Dancing links pour Conjecture de Goldbach.

Danse des premiers selon Alain Connes, fin de lapplication du crible en python.

Une gourmandise.

Repriser : patchwork plutôt que brins de laine.

Exemples : pavages du plan par des parallélogrammes pour les doubles de nombres premiers.

Mots périodiques ou comment projeter tous les restes sur 0 ou 1.

Palindromie dans les séquences booléennes conjonctions de séquences périodiques.

Conjonctions de mots booléens.

Balade dans le jardin des premiers.

Dés.

IHES sous la neige.

Théorème de Morley dans $Z/13Z$.

Conjecture de Goldbach, où l'on retrouve autrement.

Divisions euclidiennes représentées par des matrices.

Matrices du groupe affine....

Polygones en scratch.

Triangles colorées.

Théorème de Morley dans le corps des quaternions.

Nombres et sphère quantique.

Probabiliste ou quantique ?.

Spectres de la somme de somme de cosinus.

Spectre lumineux.

Décompositions de matrices en valeurs singulières.

Décomposition en valeurs singulières d'une matrice diagonale de nombres premiers.

Décomposition en valeurs singulières d'une matrice diagonale particulière.

Décomposition en valeurs singulières d'une matrice un peu creuse mais particulière.

Décomposition en valeurs singulières de matrices particulières.

Probabilités de transition.

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.

extrait des Leçons de solfège et de piano de Pascal Quignard.

Probabilités disjointes ou application du crible de Poincaré quand on élimine au maximum 2 classes de congruence sur p selon tout p premier.

Picorer l'aléa.

Entre deux.

Des premiers comme s'il en pleuvait.

Compositions palindromiques.

dessins divers : chaleur, spirales, sommes de carrés.

Section 182 des Recherches arithmétiques de Gauss.

Retour aux polynômes de Tchebychev ainsi que d'autre part aux indices de la section 53 des Recherches arithmétiques de Gauss.

Caractérisation topologique des nombres premiers.

Grouper par quatre.

Des puissances et des palindromes.

Programme de recherche des premiers par les propriétés quadratiques.

Nombres premiers et aires dans un carré.

Différents programmes de recherche de nombres premiers, dessin sur cercles unités, pièce de puzzle généralisation de CG aux impairs.

Résidus quadratiques sur colliers.

Résidus quadratiques sur colliers pour nombres pairs.

Décomposants de Goldbach sur colliers pour nombres pairs.

Ô stop !.

Conjecture de Goldbach et les impairs.

Tores trapézodaux.

Matrices de pixels.

D'un Z qui veut dire....

Conjecture de Goldbach, où l'on retrouve ζ autrement.

Goldbach's conjecture, where we find ζ in another way.

Un ensemble, une transformation, des traces.

Annexe la proposition denitac.pdf.

Pgcd et Ppcm reprsents sur diagrammes commutatifs.

Plaid cossais tropical.

Proposition de dmonstration de la conjecture de Goldbach dans le formalisme des topos.

Surprise par une somme alternée de cosinus quotientés.

Comment ils passent peut-être des courbes à leurs triangles fléchés.

Proposition de démonstration de la conjecture de Goldbach dans le formalisme des topos (mise en couleur des problèmes).

Proposition de démonstration de la conjecture de Goldbach dans le formalisme des topos, reprisée.

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).

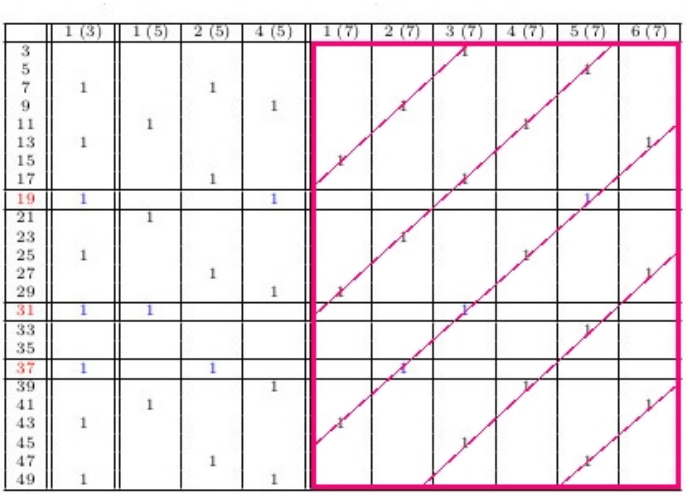
	1 (3)	1 (5)	2 (5)	4 (5)	1 (7)	2 (7)	3 (7)	4 (7)	5 (7)	6 (7)
3							1			
5									1	
7	1		1							
9				1		1				
11		1						1		
13	1									1
15					1					
17			1				1			
19	1			1					1	
21		1								
23						1				
25	1							1		
27			1							1
29				1	1					
31	1	1					1			
33									1	
35										
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)

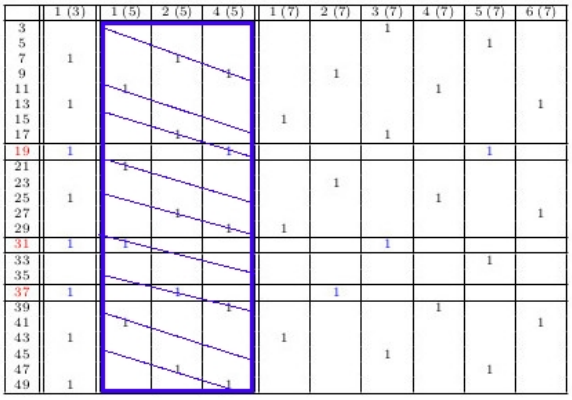
On poursuit à partir du tableau fourni à la fin de la note http://denise.vella.chemla.free.fr/DLpourCG.pdf dans le but d'y "voir les tores de chacun" (i.e. de chaque module).

	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 :



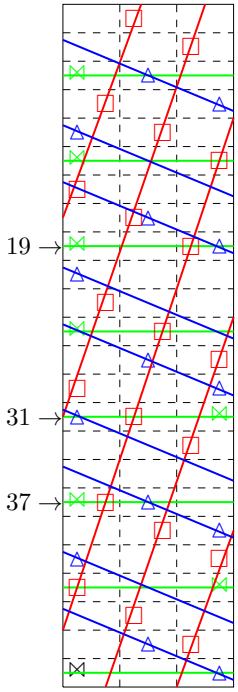
Le tore selon le module 5 :



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
43	1				1					
45							1			
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.



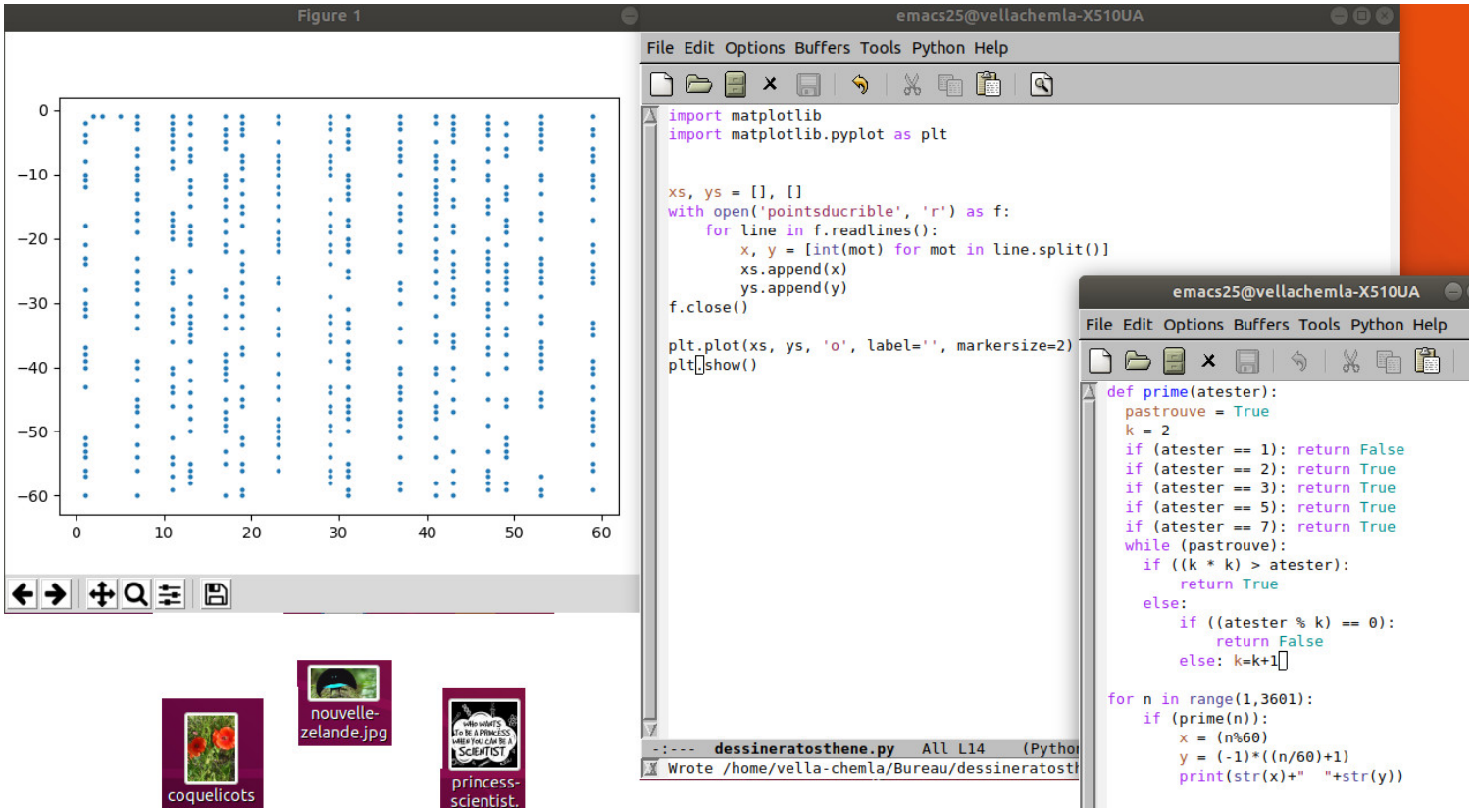


Figure 1
0
−10
−20
−30
−40
−50
−60
0
10
20
30
40
50
60
emacs25@vellachemla-X510UA
File Edit Options Buffers Tools Python Help
import matplotlib
import matplotlib.pyplot as plt
xs, ys = [], []
with open('pointsducrible', 'r') as f:
for line in f.readlines():
x, y = [int(mot) for mot in line.split()]
xs.append(x)
ys.append(y)
f.close()
plt.plot(xs, ys, 'o', label='', markersize=2)
plt.show()
-:--- dessineratosthene.py All L14 (Python
Wrote /home/vella-chemla/Bureau/dessineratosth
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.

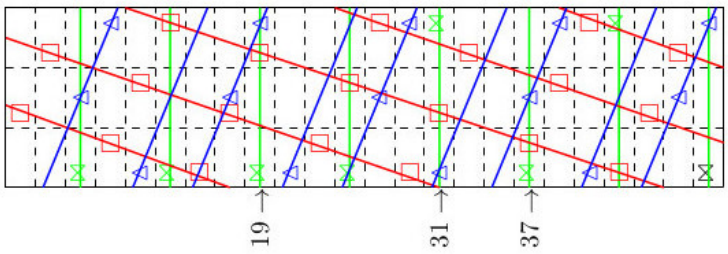
Imaginer sur ce tore un k-ième feuilletage non parallèle à un méridien du tore, différent de tous les feuilletages précédents. Seules p_k ou $2p_k$ feuilles de ce k-ième feuilletage contiennent au moins un point.

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).

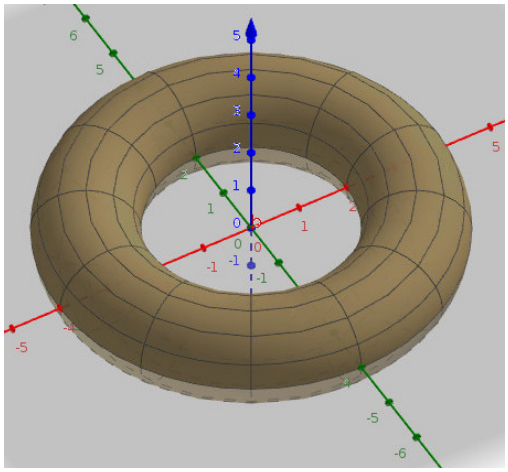


1. C'est un très joli roman, de Muriel Barbery, dans lequel un cuisinier cherche désespérément à retrouver un certain goût de son enfance.
2. Le trois-frères est un gâteau créé au XIX$^{\text{ème}}$ siècle par les trois frères Julien, célèbres pâtissiers parisiens, et qui est toujours cuit dans un moule 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.

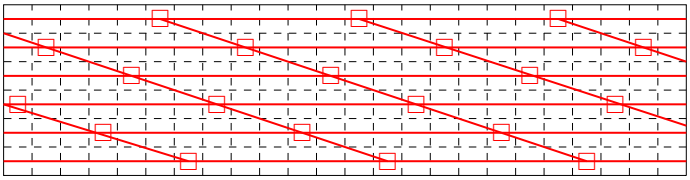
Repriser : patchwork plutôt que brins de laine (Denise Vella-Chemla, 3.1.2018)

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.

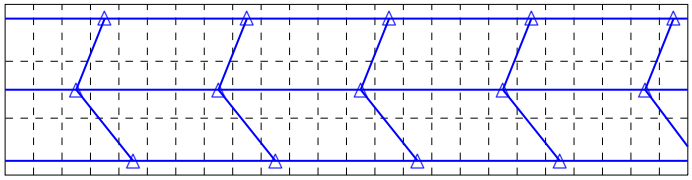
Peut-être vaudrait-il mieux considérer un maillage du tore par des polytopes dont les faces sont des parallélogrammes. Les longueurs de certains côtés des parallélogrammes seraient fixées par les modules (des nombres premiers) et les faces en question ne seraient pas des rectangles pour tous les modules 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.



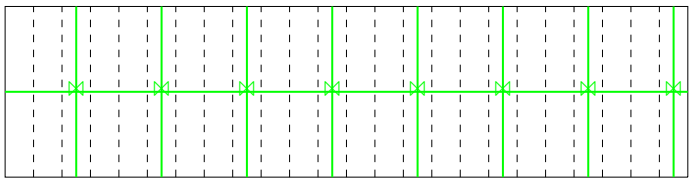
Par exemple, voici le maillage selon le module 7 à la recherche des décomposants de Goldbach de 98.



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.

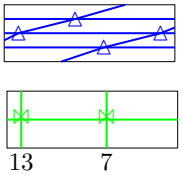


Démontrer la conjecture de Goldbach consisterait alors à démontrer qu'il existe toujours une section du tore selon un méridien [2] qui contient un sommet de chaque polytope.

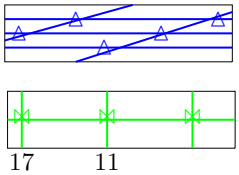
1. Cf. http://denise.vella.chemla.free.fr/topo.pdf.
2. On appelle méridien un petit cercle qui supporte le tore.

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

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



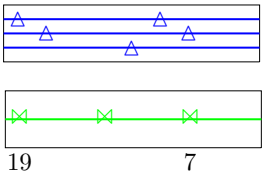
$n = 34$
$n \equiv 1\ (3),\ n \equiv 4\ (5)$
$sol \equiv 2\ (3),\ sol \equiv 1, 2, 3\ (5)$



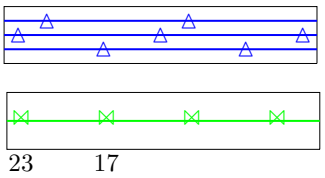
Pour les nombres suivants, on omet les petits côtés des parallélogrammes. La distance horizontale entre deux noeuds-papillon verts est toujours 3, la distance horizontale entre deux triangles bleus d'une même ligne est toujours 5, la distance horizontale entre deux carrés rouges d'une même ligne est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

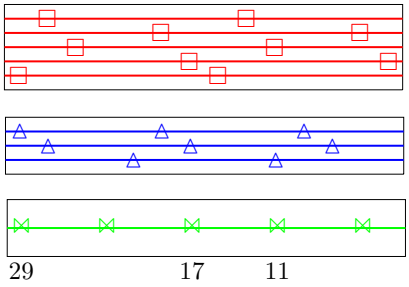
$n = 38$
$n \equiv 2\ (3),\ n \equiv 3\ (5)$
$sol \equiv 1\ (3),\ sol \equiv 1, 2, 4\ (5)$



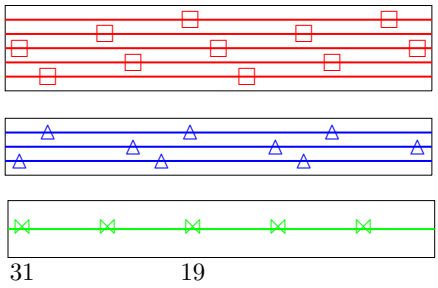
$n = 46$
$n \equiv 1\ (3),\ n \equiv 1\ (5)$
$sol \equiv 2\ (3),\ sol \equiv 2, 3, 4(5)$



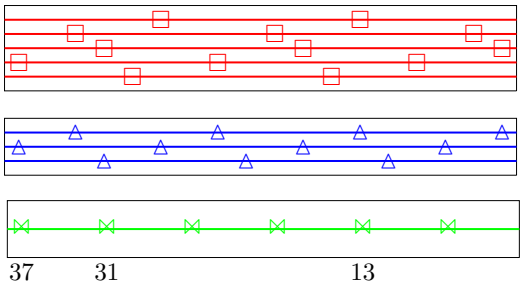
$n = 58$
$n \equiv 1\ (3),\ n \equiv 3\ (5),\ n \equiv 2\ (7)$
$sol \equiv 2\ (3),\ sol \equiv 1, 2, 4\ (5),\ sol \equiv 1, 3, 4, 5, 6\ (7)$



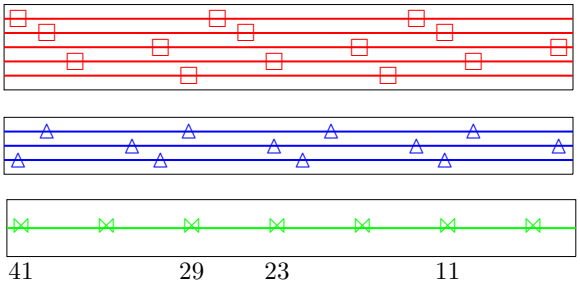
$n = 62$
$n \equiv 2\ (3),\ n \equiv 2\ (5),\ n \equiv 6\ (7)$
$sol \equiv 1\ (3),\ sol \equiv 1, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 5\ (7)$



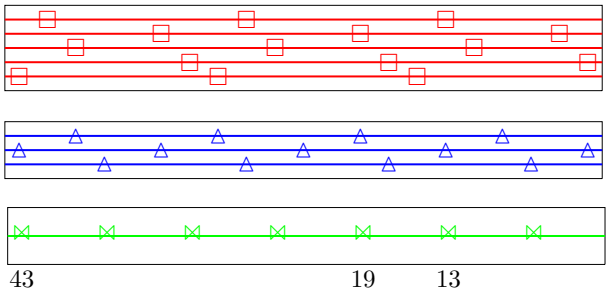
$n = 74$
$n \equiv 2\ (3),\ n \equiv 4\ (5),\ n \equiv 4\ (7)$
$sol \equiv 1\ (3),\ sol \equiv 1, 2, 3\ (5),\ n \equiv 1, 2, 3, 5, 6\ (7)$



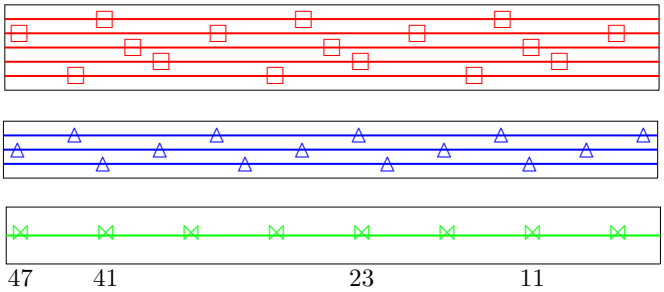
$n = 82$
$n \equiv 1\ (3),\ n \equiv 2\ (5),\ n \equiv 5\ (7)$
$sol \equiv 2\ (3),\ sol \equiv 1, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 6\ (7)$



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



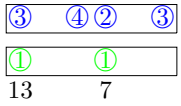
$n = 94$
$n \equiv 1\ (3),\ n \equiv 4\ (5),\ n \equiv 3\ (7)$
$sol \equiv 2\ (3),\ sol \equiv 1, 2, 3\ (5),\ sol \equiv 1, 2, 4, 5, 6\ (7)$



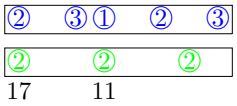
Mots périodiques ou comment projeter tous les restes sur 0 ou 1 (Denise Vella-Chemla, 4.1.2019)

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 : $26 = 3 + 23$.

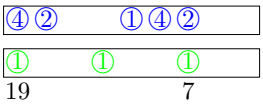
$n = 26$
$n \equiv 2\ (3),\ n \equiv 1\ (5)$
$sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5)$



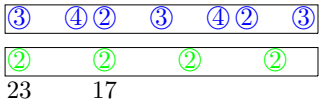
$n = 34$
$n \equiv 1\ (3),\ n \equiv 4\ (5)$
$sol \equiv 2\ (3),\ sol \equiv 1, 2, 3\ (5)$



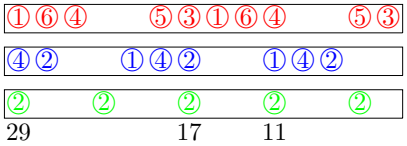
$n = 38$
$n \equiv 2\ (3),\ n \equiv 3\ (5)$
$sol \equiv 1\ (3),\ sol \equiv 1, 2, 4\ (5)$



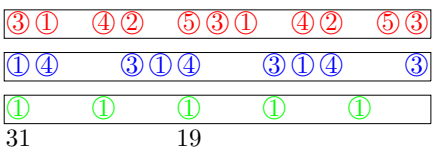
$n = 46$
$n \equiv 1\ (3),\ n \equiv 1\ (5)$
$sol \equiv 2\ (3),\ sol \equiv 2, 3, 4\ (5)$



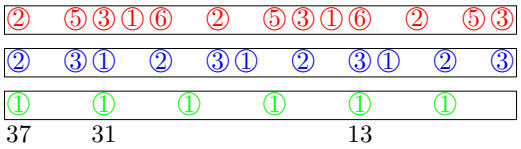
$n = 58$
$n \equiv 1\ (3),\ n \equiv 3\ (5),\ n \equiv 2\ (7)$
$sol \equiv 2\ (3),\ sol \equiv 1, 2, 4\ (5),\ sol \equiv 1, 3, 4, 5, 6\ (7)$



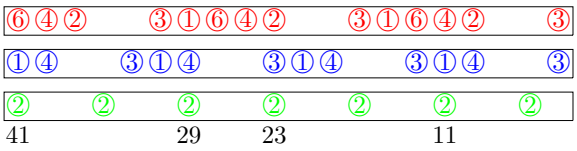
$n = 62$
$n \equiv 2\ (3),\ n \equiv 2\ (5),\ n \equiv 6\ (7)$
$sol \equiv 1\ (3),\ sol \equiv 1, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 5\ (7)$



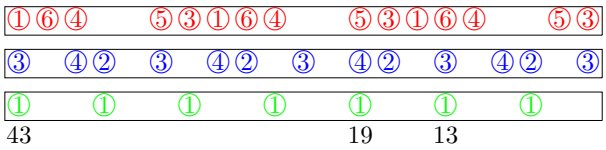
$n = 74$
$n \equiv 2\ (3),\ n \equiv 4\ (5),\ n \equiv 4\ (7)$
$sol \equiv 1\ (3),\ sol \equiv 1, 2, 3\ (5),\ n \equiv 1, 2, 3, 5, 6\ (7)$



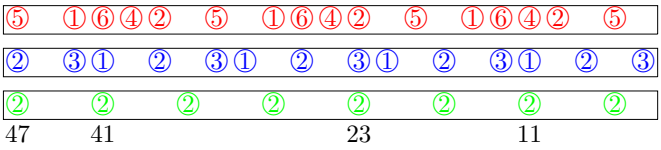
$n = 82$
$n \equiv 1\ (3),\ n \equiv 2\ (5),\ n \equiv 5\ (7)$
$sol \equiv 2\ (3),\ sol \equiv 1, 3, 4\ (5),\ sol \equiv 1, 2, 3, 4, 6\ (7)$

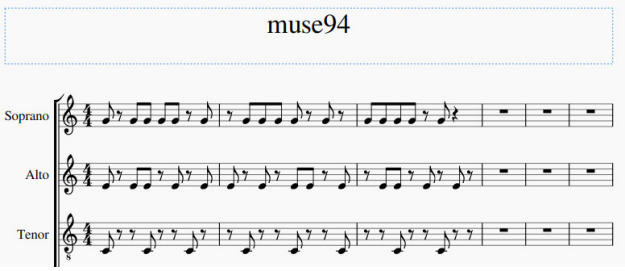


$n = 86$
$n \equiv 2\ (3),\ n \equiv 1\ (5),\ n \equiv 2\ (7)$
$sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5),\ sol \equiv 1, 3, 4, 5, 6\ (7)$



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





101111010111010111010
101101011010110101 10101
100100100100100100 10010

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 :

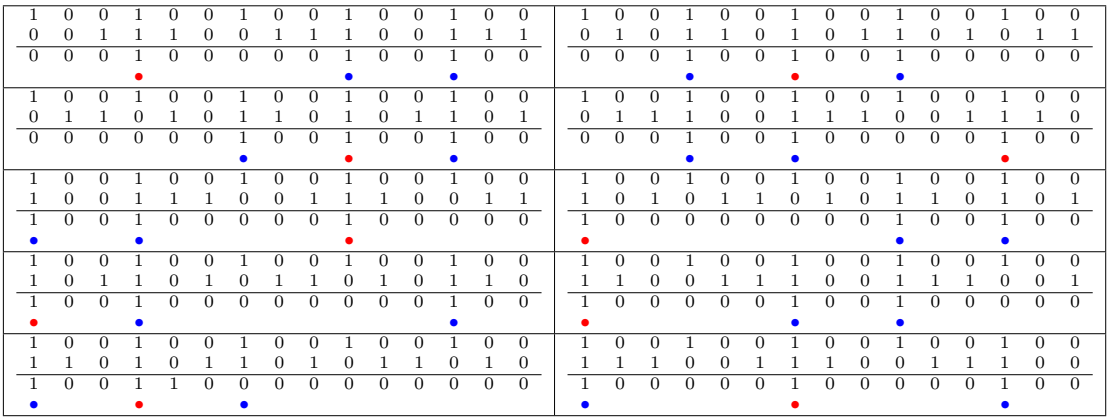
- 100,
- 010,
- 001.

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.

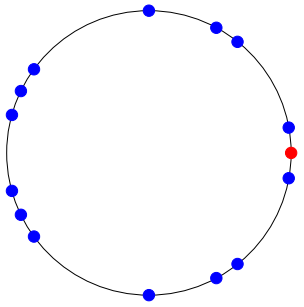
Cette propriété a pour conséquence (il faudrait le démontrer) qu'il y a toujours une solution de position très basse par rapport à la longueur du mot considéré.

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.

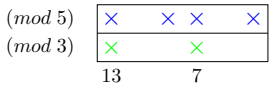
On peut cependant vérifier que ces idées sont correctes en comptant le nombre de solutions pour la chaîne calculée ci-dessus : elle contient 136 solutions (les lettres 1 à la même position dans $s1$ et $s2$) pour une longueur de $1155 = 3 \times 5 \times 7 \times 11$, $\frac{136}{1155} = 0.117$ et ce 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.

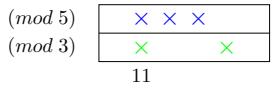
Mots périodiques ou comment projeter tous les restes sur 0 ou 1 (suite) (Denise Vella-Chemla, 9.1.2019)

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.

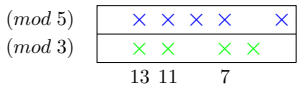
$n = 26,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\quad$ $sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5)$



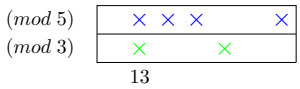
$n = 28,\ n \equiv 1\ (3),\ n \equiv 3\ (5)$ $\quad$ $sol \equiv 2\ (3),\ sol \equiv 1, 2, 4\ (5)$



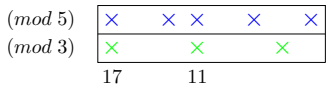
$n = 30,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\quad$ $sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5)$



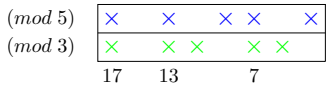
$n = 32,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\quad$ $sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5)$



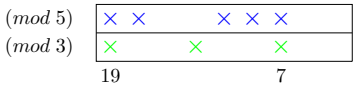
$n = 34,\ n \equiv 1\ (3),\ n \equiv 4\ (5)$ $\quad$ $sol \equiv 2\ (3),\ sol \equiv 1, 2, 3\ (5)$



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



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

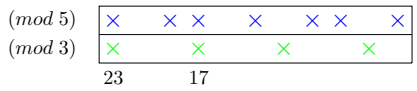


$n = 40,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\quad$ $sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5)$

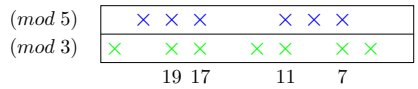
$n = 42,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\quad$ $sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5)$

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

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

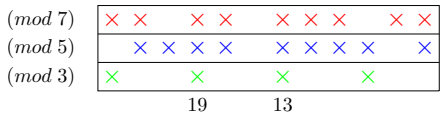


$n = 48,\ n \equiv 2\ (3),\ n \equiv 1\ (5)$ $\qquad$ $sol \equiv 1\ (3),\ sol \equiv 2, 3, 4\ (5)$



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

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

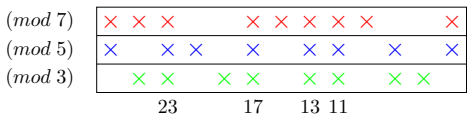


$n = 52,\ n \equiv 1\ (3),\ n \equiv 2\ (5),\ n \equiv 3\ (7)$

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

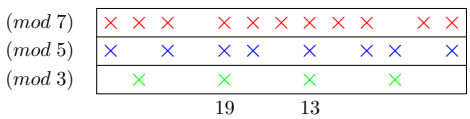
$n = 54,\ n \equiv 0\ (3),\ n \equiv 4\ (5),\ n \equiv 5\ (7)$

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



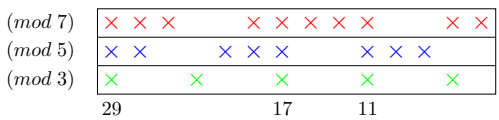
$n = 56,\ n \equiv 2\ (3),\ n \equiv 1\ (5),\ n \equiv 0\ (7)$

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



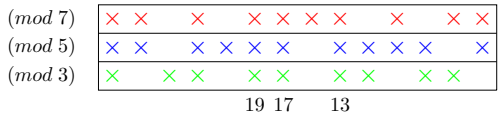
$n = 58,\ n \equiv 1\ (3),\ n \equiv 3\ (5),\ n \equiv 2\ (7)$

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



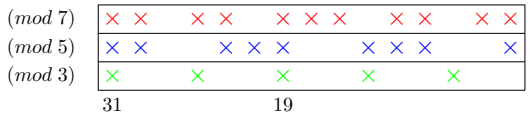
$n = 60,\ n \equiv 0\ (3),\ n \equiv 0\ (5),\ n \equiv 4\ (7)$

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



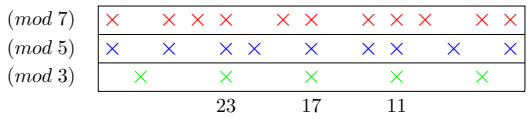
$n = 62,\ n \equiv 2\ (3),\ n \equiv 2\ (5),\ n \equiv 6\ (7)$

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



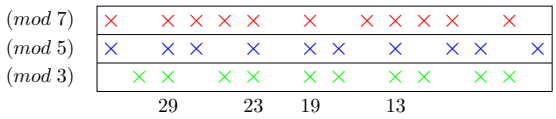
$n = 64,\ n \equiv 1\ (3),\ n \equiv 4\ (5),\ n \equiv 1\ (7)$

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



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

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

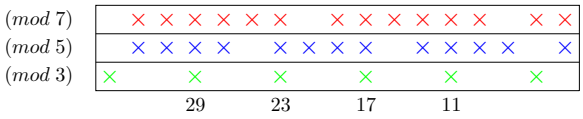


$n = 68,\ n \equiv 2\ (3),\ n \equiv 3\ (5),\ n \equiv 5\ (7)$

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

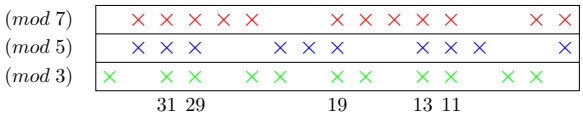
$n = 70,\ n \equiv 1\ (3),\ n \equiv 0\ (5),\ n \equiv 0\ (7)$

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



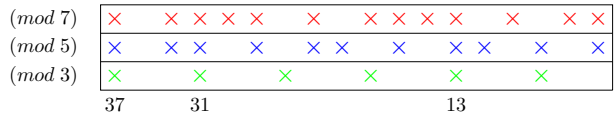
$n = 72,\ n \equiv 0\ (3),\ n \equiv 2\ (5),\ n \equiv 2\ (7)$

