple de ce fait.

On obtient donc comme probabilité globale qu'un nombre x soit d'une part premier, et d'autre part ne partage aucun de ses restes avec n dans une division par un nombre premier inférieur à $\sqrt{n}$ (en fait quelconque) [2] :

$$\frac{\frac{n}{2}}{ln\left(\frac{n}{2}\right)} \times (-\zeta(-1))$$

soit :

$$\frac{n}{2\ ln\ n - 2\ ln\ 2} \times \frac{1}{12}.$$

Ceci semble rendre la conjecture de Goldach vraie à partir de $n = 92$ [3].

Tentative de réécriture mathématique :

On cherche à démontrer que $\forall n$ pair, $\exists x, 3 \leq x \leq n/2$ premier impair tel que $n-x$ est premier aussi.

$$\begin{array}{lll} (1)\quad x \text{ premier} & \iff \forall p \text{ premier} \leq \sqrt{x}, & x \not\equiv 0\ (mod\ p). \\ (2)\quad n-x \text{ premier} & \iff \forall p \text{ premier} \leq \sqrt{n-x}, & n-x \not\equiv 0\ (mod\ p) \\ & \iff \forall p \text{ premier} \leq \sqrt{n-x}, & x \not\equiv n\ (mod\ p). \end{array}$$

On peut remplacer dans (1) la condition $\forall p$ premier $\leq \sqrt{x}$ par la condition plus forte $\forall p$ premier $\leq \sqrt{n/2}$ puisqu'on a posé $x \leq n/2$.

---

1. Par définition $S = 1+2+3+4+5+....$ On remarque qu'en faisant la différence terme à terme :

$$\begin{array}{rccccl} S-B= & 1+2 & +3+4 & +5+6 & ... & \\ & -1+2 & -3+4 & -5+6 & ... & \\ = & 0+4 & +0+8 & +0+12 & ... = 4(1+2+3+...) = 4S & \end{array}$$

Donc $S-4S = B$, i.e. $-3S = B$, d'où $S = -\frac{B}{3} = -\frac{\frac{1}{4}}{3}$ Ainsi, on retrouve le résultat attendu : $S = -\frac{1}{12}$.

2. Le fait pour x de ne partager aucun reste avec n dans les divisions par les nombres premiers inférieurs à $\sqrt{n}$ n'a rien à voir avec le fait d'être premier à n. Cette condition est nécessaire (i.e. *impliquée*) mais non suffisante (i.e. *impliquante*). Par exemple, 17 et 81, dont la somme vaut 98, sont tous les deux premiers à 98, mais ils n'en sont pas pour autant des décomposants de Goldbach (de 98) puisque 17 partage le reste de 2 avec 98 lorsqu'on les divise par 3 (Gauss écrit cela $17 \equiv 98\ (mod\ 3)$, c'est lui qui a attiré l'attention de tous sur l'importance de travailler dans les corps premiers).

3. $\frac{92}{2\ ln\ 92 - 2\ ln\ 2}.\frac{1}{12} = 1.0012254835$ alors que $\frac{90}{2\ ln\ 90 - 2\ ln\ 2)}.\frac{1}{12} = 0.9851149163$.

On minore le nombre de nombres premiers inférieurs à $\frac{n}{2}$ par $\frac{\frac{n}{2}}{log\left(\frac{n}{2}\right)}$.

Il s'agit alors de trouver combien de nombres dans cet ensemble de nombres premiers inférieurs à $\frac{n}{2}$, dont on a le cardinal, partagent leur reste avec n ; le partage d'un reste avec n le nombre pair considéré consiste à "fixer" le reste possible et donc à diminuer le nombre de restes possibles de 1 selon chaque module ; on doit multiplier le cardinal $\pi\left(\frac{n}{2}\right)$ minoré par $\frac{\frac{n}{2}}{log\left(\frac{n}{2}\right)}$ (qui correspond à la condition (1) ci-dessus) par la probabilité qu'il y ait un partage de reste selon chaque nombre premier indépendamment (qui correspond à la condition (2) ci-dessus) et cette probabilité a comme valeur $-\zeta(-1) = \frac{1}{12}$. C'est un cardinal d'ensemble qu'on obtient par ce procédé de multiplication d'un cardinal par une probabilité. Un tel calcul semble faire sens et assure un cardinal d'au moins 1 à partir de 92.

Bibliographie

[1] J. B. Rosser et L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, dedicated to Hans Rademacher for his seventieth birthday, Illinois J. Math., Volume 6, Issue 1 (1962), 64-94.

Goldbach's conjecture, where we find ζ in another way (Denise Vella-Chemla, 29.5.2019)

One considers here Goldbach's conjecture that asserts that every even number strictly greater than 2 is the sum of two primes.

One recalls that a prime number x lesser than $\frac{n}{2}$, that doesn't share any of its division rest with n an even number strictly greater than 2, in all divisions by a prime number lesser than $\sqrt{n}$, is a Goldbach component of n (i.e. $n - x$ is prime too).

Indeed, if x lesser than $\frac{n}{2}$ doesn't share any of its division rest with n in any division by a prime lesser than $\sqrt{n}$, then $n - x$ is prime.

The asymptotic probability that an integer x lesser than $\frac{n}{2}$ be prime is provided by the prime number theorem ; it equals :

$$\frac{\frac{n}{2}}{ln\left(\frac{n}{2}\right)}$$

The minoration of $\pi(k)$ (the number of prime numbers lesser than k) by $\frac{k}{ln\ k}$ is provided in [1], page 69, for all $x \geq 17$.

Let us suppose now that x is prime. Let us study the probabilities that divisions rests of x and n are equal when one divides them by all the prime numbers lesser than $\sqrt{n}$.

Since we supposed x to be prime, we know at least that x has no rest equal to zero when we divide it by a prime number lesser than $\sqrt{n}$.

n has a certain rest, when we divide it by a prime number lesser than $\sqrt{n}$ and x has to "avoid" the rest in question (it can't have the same).

If we consider a division of n by one of its prime divisors, in which the rest is null, x has only this rest zero (0) to avoid. However x can't have (has yet avoided) the rest 0 since it's prime. It remains $p - 1$ possible rests for x when we divide it by p.

Let us consider now a division of n by a prime number which is not an n's divisor, let us call it d. n has, when we divide it by d a rest that is different from 0 that x must avoid. In this case, x has the choice between $p - 2$ possible rests in its division by p, that it can have with equal probabilities the one or the other but we are going to use the fact that $\frac{1}{p-2} > \frac{1}{p-1}$ to minorate each probability modulo a given prime number p by $\frac{1}{p-1}$, to homogeneize the different possible cases (if we are considering or not a prime divisor of n).