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



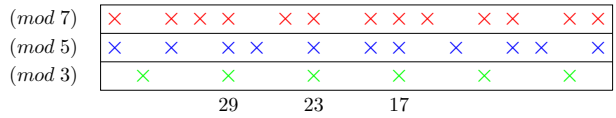
$n = 74,\ n \equiv 2\ (3),\ n \equiv 4\ (5),\ n \equiv 4\ (7)$

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



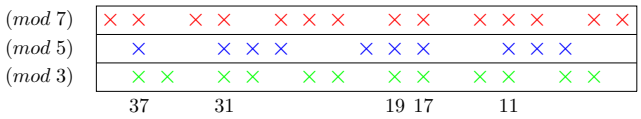
$n = 76,\ n \equiv 1\ (3),\ n \equiv 1\ (5),\ n \equiv 6\ (7)$

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



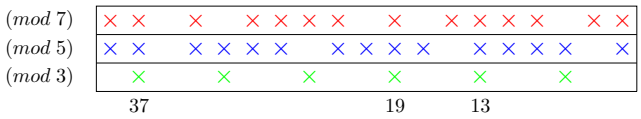
$n = 78,\ n \equiv 0\ (3),\ n \equiv 3\ (5),\ n \equiv 1\ (7)$

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



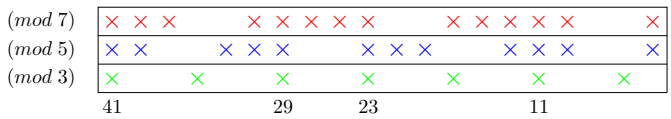
$n = 80,\ n \equiv 2\ (3),\ n \equiv 0\ (5),\ n \equiv 3\ (7)$

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



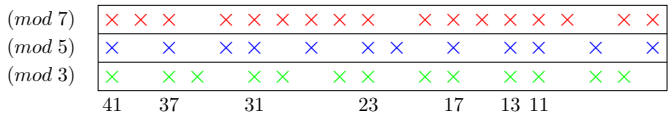
$n = 82,\ n \equiv 1\ (3),\ n \equiv 2\ (5),\ n \equiv 5\ (7)$

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



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

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

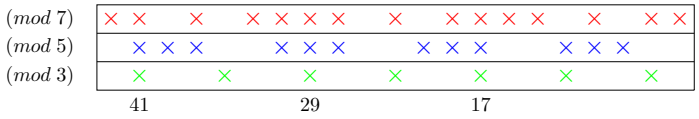


$n = 86,\ n \equiv 2\ (3),\ n \equiv 4\ (5),\ n \equiv 2\ (7)$

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

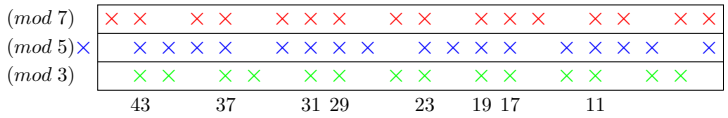
$n = 88,\ n \equiv 1\ (3),\ n \equiv 3\ (5),\ n \equiv 4\ (7)$

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



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

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

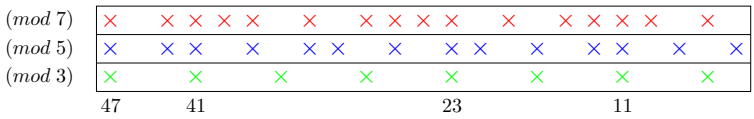


$n = 92,\ n \equiv 2\ (3),\ n \equiv 2\ (5),\ n \equiv 1\ (7)$

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

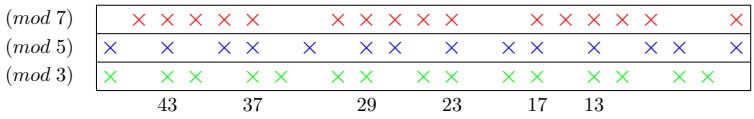
$n = 94,\ n \equiv 1\ (3),\ n \equiv 4\ (5),\ n \equiv 3\ (7)$

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



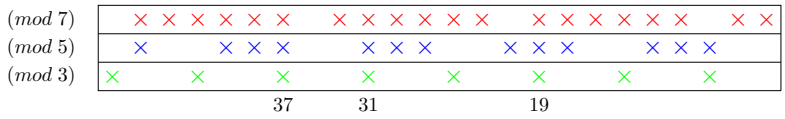
$n = 96,\ n \equiv 0\ (3),\ n \equiv 1\ (5),\ n \equiv 5\ (7)$

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



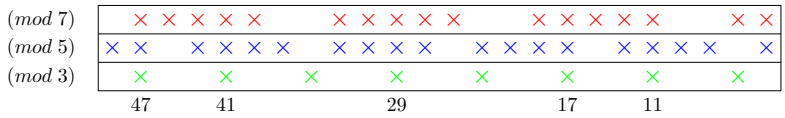
$n = 98,\ n \equiv 2\ (3),\ n \equiv 3\ (5),\ n \equiv 0\ (7)$

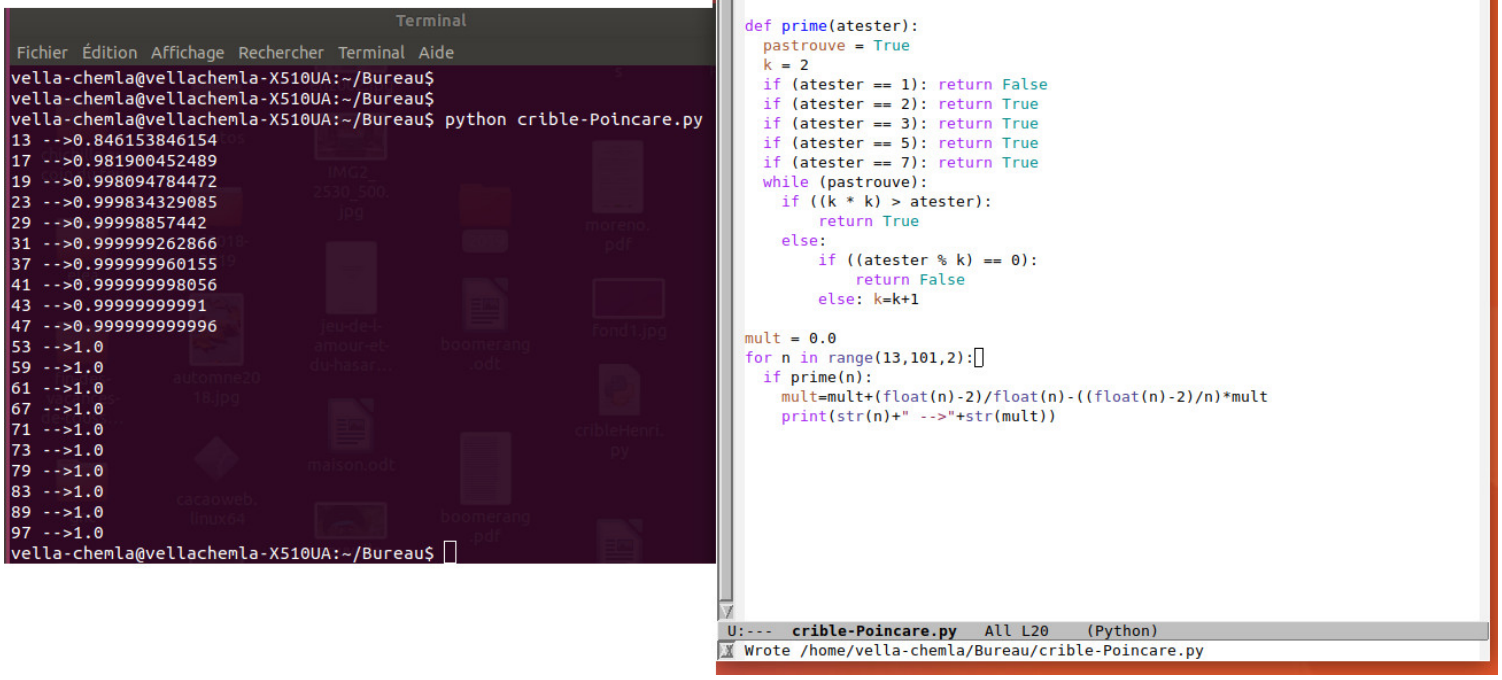
$$sol \equiv 1\ (3),\ sol \equiv 1, 2, 4\ (5),\ sol \equiv 1, 2, 3, 4, 5, 6\ (7)$$



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

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



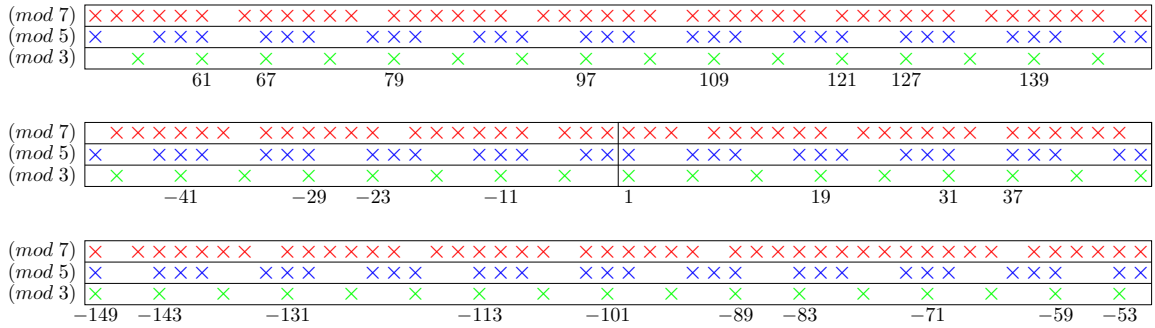

Terminal
Fichier Édition Affichage Rechercher Terminal Aide
vella-chemla@vellachemla-X510UA:~/Bureau$
vella-chemla@vellachemla-X510UA:~/Bureau$
vella-chemla@vellachemla-X510UA:~/Bureau$ python crible-Poincare.py
13 -->0.846153846154
17 -->0.981900452489
19 -->0.998094784472
23 -->0.999834329085
29 -->0.99998857442
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.

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

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 $\ldots, 12, 12, (0), 18, 12, 6, 24, 6, 12, 18, 12, 12, 6, 12, \ldots$, on constate la palindromie des écarts autour de l'écart 24. On le colore en bleu pour bien voir cette palindromie autour de lui.

$$\ldots, 12, 12, 18, 12, 6, 24, 6, 12, 18, 12, 12, 6, 12, \ldots$$

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

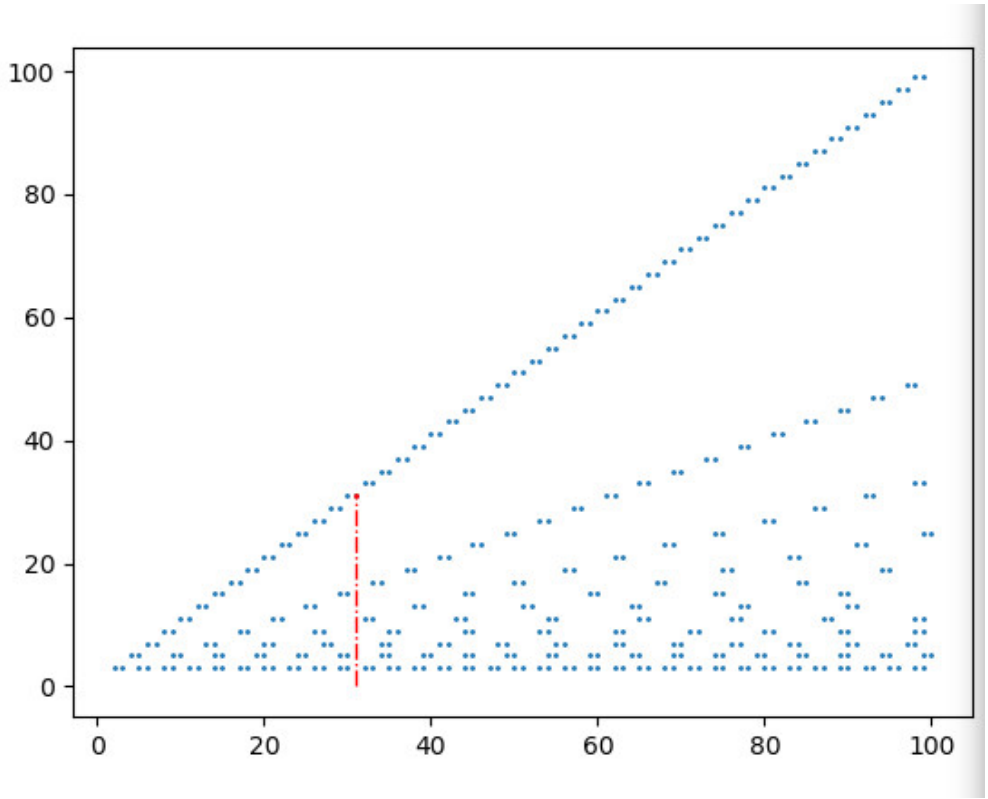
1. $\prod$ désigne le produit ici, et ne doit pas être confondu avec $\pi(n)$ utilisé pour dénoter le nombre de nombres premiers inférieurs ou égaux à n.

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 :

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

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

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

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

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

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 $\begin{pmatrix} \frac{2}{7} & \frac{5}{7} \end{pmatrix}$.

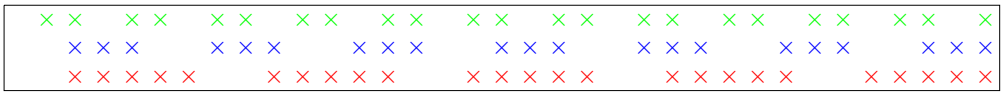
On calcule les probabilités par une sorte de produit tensoriel représenté à notre manière ainsi :

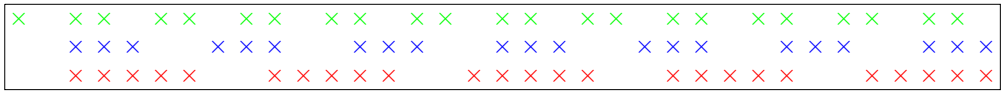
$$\begin{aligned} \begin{pmatrix} \frac{1}{3} & \frac{2}{3} \end{pmatrix} \begin{pmatrix} \frac{2}{5} & \frac{3}{5} \end{pmatrix} \begin{pmatrix} \frac{2}{7} & \frac{5}{7} \end{pmatrix} &= \begin{pmatrix} \frac{2}{15} & \frac{4}{15} & \frac{3}{15} & \frac{6}{15} \end{pmatrix} \begin{pmatrix} \frac{2}{7}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

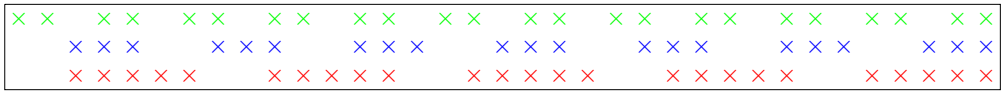
On a bien sûr obtenu 2^3 quantités (des cardinaux ensemblistes), à retrouver précisément parmi les colonnes de la première à la 105-ième.

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.

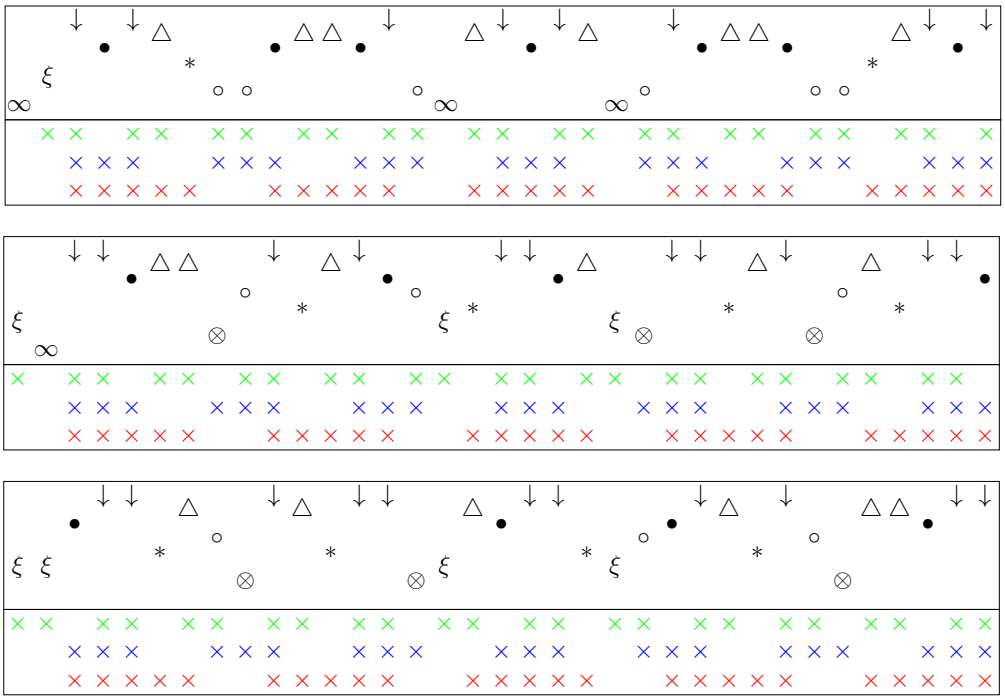
D'abord, dessinons des croix dans 3 grilles à lire à la suite l'une de l'autre, et qui respectent bien les motifs rythmiques qu'on s'est fixé (1/3, 2/3 pour la première ligne de chaque grille, 2/5, 3/5 pour la seconde ligne, et 2/7, 5/7 pour la troisième ligne.







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.

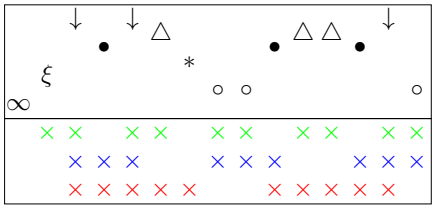


On retrouve nos cardinaux d'ensembles : 4 ∞, 6 $\otimes$, 8 ξ, 10 $*$, 12 $\circ$, 15 $\bullet$, 20 $\triangle$ et 30 $\downarrow$.

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.

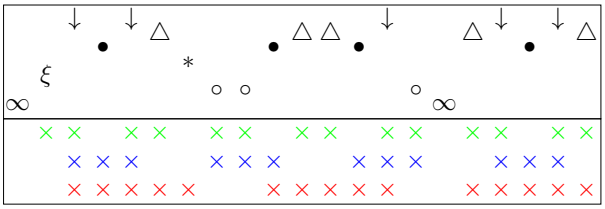
Imaginons maintenant que l'on ne veuille prendre qu'une sous-partie de la séquence des symboles, par exemple ses 15 premières colonnes, histoire de bien couper la séquence totale en 7, ou bien ses 21 premières colonnes (pour la couper en 5) ou enfin, ses 35 premières colonnes (pour la couper en 3, cette 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, ...)	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, ...)	7 $\bullet$ (1, ...)	15
3 $\triangle$ (6, ...)	5 $\triangle$ (4)	8 $\triangle$ (2, ...)	20
3 $\downarrow$ (10)	5 $\downarrow$ (6)	8 $\downarrow$ (3, ...)	30
15 (47/7 = 6, ...)	21 (31/7 = 4, ...)	35 (22/7 = 3, ...)	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 $(1, 2, \ldots, p-1)$, 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 :

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

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 :

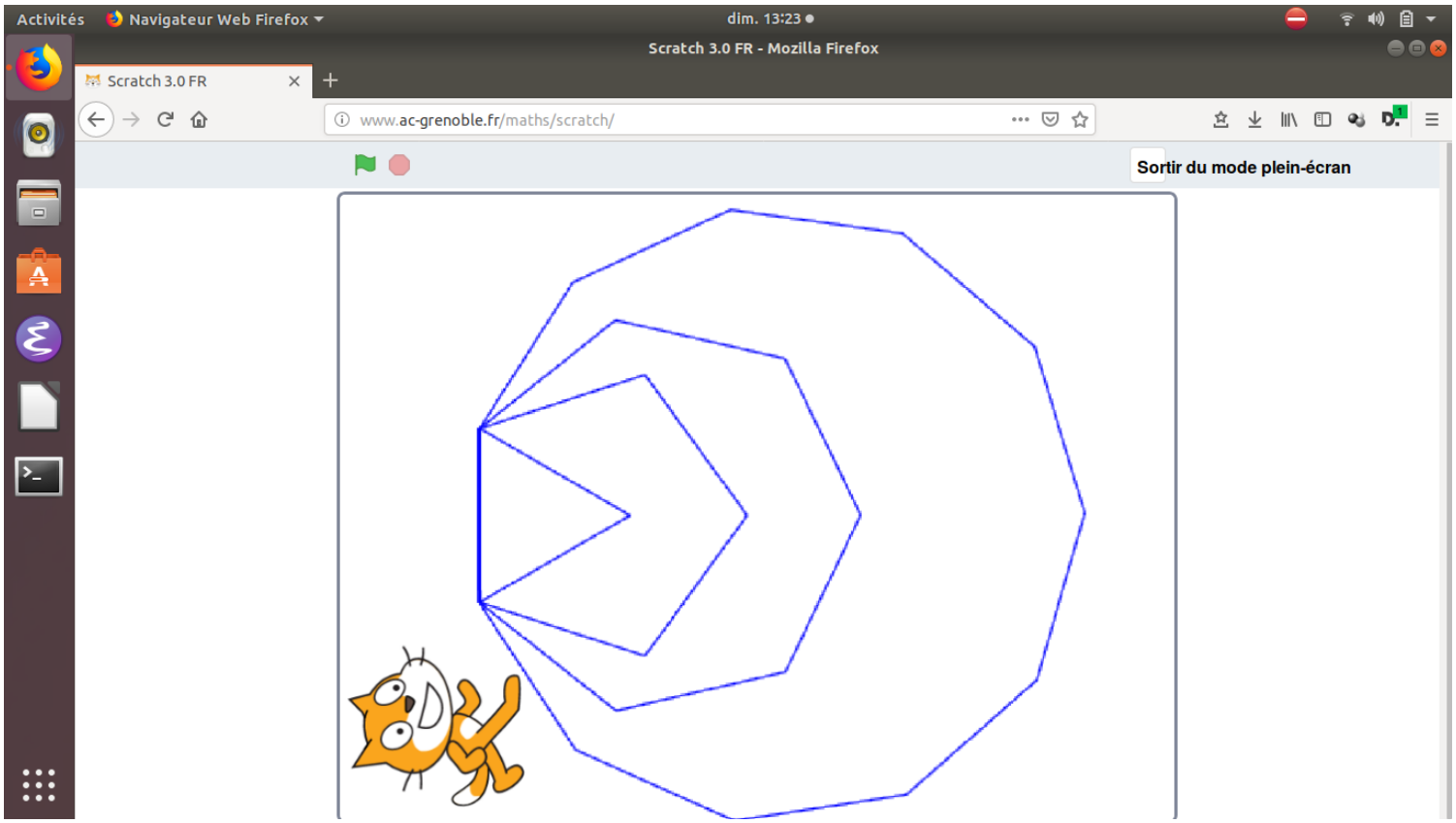
$$\begin{pmatrix} 0 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b' & a' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 1 \end{pmatrix}$$

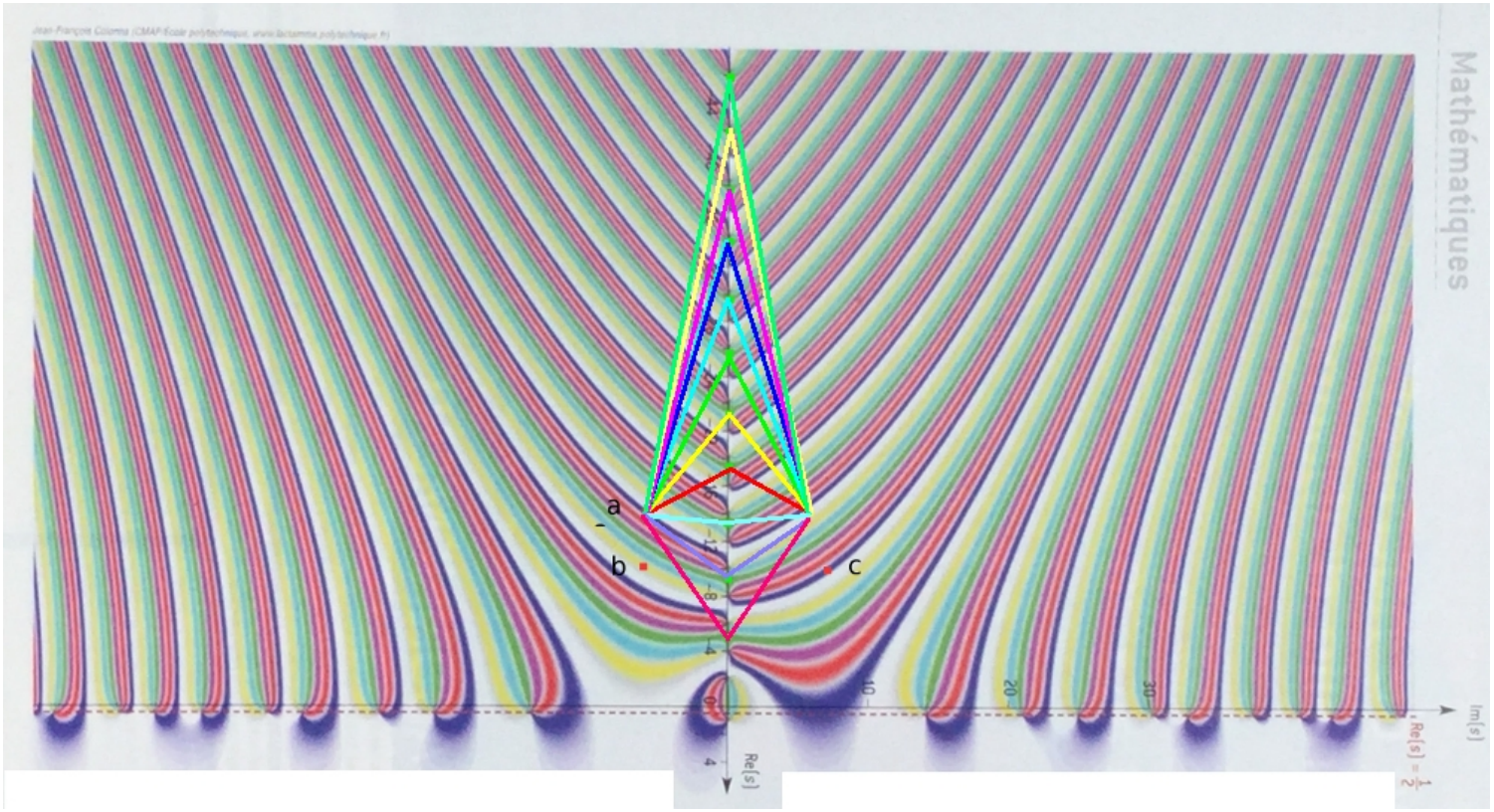
et

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

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	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$	$\begin{pmatrix}4&3\\0&1\end{pmatrix}$	$\begin{pmatrix}6&2\\0&1\end{pmatrix}$	$\begin{pmatrix}0&2\\0&1\end{pmatrix}$					


Activités
Navigateur Web Firefox
dim. 13:23
Scratch 3.0 FR - Mozilla Firefox
Scratch 3.0 FR
www.ac-grenoble.fr/maths/scratch/
Sortir du mode plein-écran


Jean-François Colonna (CMAP/Ecole polytechnique, www.lactamme.polytechnique.fr)
Mathématiques
a
b
c
Re(s)
Im(s)
Re(s) = 1/2

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 :

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

qui est de la forme :

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

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)

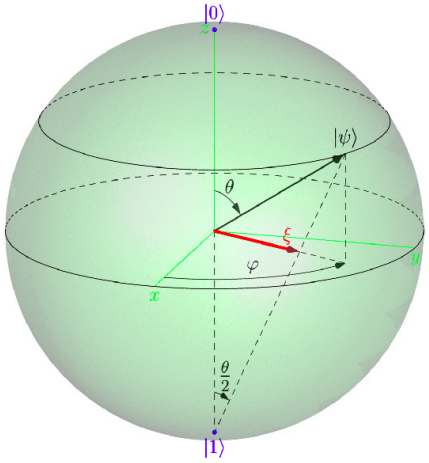
Ayant touché du doigt à l'été 2018 tout l'aléa qui semble gouverner le fait d'être ou de ne pas être premier pour un entier naturel donné, on souhaiterait ici modéliser les entiers naturels en utilisant des qubits sur la sphère quantique.

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].



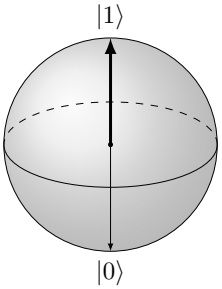
On rappelle qu'un nombre n étant donné, on a les définitions suivantes :

- 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.

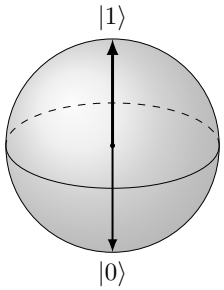
Le résultat de la division de n par d est aléatoire dans la mesure où on ne connaît pas n : quand d divisera n, le qubit fixera sa valeur sur $|0\rangle$ tandis qu'il fixera sa valeur sur $|1\rangle$ si d ne divise pas n.

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 $|0\rangle$.

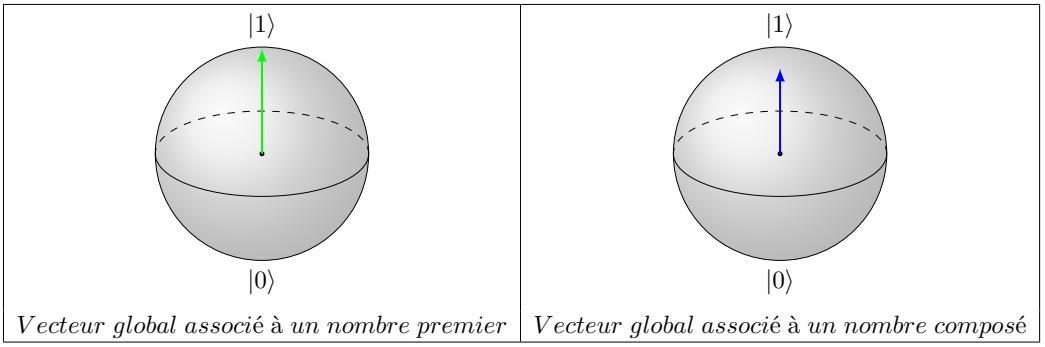


1. page dont on n'a pas trouvé le nom de l'auteur.

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.

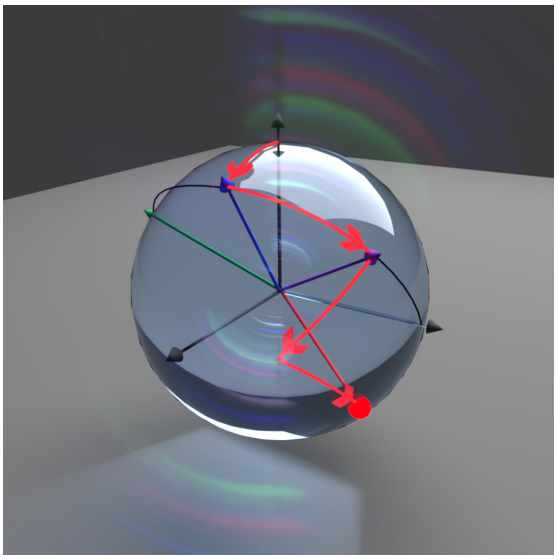


Vecteur global associé à *un nombre premier* | *Vecteur global associé* à *un nombre composé*

La superbe illustration suivante, trouvée à la page

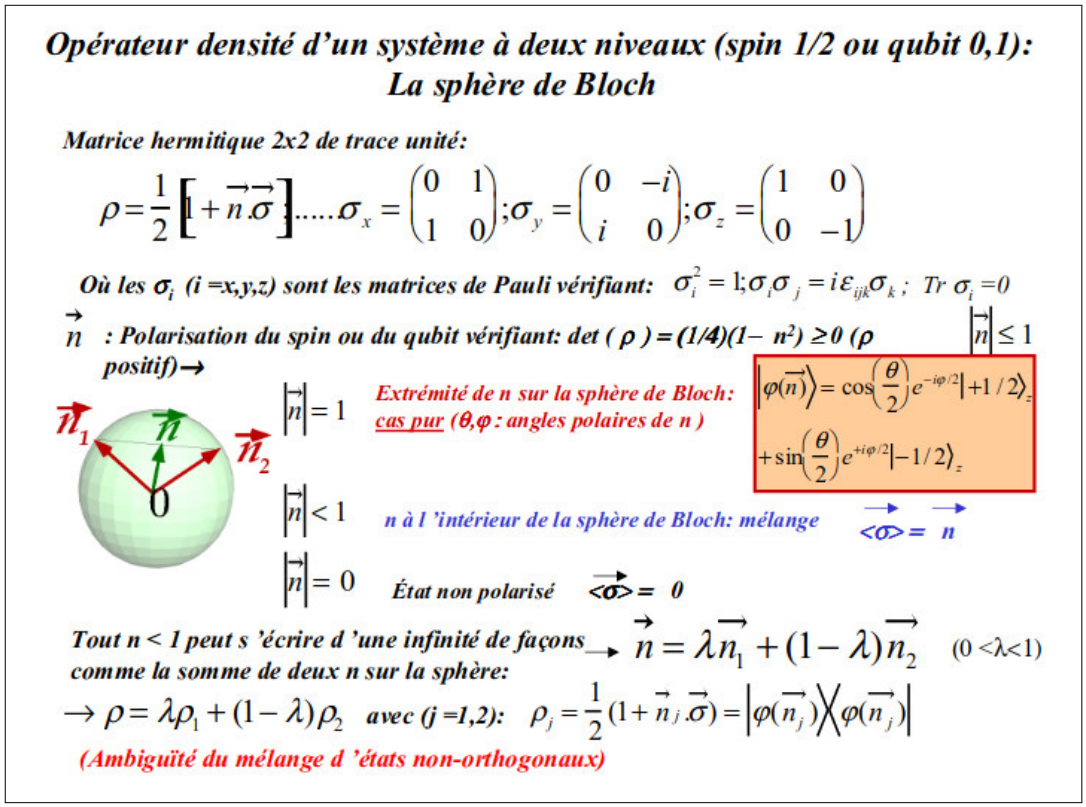
https://www.eurekalert.org/multimedia/pub/120313.php,

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$_S Haroche_0$80102.*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 : $état_x, état_y, état_{x+2}, état_{y-2} \longrightarrow \text{état}_{x+2}, état_y$.

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

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.

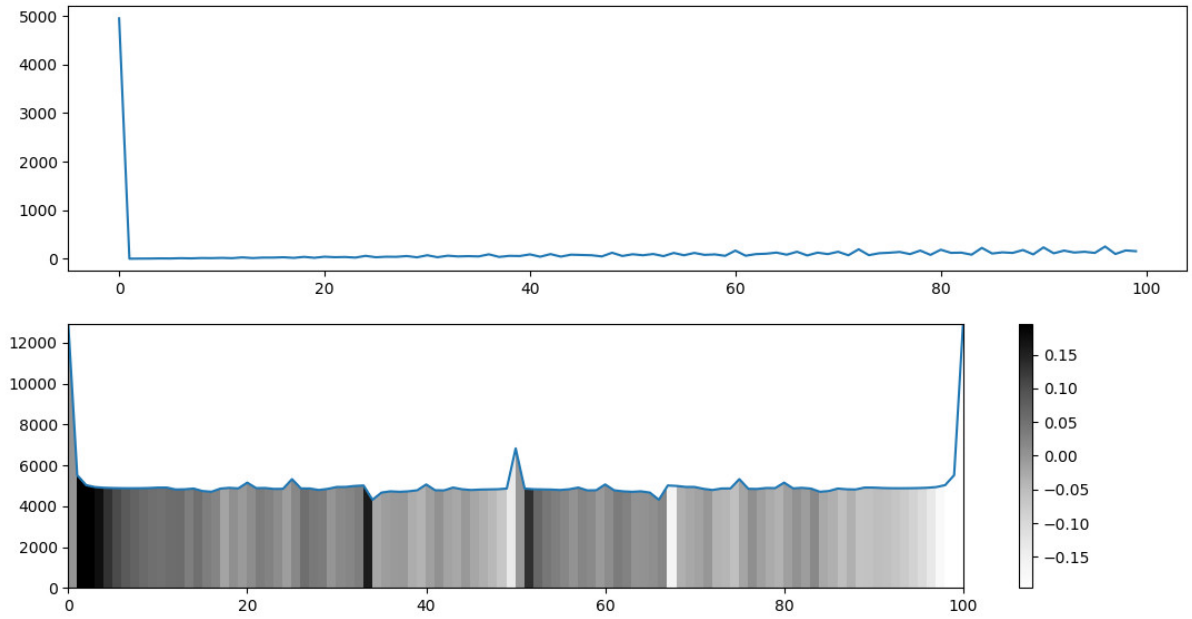
Comme la matrice, dans le cas quantique, doit être unitaire, il semblerait que ses éléments doivent prendre les valeurs $\frac{1}{\sqrt{p-1}}$ et $\sqrt{\frac{p-2}{p-1}}$ pour qu'on ait bien $\left(\frac{1}{\sqrt{p-1}}\right)^2 + \left(\sqrt{\frac{p-2}{p-1}}\right)^2 = \frac{1}{p-1} + \frac{p-2}{p-1}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

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 $(|0_p\rangle + |1_p\rangle)/\sqrt{p-1}$.

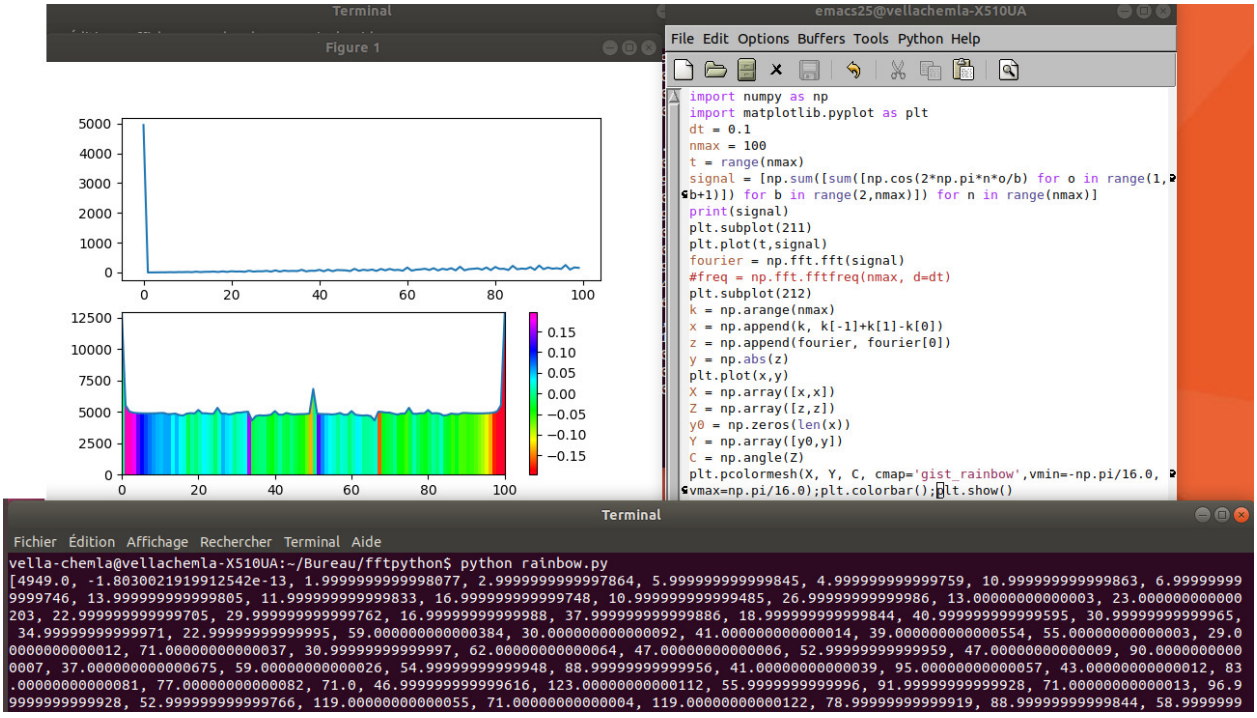
On n'a cependant pas les moyens de mettre en oeuvre ce dispositif d'une quelconque manière.

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)

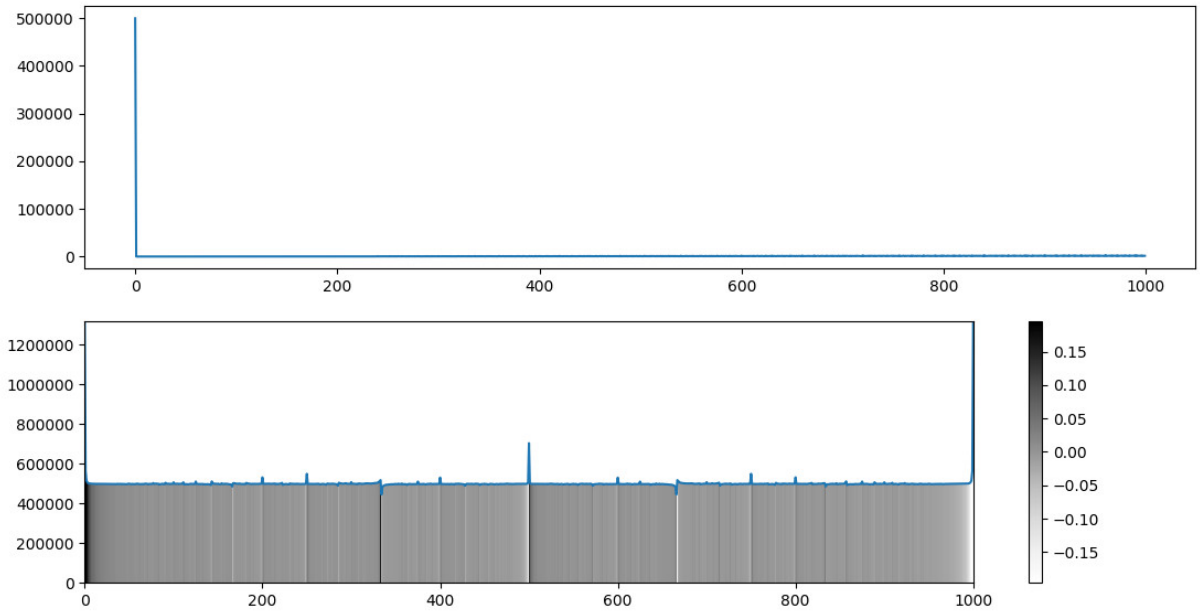
Spectres de la somme de somme de cosinus (Denise Vella-Chemla, 4.3.2019)



Couleurs arc-en-ciel

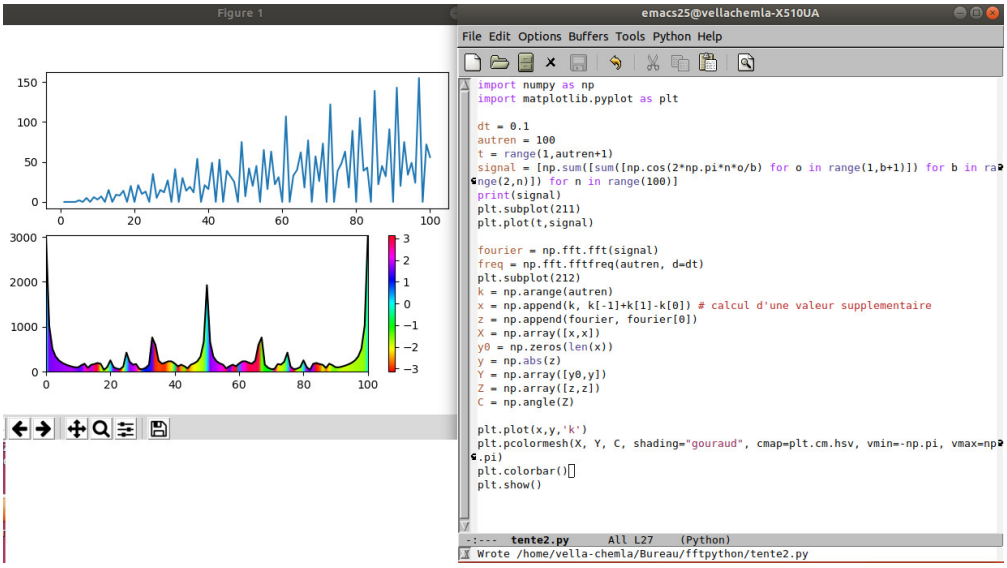


Idem jusqu'à 1000



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



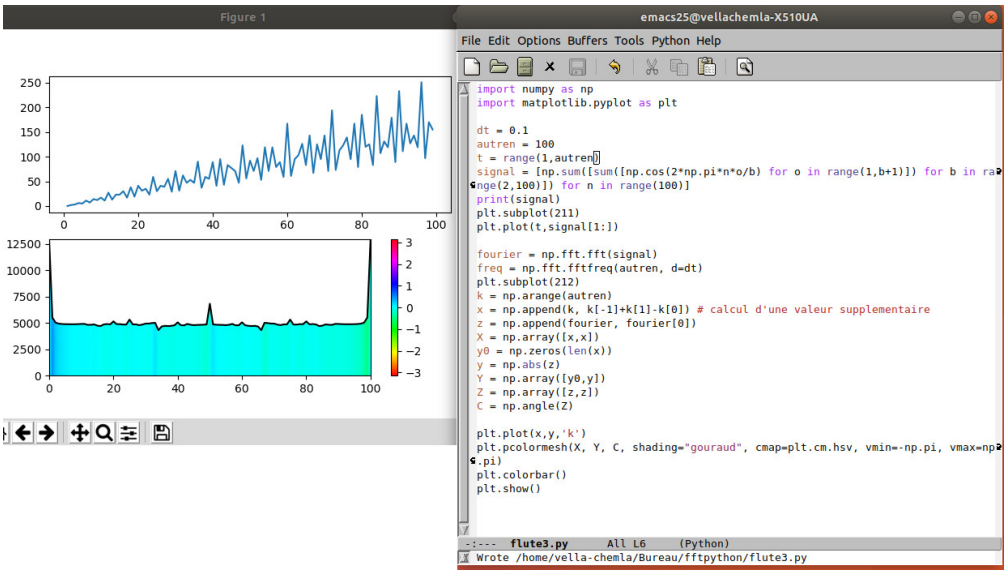


Figure 1
emacs25@vellachemla-X510UA
File Edit Options Buffers Tools Python Help
import numpy as np
import matplotlib.pyplot as plt
dt = 0.1
autren = 100
t = range(1,autren)
signal = [np.sum([sum([np.cos(2*np.pi*n*o/b) for o in range(1,b+1)]) for b in range(2,100)]) for n in range(100)]
print(signal)
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

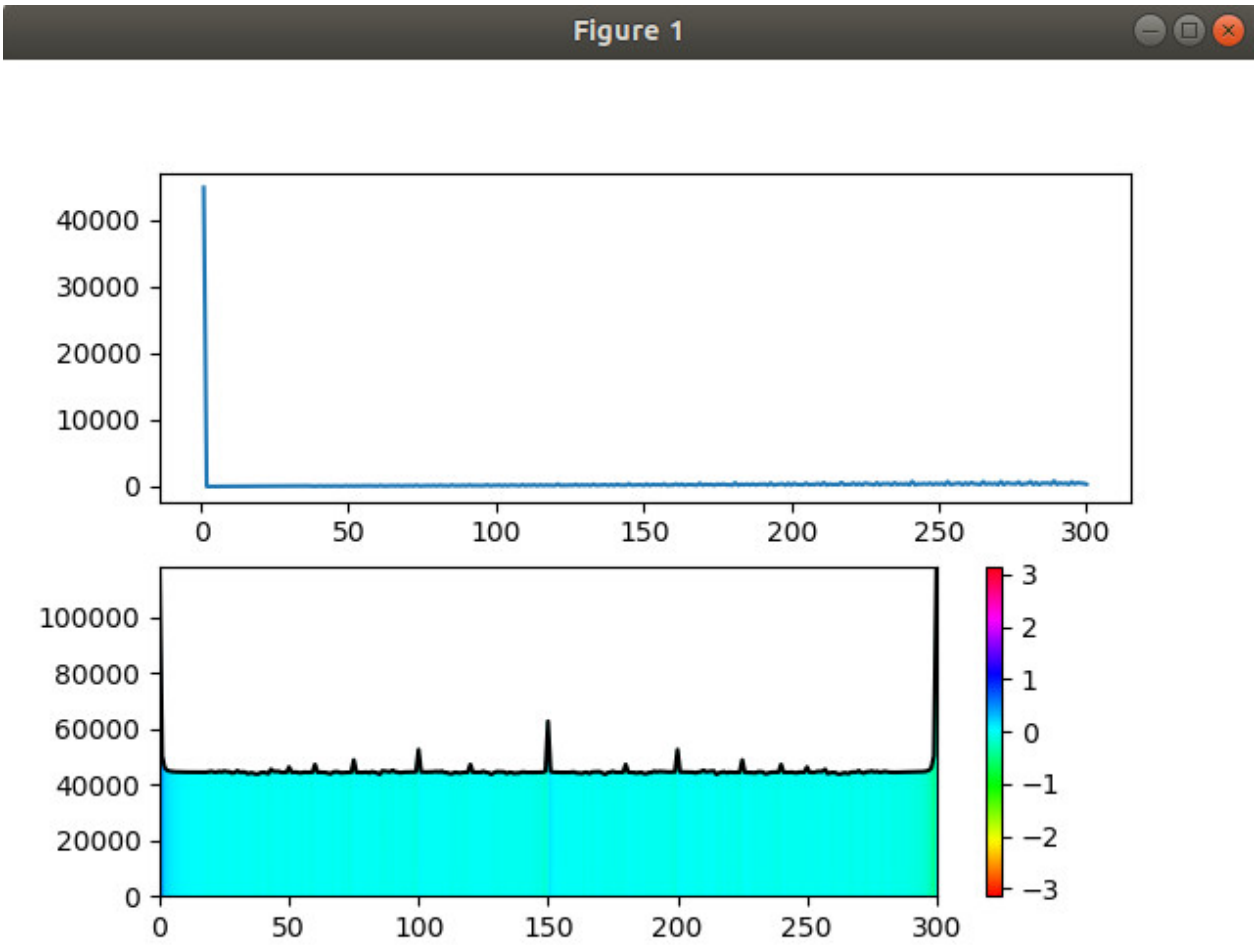
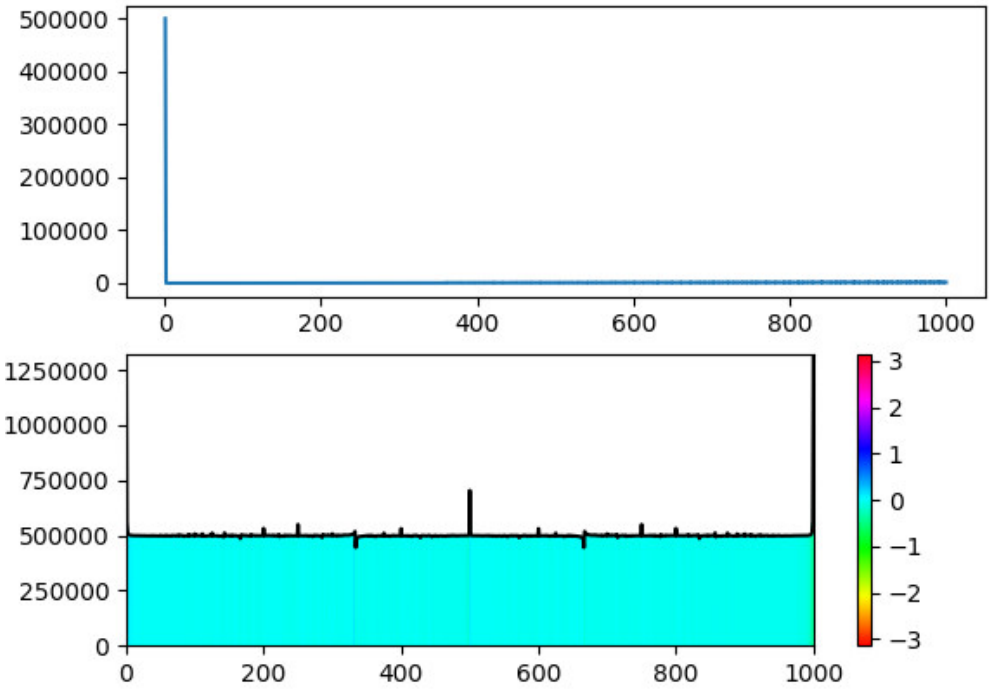


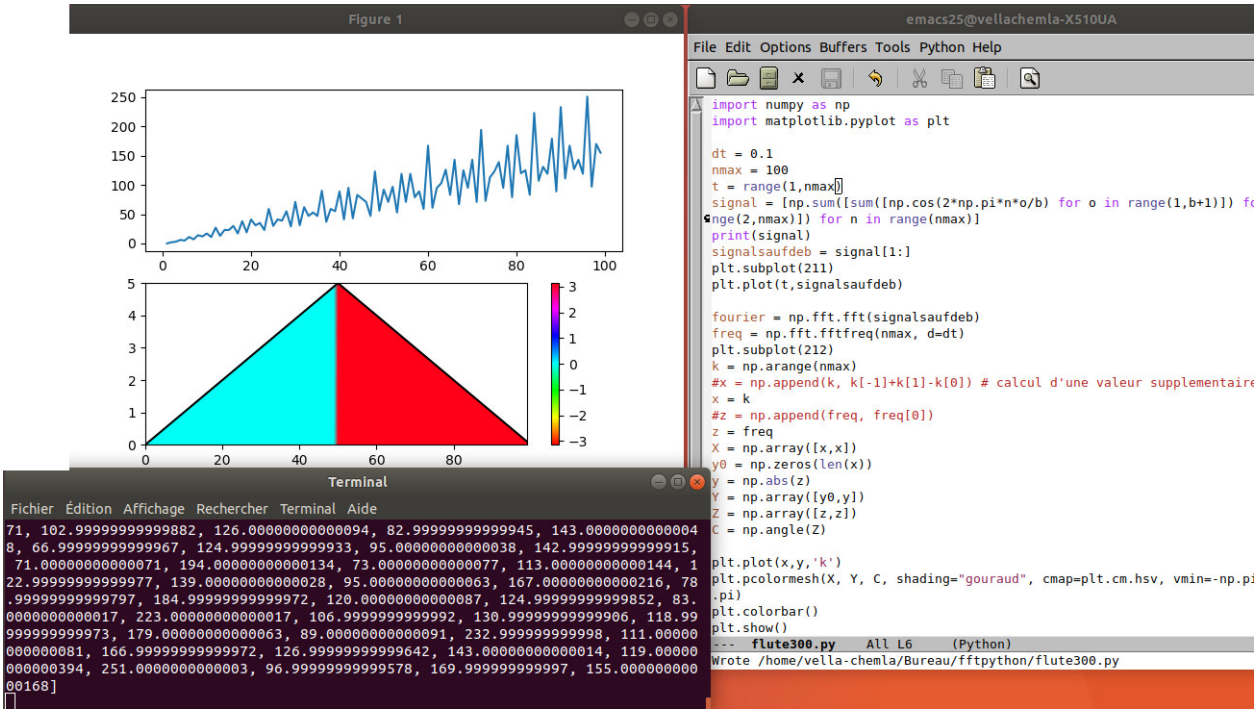
Figure 1
40000
30000
20000
10000
0
0
50
100
150
200
250
300
100000
80000
60000
40000
20000
0
3
2
1
0
−1
−2
−3

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) :

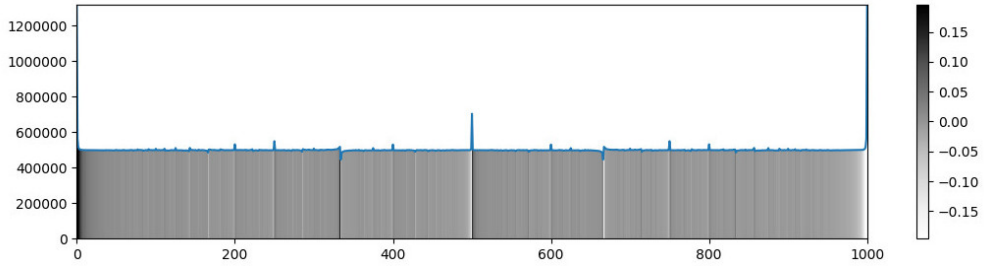
$$signal(t) = \sum_{b=2}^{t} \sum_{o=1}^{b} \cos \frac{2\pi\ t\ o}{b}$$

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()
```

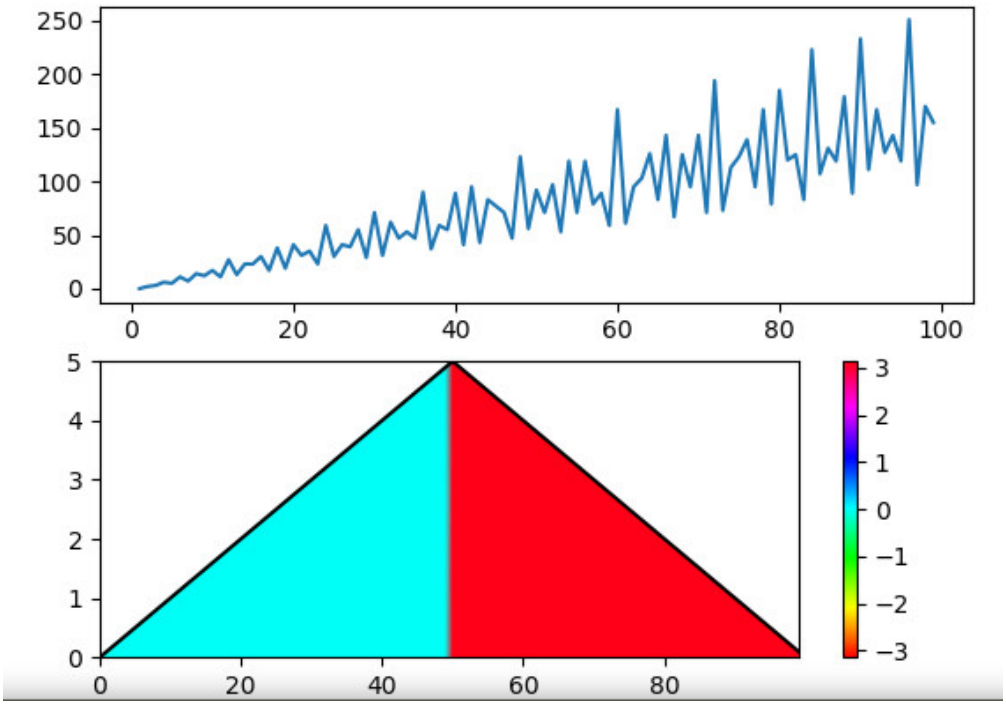
1. jusqu'à 1000.

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 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) :

```python
# 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 :

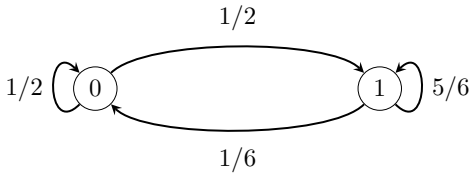
$$M = \begin{array}{c} \\ G \\ \neg\, G \end{array} \begin{array}{c} \begin{array}{cc} G & \neg\, G \end{array} \\ \begin{pmatrix} 1/2 & 1/2 \\ 1/6 & 5/6 \end{pmatrix} \end{array}$$

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.

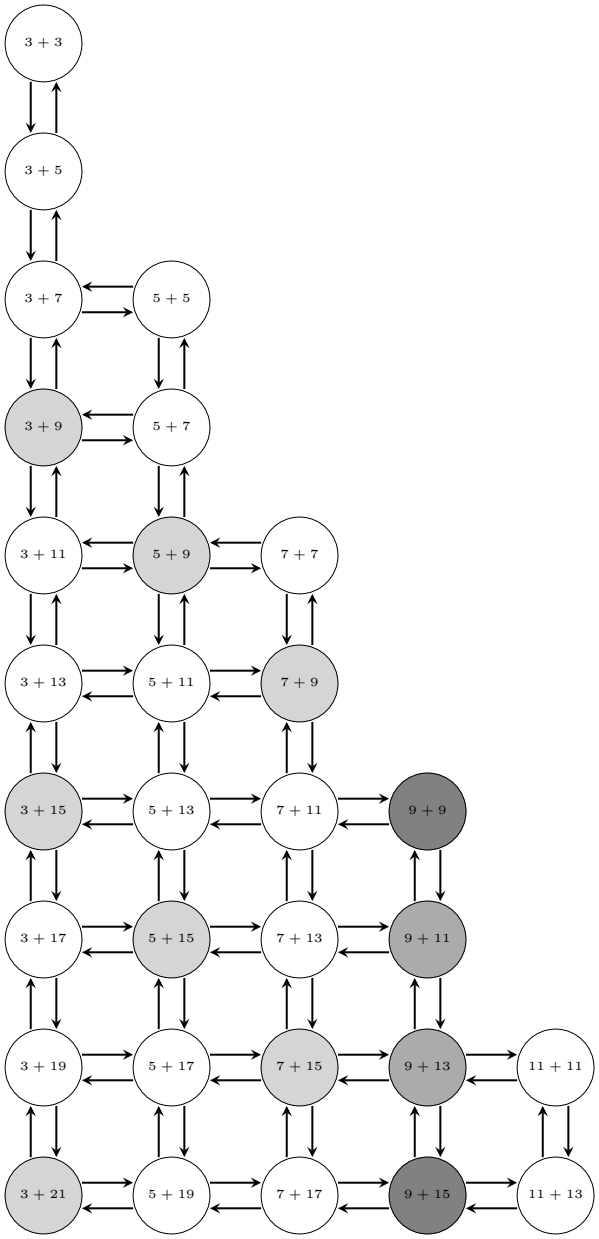
Les valeurs $1/6$ et $5/6$ de la seconde ligne se justifient par le fait que 10 règles parmi les 12 règles restantes (règles des seconde, troisième et quatrième lignes), qui présentent au moins une lettre c en $3^{\text{ème}}$ ou $4^{\text{ème}}$

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.

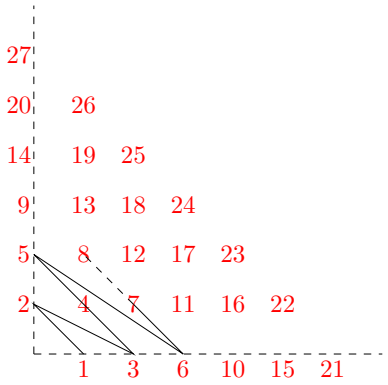
```
from math import *

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 :

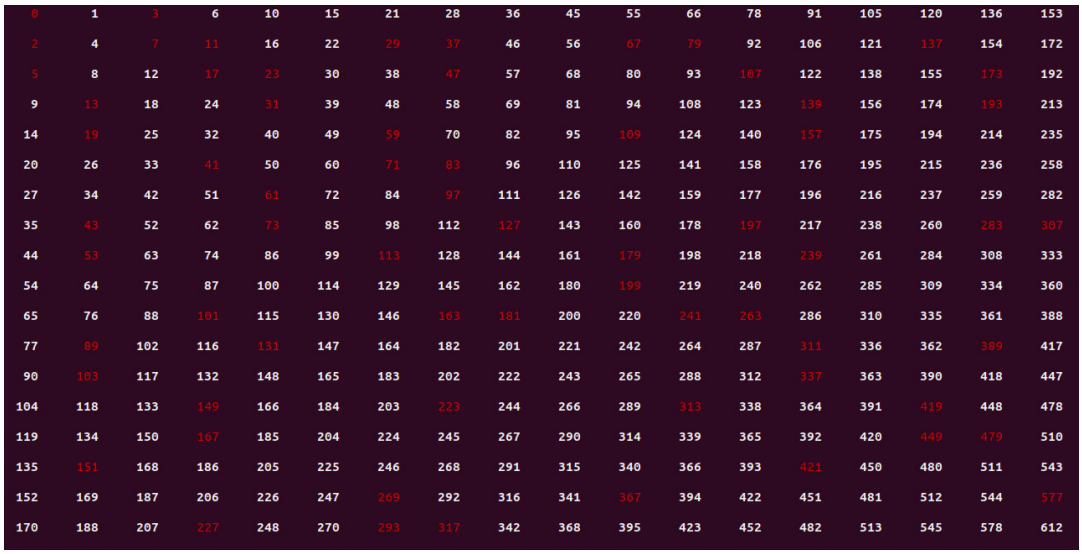


Voici le programme qui permet d'obtenir une telle numérotation [1] :

```
#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

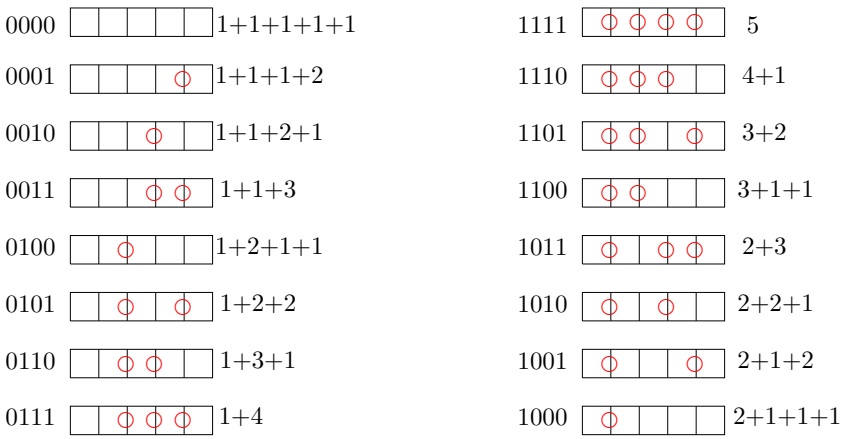
$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^k = \frac{1}{2} \begin{pmatrix} 2 & 2k & k^2 - k \\ 0 & 2 & 2k \\ 0 & 0 & 2 \end{pmatrix}$$

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.