Let us see examples, to fix ideas : in a division by prime number 3, we minorate the number of possibilities by 2 possibilities for the division rests (1 or 2), and x has one chance among two (i.e. 1/2) to obtain one or the other.

In a division by 5, it remains 4 possibilities for x to have some division rest among 1, 2, 3 or 4, and x has one chance among 4 (i.e. 1/4) to obtain the one or the other.

In a division by 7, it remains 6 possibilities for x to have its division rest among 1, 2, 3, 4, 5 or 6, and x has one chance among 6 (i.e. 1/6) to obtain the one or the other.

More generally, in a division by p, one minorates the probability for x and n to have the same division rest in the following way : there are $p - 1$ division rests possibilities at most for x (that are 1, 2, ..., $p - 1$), and x has one chance among $p - 1$ (i.e. $\frac{1}{p-1}$ to obtain the one or the other of those division rests).

All those events (rests sharings) having independent probabilities, the probability to obtain their conjunction is the product of the probabilities of each event alone (the considered events being "x and n have the same rest in a division by 3", or "x and n have the same rest in a division by 5", etc.).

This product of probabilities can be written :

$$\prod_{p\ premier\ <\sqrt{n}} \frac{1}{p-1}$$

We can transform this in :

$$\prod_{p\ premier\ <\sqrt{n}} \frac{1}{p^{-(-1)}-1}$$

and then in

$$-\prod_{p\ premier\ <\sqrt{n}} \frac{1}{1-p^{-(-1)}}$$

We can extend this product to the set of all primes in infinite number because in fact, it's modulo every prime number that n and x have not to be in the same congruence class (i.e. mustn't share their rest), for the complementary of x to n (i.e. $n-x$) to be prime too. One can recognize then $-\zeta(-1)$ in the calculus of the product for x and n have different rests in a division by whatever prime number. Ramanujan demonstrated that $\zeta(-1) = -\frac{1}{12}$. The note [1] provides a simple demonstration of this fact.

We obtain the cardinal of a set of numbers x that are prime on one side, and that don't have the same division rest than n in a division by any prime number lesser than $\sqrt{n}$ (and in fact by any prime) [2] on the other side :

$$\frac{\frac{n}{2}}{ln\left(\frac{n}{2}\right)} \times (-\zeta(-1))$$

that is :

$$\frac{n}{2\ ln\ n - 2\ ln\ 2} \times \frac{1}{12}.$$

This seems to make Goldbach's conjecture true above $n = 92$ [3].

Attempt to write this reasoning more formally :

We want to demonstrate that $\forall n$ even, $\exists x, 3 \leq x \leq n/2$ odd prime such that $n-x$ is prime too.

$$\begin{array}{lll} (1)\quad x \text{ prime} & \iff \forall p \text{ prime} \leq \sqrt{x}, & x \not\equiv 0\ (mod\ p). \\ (2)\quad n-x \text{ prime} & \iff \forall p \text{ prime} \leq \sqrt{n-x}, & n-x \not\equiv 0\ (mod\ p) \\ & \iff \forall p \text{ prime} \leq \sqrt{n-x}, & x \not\equiv n\ (mod\ p). \end{array}$$

1. Par définition $S = 1+2+3+4+5+....$

One notes than calculating term by term the difference :

$$\begin{array}{rccccl} S-B= & 1+2 & +3+4 & +5+6 & ... & \\ & -1+2 & -3+4 & -5+6 & ... & \\ = & 0+4 & +0+8 & +0+12 & ... & = 4(1+2+3+...) = 4S \end{array}$$

So $S-4S = B$, i.e. $-3S = B$, d'où $S = -\frac{B}{3} = -\frac{\frac{1}{4}}{3}$ So one finds the expected result : $S = -\frac{1}{12}$.

2. The fact that x doesn't share any division rest with n in divisions by prime numbers lesser than $\sqrt{n}$ is not the same as the fact to be prime to n (to have no common factor greater than 1 with n). This last condition is necessary (i.e. *implied*) but not sufficient (i.e. *implying*). For instance, 17 and 81, that have a sum equal to 98, are both *prime to* 98, but they are not Goldbach'decomponents of 98 since 17 shares its division rest 2 with 98 when we divide them by 3 (Gauss writes this $17 \equiv 98\ (mod\ 3)$, he is the one who drew attention of everyone on the importance to work in prime fields).

3. $\frac{92}{2\ ln\ 92 - 2\ ln\ 2}.\frac{1}{12} = 1.0012254835$ alors que $\frac{90}{2\ ln\ 90 - 2\ ln\ 2)}.\frac{1}{12} = 0.9851149163$.

One can replace in (1) the condition $\forall p$ prime $\leq \sqrt{x}$ by the strongest condition $\forall p$ prime $\leq \sqrt{n/2}$ since we let $x \leq n/2$.

One can minorate the number of prime numbers lesser than $\frac{n}{2}$ by $\frac{\frac{n}{2}}{log\left(\frac{n}{2}\right)}$.

It matters then to find how many numbers in this set of prime numbers lesser than $\frac{n}{2}$, set whose we know the cardinal, share their division rest with n ; sharing a rest with n, the even number considered, consists in "fixing" the possible rest and so to make decrease by 1 the number of possible rests for each module ; we must multiply the cardinal $\pi\left(\frac{n}{2}\right)$ minorated by $\frac{\frac{n}{2}}{log\left(\frac{n}{2}\right)}$ (that corresponds to the condition (1) above) by the probability there would be a rest sharing modulo each prime number independently (that corresponds to the condition (2) above) and this probability has as value $-\zeta(-1) = \frac{1}{12}$. It's a set cardinal one obtains by this process of multiplying a set cardinal by a probability. Such a calculus seems to make sense and seems to ensure a cardinal equal at least to 1 above 92.

Bibliography

[1] J. B. Rosser et L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, dedicated to Hans Rademacher for his seventieth birthday, Illinois J. Math., Volume 6, Issue 1 (1962), 64-94.

Un ensemble, une transformation, des traces (Denise Vella-Chemla, 10.7.2019)

On se place dans un ensemble très particulier ; il s'agit de l'ensemble des matrices booléennes qui sont puissances de la matrice suivante :

$$G = \begin{pmatrix}
0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 1 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 1 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 0 & 1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & 1 & 0 & 0 & 0 & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 1 & 0 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 1 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 1 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 0 & 0 & 0 & 1 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 1 & 0 & 0 & 0 & 0 & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{pmatrix}$$

Cette matrice est infinie, elle contient sur sa diagonale des matrices circulantes de taille 2×2, 3×3, 4×4, etc.