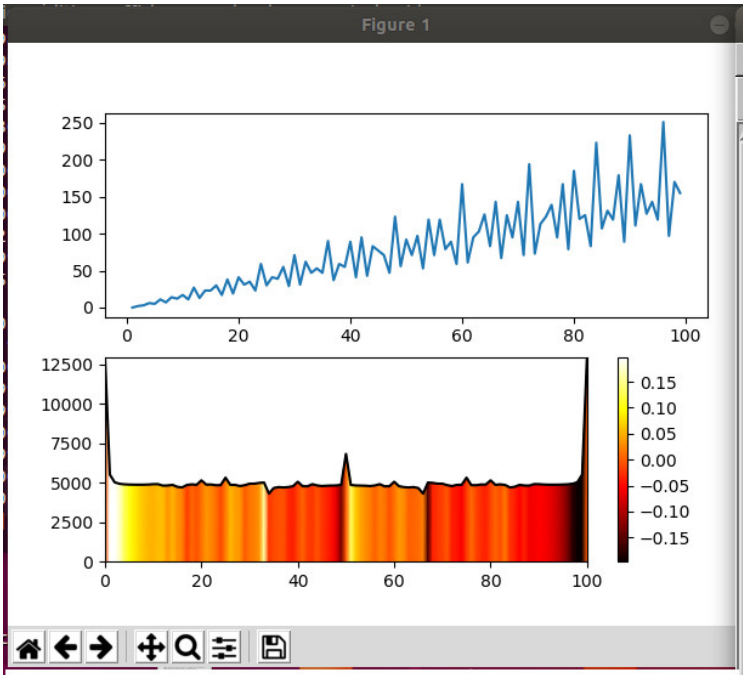
Voici les mots palindromiques pour l'entier 7, au nombre de 8 : les deux mots triviaux 000000 (correspondant à 1+1+1+1+1+1+1) et 111111 (correspondant à 7) ; et les moins triviaux, 001100 (correspondant à 1+1+3+1+1), 010010 (resp. 1+2+1+2+1), 011110 (ou 1+5+1), 101101 (ou 2+3+2), 110011 (ou 3+1+3) et 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.



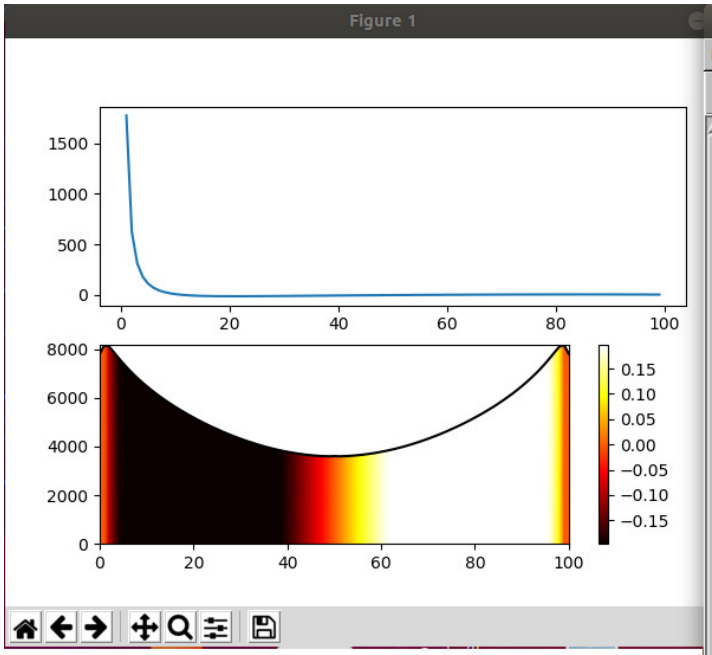
emacs25@vellachemla-X510UA

File Edit Options Buffers Tools Python Help

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

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

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

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

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

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

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



emacs25@vellachemla-X510UA

File Edit Options Buffers Tools Python Help

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

dt = 0.1
autren = 100
t = range(1,autren)
signal = [np.sum([sum([np.cos(2*np.pi*n*o/b)/(2*np.pi*n*o/b) if (n != 0) else 1 \
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.p\
i/16.0)
plt.colorbar()
plt.show()
```

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

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

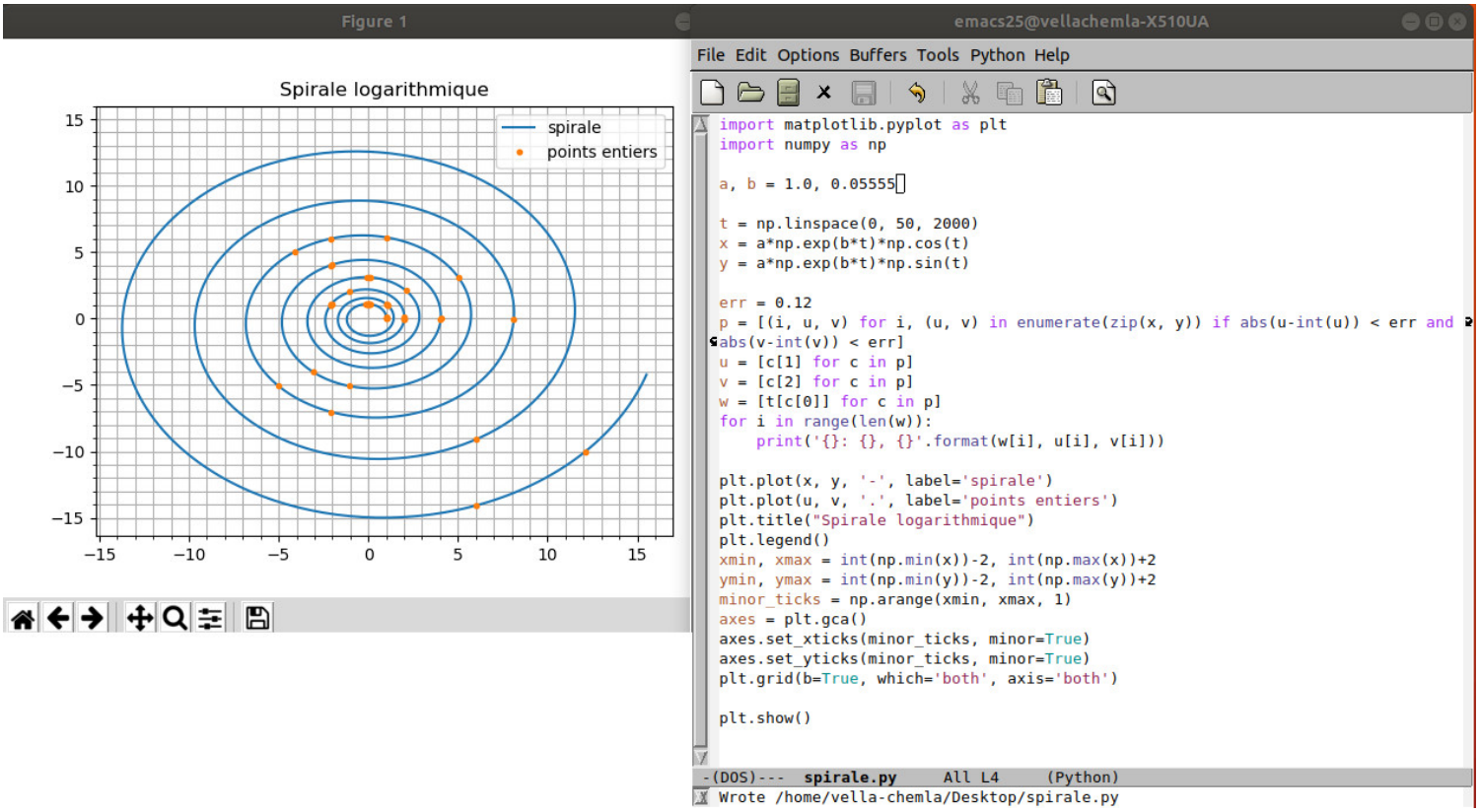
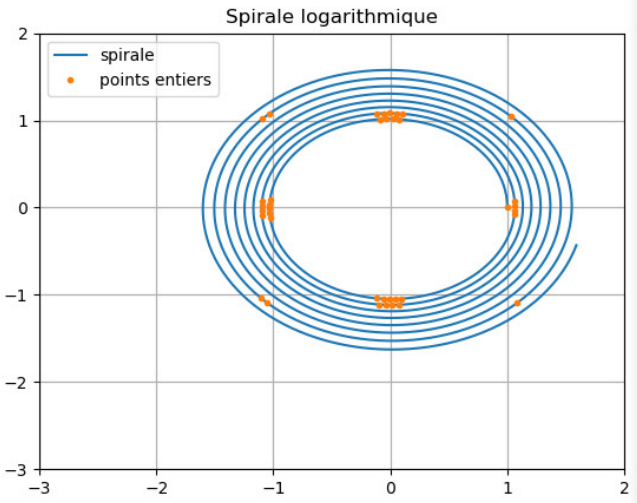


Figure 1
Spirale logarithmique
spirale
points entiers
15
10
5
0
−5
−10
−15
−15
−10
−5
0
5
10
15
emacs25@vellachemla-X510UA
File Edit Options Buffers Tools Python Help
import matplotlib.pyplot as plt
import numpy as np
a, b = 1.0, 0.05555
t = np.linspace(0, 50, 2000)
x = a*np.exp(b*t)*np.cos(t)
y = a*np.exp(b*t)*np.sin(t)
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

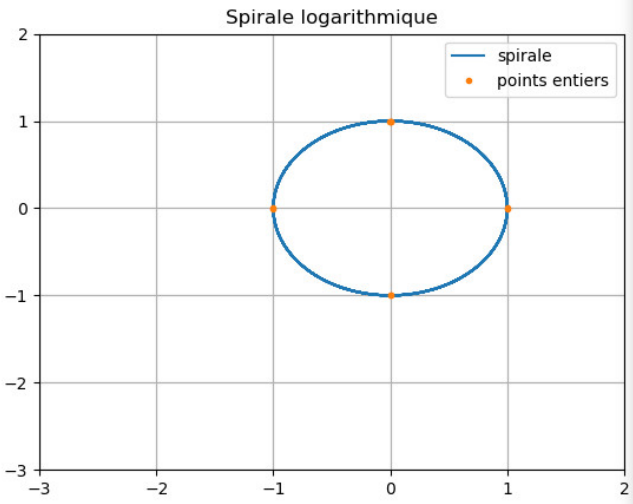
File Edit Options Buffers Tools Python Help

```
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



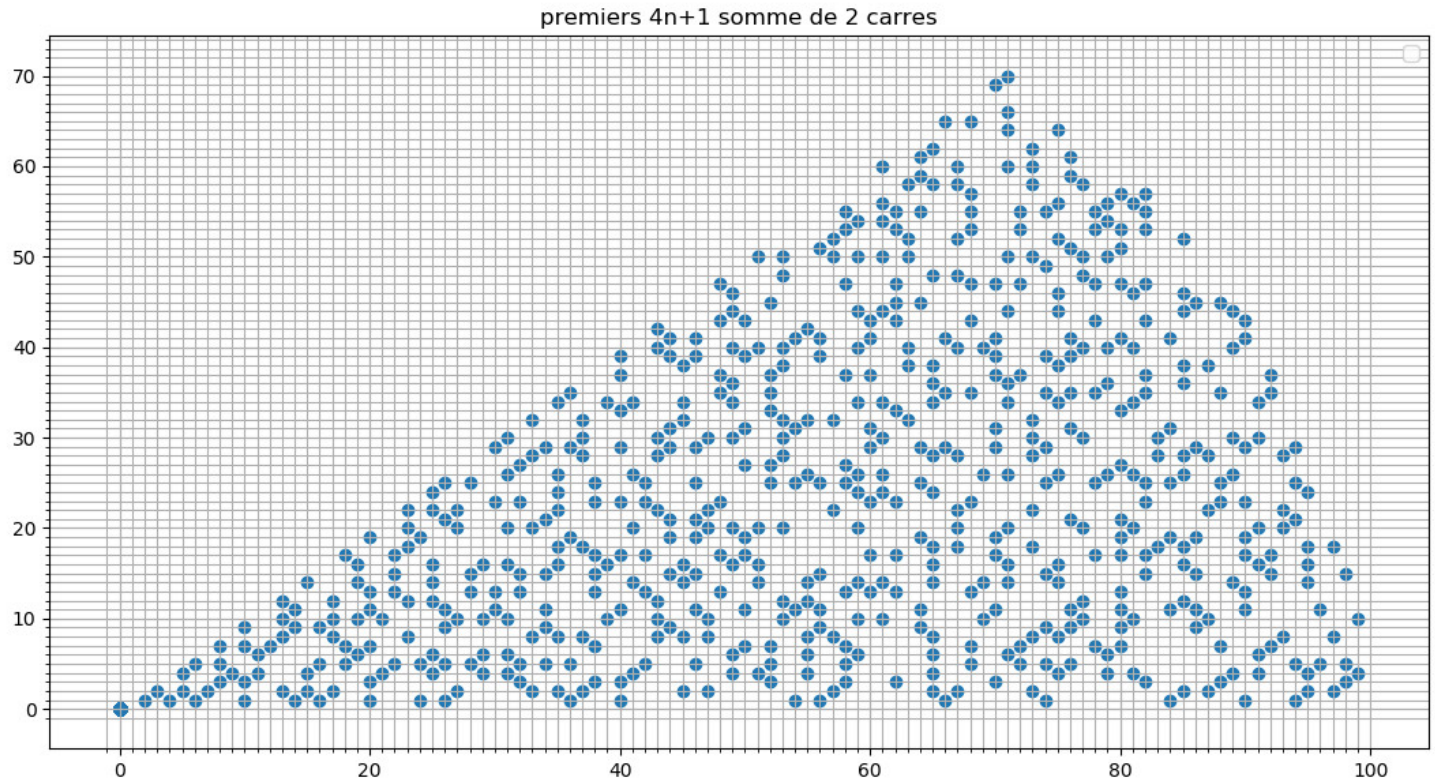
emacs25@vellachemla-X510UA

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
0
10
20
30
40
50
60
70
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 :

$x \mid y$	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...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 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].

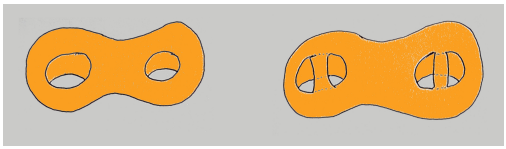
On fournit en annexe une représentation imagée obtenue par programme en python des nombres premiers $4k+1$ sommes de 2 carrés.

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 :

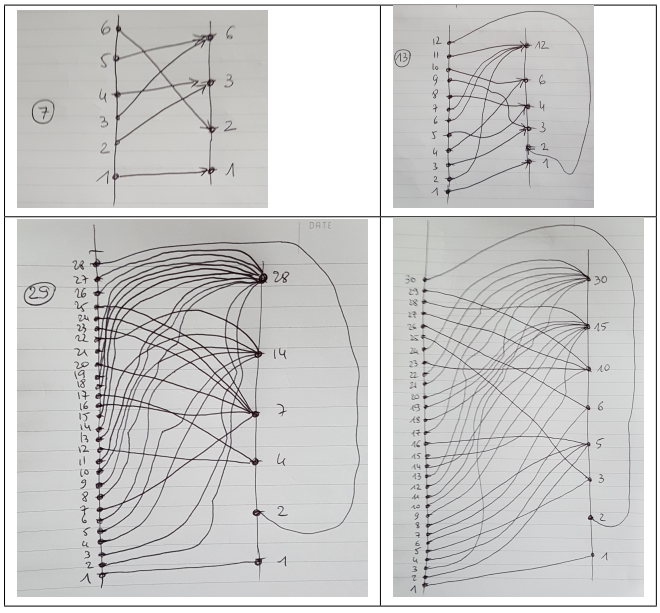
1) *première méthode envisagée* : on trouve dans la littérature qu'il est possible de compter le nombre de solutions d'une équation de la forme $x^p \equiv 1\ (mod\ k)$ sur un tore à p trous. Peut-être peut-on envisager de "dupliquer chaque trou" en comblant une sorte de tunnel de matière au milieu du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

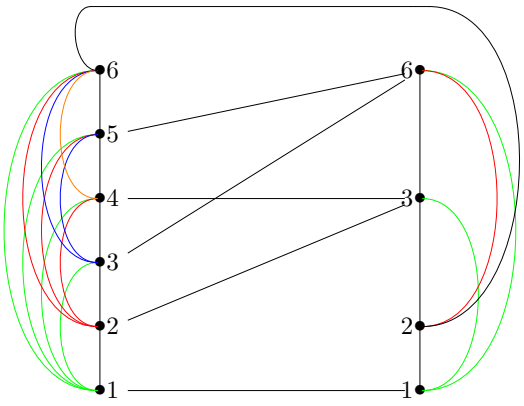
Le fait que 1 soit systématiquement d'indice 1 et $p-1$ d'indice 2 va nous permettre de transformer la représentation de la fonction "puissance qui permet d'atteindre l'unité" en une courbe fermée qui se croisera plusieurs fois elle-même ; les points de croisement seront vus comme des sommets, les éléments 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 :

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

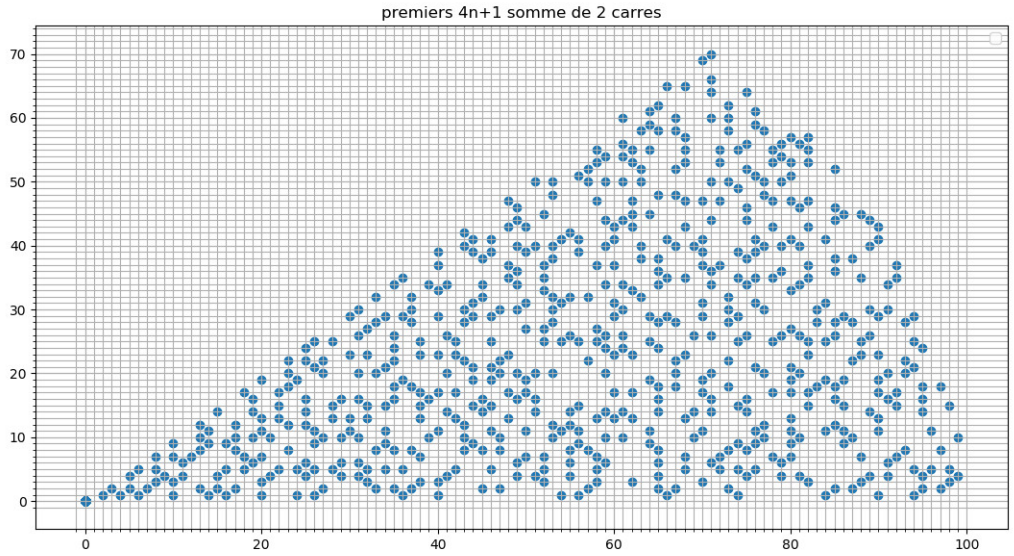
Ainsi dans cas $\psi\ 1 = \ 1, \psi\ 2 = \ 1, \psi\ 3 = \ 2, \psi\ 6 = \ 2, \psi\ 9 = \ 6, \psi\ 18 = \ 6$. Avec une légère attention on voit qu'il y en a, relativement à chaque exposant, autant qu'il y a de nombres premiers avec cet exposant et non plus grands que lui, ou bien, en reprenant le signe 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 :

$$G_1 \to G_3 \to G_2 \to G_5 \to G_4$$

Pour 29, en multipliant par 2, on parcourt les groupements ainsi :

$$G_1 \to G_3 \to G_5 \to G_6 \to G_2 \to G_4 \to G_7$$

Pour 25, en multipliant par 2, on parcourt les groupements ainsi :

$$G_1 \to G_3 \to G_2 \to G_6 \to G_5 \to G_6 \ (cycle\ sur\ G_6)$$

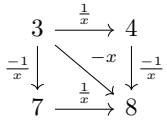
Pour 27, en multipliant par 2, on parcourt les groupements ainsi :

$$G_1 \to G_3 \to G_6 \to G_4 \to G_4 (cycle\ sur\ G_4)$$

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" ;
}
```

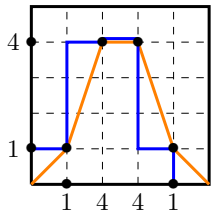
Voici le résultat de ce programme :

```
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)

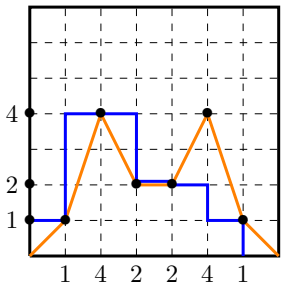
Dans les dessins ci-dessous, on représente sur un carré les résidus modulaires quadratiques de Gauss.

Résidus quadratiques modulo 5



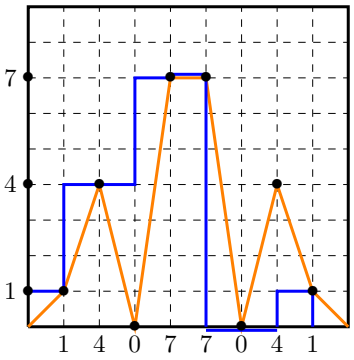
$$Aire = 10 = p\left(\frac{p-1}{2}\right)$$

Résidus quadratiques modulo 7



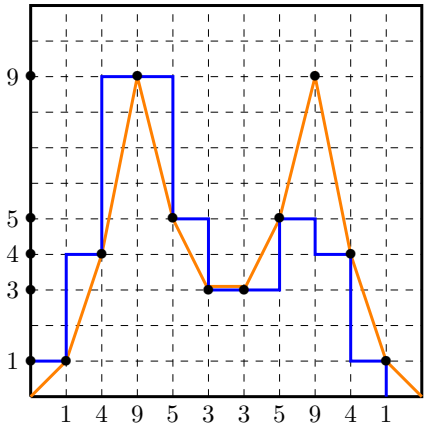
$$Aire = 14 = p\left(\frac{p-3}{2}\right)$$

Résidus quadratiques modulo 9



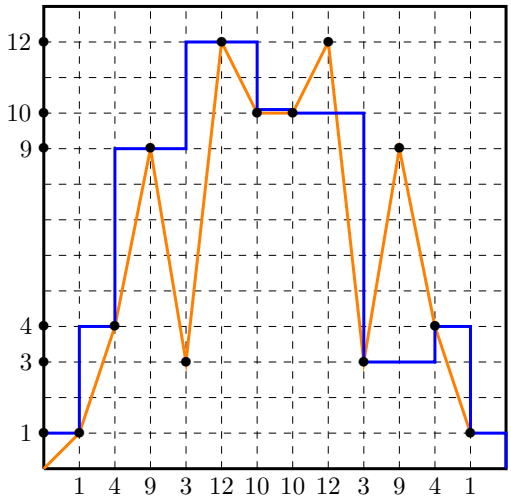
$$Aire = 24 < p\left(\frac{p-1}{2}\right)$$

Résidus quadratiques modulo 11



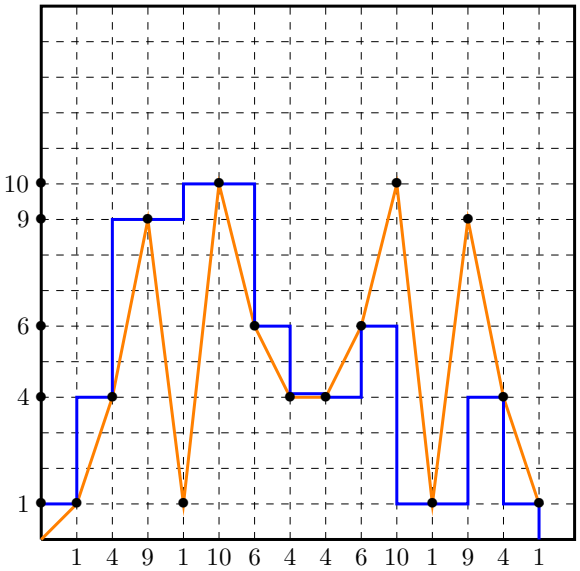
$$Aire = 44 = p\left(\frac{p-3}{2}\right)$$

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.

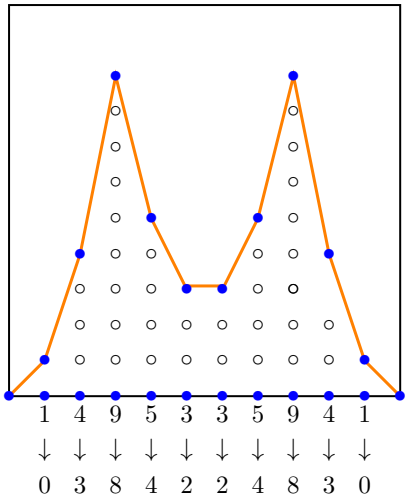
On essaie de trouver une formule qui permettrait de calculer l'aire plus rapidement, les dessins aident visuellement à la trouver.

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.



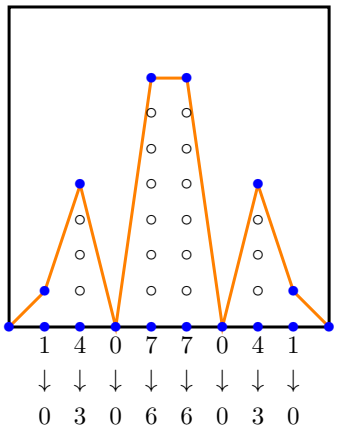
$$Bord = 22$$
$$Int = 34$$
$$Aire = 0.5 \times 22 + 34 - 1 = 44$$

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

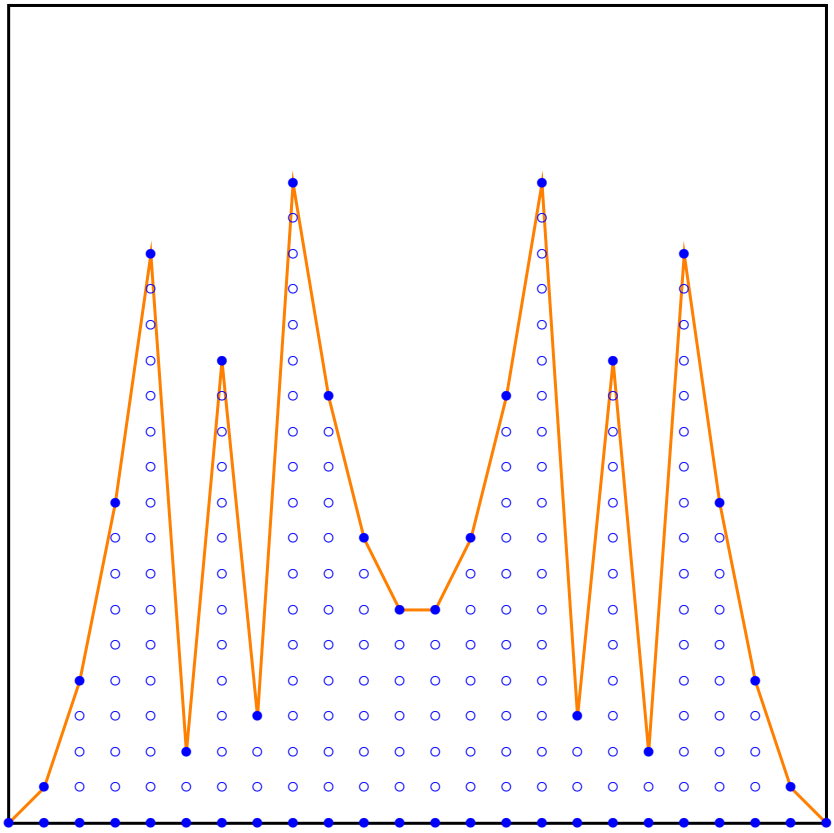


$$Aire = 5 + 14 + 5 = Int + \frac{1}{2}Bord - 3$$

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" ;
}
```

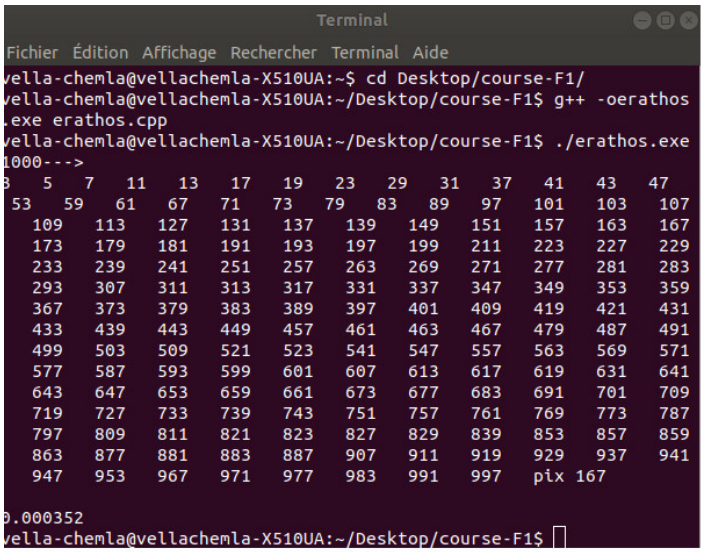
-:--- **erathos.cpp** All L7 (C++/l Abbrev)

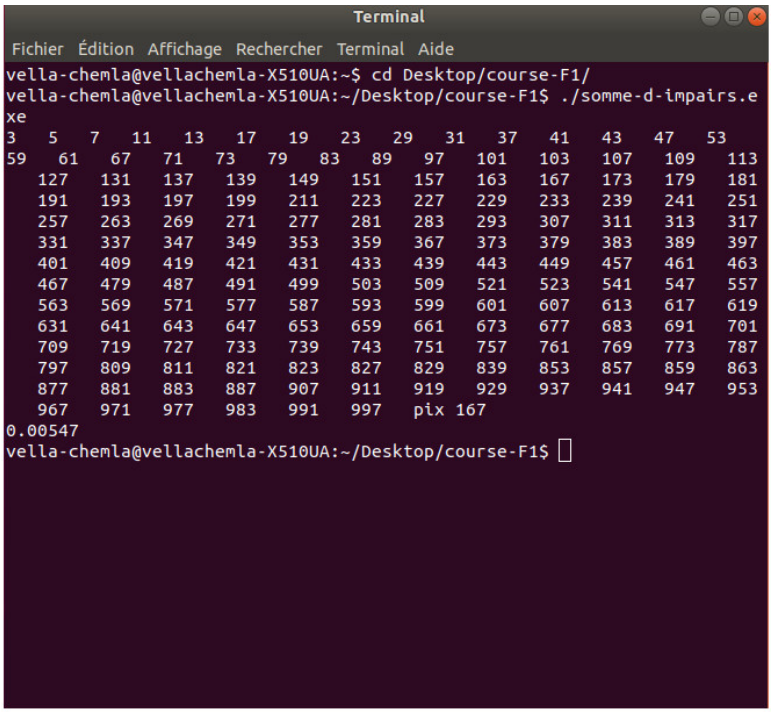
emacs25@vellachemla-X510UA

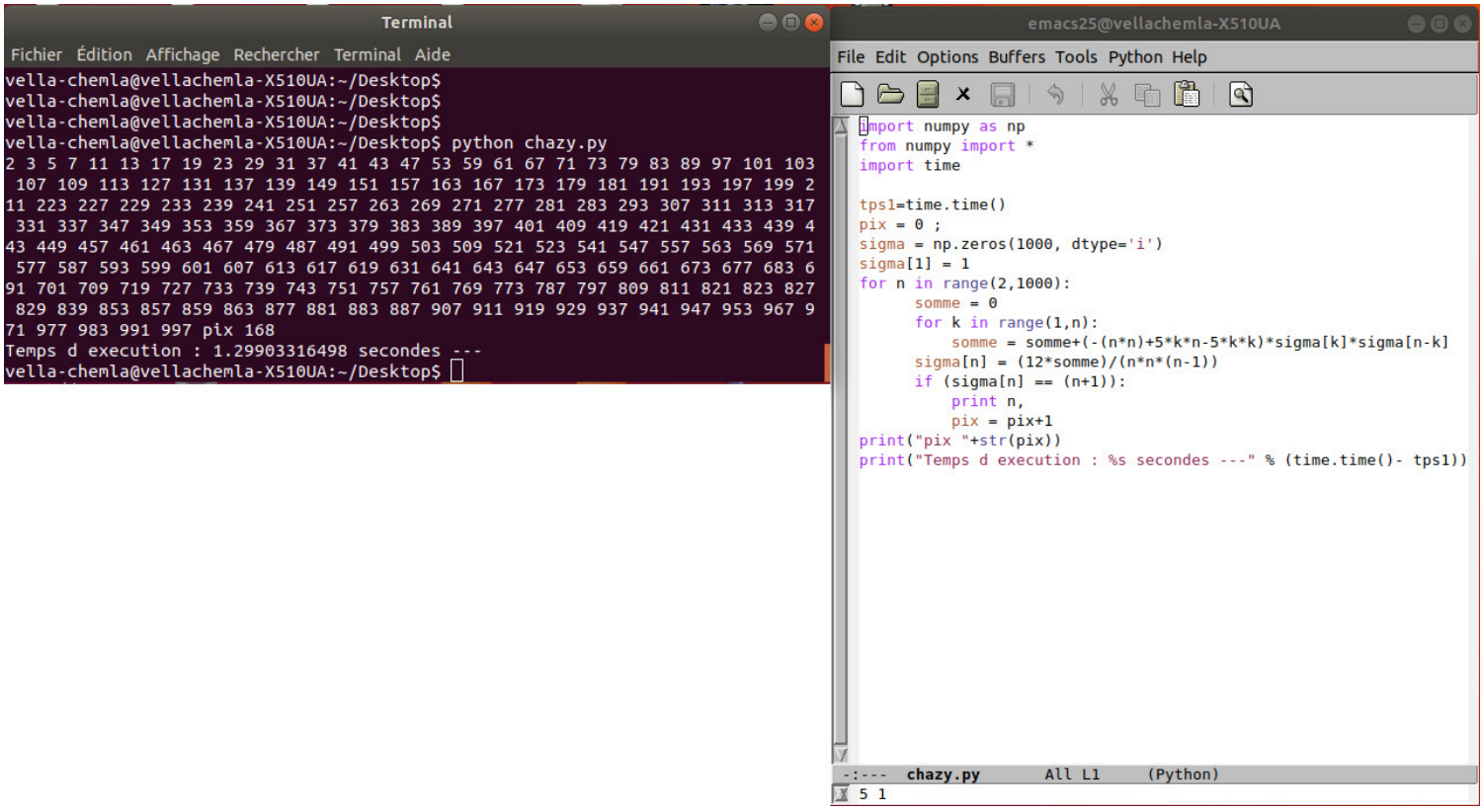
File Edit Options Buffers Tools C++ Help

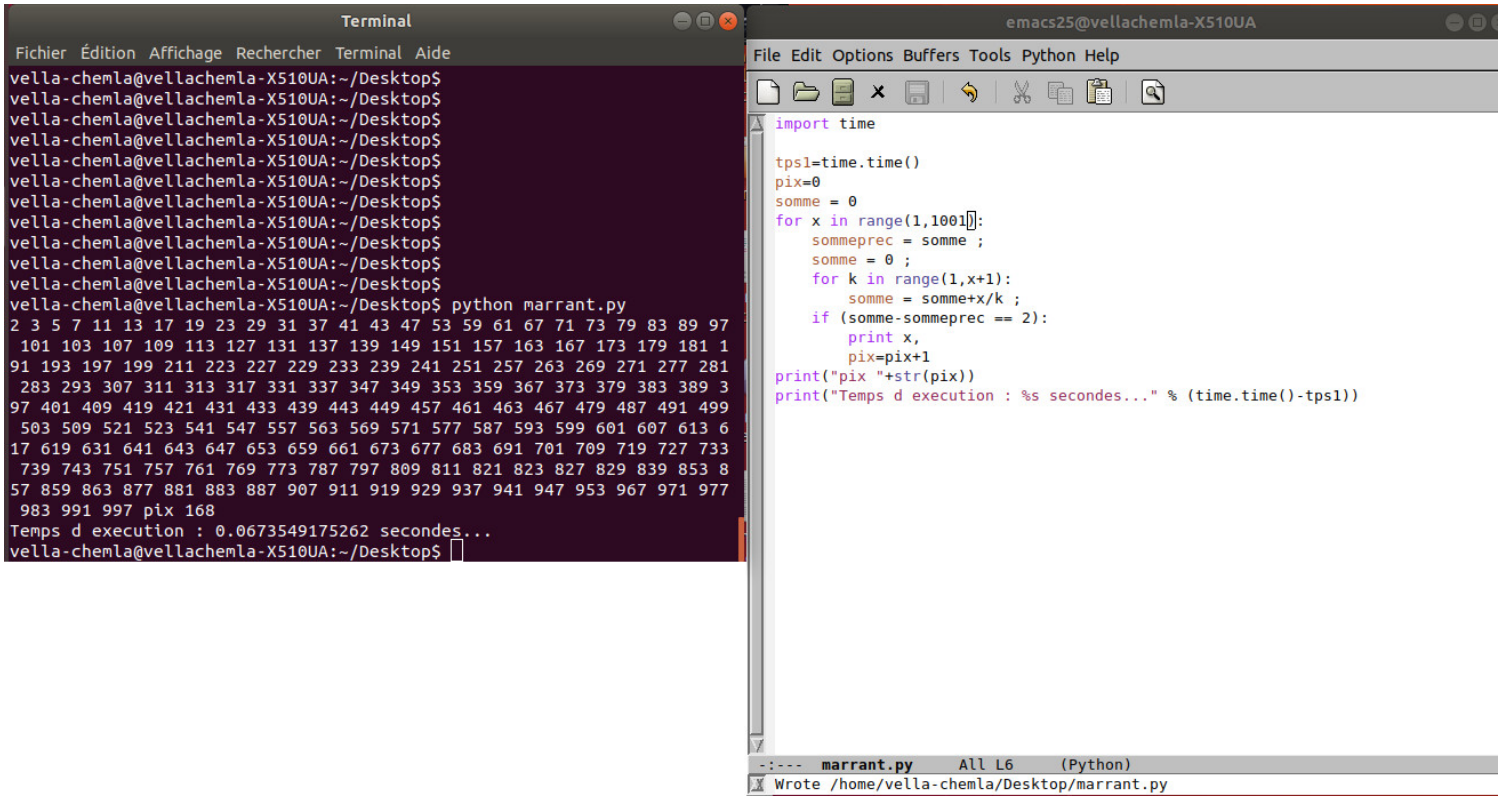
```cpp
#include <iostream>
#include <stdio.h>
#include <time.h>