On a une opération : l'élévation à la puissance de la matrice ci-dessus qui nous fait atteindre certaines matrices carrées booléennes et pas d'autres.

Une simple étude nous fait comprendre que la trace de la matrice atteinte par élévation à la puissance k de la matrice G permet de caractériser si k est premier ou non.

En effet, on a p est premier $\iff Trace(G^p) = p$.

Quand on élève une matrice circulante de taille $k \times k$ à la puissance k, tous ses 1 s'alignent bien sur la diagonale pour obtenir la matrice Identité de taille k. Il en sera de même des 1 appartenant aux matrices circulantes de taille les diviseurs de k si k est composé.

La complexité d'un tel algorithme pour caractériser la primalité d'un nombre étant de l'ordre de n^7 (en considérant la taille d'une matrice - en $\frac{n(n+1)}{2}$ -, le coût d'une multiplication matricielle en n^3, etc.), elle est complètement prohibitive. L'intérêt de cette idée est peut-être simplement de caractériser la primalité par certaines traces matricielles.

Cette méthode n'utilise qu'un ensemble (celui des matrices booléennes carrées à blocs de matrices circulantes sur leur diagonale) et une transformation (l'élévation d'une matrice à une certaine puissance) ; la transformation en question fait sortir de ou entrer dans l'ensemble des nombres premiers suivant le nombre (l'exposant de G) considéré.

Annexe à la proposition denitac.pdf (Denise Vella-Chemla, 23.7.2019)

On cherche à décomposer un nombre pair n en somme de 2 nombres premiers $p_1 + p_2$.

On ne peut pas faire référence à $\zeta(-1)$ comme on l'a fait dans [1]. On peut cependant, pour obtenir une minoration du nombre de décomposants de Goldbach de n, utiliser le cardinal $\left|\mathcal{P}_{\frac{n}{2}}\right|$ de l'ensemble des nombres premiers inférieurs ou égaux à $\frac{n}{2}$ et le multiplier par le produit $\prod_{p\leq\sqrt{n}}\left(1-\frac{1}{p}\right)$ qui compte combien de chances a le nombre premier p_1 de ne pas partager son reste avec n selon chaque module p inférieur à $\sqrt{n}$ (le fait de ne pas partager son reste avec n permet à p_1 d'avoir un complémentaire à n (appelé p_2) qui est premier également).

La minoration [1] de $\pi(x)$ (le nombre de nombres premiers inférieurs à x) par $\frac{x}{\log x}$ est fournie dans [2], page 69, pour $x \geq 17$ (Corollaire 1, (3.5), du Théorème 2, dont la démonstration est fournie au paragraphe 7 de [2]).

On a en conséquence $|\mathcal{P}_{\frac{n}{2}}| > \frac{\frac{n}{2}}{\log\left(\frac{n}{2}\right)}$.

La minoration de $\prod_{p\leq\sqrt{n}}\left(1-\frac{1}{p}\right)$ est également fournie dans [2], page 70 (c'est le corollaire (3.27) du Théorème 7 dont la démonstration est fournie au paragraphe 8 de [2], avec γ la constante d'Euler-Mascheroni).

$$(3.27) \qquad \frac{e^{-\gamma}}{\log x}\left(1-\frac{1}{\log^2 x}\right) < \prod_{p\leq x}\left(1-\frac{1}{p}\right) \quad \text{pour } 1 < x.$$

En multipliant ces expressions ensemble, on obtient que le nombre de décomposants de Goldbach de n doit être supérieur à :

$$\frac{n/2}{\log(n/2)}\frac{e^{-\gamma}}{\log\sqrt{n}}\left(1-\frac{1}{\log^2\sqrt{n}}\right)$$

qui est strictement supérieur à 1 à partir de 24.

Bibliographie

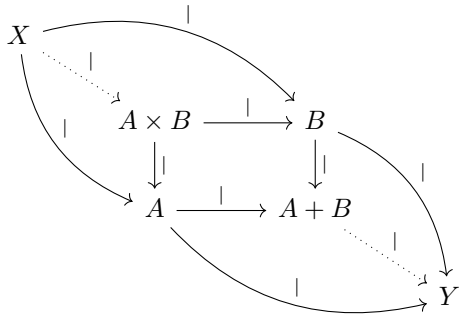
[1] http://denisevellachemla.eu/denitac.pdf.

[2] J. B. Rosser et L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, dedicated to Hans Rademacher for his seventieth birthday, Illinois J. Math., Volume 6, Issue 1 (1962), 64-94.

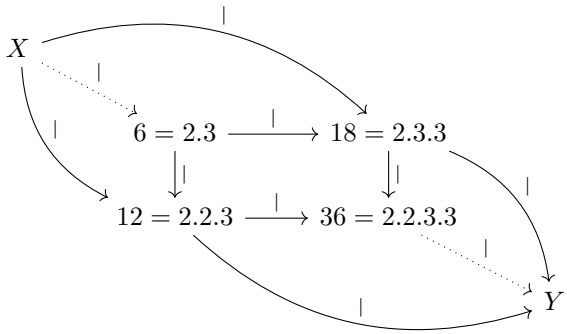
1. Cette minoration est à distinguer du Théorème des nombres premiers, prouvé indépendamment par Hadamard et La Vallée-Poussin, et qui fournit une tendance asymptotique pour $\pi(x)$.

Pgcd et Ppcm représentés sur diagrammes commutatifs (D. Chemla, 15.9.2019)

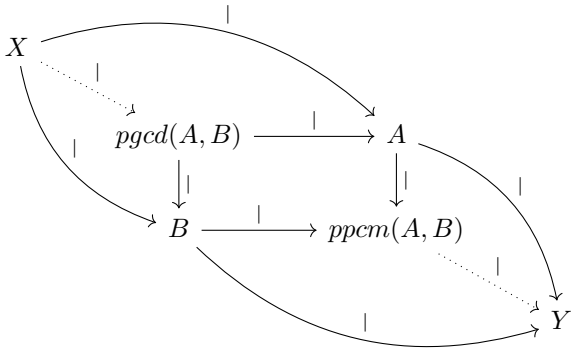
Le symbole | signifie *"divise"*.



Avec des nombres pour fixer les idées.



On lit sur ce diagramme que 36, le *ppcm* (plus petit commun multiple) de 12 et 18, divise tout nombre Y que 12 et 18 divisent.
On y lit également que tout nombre X qui divise 6, le *pgcd* (plus grand commun diviseur) de 12 et 18, divise chacun d'entre eux, i.e. divise 12 et divise 18.
Dans l'exemple, on peut remplacer par exemple X par 2 ou 3 et Y par 72 ou 180.

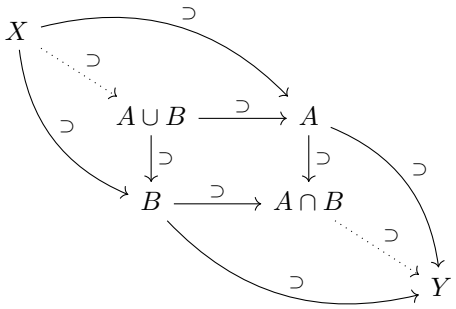


On voit ainsi le *pgcd* comme une intersection ensembliste (les ensembles pouvant contenir un facteur avec une certaine multiplicité, plusieurs fois : par exemple, deux occurrences de 2 et deux occurrences de 3 sont "contenues" dans 36).
Le *ppcm* est vu comme une union. C'est l'idée intuitive que l'on en avait naturellement.
On avait eu plaisir à retrouver une telle idée dans un article de Charles-Ange Laisant *Remarques arithmétiques sur les nombres composés*[*].

En termes ensemblistes, on dirait que tout ensemble inclus à la fois dans l'ensemble A et dans l'ensemble B est inclus dans leur intersection $A \cap B$ et que l'union $A \cup B$ de deux ensembles A et B est incluse dans tout ensemble qui les inclut chacun.

Le symbole $\supset$ signifie *"a comme sous-ensemble"*.

∗. cf. http://www.numdam.org/article/BSMF_1888_16_150_1.pdf



Remarque : on pourrait inverser le sens de toutes les flèches, en considérant les relations inverses (*"est divisé par"*, *"est inclus dans"*) et les catégories duales.

Plaid écossais tropical (Denise Vella-Chemla, 25.9.2019)

1. Le maillage Goldbach

En 2005 (cf. [5]), au tout début de ces recherches que l'on mène sur la conjecture de Goldbach, on avait choisi de représenter les décompositions de Goldbach sur un maillage tel que celui-ci :

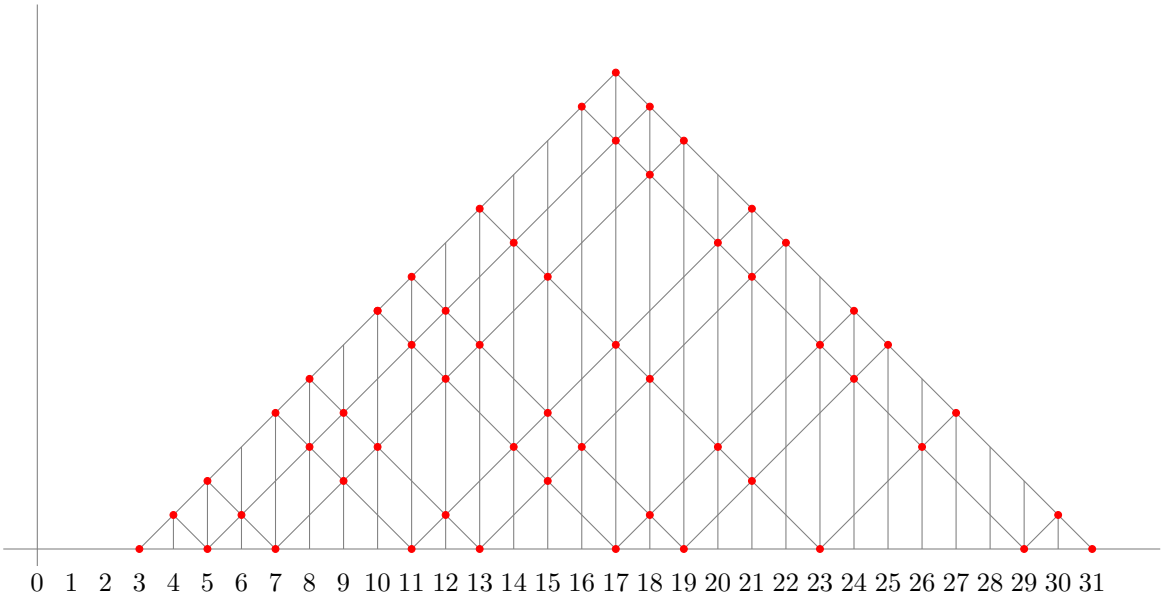


FIGURE 1 : Le treillis Goldbach

2. Les décompositions additives

Chaque point marqué d'un symbole • correspond à une décomposition additive dont les deux sommants sont des nombres premiers.

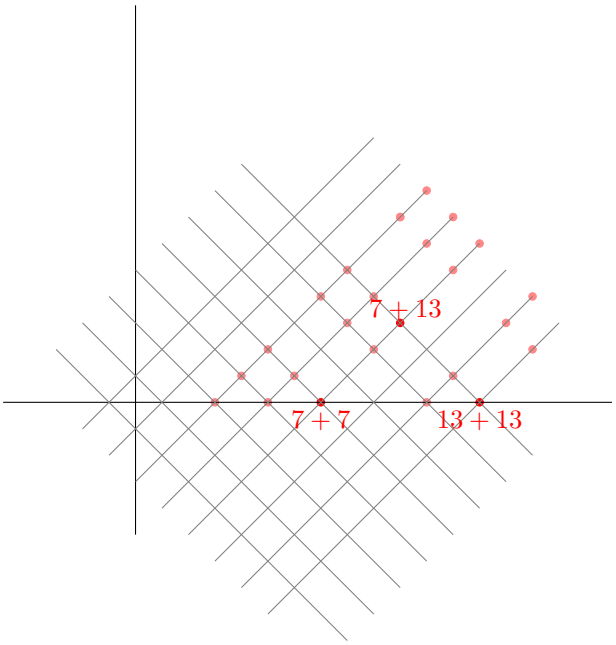


FIGURE 2 : Décompositions additives

Les décompositions additives qui sont sur l'axe des abscisses correspondent aux doubles de nombres premiers ; les nombres premiers vérifient trivialement la conjecture de Goldbach car pour eux, $2p = p + p$ est une décomposition de Goldbach, i.e. une décomposition d'un nombre pair, leur double, en somme de deux nombres premiers, identiques.

On souhaiterait voir ces décompositions triviales comme se trouvant à l'intersection de deux droites tropicales qui correspondraient à un dessin légèrement similaire à celui que l'on trouve à la page 21 de [2].