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" ;
}
```

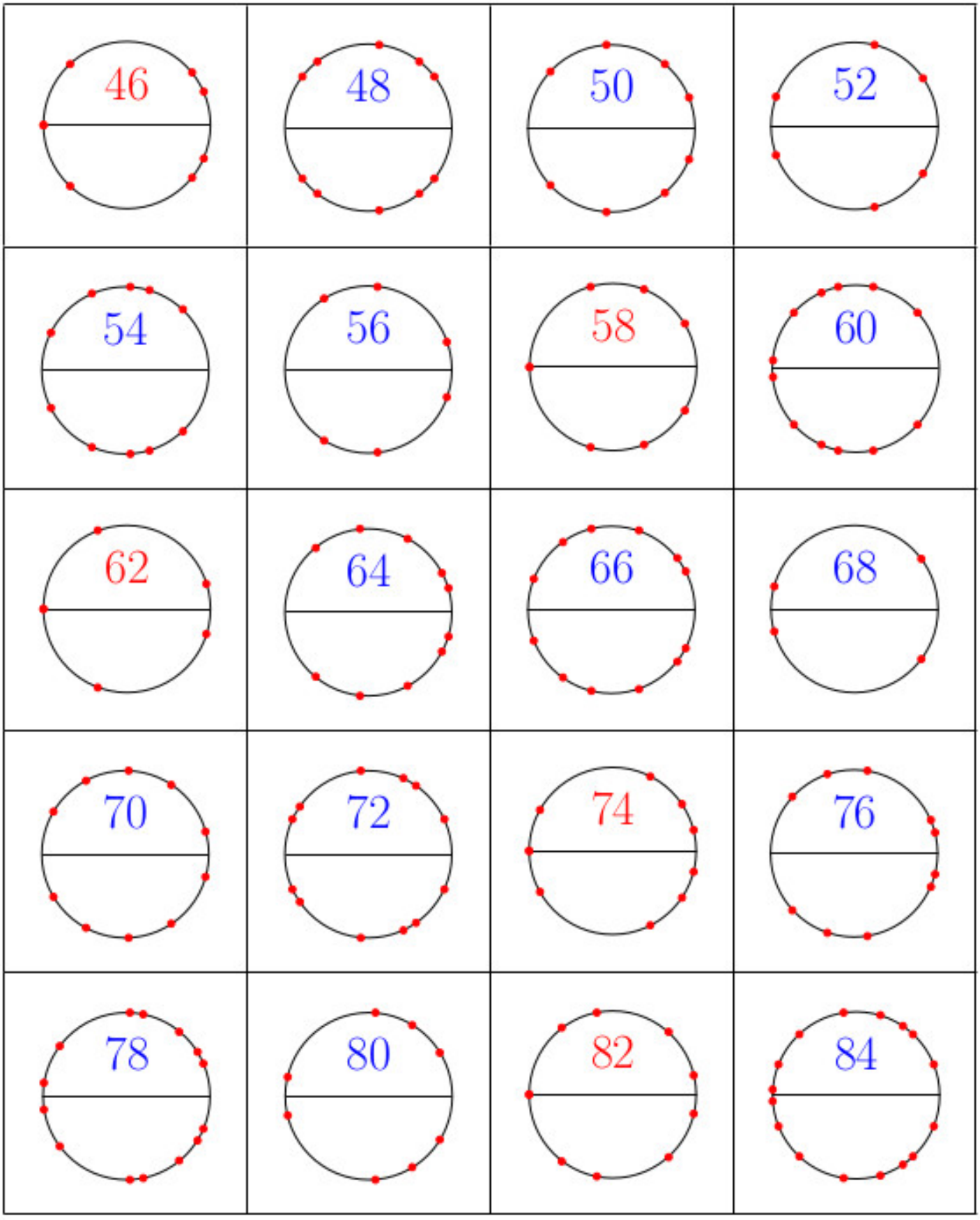
-:--- **somme-d-impairs.cpp** All L6 (C++/l Abbrev)

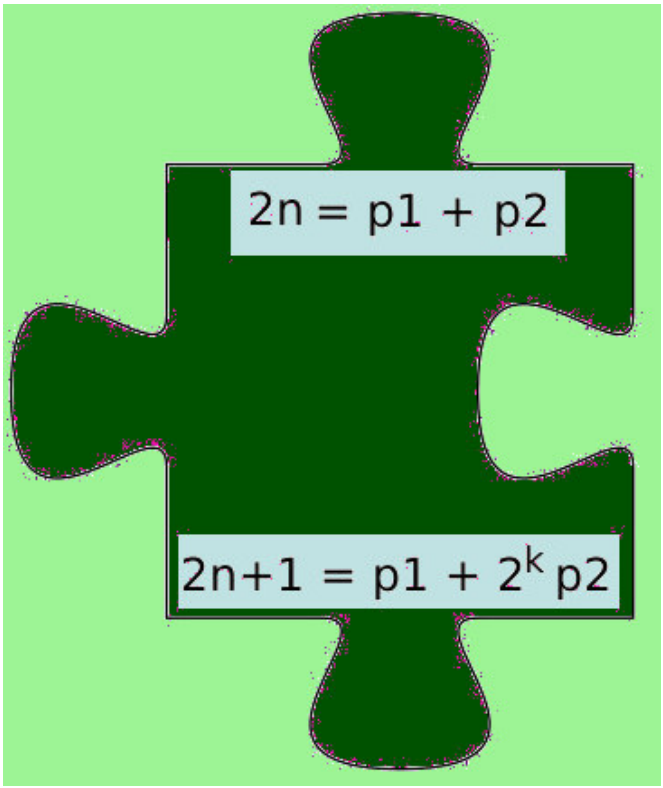

Terminal
Fichier Édition Affichage Rechercher Terminal Aide
vella-chemla@vellachemla-X510UA:~$ cd Desktop/course-F1/
vella-chemla@vellachemla-X510UA:~/Desktop/course-F1$ g++ -oerathos
.exe erathos.cpp
vella-chemla@vellachemla-X510UA:~/Desktop/course-F1$ ./erathos.exe
1000--->
3 5 7 11 13 17 19 23 29 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$

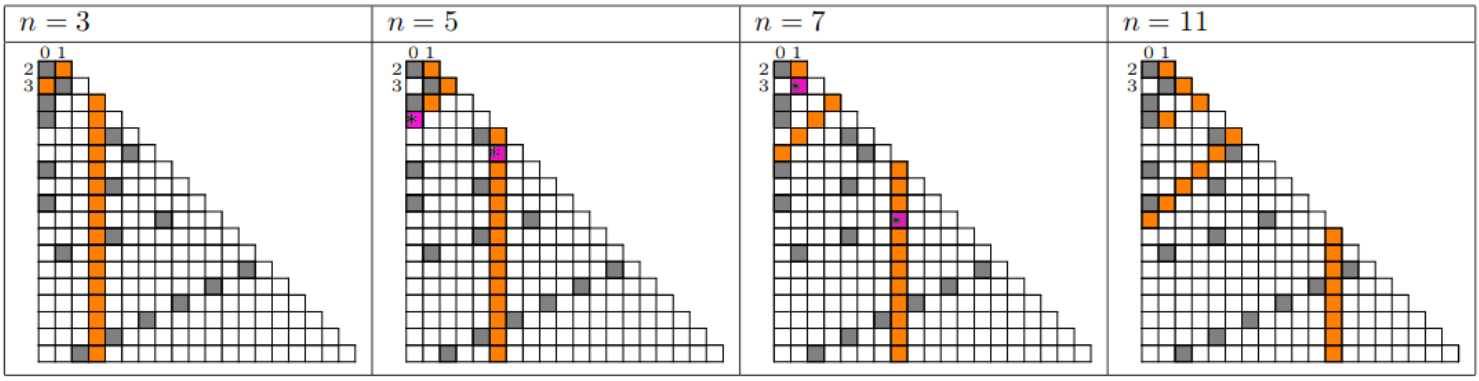

Terminal
Fichier Édition Affichage Rechercher Terminal Aide
vella-chemla@vellachemla-X510UA:~$ cd Desktop/course-F1/
vella-chemla@vellachemla-X510UA:~/Desktop/course-F1$ ./somme-d-impairs.e
xe
3 5 7 11 13 17 19 23 29 31 37 41 43 47 53
59 61 67 71 73 79 83 89 97 101 103 107 109 113
127 131 137 139 149 151 157 163 167 173 179 181
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$
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


$n = 3$
$n = 5$
$n = 7$
$n = 11$
$n = 13$
$n = 17$
$n = 19$

Voici la forme générale de la matrice G.

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

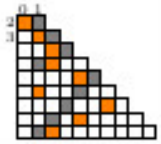
Tous les ... sont des 0.

D'un Z qui veut dire... (Denise Vella-Chemla, 15.6.2019)

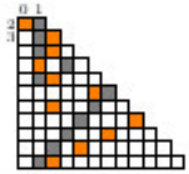
$2p = p + p$: un nombre premier vérifie trivialement la conjecture de Goldbach. On repère de belles lettres Z dans le bas des tores trapézoïdaux qu'on a choisis pour représenter les restes des nombres dans des divisions par les entiers successifs à commencer par 2.

14

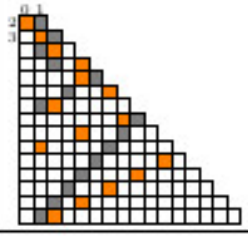
22



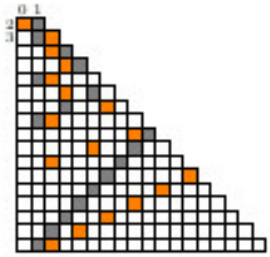
26



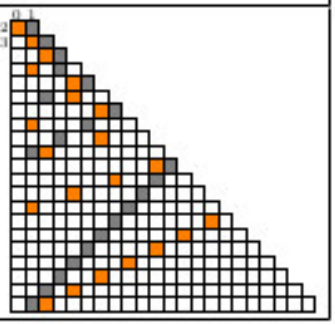
34



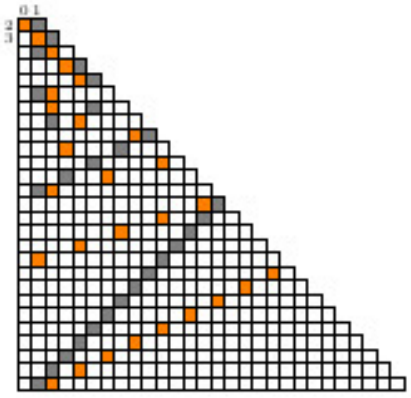
38



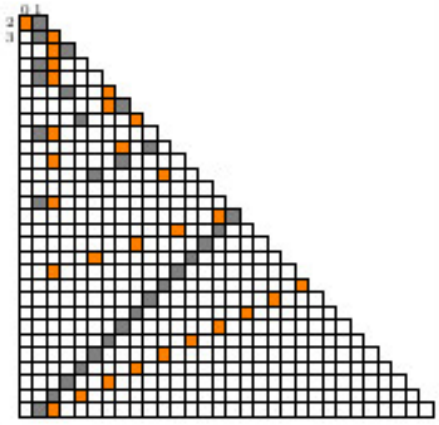
46



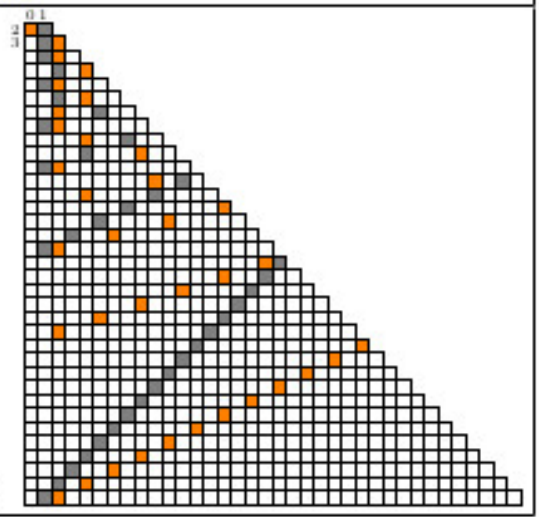
58



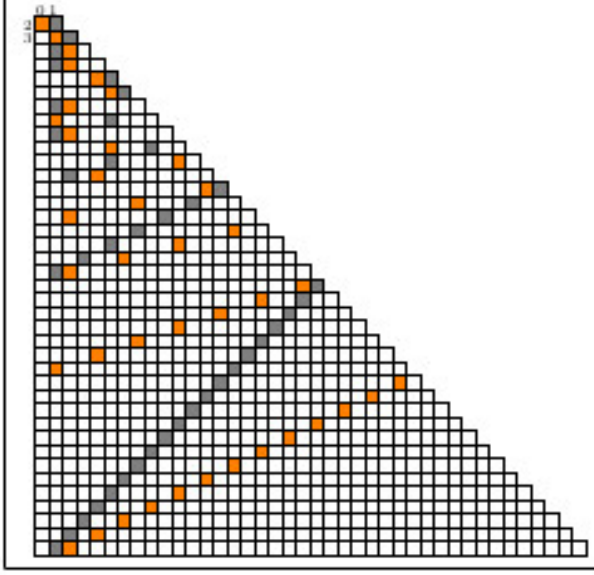
62



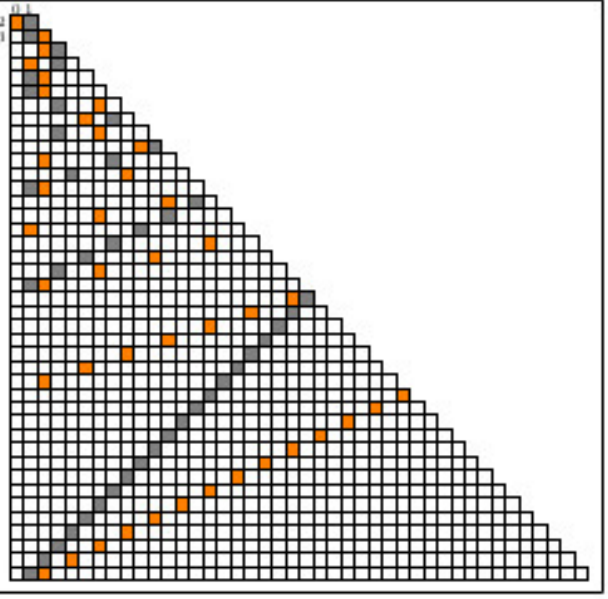
74



82



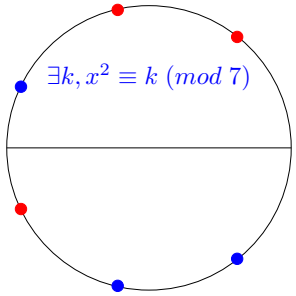
86



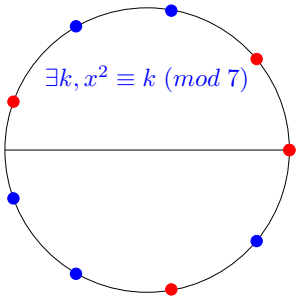
Résidus quadratiques sur colliers (Denise Vella-Chemla, 22.5.2019)

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 $4k+3$.

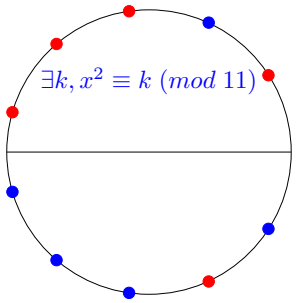
Solutions de $\exists k, x^2 \equiv k\ (mod\ 7)$: 1, 2, 4.
7 est premier.
Il y a 3 solutions.



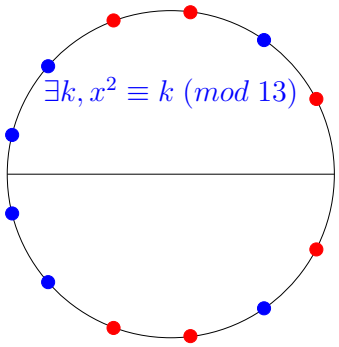
Solutions de $\exists k, x^2 \equiv k\ (mod\ 9)$: 0, 1, 4, 7.
9 est composé.
Il y a 4 solutions.



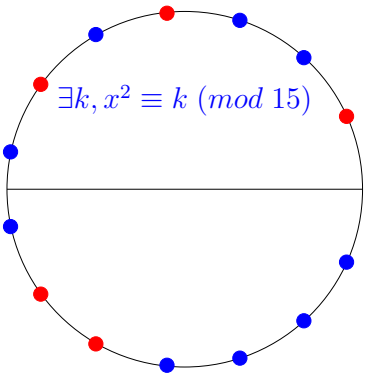
Solutions de $\exists k, x^2 \equiv k\ (mod\ 11)$: 1, 3, 4, 5, 9.
11 est premier.
Il y a 5 solutions.



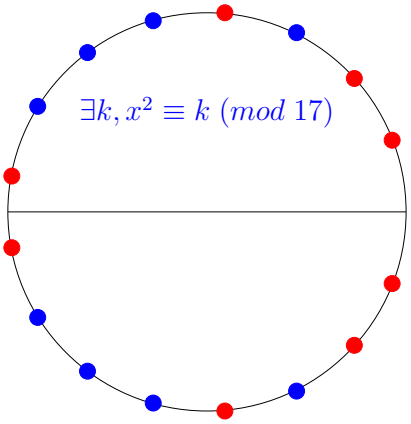
Solutions de $\exists k, x^2 \equiv k \ (mod\ 13)$: 1, 3, 4, 9, 10, 12.
13 est premier.
Il y a 6 solutions.



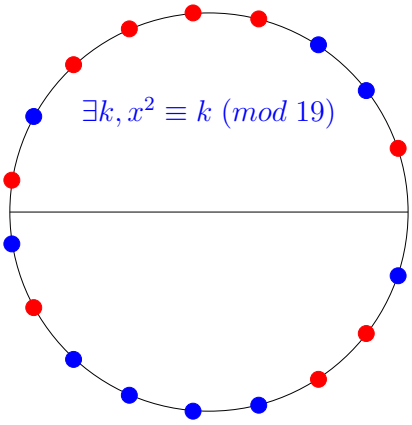
Solutions de $\exists k, x^2 \equiv k \ (mod\ 15)$: 1, 4, 6, 9, 10.
15 est composé.
Il y a 5 solutions.



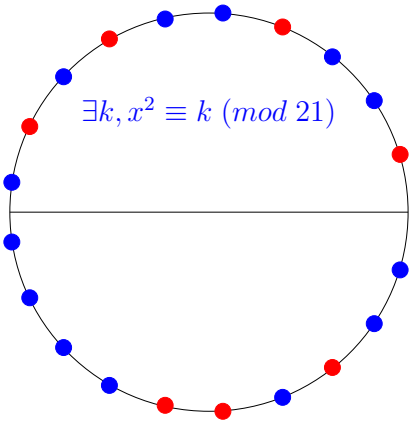
Solutions de $\exists k, x^2 \equiv k \ (mod\ 17)$: 1, 2, 4, 8, 9, 13, 15, 16.
17 est premier.
Il y a 8 solutions.



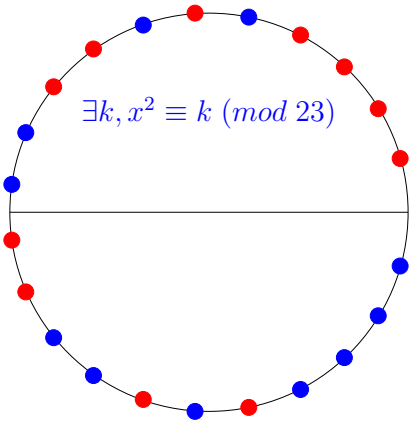
Solutions de $\exists k, x^2 \equiv k \ (mod\ 19)$: 1, 4, 5, 6, 7, 9, 11, 16, 17.
19 est premier.
Il y a 9 solutions.



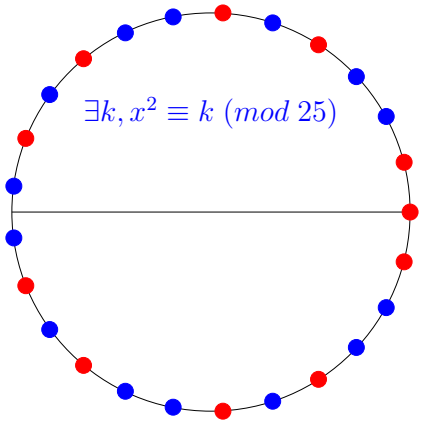
Solutions de $\exists k, x^2 \equiv k \ (mod\ 21)$: 1, 4, 7, 9, 15, 16, 18.
21 est composé.
Il y a 4 solutions.



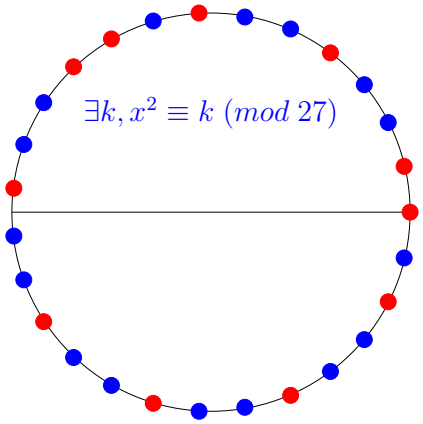
Solutions de $\exists k, x^2 \equiv k \ (mod\ 23)$: 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.
23 est premier.
Il y a 11 solutions.



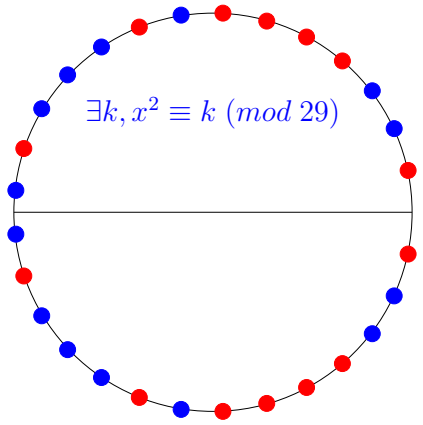
Solutions de $\exists k, x^2 \equiv k \ (mod\ 25)$: 0, 1, 4, 6, 9, 11, 14, 16, 19, 21, 24.
25 est composé.
Il y a 11 solutions.



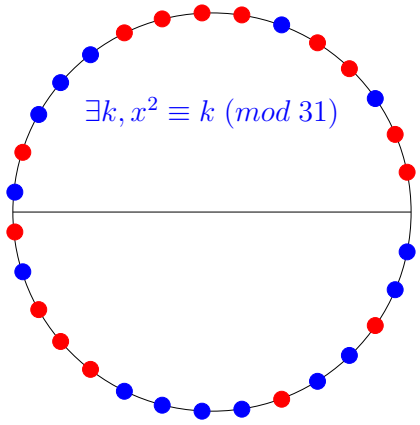
Solutions de $\exists k, x^2 \equiv k \ (mod\ 27)$: 0, 1, 4, 7, 9, 10, 13, 16, 19, 22, 25.
27 est composé.
Il y a 10 solutions.



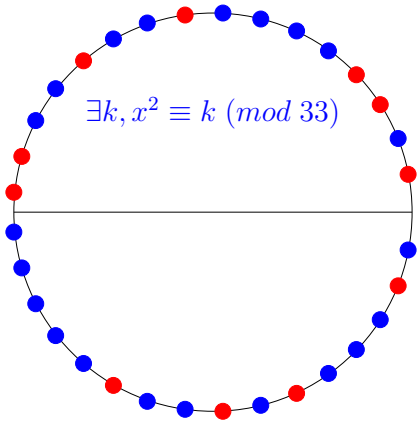
Solutions de $\exists k, x^2 \equiv k \ (mod\ 29)$: 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28.
29 est premier.
Il y a 14 solutions.



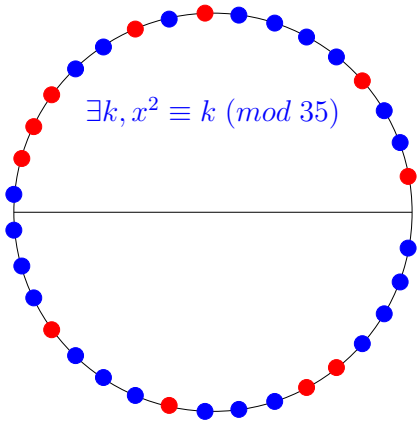
Solutions de $\exists k, x^2 \equiv k \ (mod\ 31)$: 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28.
31 est premier.
Il y a 15 solutions.



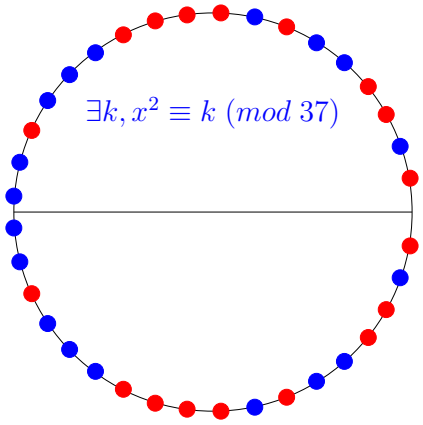
Solutions de $\exists k, x^2 \equiv k \ (mod\ 33)$: 1, 3, 4, 9, 12, 15, 16, 22, 25, 27, 31.
33 est composé.
Il y a 11 solutions.



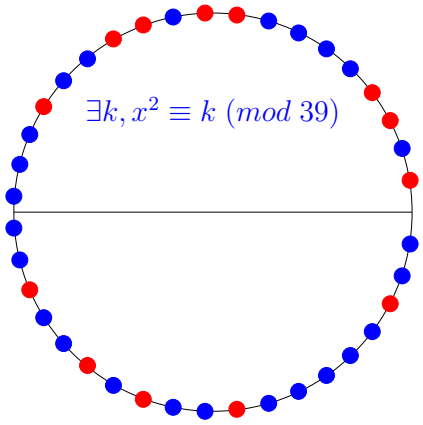
Solutions de $\exists k, x^2 \equiv k \ (mod\ 35)$: 1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30.
35 est composé.
Il y a 11 solutions.



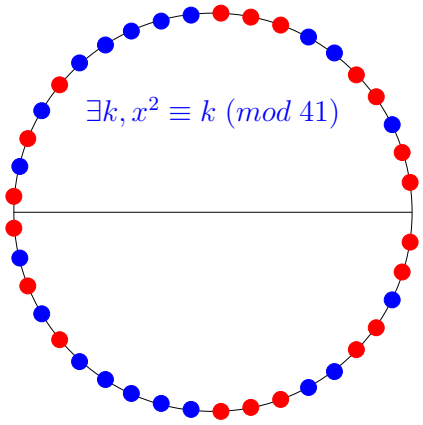
Solutions de $\exists k, x^2 \equiv k \ (mod\ 37)$: 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36.
37 est premier.
Il y a 18 solutions.



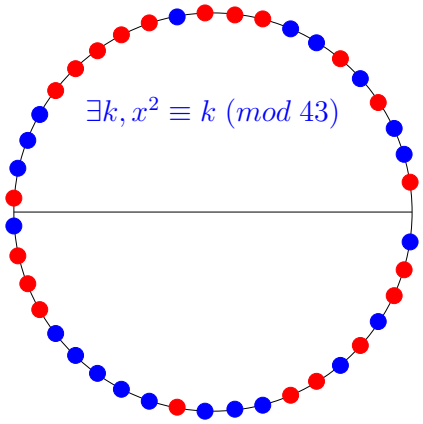
Solutions de $\exists k, x^2 \equiv k \ (mod\ 39)$: 1, 3, 4, 9, 10, 12, 13, 16, 22, 25, 27, 30, 36.
39 est composé.
Il y a 13 solutions.



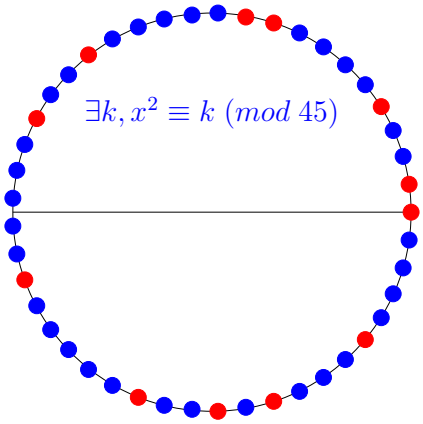
Solutions de $\exists k, x^2 \equiv k \ (mod\ 41)$: 1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40.
41 est premier.
Il y a 20 solutions.



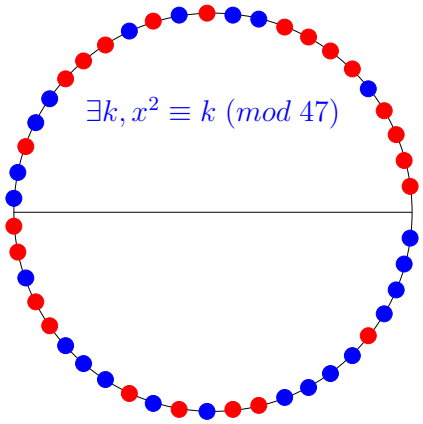
Solutions de $\exists k, x^2 \equiv k \ (mod\ 43)$: 1, 4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23, 24, 25, 31, 35, 36, 38, 40, 41.
43 est premier.
Il y a 21 solutions.



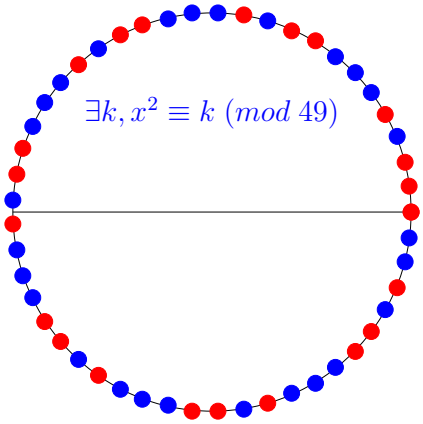
Solutions de $\exists k, x^2 \equiv k \ (mod\ 45)$: 0, 1, 4, 9, 10, 16, 19, 25, 31, 34, 36, 40.
45 est composé.
Il y a 12 solutions.



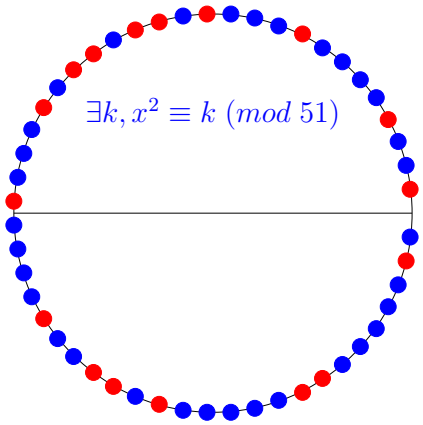
Solutions de $\exists k, x^2 \equiv k \ (mod\ 47)$: 1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42.
47 est premier.
Il y a 23 solutions.



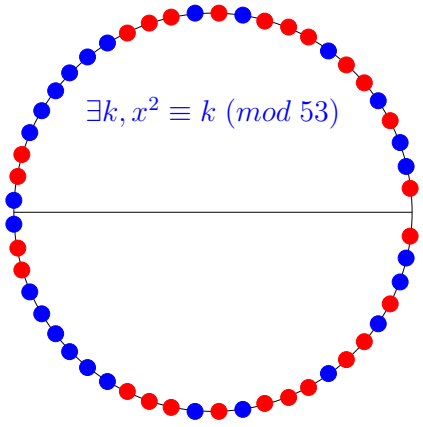
Solutions de $\exists k, x^2 \equiv k \ (mod\ 49)$: 0, 1, 2, 4, 8, 9, 11, 15, 16, 18, 22, 23, 25, 29, 30, 32, 36, 37, 39, 43, 44, 46.
49 est composé.
Il y a 22 solutions.



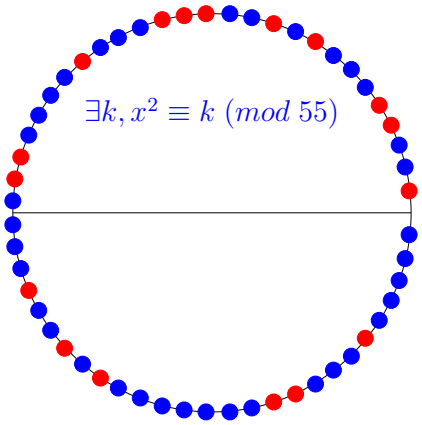
Solutions de $\exists k, x^2 \equiv k \ (mod\ 51)$: 1, 4, 9, 13, 15, 16, 18, 19, 21, 25, 30, 33, 34, 36, 42, 43, 49.
51 est composé.
Il y a 4 solutions.



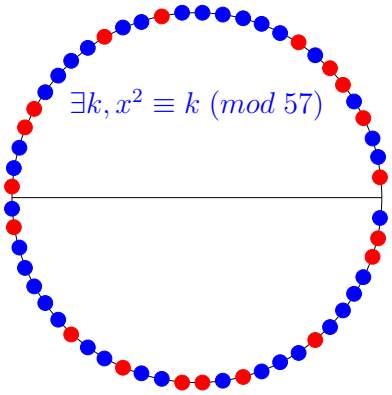
Solutions de $\exists k, x^2 \equiv k \ (mod\ 53)$: 1, 4, 6, 7, 9, 10, 11, 13, 15, 16, 17, 24, 25, 28, 29, 36, 37, 38, 40, 42, 43, 44, 46, 47, 49, 52.
53 est premier.
Il y a 4 solutions.



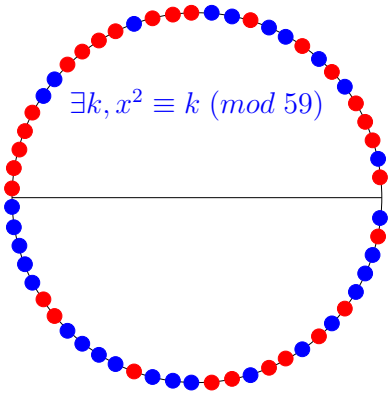
Solutions de $\exists k, x^2 \equiv k \ (mod\ 55)$: 1, 4, 5, 9, 11, 14, 15, 16, 20, 25, 26, 31, 34, 36, 44, 45, 49.
55 est composé.
Il y a 4 solutions.



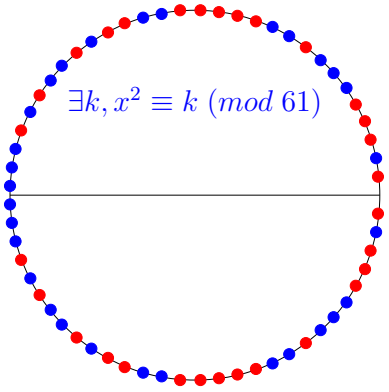