En algèbre tropicale ([1], |3]), les deux éléments ci-dessous sont deux droites, dans une algèbre max-plus, par exemple. Dans une telle algèbre, on dispose de deux opérations : l'addition (qui remplace la multiplication de l'algèbre telle qu'on la pratique habituellement) et le maximum entre deux nombres (qui remplace l'addition de l'algèbre usuelle). Comme le remplacement des signes $+$ par $\otimes$ et $\times$ par $\odot$ ne facilite pas la lecture, on conserve le mot *max*.

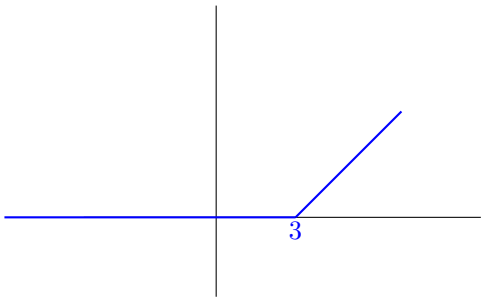


FIGURE 3 : Une droite tropicale d'équation $y = max(x - 3, 0)$

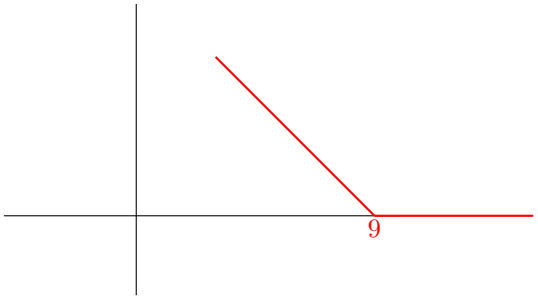


FIGURE 4 : Une autre droite tropicale d'équation $y = max(9 - x, 0)$

Les décompositions triviales de la forme $p + p$ se trouvent à l'intersection de la droite tropicale sur la partie non horizontale * de laquelle se trouvent toutes les décompositions de la forme $x + p$ et de la droite tropicale sur la partie non-horizontale de laquelle se trouvent les décompositions de la forme $p + y$ (cf. [6]).

On aimerait interpréter ces décompositions triviales comme des limites : de même que le *pgcd* et le *ppcm* de deux nombres sont égaux lorsque ces deux nombres sont égaux (cf [7]), on aimerait ici voir les nombres premiers comme présentant la propriété d'être égaux à la fois au plus petit nombre premier qui leur est supérieur et au plus grand nombre premier qui leur est inférieur, propriété que ne partagent pas les nombres composés.

On n'a cependant pas trouvé le moyen de distinguer les décompositions qui font intervenir deux nombres premiers de celles qui ont pour sommants un, voire deux, nombres composés. Il faudrait trouver un moyen de faire que les nombres premiers se projettent sur 0 tandis que les nombres composés se projetteraient sur 1.

Comme on n'a pas avancé d'un pouce, on se cache derrière une phrase de Max Karoubi, que son maître lui aurait dite : "Ce n'est pas comme ça qu'on écrit des maths !" (cf. video [4]).

∗. qui ne coïncide pas avec l'axe des abscisses.

Bibliographie

[1] E. Brugallé, Un peu de géométrie tropicale, 2009.
https://arxiv.org/abs/0911.2203

[2] A. Connes, C. Consani, On Absolute Algebraic Geometry, the affine case, 2019.
https://arxiv.org/abs/1909.09796

[3] S. Gaubert, Max-plus algebra... a guided tour, SIAM Conference on Control and its applications, 2009.
http://www.cmap.polytechnique.fr/ gaubert/siamct09/slidesgaubertsiamct09.pdf

[4] M. Karoubi, sur le site de Leila Schneps, Grothendieck circle, 2008.
https://webusers.imj-prg.fr/ leila.schneps/grothendieckcircle/Karoubi2008.mp4

[5] D. Vella-Chemla, Vers une preuve de la conjecture de Goldbach, 2005.
http://denisevellachemla.eu/octobre2005.pdf

[6] D. Vella-Chemla, Etudier Ritz-Rydberg, 2012.
http://denisevellachemla.eu/j2042012.pdf

[7] D. Vella-Chemla, Pgcd, ppcm représentés sur diagrammes commutatifs, 2019.
http://denisevellachemla.eu/pgcd-ppcm-categ.pdf

Proposition de démonstration de la conjecture de Goldbach dans le formalisme des topos (Denise Vella-Chemla, 5.10.2019)

La conjecture de Goldbach binaire stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. La démonstration proposée ici utilise des concepts de la théorie des topos. Colin McLarty, dans une conférence du cycle Lectures Grothendieckiennes, parle de la notion d'"espace étalé" (cf. Annexe 1). Goldblatt, dans *Topoi, the categorial analysis of logic*, fournit un dessin très éclairant pour cette notion (cf. Annexe 2). On trouve la définition des mots *fibre* et *germe* dans l'article de Wikipedia consacré aux *faisceaux* (cf. Annexe 3). L'article wikipedia renvoie à la définition première (en mathématique) du mot *fibre*, qu'on trouve à la page 25 du premier volume I des Éléments de Géométrie Algébrique (EGA I) d'Alexander Grothendieck ([1], cf. Annexe 4).

L'étude de la conjecture de Goldbach fait appréhender que les décomposants de Goldbach d'un nombre pair n, qui sont compris entre la racine carrée de n et la moitié de n, sont à trouver dans l'intersection des ensembles de nombres qui ne sont ni congrus à 0, ni congrus à n selon tout module premier p_k compris entre 3 et la racine carré de n. On prend comme borne inférieure de l'intervalle à considérer 3 plutôt que 2, parce que, pour alléger la formulation, on choisit d'oublier tous les nombres pairs comme décomposants de Goldbach potentiels de n.

Selon chaque module premier p_k, la modélisation nécessite seulement trois fibres et trois germes : la fibre qui relie l'ensemble des nombres divisibles par p_k au germe 0_{p_k}, la fibre qui relie l'ensemble des nombres congrus à n (*modulo* p_k) au germe n_{p_k}, et la fibre qui relie l'ensemble de tous les nombres impairs compris entre 3 et $\frac{n}{2}$, que l'on appellera *ensemble des nombres restant* (i.e. qui sont passés à travers ce double-crible de n'être ni congrus à 0 ni congrus à n modulo p_k), une troisième fibre donc, qui lie l'*ensemble des nombres restant* à un germe qu'on notera $\neg 0_{p_k} \wedge \neg n_{p_k}$ (on peut aussi appeler ce dernier ensemble l'ensemble des "ni 0 ni n selon p_k").