Solutions de $\exists k, x^2 \equiv k \ (mod\ 57)$: 1, 4, 6, 7, 9, 16, 19, 24, 25, 28, 30, 36, 39, 42, 43, 45, 49, 54, 55.
57 est composé.
Il y a 4 solutions.



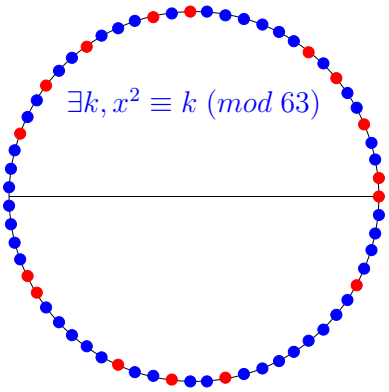
Solutions de $\exists k, x^2 \equiv k \ (mod\ 59)$: 1, 3, 4, 5, 7, 9, 12, 15, 16, 17, 19, 20, 21, 22, 25, 26, 27, 28, 29, 35, 36, 41, 45, 46, 48, 49, 51, 53, 57.
59 est premier.
Il y a 29 solutions.



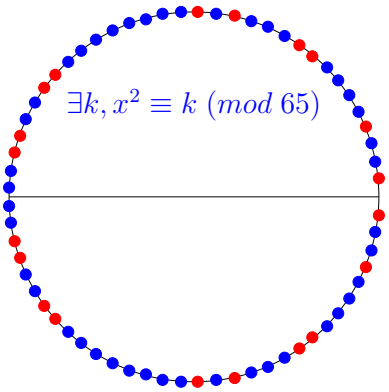
Solutions de $\exists k, x^2 \equiv k \ (mod\ 61)$: 1, 3, 4, 5, 9, 12, 13, 14, 15, 16, 19, 20, 22, 25, 27, 34, 36, 39, 41, 42, 45, 46, 47, 48, 49, 52, 56, 57, 58, 60.
61 est premier.
Il y a 30 solutions.



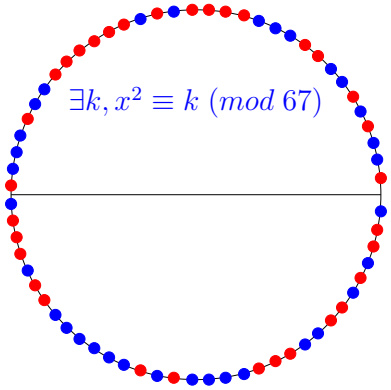
Solutions de $\exists k, x^2 \equiv k \ (mod\ 63)$: 0, 1, 4, 7, 9, 16, 18, 22, 25, 28, 36, 37, 43, 46, 49, 58.
63 est composé.
Il y a 16 solutions.



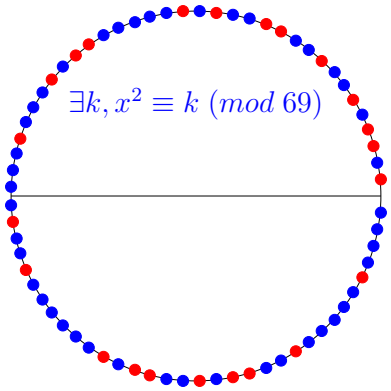
Solutions de $\exists k, x^2 \equiv k \ (mod\ 65)$: 1, 4, 9, 10, 14, 16, 25, 26, 29, 30, 35, 36, 39, 40, 49, 51, 55, 56, 61, 64.
65 est composé.
Il y a 20 solutions.



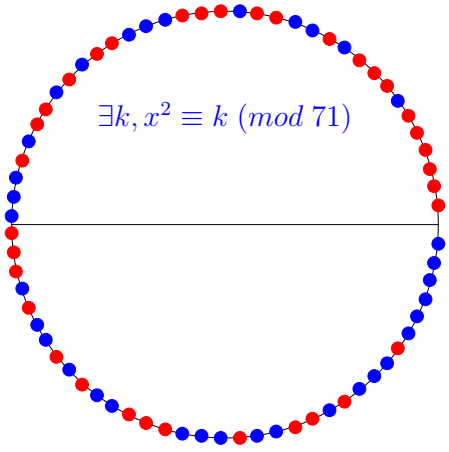
Solutions de $\exists k, x^2 \equiv k \ (mod\ 67)$: 1, 4, 6, 9, 10, 14, 15, 16, 17, 19, 21, 22, 23, 24, 25, 26, 29, 33, 35, 36, 37, 39, 40, 47, 49, 54, 55, 56, 59, 60, 62, 64, 65.
67 est premier.
Il y a 33 solutions.



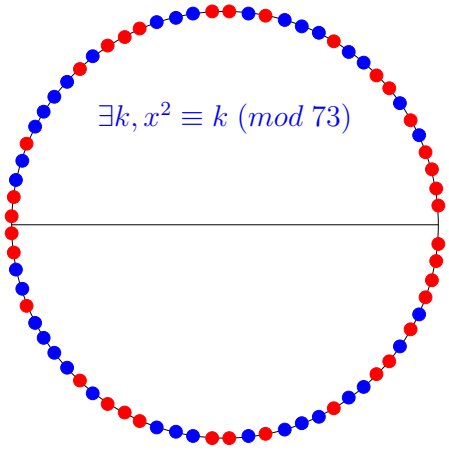
Solutions de $\exists k, x^2 \equiv k \ (mod\ 69)$: 1, 3, 4, 6, 9, 12, 13, 16, 18, 24, 25, 27, 31, 36, 39, 46, 48, 49, 52, 54, 55, 58, 64.
69 est composé.
Il y a 23 solutions.



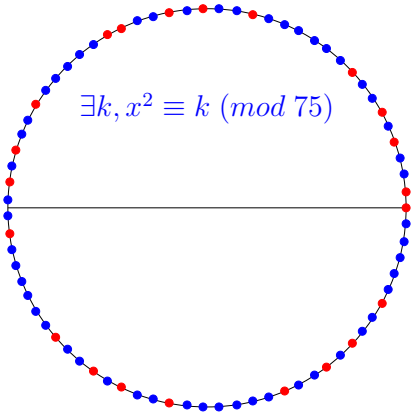
Solutions de $\exists k, x^2 \equiv k \ (mod\ 71)$: 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 19, 20, 24, 25, 27, 29, 30, 32, 36, 37, 38, 40, 43, 45, 48, 49, 50, 54, 57, 58, 60, 64.
71 est premier.
Il y a 35 solutions.



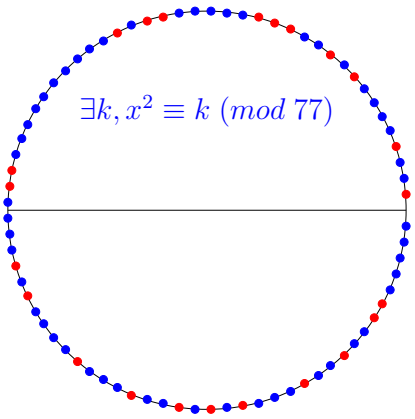
Solutions de $\exists k, x^2 \equiv k \ (mod\ 73)$: 1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 19, 23, 24, 25, 27, 32, 35, 36, 37, 38, 41, 46, 48, 49, 50, 54, 55, 57, 61, 64, 65, 67, 69, 70, 71, 72.
73 est premier.
Il y a 36 solutions.



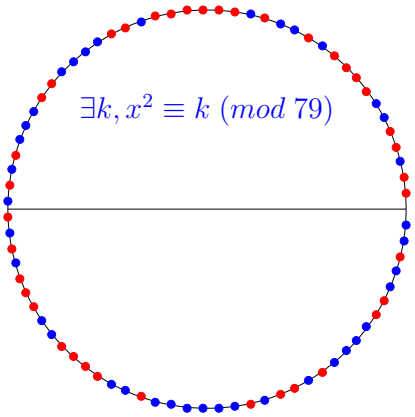
Solutions de $\exists k, x^2 \equiv k \ (mod\ 75)$: 0, 1, 4, 6, 9, 16, 19, 21, 24, 25, 31, 34, 36, 39, 46, 49, 51, 54, 61, 64, 66, 69.
75 est composé.
Il y a 22 solutions.



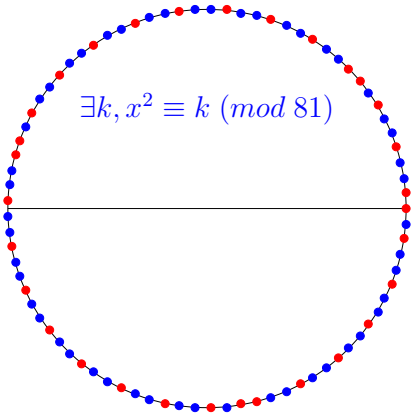
Solutions de $\exists k, x^2 \equiv k \ (mod\ 77)$: 1, 4, 9, 11, 14, 15, 16, 22, 23, 25, 36, 37, 42, 44, 49, 53, 56, 58, 60, 64, 67, 70, 71.
77 est composé.
Il y a 23 solutions.



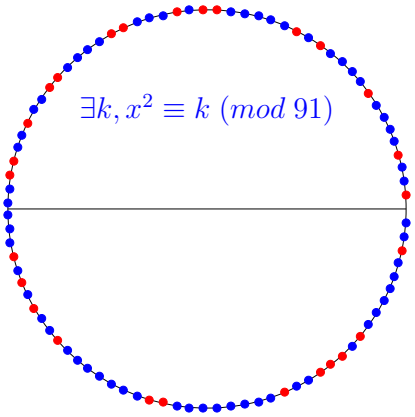
Solutions de $\exists k, x^2 \equiv k \ (mod\ 79)$: 1, 2, 4, 5, 8, 9, 10, 11, 13, 16, 18, 19, 20, 21, 22, 23, 25, 26, 31, 32, 36, 38, 40, 42, 44, 45, 46, 49, 50, 51, 52, 55, 62, 64, 65, 67, 72, 73, 76.
79 est premier.
Il y a 39 solutions.



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.

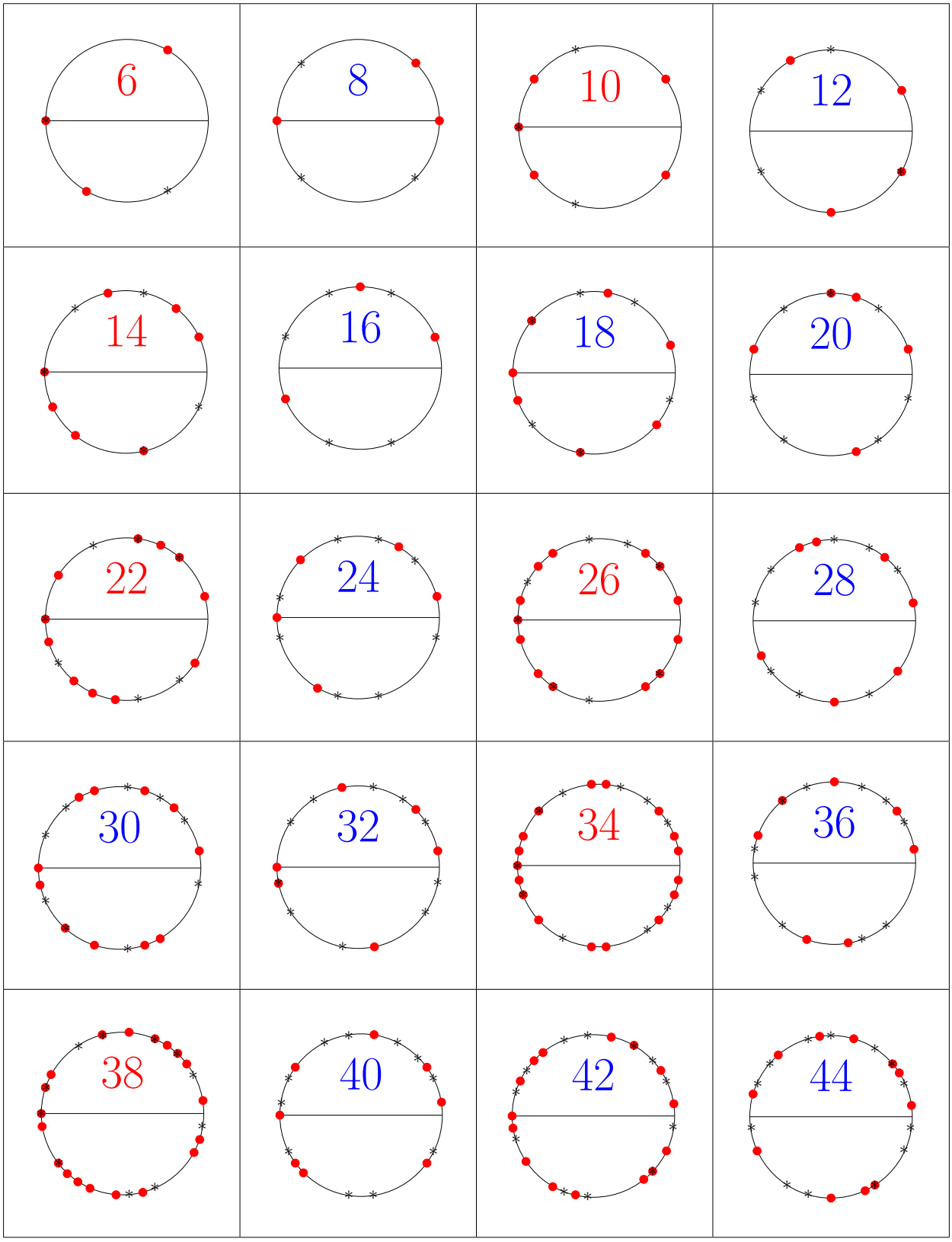


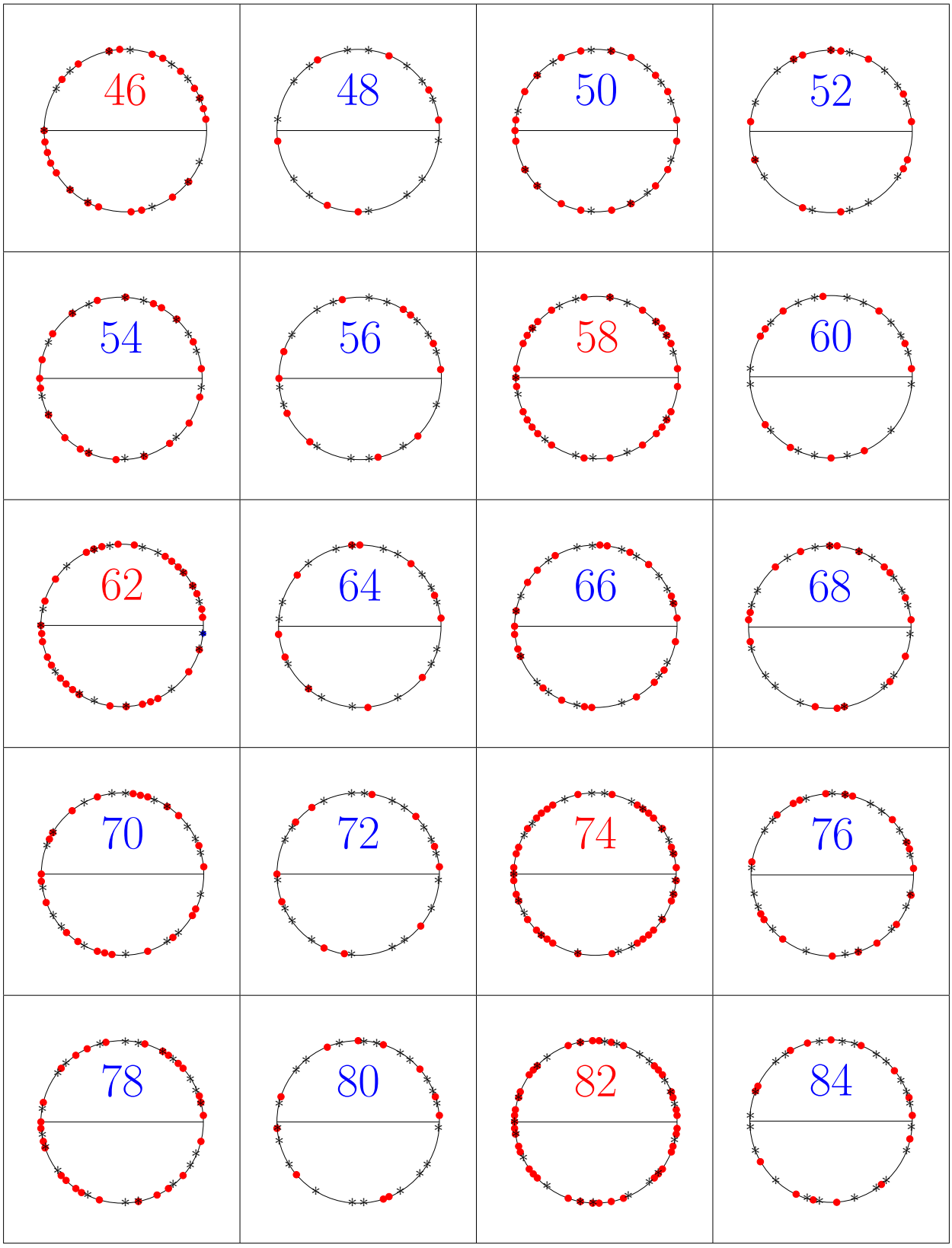
Solutions de $\exists k, x^2 \equiv k \ (mod\ 91)$: 1, 4, 9, 14, 16, 22, 23, 25, 29, 30, 35, 36, 39, 42, 43, 49, 51, 53, 56, 64, 65, 74, 77, 78, 79, 81, 88.
91 est composé.
Il y a 27 solutions.

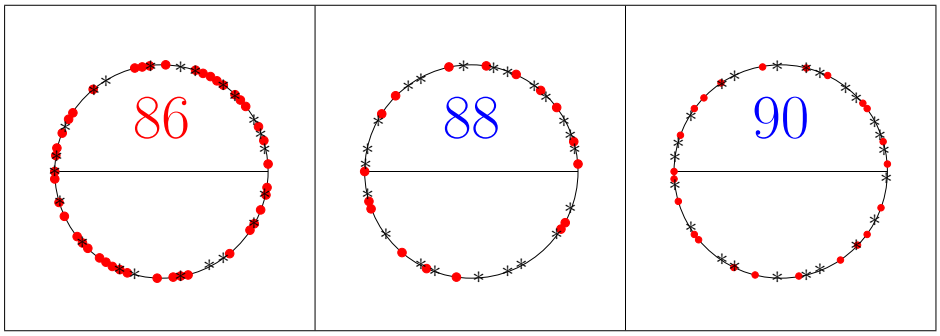


Résidus quadratiques sur colliers pour nombres pairs (Denise Vella-Chemla, 23.5.2019)

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.

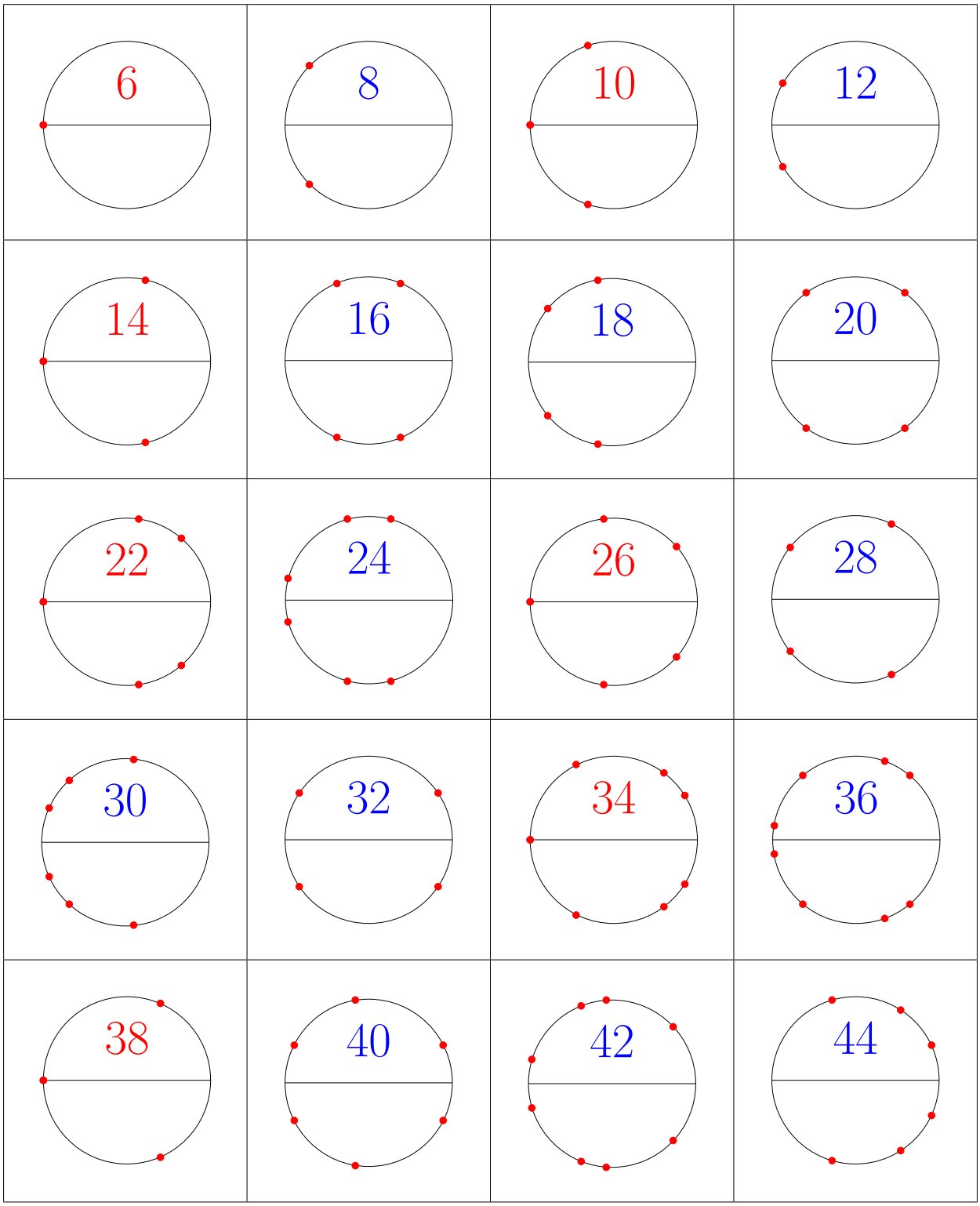


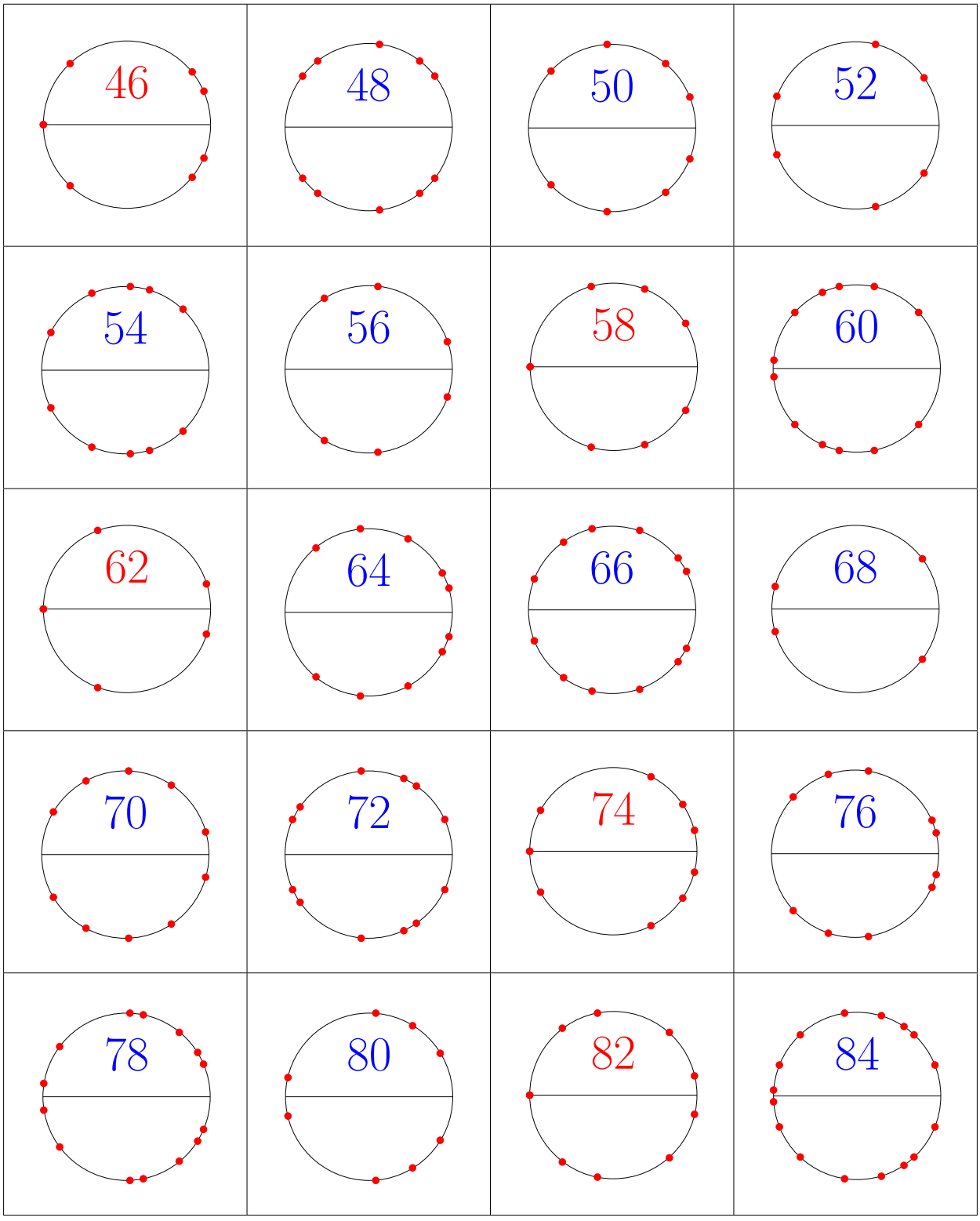

46
48
50
52
54
56
58
60
62
64
66
68
70
72
74
76
78
80
82
84

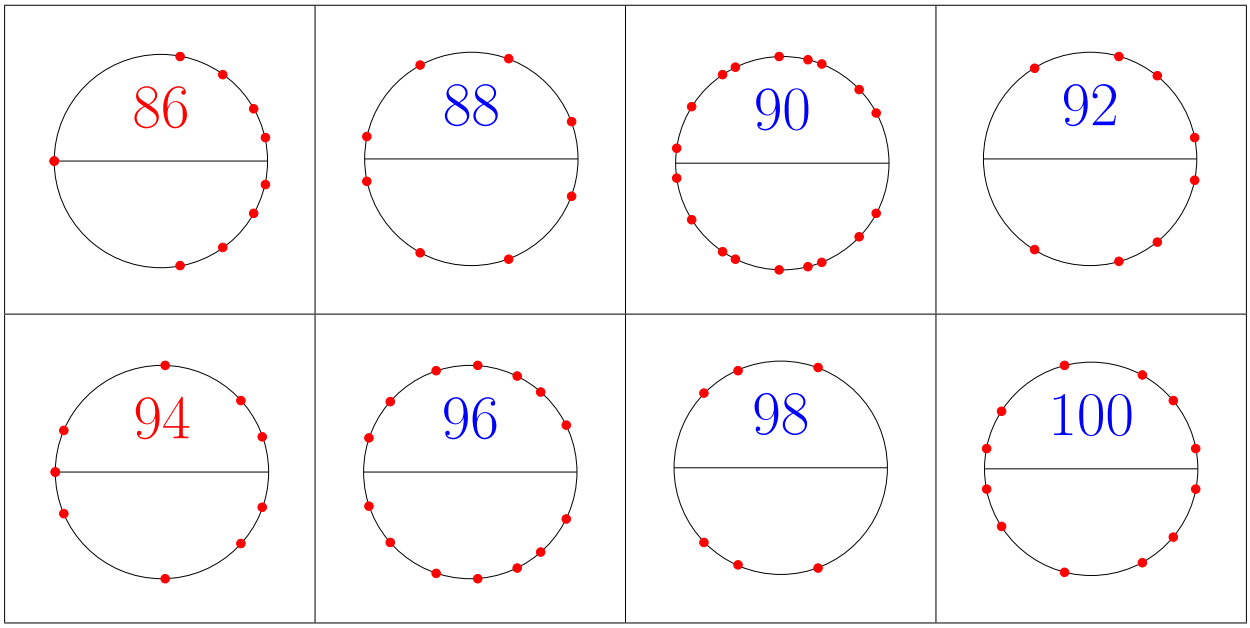

86
88
90

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

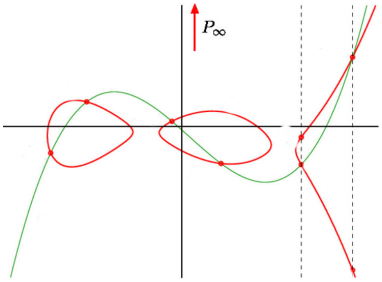

86
88
90
92
94
96
98
100

Ô stop ! (Denise Vella-Chemla, 31.5.2019)

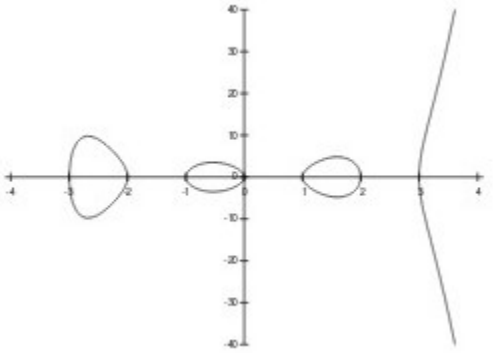
Il s'agit de garder en mémoire le fait qu'en calculant les indices de la section 53 des Recherches arithmétiques de Gauss (consultables ici http://denise.vella.chemla.free.fr/indices-RA53.pdf), on a réalisé à nouveau que la caractéristique des nombres premiers est d'avoir une solution au moins à l'équation $x^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ (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.

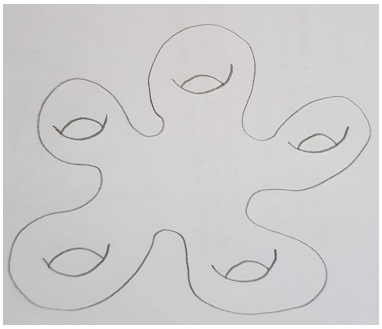
Exemple d'une courbe hyperelliptique de genre 2 associable au nombre premier 5



Exemple d'une courbe hyperelliptique de genre 3 associable au nombre premier 7



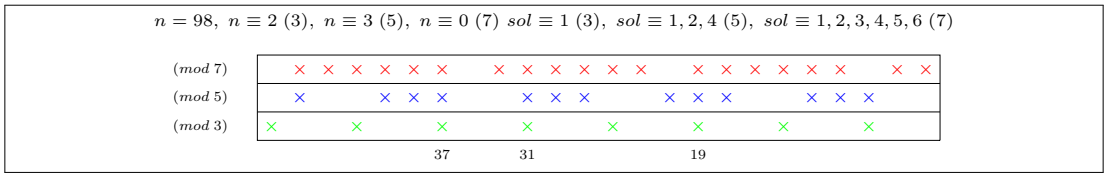
Exemple d'une surface de Riemann à 5 trous associable au nombre premier 11



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 :

$$\frac{n}{2} \leq n' \leq n$$

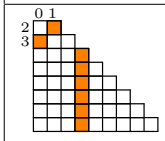
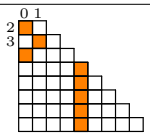
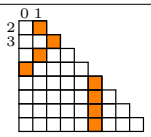
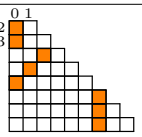
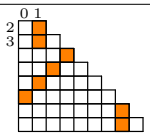
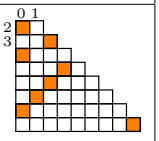
et

$$p_1 \not\equiv n \ (mod\ m) \text{ pour tout } m \text{ premier tel que } 3 \leq m \leq \sqrt{n} \qquad (1)$$

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.

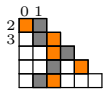
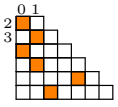
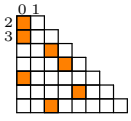
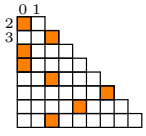
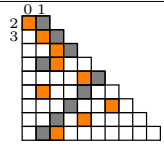
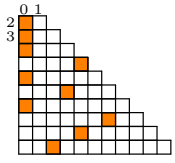
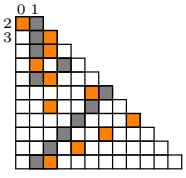
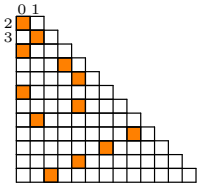
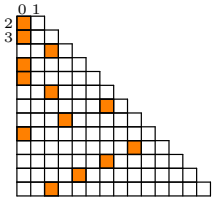
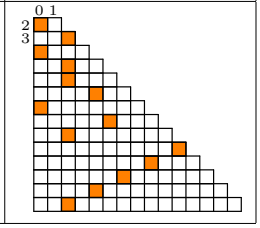
Tores trapézoïdaux (Denise Vella-Chemla, 9.6.2019)

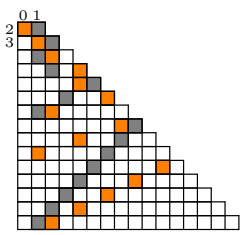
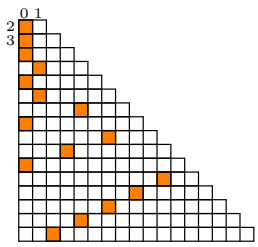
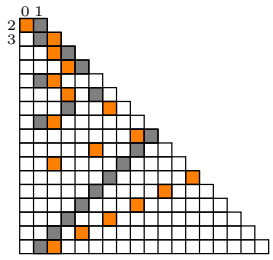
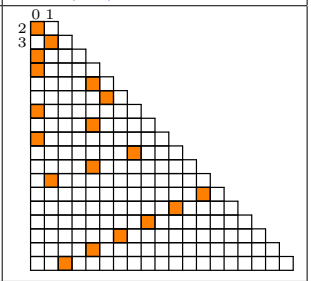
On observe d'abord des pixels qui avancent dans un tore trapézoïdal de taille donnée (utile par exemple si on cherche les décomposants de Goldbach de 20).
Les indices des colonnes de chaque tore trapézoïdal représenté par une matrice triangulaire basse de pixels sont égaux à 0, 1, 2, etc.
Les indices 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.

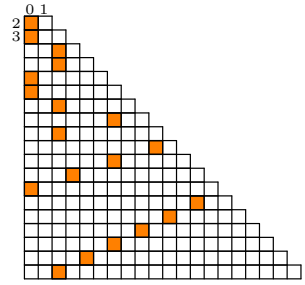
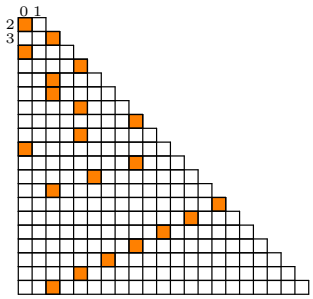
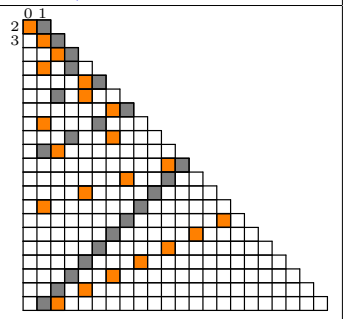
$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
					

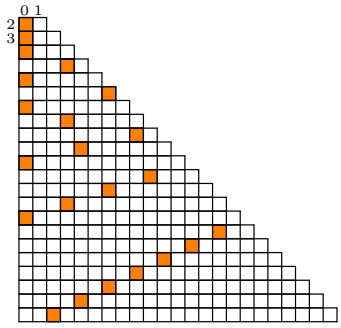
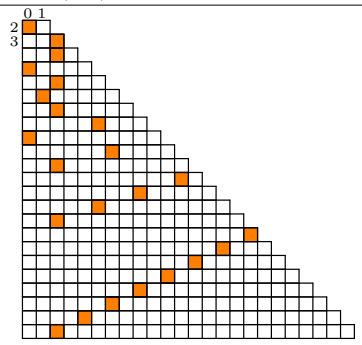
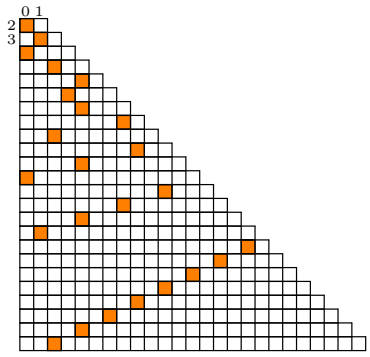
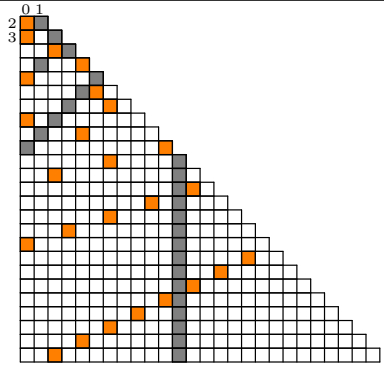
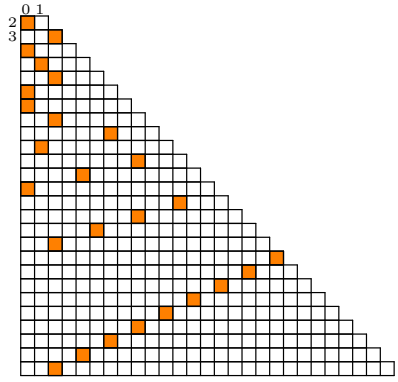
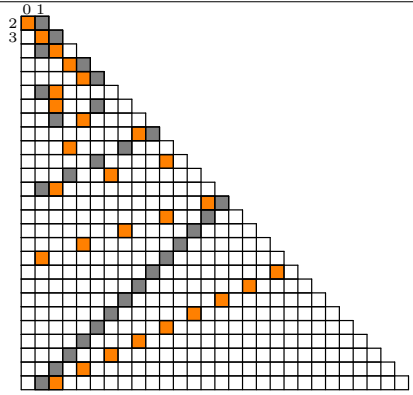
On fournit ci-dessous les tores associés aux seuls nombres pairs. Pour voir le mouvement d'un pixel d'un tore à l'autre, rappelons-nous qu'il saute une case de nombre pair en nombre pair. On montre pour les nombres pairs $2p$ (en orange) doubles d'un nombres premier p (en gris) ce dcomposant de Goldbach 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).

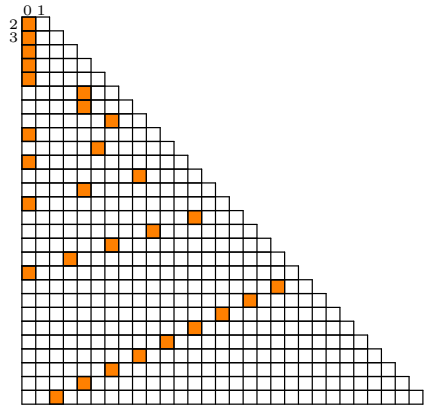
14 : 3, 7	16 : 3, 5	18 : 5, 7	20 : 3, 7	22 : 3, 5, 11
				
24 : 5, 7, 11	**26 : 3, 7, 13**	**28 : 5, 11**	**30 : 7, 11, 13**	**32 : 3, 13**
				

34 : 3, 5, 11, 17	36 : 5, 7, 13, 17	38 : 7, 19	40 : 3, 11, 17
			

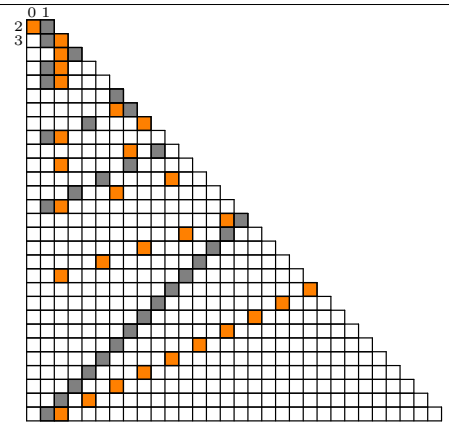
42 : 5, 11, 13, 19	44 : 7, 13	46 : 17, 23
		

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**
	

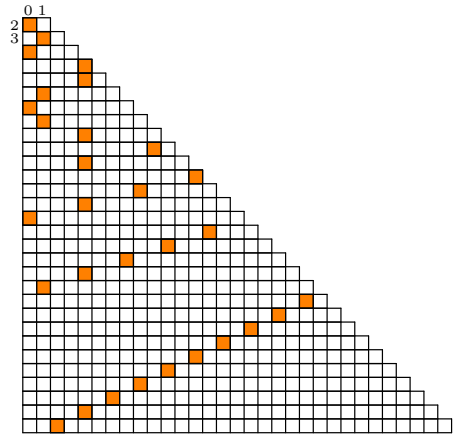
60 : 7, 11, 13, 17, 19, 23, 29



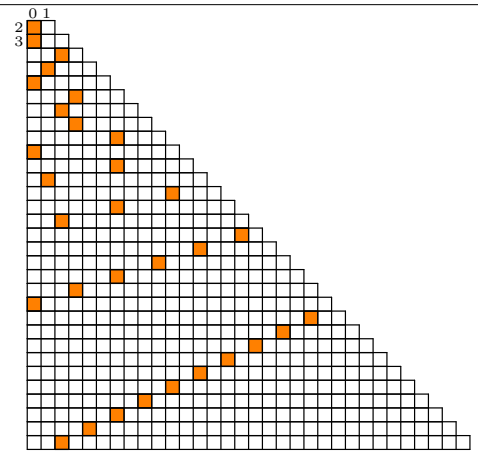
62 : 13, 19, 31



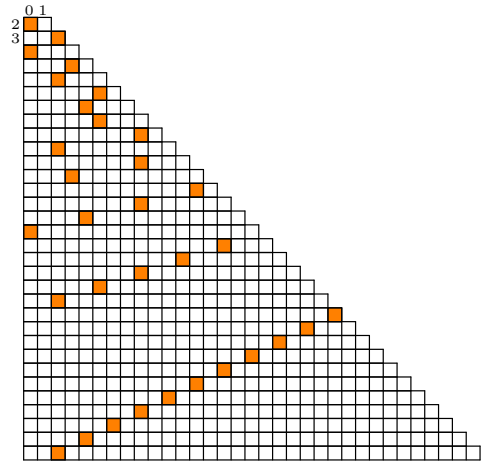
64 : 11, 17, 23



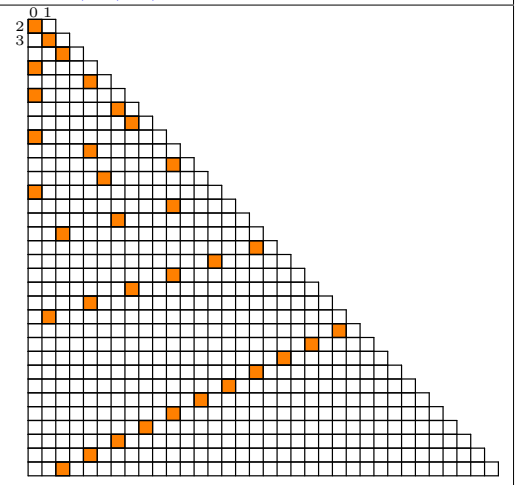
66 : 13, 19, 23, 29

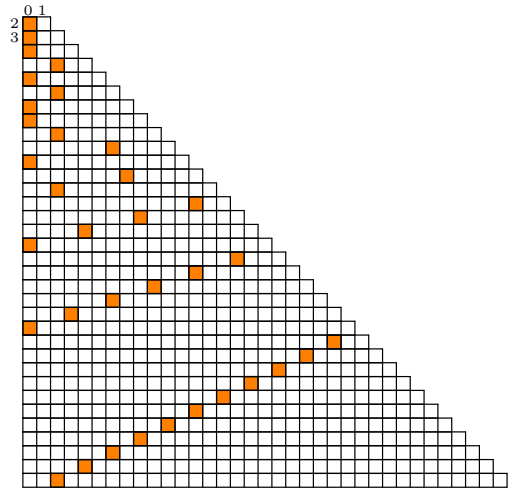
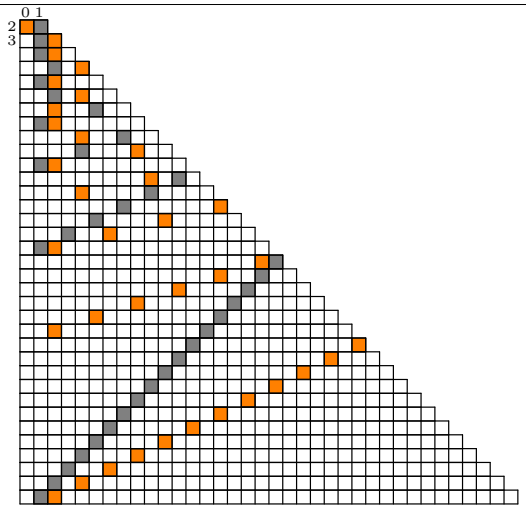
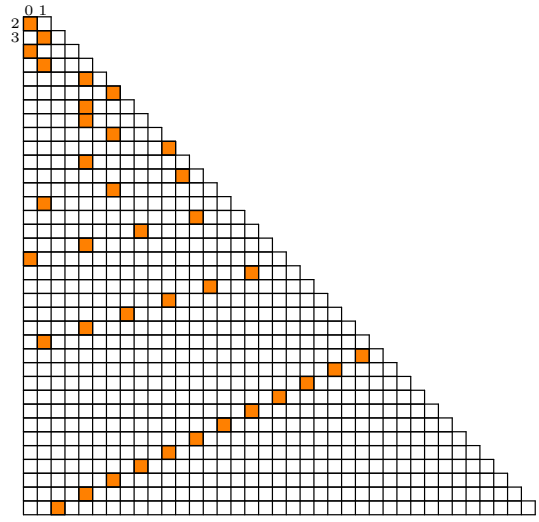
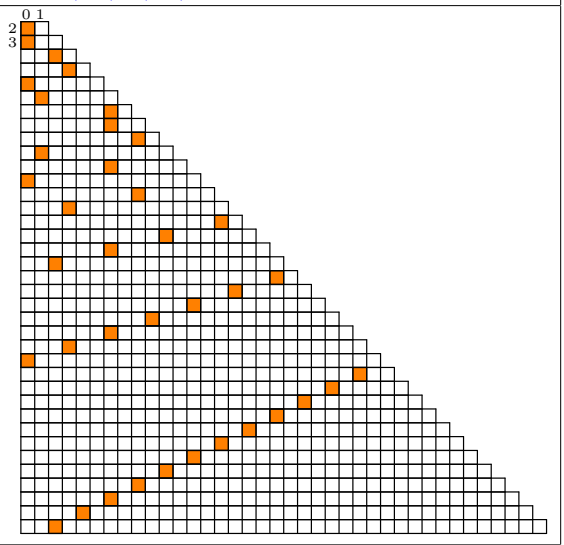


68 : 31

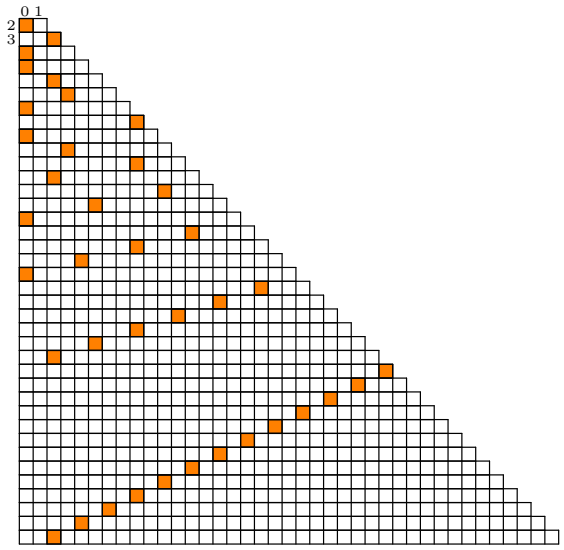


70 : 11, 17, 23, 29

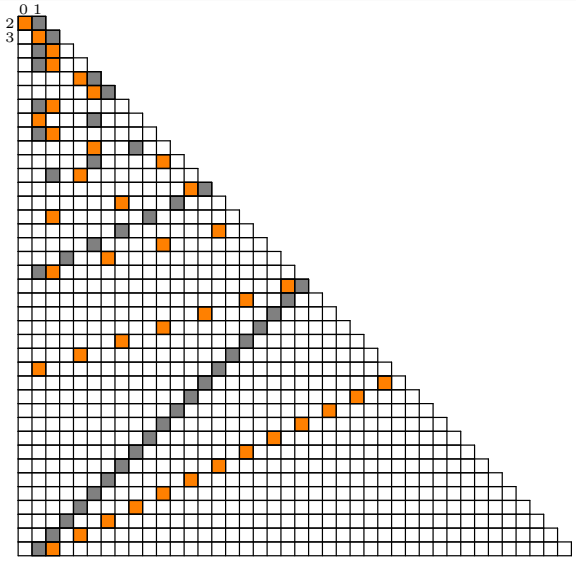


72 : 11, 13, 19, 29, 31	74 : 13, 31, 37
	
76 : 17, 23, 29	78 : 11, 17, 19, 31, 37
	

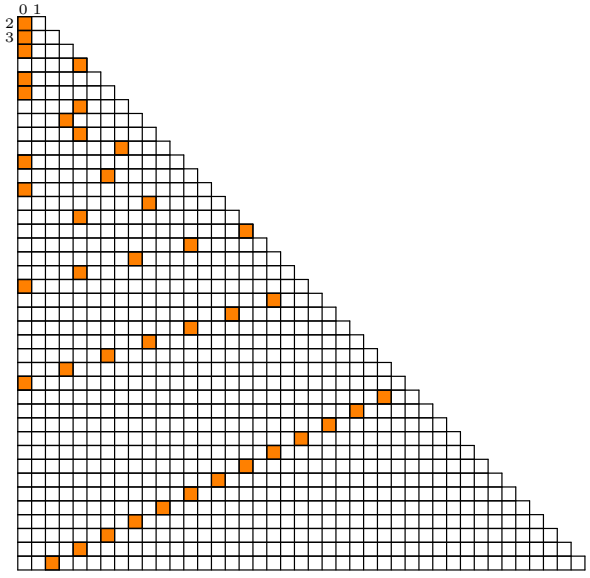
80 : 13, 19, 37



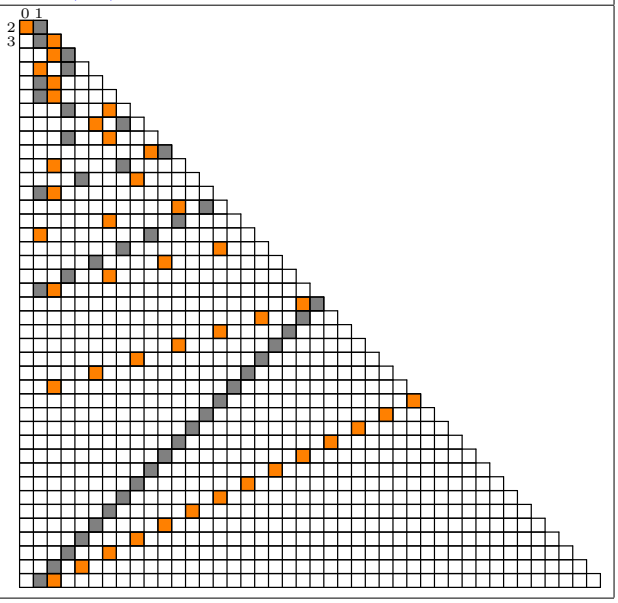
82 : 11, 23, 29, 41



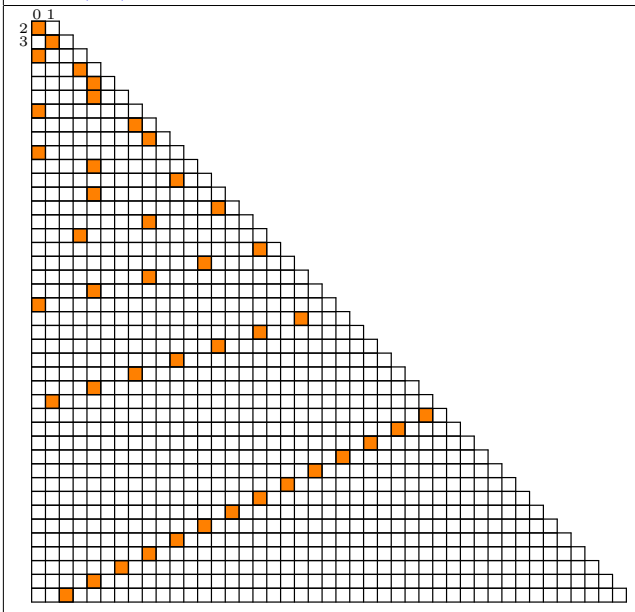
84 : 11, 13, 17, 23, 31, 37, 41



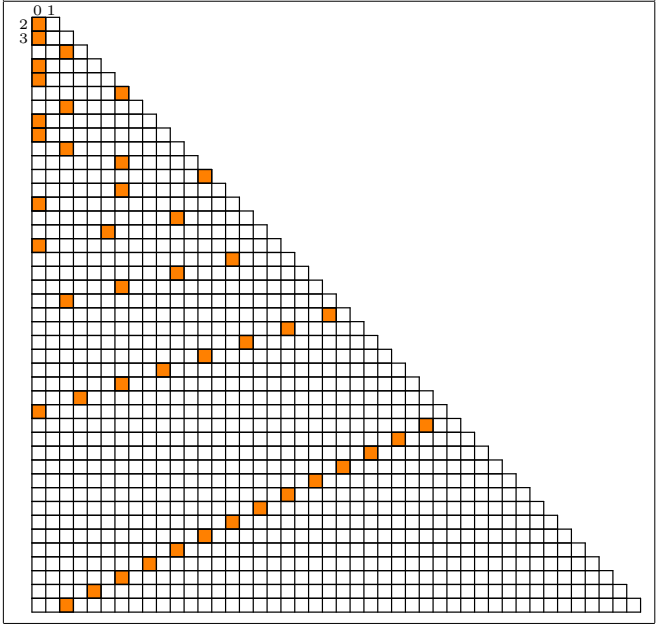
86 : 13, 19, 43



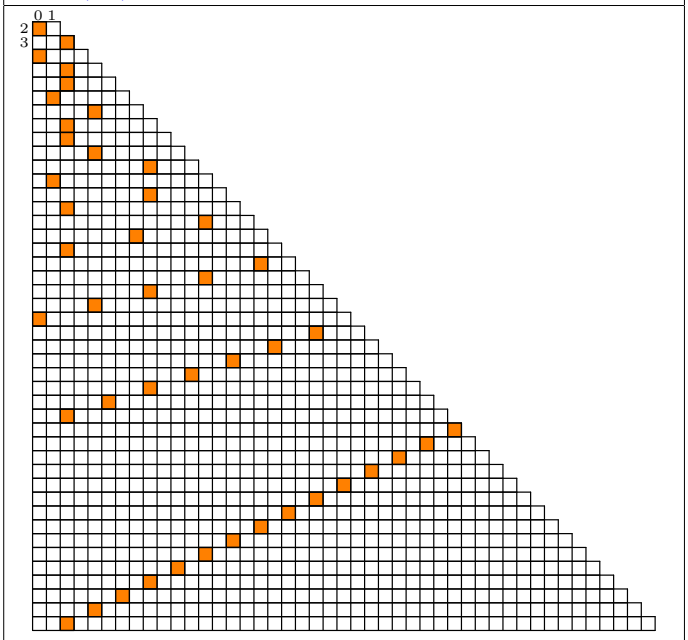
88 : 17, 29, 41



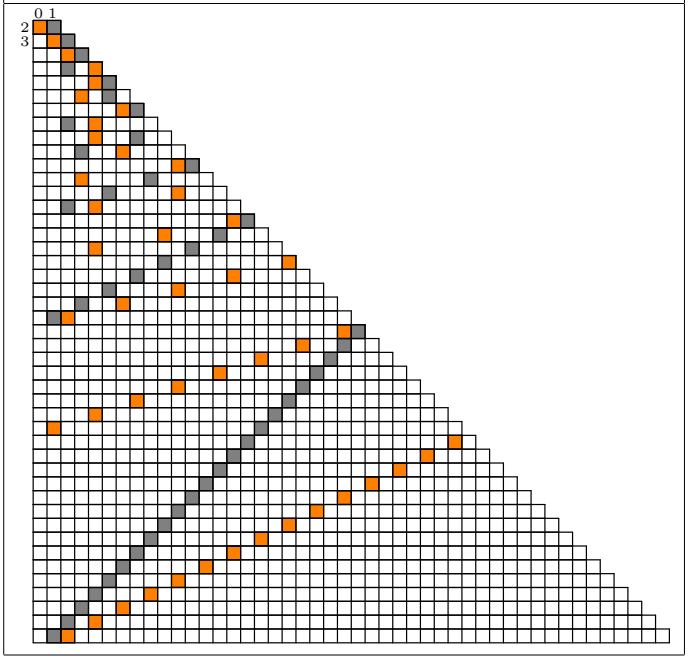
90 : 11, 17, 19, 23, 29, 31, 37, 43



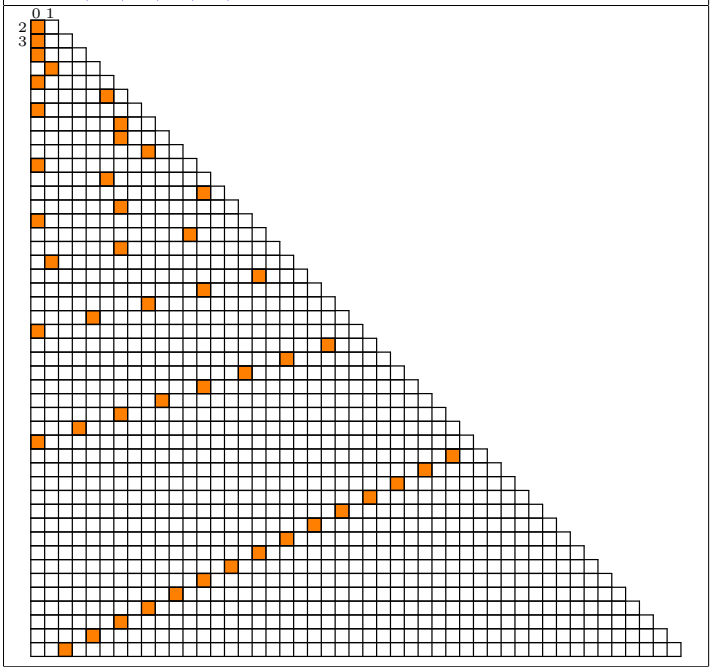
92 : 13, 19, 31



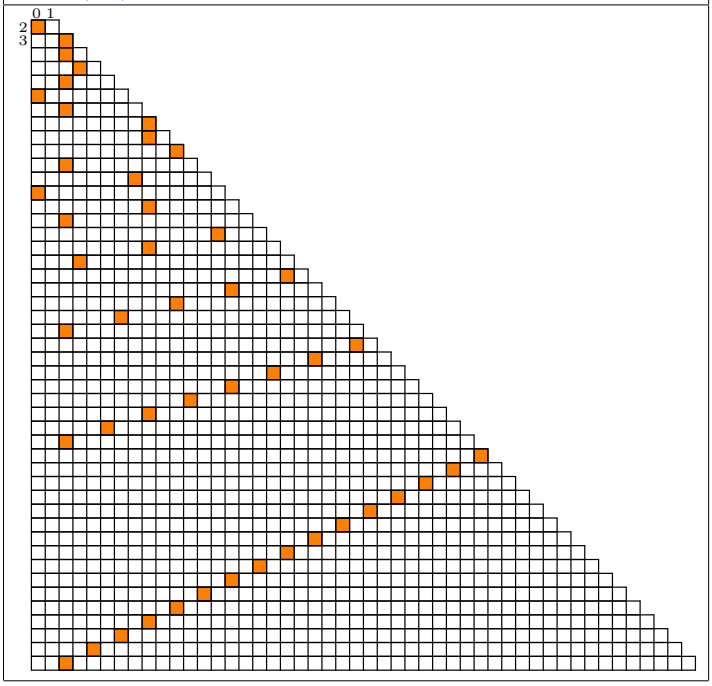
94 : 11, 23, 41, 47

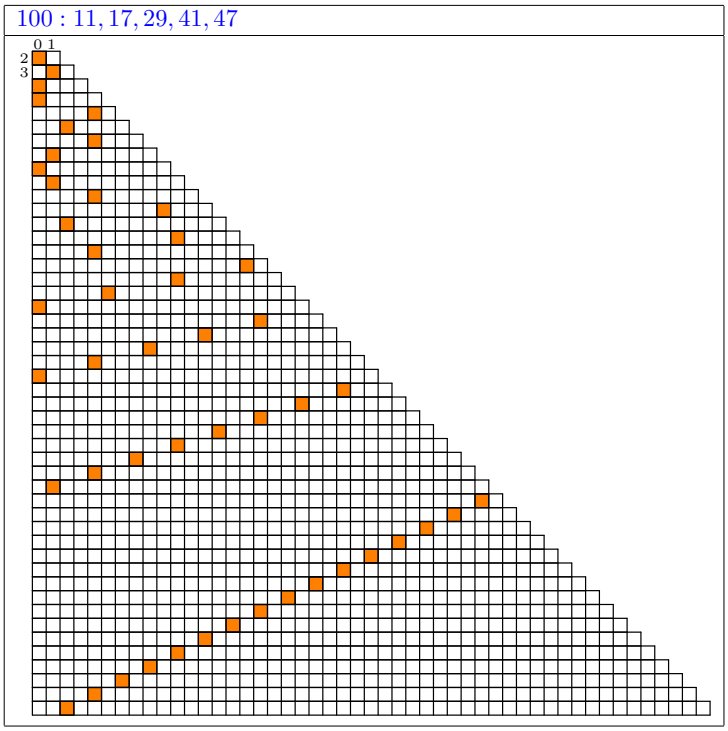


96 : 13, 17, 23, 29, 37, 43

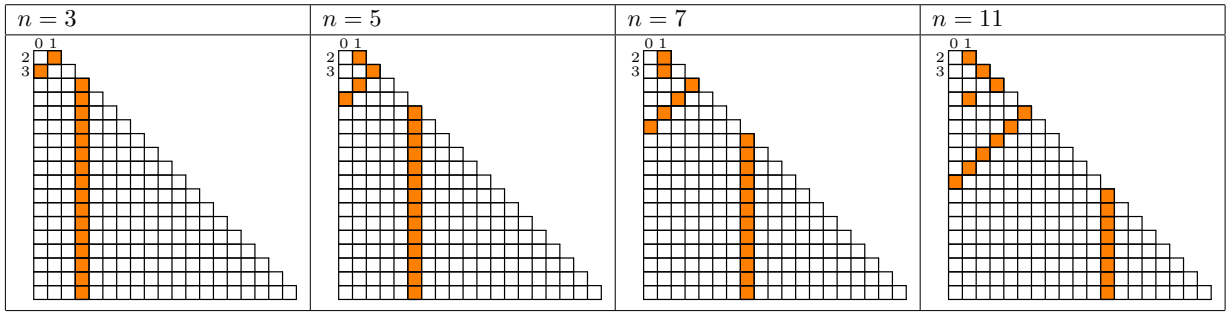


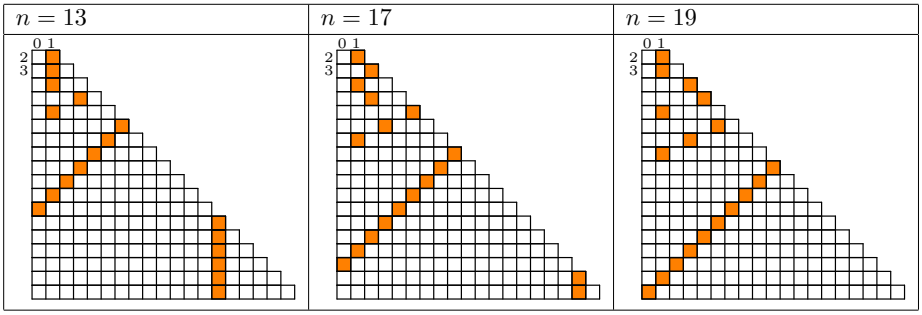
98 : 19, 31, 37



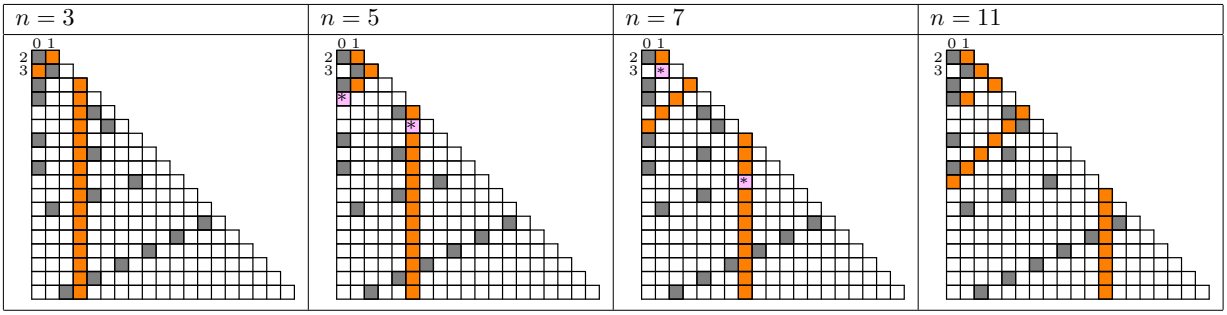


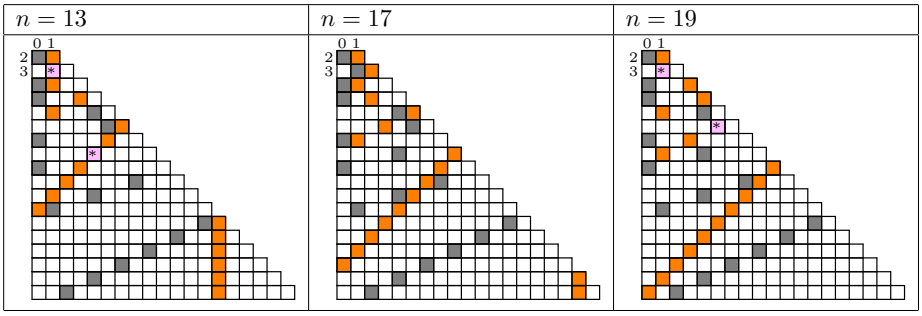
Ci-dessous, on peut observer les tores des nombres premiers 3, 5, 7, 11, 13, 17, 19 à la recherche des décomposants de Goldbach de 40.





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

$$(0,0),(0,1),(0,2),(0,3),(0,4),$$
$$(1,0),(1,1),(1,2),(1,3),(1,4),$$
$$(2,0),(2,1),(2,2),(2,3),(2,4),$$
$$(3,0),(3,1),(3,2),(3,3),(3,4),$$
$$(4,0),(4,1),(4,2),(4,3),(4,4).$$

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.

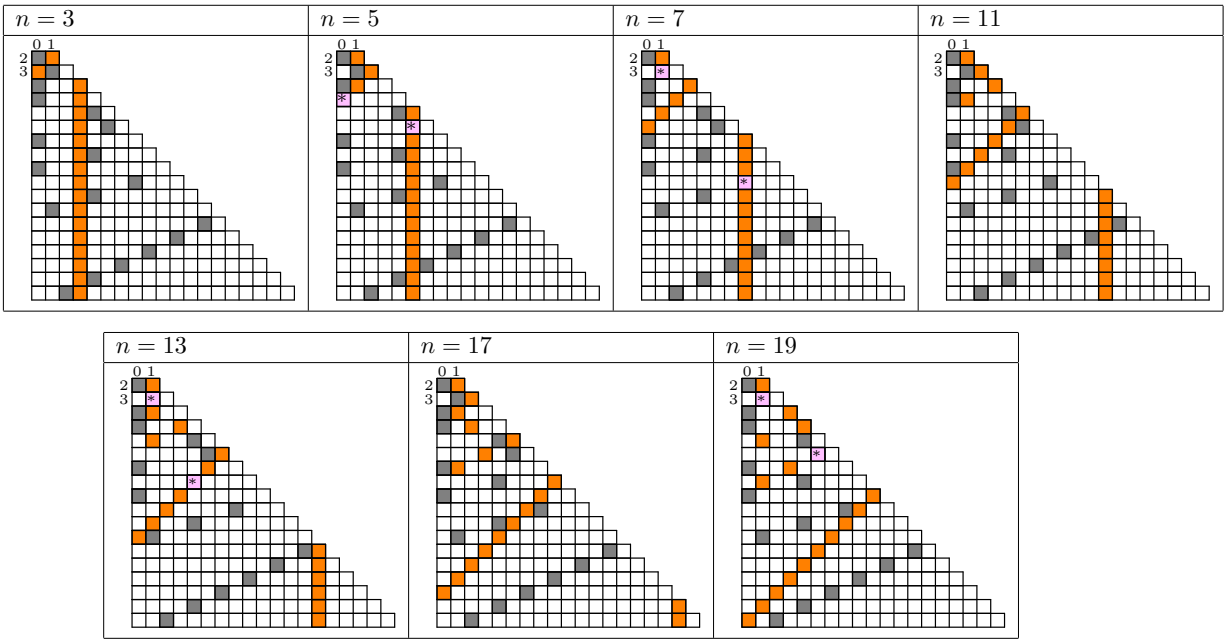
Référence

[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 :

1010010001000010000 0...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.

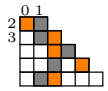
$$\begin{pmatrix}
0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 1 & 0 & \dots & \dots & \dots & \dots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

Tous les ... sont des 0.

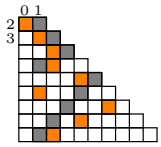
D'un Z qui veut dire... (Denise Vella-Chemla, 15.6.2019)

$2p = p + p$: 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.

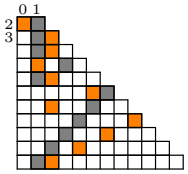
14



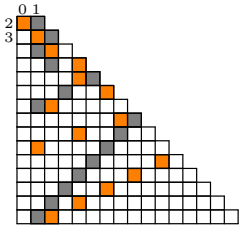
22



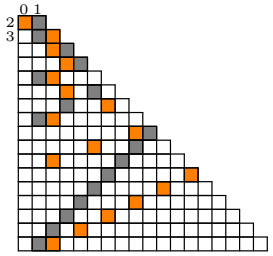
26



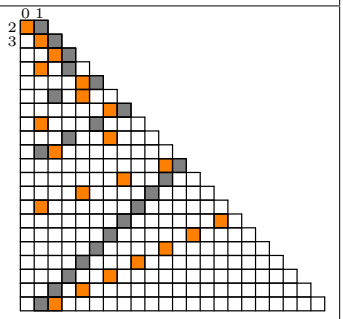
34



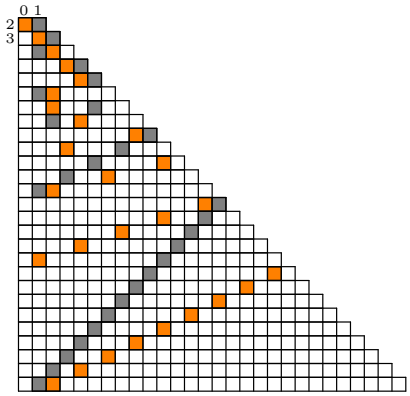
38



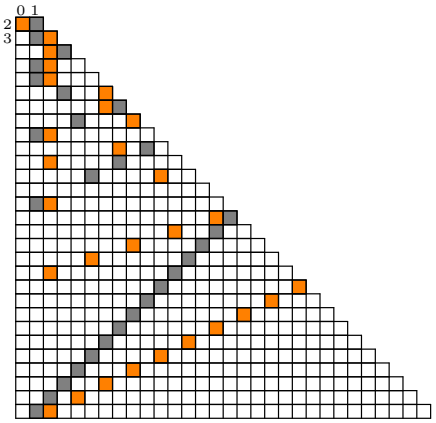
46



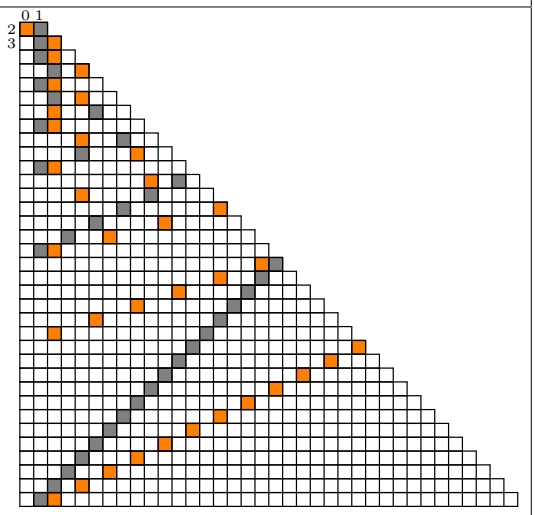
58



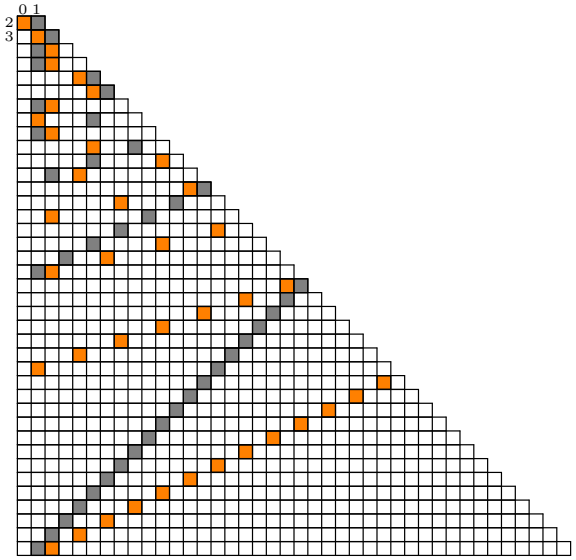
62



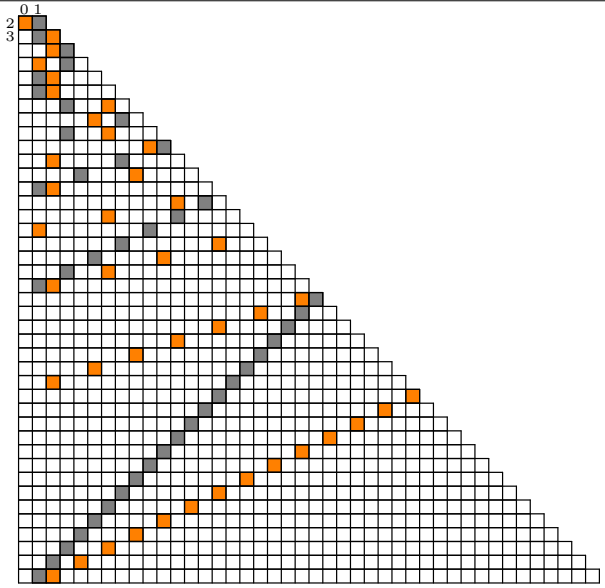
74



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 :

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

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).

$$\text{(3.27)} \qquad \frac{e^{-\gamma}}{\log x}\left(1-\frac{1}{\log^2 x}\right) < \prod_{p\leq x}\left(1-\frac{1}{p}\right) \quad \text{pour } 1 < x.$$

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

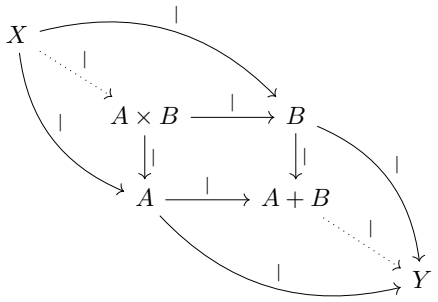
[1] http://denisevellachemla.eu/denitac.pdf.

[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.

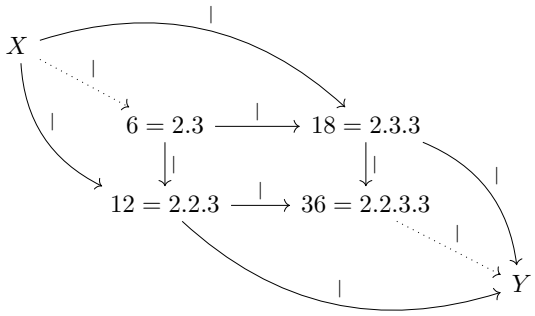
1. Cette minoration est à distinguer du Théorème des nombres premiers, prouvé indépendamment par Hadamard et La Vallée-Poussin, et qui fournit une tendance asymptotique pour $\pi(x)$.

Pgcd et Ppcm représentés sur diagrammes commutatifs (D. Chemla, 15.9.2019)

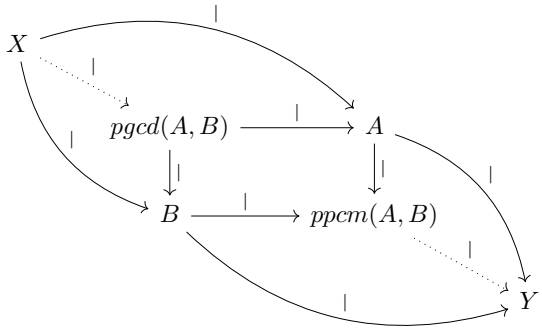
Le symbole | signifie *"divise"*.



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.

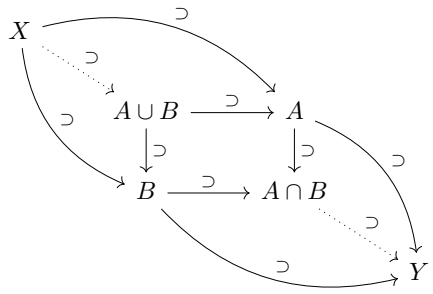


On voit ainsi le *pgcd* comme une intersection ensembliste (les ensembles pouvant contenir un facteur avec une certaine multiplicité, plusieurs fois : par exemple, deux occurrences de 2 et deux occurrences de 3 sont "contenues" dans 36).
Le *ppcm* est vu comme une union. C'est l'idée intuitive que l'on 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 :

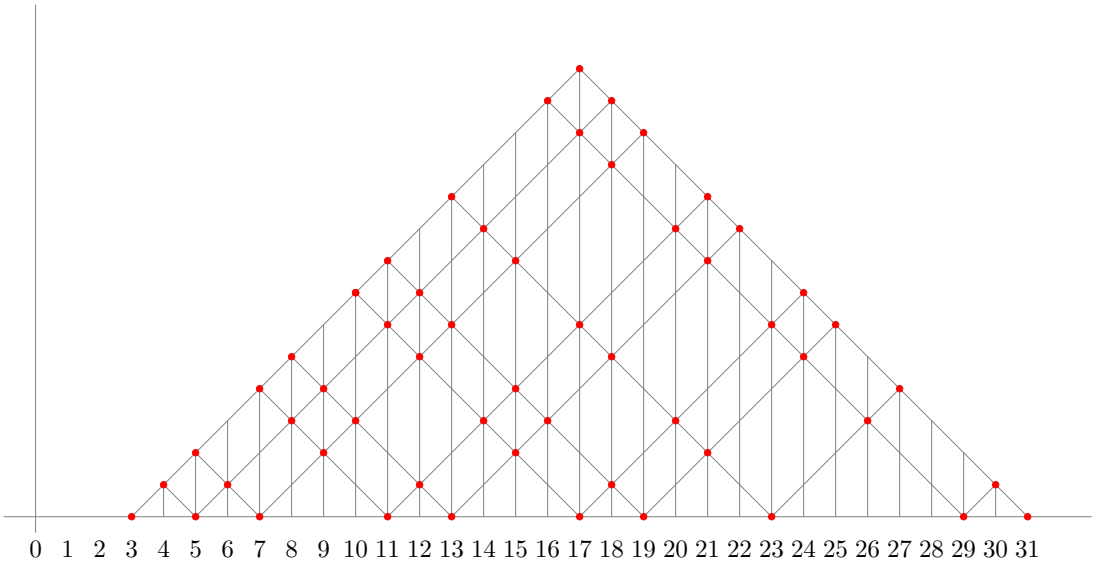


FIGURE 1 : Le treillis Goldbach

2. Les décompositions additives

Chaque point marqué d'un symbole • correspond à une décomposition additive dont les deux sommants sont des nombres premiers.

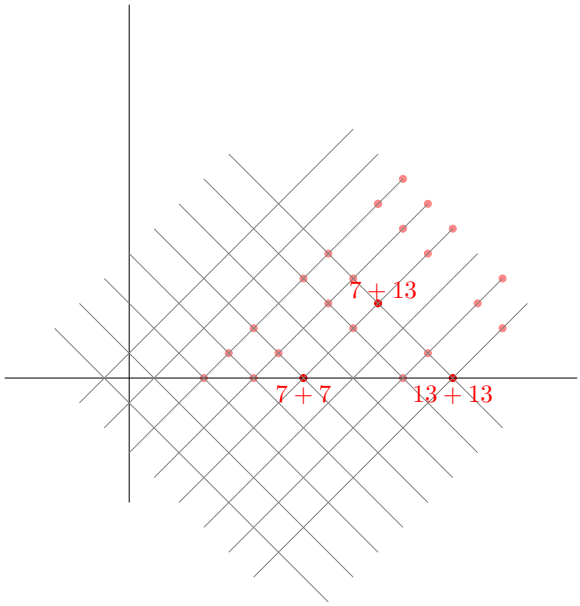


FIGURE 2 : Décompositions additives

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*.

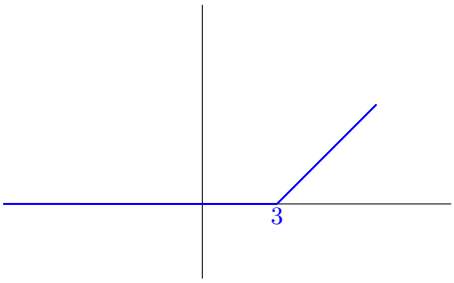


FIGURE 3 : Une droite tropicale d'équation $y = max(x - 3, 0)$

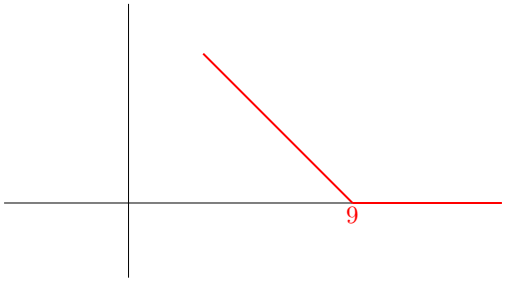


FIGURE 4 : Une autre droite tropicale d'équation $y = max(9 - x, 0)$

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).

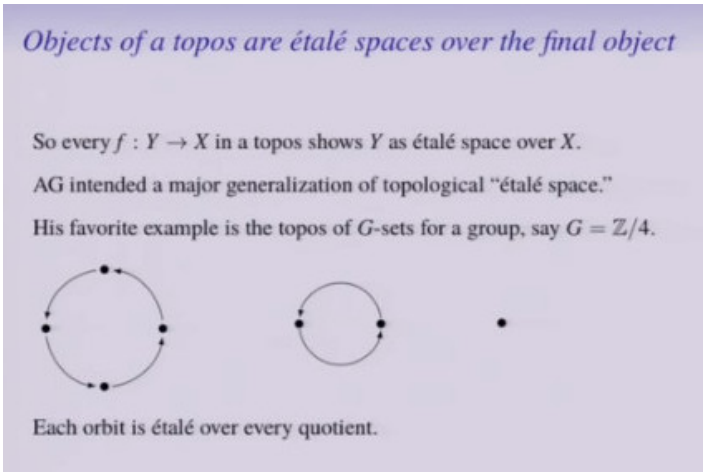
Ce calcul permet d'aboutir clairement à une contradiction car il dépasse grandement le nombre effectif de nombres impairs compris entre 3 et $\frac{n}{2}$ qui est égal à $\left\lfloor \frac{n-2}{4} \right\rfloor$ (on a en effet obtenu pour le cas limite un cardinal au moins égal au double du cardinal 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:

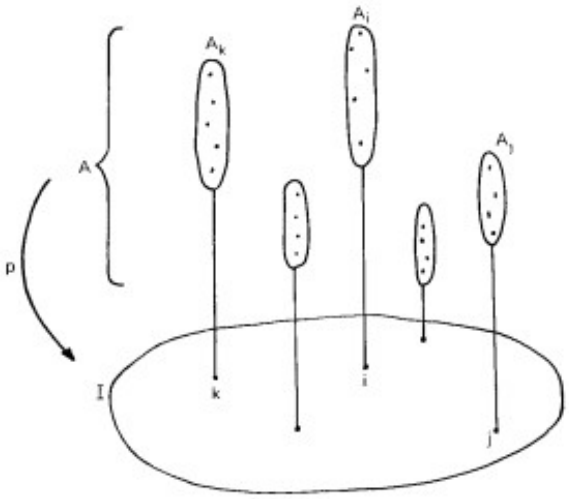


Fig. 4.4.

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.

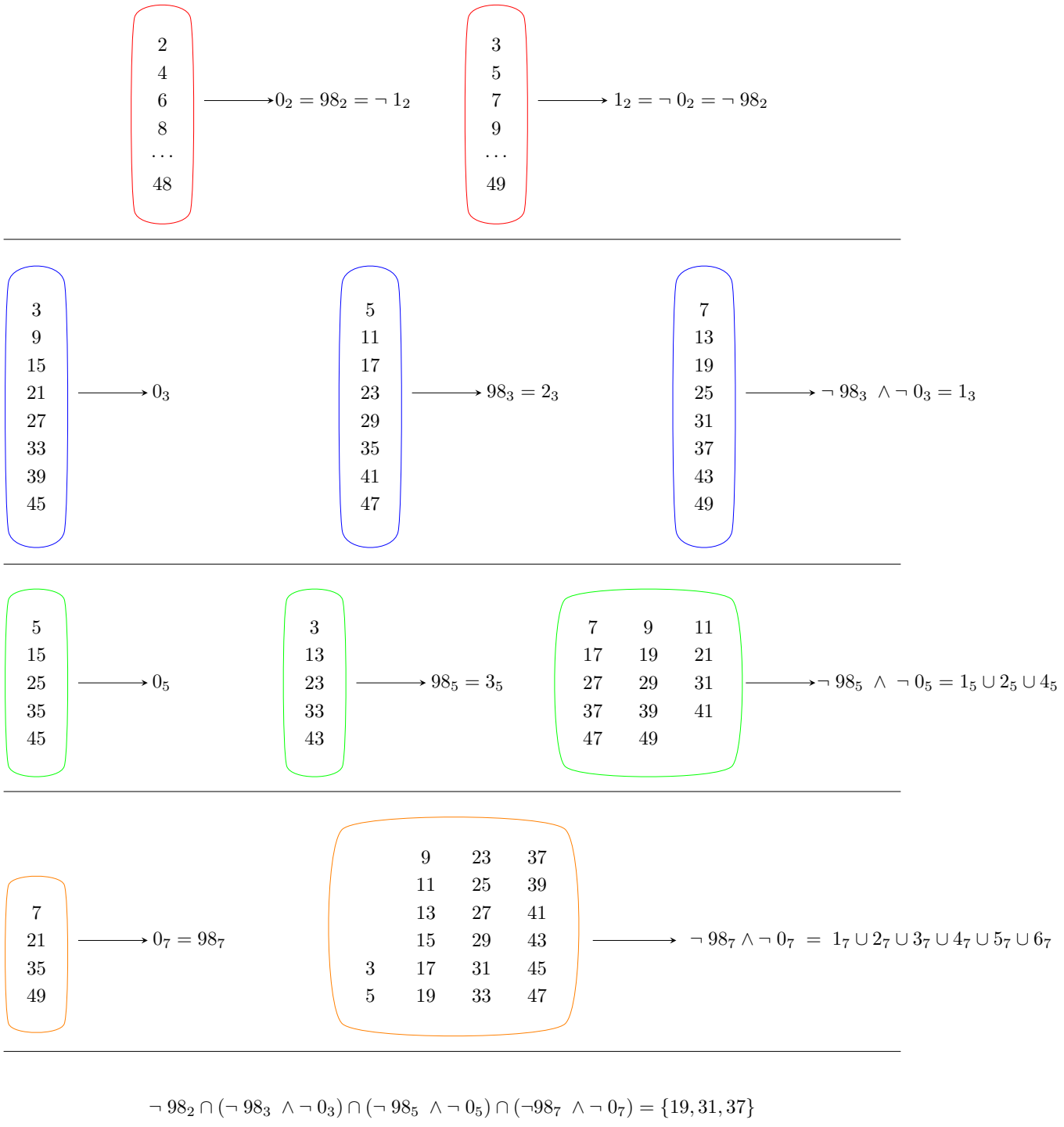
Annexe 5 : Somme des inverses des puissances de 2

$$\sum_{i=1}^{n} \frac{1}{2^i} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^n}$$

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.

Surprise par une somme alternée de cosinus quotientés (Denise Vella-Chemla, 20.11.2019)

On vient de découvrir les résultats d'un programme qui nous époustouflent. Les voici : en alternant une somme de cosinus, et en ne conservant que les cosinus égaux à 1 ou -1, on obtient une fonction qui associe aux nombres premiers de la forme $n = 4k + 1$ une image égale à $\frac{n-1}{2} - 2$ tandis que cette fonction associe aux nombres premiers de la forme $n = 4k + 3$ une image égale à $\frac{n-1}{2}$ et qu'enfin, elle associe des nombres différents de ces deux expressions aux nombres composés.

Voici le programme en python qui calcule la fonction en question :