Il s'agit de démontrer que l'intersection de tous les *ensembles de nombres restant* selon chacun des modules premiers p_k compris entre 3 et $\sqrt{n}$ est non vide.

Supposons que l'intersection des *ensembles de nombres restant selon chacun des modules* p_k est vide. Alors, cela implique la nécessité que les ensembles de nombres en question (les *ensembles de nombres restant*) soient des ensembles disjoints. Si tous ces ensembles sont disjoints, on obtient le cardinal de leur union, qui est alors une union disjointe, comme somme des cardinaux de chacun de ces ensembles. Or le cardinal de chacun des ensembles pris séparément est simple à calculer : il est de la forme $\left\lceil \frac{n}{2p_k} \right\rceil$ pour chacun des modules premiers p_k (compris entre 3 et $\sqrt{n}$) *. Le problème est qu'on ne connaît pas la valeur des p_k successifs.

Alors, pour calculer ce cardinal de l'union disjointe, on va se placer dans le cas limite, c'est-à-dire qu'on va supposer (ce qui n'est bien sûr pas le cas) que les nombres premiers sont très écartés les uns des autres : on va considérer que chacun des nombres premiers successifs p_k est juste inférieur au double du nombre premier précédent p_{k-1}. C'est le résultat le plus lâche dont on dispose, appelé *postulat de Bertrand* et démontré par Tchebychev (énonçable simplement par la formule *"il y a toujours un nombre premier entre un nombre et son double."*). Si les nombres premiers étaient ainsi écartés au maximum, on aurait pour chaque nombre premier "précédent" p_{k-1} un cardinal de *l'ensemble des nombres restant* modulo p_{k-1} qui serait environ moitié moins grand que le cardinal de l'*ensemble des nombres restant* pour le nombre premier "suivant" p_k. On va donc considérer en premier le cardinal de l'*ensemble de nombres restant* pour le nombre premier p_{max}, qui est le nom par lequel on désigne le plus grand nombre premier inférieur à la racine carrée de n. Ce cardinal est égal à $\left\lceil \frac{n}{2\ p_{max}} \right\rceil$. Et on imagine que les *ensembles des nombres restant* pour les nombres premiers successifs (du plus grand au plus petit) inférieurs à p_{max} sont chacun de taille moitié moindre que celle de l'*ensemble des nombres restant* pour le nombre premier suivant dans la succession.

$*$. On peut compter les nombres des différents ensembles pour le cas $n = 98$ en annexe 6 pour s'en convaincre.

Dans ce cas imaginaire et très laxiste, on aurait ainsi la somme des cardinaux des ensembles disjoints qui serait égale à :

$$\left\lceil \frac{n}{2\ p_{max}} \right\rceil \left(1 + \sum_{i=1}^{\pi(n/2)-1} \frac{1}{2^i} \right) \ = \ \left\lceil \frac{n}{2\ p_{max}} \right\rceil \left(1 + \left(1 - \frac{1}{2^{\pi(n/2)-1}} \right) \right).$$

Ce résultat provient du fait que la somme des inverses des puissances de 2, de la première puissance, égale à 2, jusqu'à la $k^{\text{ième}}$ puissance, égale à 2^k, est égale à $1 - \frac{1}{2^k}$ (cf. Annexe 5).

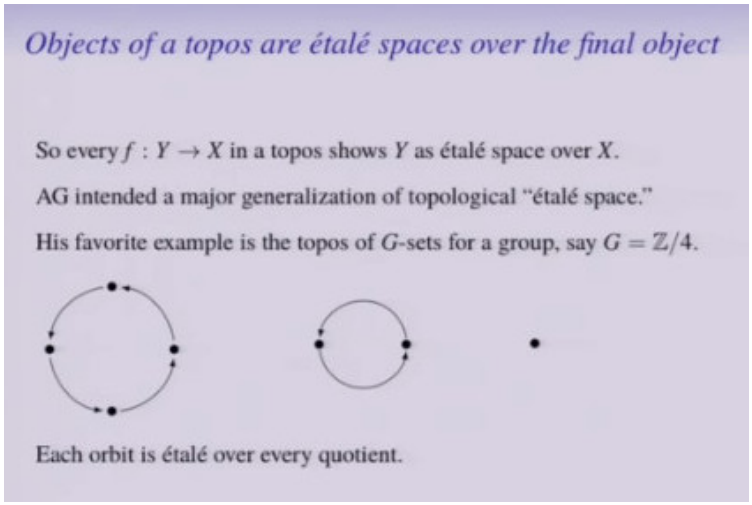
Ce calcul permet d'aboutir clairement à une contradiction car il dépasse grandement le nombre effectif de nombres impairs compris entre 3 et $\frac{n}{2}$ qui est égal à $\left\lfloor \frac{n-2}{4} \right\rfloor$ (on a en effet obtenu pour le cas limite un cardinal au moins égal au double du cardinal du plus gros *ensemble de nombres restant* ; dans un cas non limite, le cardinal global serait encore plus grand, les nombres premiers étant bien plus rapprochés en réalité que dans le cas limite considéré).

Puisqu'on a abouti à une contradiction, l'*ensemble des nombres restant*, ou ensemble des nombres ni congrus à 0, ni congrus à n selon tout nombre premier p_k compris entre 3 et $\sqrt{n}$, ne peut être vide et il contient un décomposant de Goldbach de n au moins.

L'annexe 6 fournit les fibres et germes utilisés pour trouver les décomposants de Goldbach 19, 31 et 37 du nombre pair 98.

Annexe 1 : Conférence de McLarty (notion d'*espace étalé*)

Voici une capture d'écran :



de la video https://www.youtube.com/watch?v=5AR55ZsHmKI, *Grothendieck's 1973 topos lectures* (à la minute 38).

Annexe 2 : Définition de la notion de *bundle* par Goldblatt

For the benefit of the reader unfamiliar with topology we shall delay its introduction and first consider the underlying set-theoretic structure of the sheaf concept, to be called a *bundle*.

Let us assume we have a collection $\mathcal{A}$ of sets, no two of which have any elements in common. That is, any two members of $\mathcal{A}$ are sets that are disjoint. We need a convenient notation for referring to these sets so we presume we have a set I of *labels*, or *indices*, for them. For each index $i \in I$, there is a set A_i that belongs to our collection, and each member of $\mathcal{A}$ is labelled in this way, so we write $\mathcal{A}$ as the collection of all these A_i's,

$$\mathcal{A} = \{A_i : i \in I\}.$$

The fact that the members of $\mathcal{A}$ are pairwise disjoint is expressed by saying that for *distinct* indices $i, j \in I$

$$A_i \cap A_j = \emptyset$$

We visualise the A_i's as "sitting over" the index set I thus:

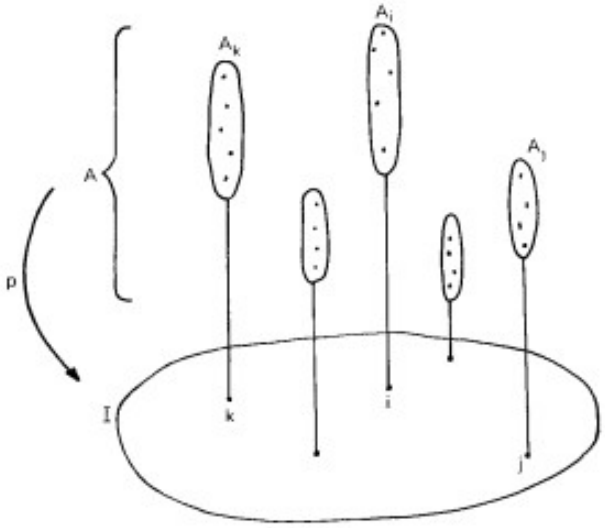


Fig. 4.4.

If we let A be the union of all the A_i's, i.e.

$$A = \{x : \text{for some } i,\ x \in A_i\}$$

then there is an obvious map $p : A \to I$. If $x \in A$ then there is exactly one A_i such that $x \in A_i$, by the disjointness condition. We put $p(x) = i$. Thus

Annexe 3 : Définition des notions de *fibre* et *germe* dans Wikipedia

Fibres et germes [modifier | modifier le code]

Soit $\mathcal{F}$ un préfaisceau sur X à valeurs dans une catégorie $\mathcal{C}$ qui admet des limites inductives. La **fibre** (EGA, 0.3.1.6) (terminologie anglaise : « stalk », *tige*) de $\mathcal{F}$ en un point x de X est par définition l'objet de $\mathcal{C}$ limite inductive

$$\mathcal{F}_x = \varinjlim_{U \ni x} \mathcal{F}(U),$$

la limite étant prise sur tous les ouverts contenant x, la relation d'ordre sur ces ouverts étant l'inclusion $V \subset U$, et les morphismes de transition étant les morphismes de restriction $\rho_{VU} : \mathcal{F}(U) \to \mathcal{F}(V)$.

Lorsque $\mathcal{C}$ est une catégorie concrète, l'image canonique d'une section s dans $\mathcal{F}_x$ est le **germe** de s au point x, noté s_x.

Remarque. Certains auteurs appellent *germe* de $\mathcal{F}$ en un point x ce qui est appelé ci-dessus la *fibre* de $\mathcal{F}$ en ce point.

Annexe 4 : Extrait des EGA I : définitions

(3.1.6) Supposons maintenant que la catégorie $\boldsymbol{K}$ admette des *limites inductives* (T, 1.8) ; alors, pour tout préfaisceau (et en particulier tout faisceau) $\mathscr{F}$ sur X à valeurs dans $\boldsymbol{K}$ et tout $x \in X$, on peut définir la *fibre* $\mathscr{F}_x$ comme l'objet de $\boldsymbol{K}$ limite inductive des $\mathscr{F}(U)$ selon l'ensemble filtrant (pour $\supset$) des voisinages ouverts U de x dans X, et pour les morphismes $\rho_U^V : \mathscr{F}(V) \to \mathscr{F}(U)$. Si $u : \mathscr{F} \to \mathscr{G}$ est un morphisme de préfaisceaux à valeurs dans $\boldsymbol{K}$, on définit pour tout $x \in X$ le morphisme $u_x : \mathscr{F}_x \to \mathscr{G}_x$ comme la limite inductive des $u_U : \mathscr{F}(U) \to \mathscr{G}(U)$ selon l'ensemble des voisinages ouverts de x ; on définit ainsi $\mathscr{F}_x$ comme foncteur covariant en $\mathscr{F}$, à valeurs dans $\boldsymbol{K}$, pour tout $x \in X$.

Lorsque $\boldsymbol{K}$ est en outre définie par une espèce de structure avec morphismes Σ, on appelle encore *sections au-dessus de* U d'un *faisceau* $\mathscr{F}$ à valeurs dans $\boldsymbol{K}$ les éléments de $\mathscr{F}(U)$, et on écrit alors $\Gamma(U, \mathscr{F})$ au lieu de $\mathscr{F}(U)$; pour $s \in \Gamma(U, \mathscr{F})$, V ouvert contenu dans U, on écrit $s|V$ au lieu de $\rho_V^U(s)$; pour tout $x \in U$, l'image canonique de s dans $\mathscr{F}_x$ est le *germe* de s au point x, noté s_x (*nous n'emploierons jamais la notation $s(x)$ dans ce sens*, cette notation étant réservée pour une autre notion relative aux faisceaux particuliers qui seront considérés dans ce Traité (5.5.1)).

Si alors $u : \mathscr{F} \to \mathscr{G}$ est un morphisme de faisceaux à valeurs dans $\boldsymbol{K}$, on écrira $u(s)$ au lieu de $u_V(s)$ pour tout $s \in \Gamma(U, \mathscr{F})$.

Si $\mathscr{F}$ est un faisceau de groupes commutatifs, ou d'anneaux, ou de modules, on dit que l'ensemble des $x \in X$ tels que $\mathscr{F}_x \neq \{0\}$ est le *support* de $\mathscr{F}$, noté $\mathrm{Supp}(\mathscr{F})$; cet ensemble n'est pas nécessairement fermé dans X.

Lorsque $\boldsymbol{K}$ est définie par une espèce de structure avec morphismes, *nous nous abstiendrons systématiquement de faire intervenir le point de vue des « espaces étalés »* en ce qui concerne les faisceaux à valeurs dans $\boldsymbol{K}$; autrement dit, nous ne considérerons jamais un faisceau comme un espace topologique (ni même comme l'ensemble réunion de ses fibres), et nous ne considérerons pas davantage un morphisme $u : \mathscr{F} \to \mathscr{G}$ de tels faisceaux sur X comme une application continue d'espaces topologiques.

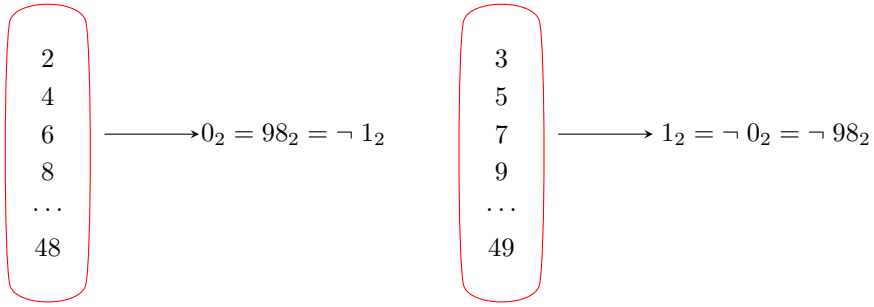
Annexe 5 : Somme des inverses des puissances de 2

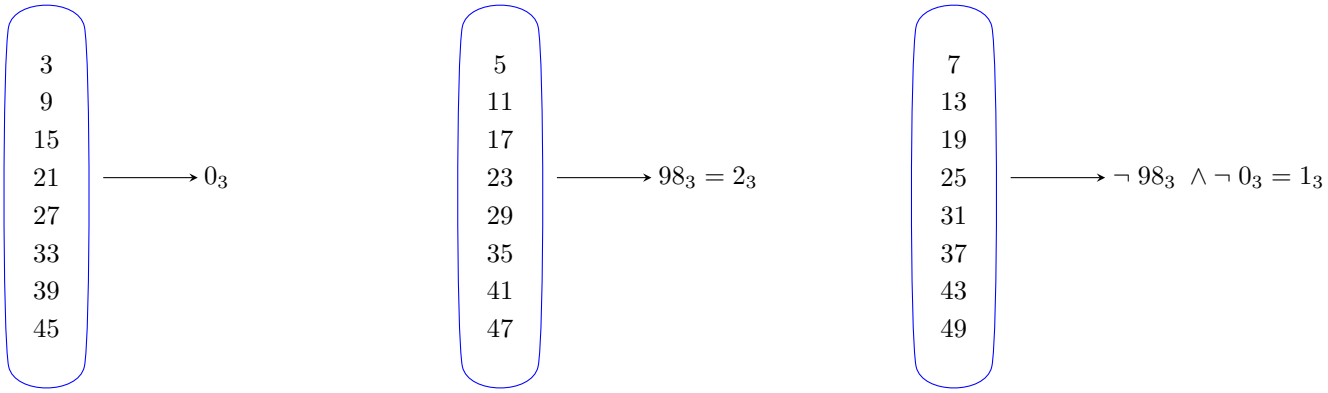
$$\sum_{i=1}^{n} \frac{1}{2^i} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^n}$$

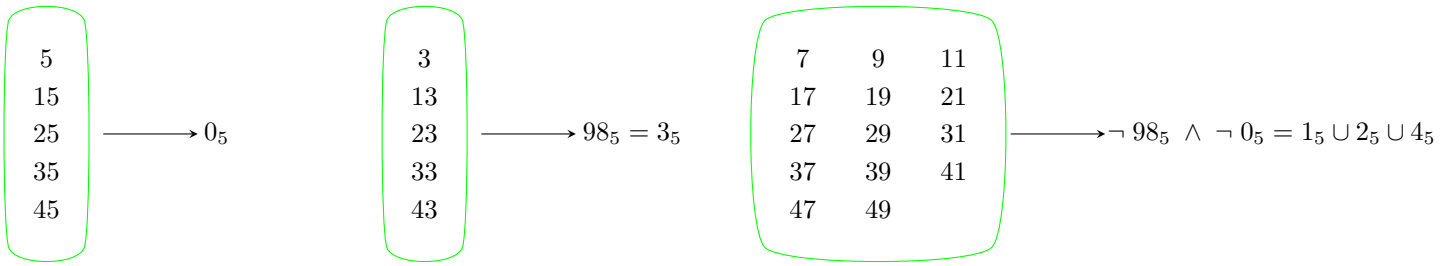
Il s'agit d'une suite géométrique de raison $\frac{1}{2}$ et de premier terme égal à $\frac{1}{2}$. La formule donne donc :

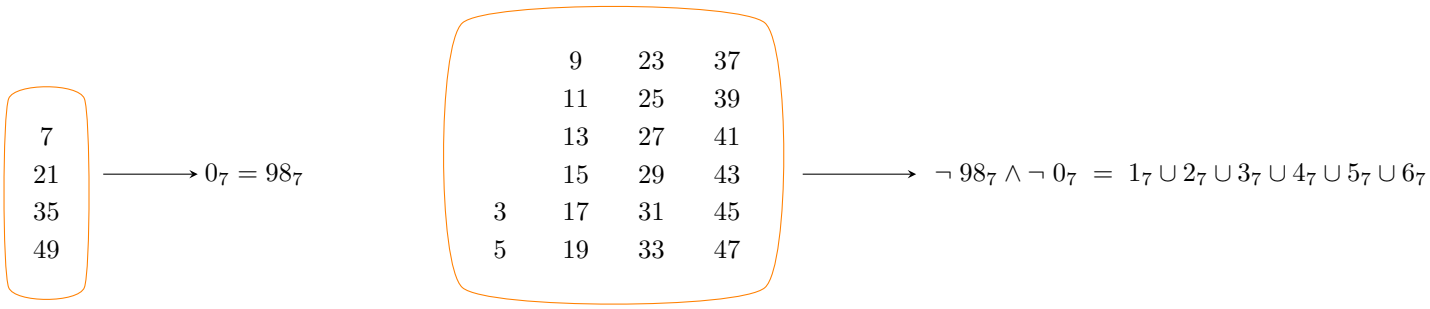
$$S_n = \frac{1}{2} \frac{1 - \frac{1}{2}^n}{1 - \frac{1}{2}} = \frac{1}{2} \frac{1 - \frac{1}{2^n}}{\frac{1}{2}} = 1 - \frac{1}{2^n}$$

Annexe 6 : Décomposants de Goldbach de 98









$$\neg\, 98_2 \cap (\neg\, 98_3 \ \wedge \neg\, 0_3) \cap (\neg\, 98_5 \ \wedge \neg\, 0_5) \cap (\neg 98_7 \ \wedge \neg\, 0_7) = \{19, 31, 37\}$$

$$98 \ = \ 19{+}79 \ = \ 31{+}67 \ = \ 37{+}61$$

Bibliographie

[1] Alexander Grothendieck, Éléments de Géométrie Algébrique (EGA), I. Le langage des schémas, Publications mathématiques de l'I.H.É.S., tome 4 (1960), p. 5-228.