```
import math
from math import atan, cos

PI = 4.0 * atan(1.0)
print int(-1)␣=␣+str(int(-1))
print int(1)␣=␣+str(int(1))
print int(-0.6)␣=␣+str(int(-0.6))
print int(-0.2)␣=␣+str(int(-0.2))
print int(-0.5)␣=␣+str(int(-0.5))
print int(0.6)␣=␣+str(int(0.6))
print int(0.2)␣=␣+str(int(0.2))
print int(0.5)␣=␣+str(int(0.5))

for n in range(2,101):
  oppose = 1
  somme = 0.0
  chaine=␣
  for i in range(2,n):
    sommeinterm = 0.0
    for j in range(1,i+1):
      oppose = (-1)*oppose
      sommeinterm += oppose*int(cos(2.0 * PI * float(n) * float(j) / float(i)))
      somme += oppose*int(cos(2.0 * PI * float(n) * float(j) / float(i)))
      print(str(n)+"␣somme␣globale␣␣␣"+str(somme-1))
```

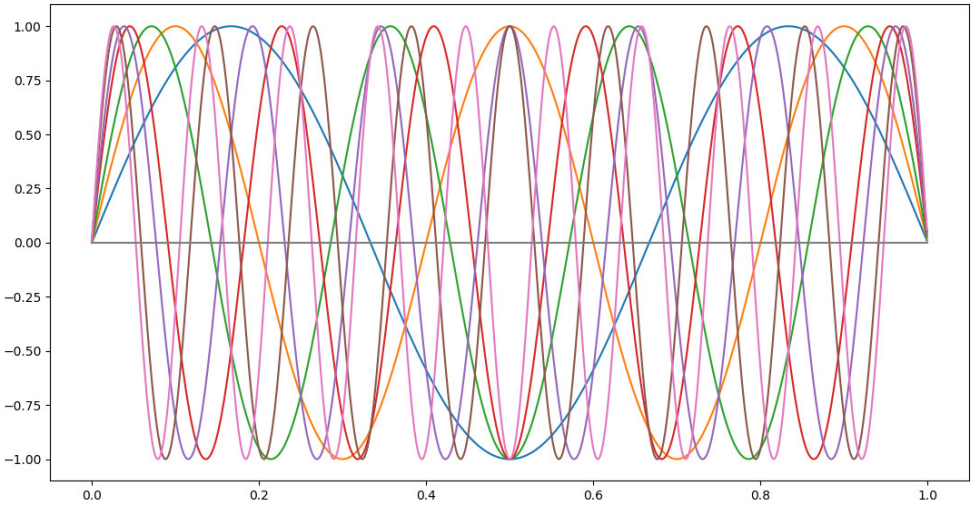
Voici les images des nombres de 1 à 100 fournies par la fonction :

sac(1) = -1	sac(21) = 28	sac(41) = 18	sac(61) = 28	sac(81) = 126
sac(2) = -1	sac(22) = -13	sac(42) = -61	sac(62) = -33	sac(82) = -41
sac(3) = 1	sac(23) = 11	sac(43) = 21	sac(63) = 123	sac(83) = 41
sac(4) = -2	sac(24) = -18	sac(44) = -26	sac(64) = -2	sac(84) = -122
sac(5) = 0	sac(25) = 18	sac(45) = 80	sac(65) = 78	sac(85) = 104
sac(6) = -5	sac(26) = -13	sac(46) = -25	sac(66) = -97	sac(86) = -45
sac(7) = 3	sac(27) = 33	sac(47) = 23	sac(67) = 33	sac(87) = 127
sac(8) = -2	sac(28) = -18	sac(48) = -34	sac(68) = -34	sac(88) = -50
sac(9) = 6	sac(29) = 12	sac(49) = 46	sac(69) = 100	sac(89) = 42
sac(10) = -5	sac(30) = -41	sac(50) = -41	sac(70) = -93	sac(90) = -165
sac(11) = 5	sac(31) = 15	sac(51) = 73	sac(71) = 35	sac(91) = 129
sac(12) = -10	sac(32) = -2	sac(52) = -26	sac(72) = -66	sac(92) = -50
sac(13) = 4	sac(33) = 46	sac(53) = 24	sac(73) = 34	sac(93) = 136
sac(14) = -9	sac(34) = -17	sac(54) = -69	sac(74) = -37	sac(94) = -49
sac(15) = 19	sac(35) = 45	sac(55) = 71	sac(75) = 149	sac(95) = 123
sac(16) = -2	sac(36) = -34	sac(56) = -34	sac(76) = -42	sac(96) = -66
sac(17) = 6	sac(37) = 16	sac(57) = 82	sac(77) = 112	sac(97) = 46
sac(18) = -17	sac(38) = -21	sac(58) = -29	sac(78) = -113	sac(98) = -97
sac(19) = 9	sac(39) = 55	sac(59) = 29	sac(79) = 39	sac(99) = 197
sac(20) = -10	sac(40) = -18	sac(60) = -82	sac(80) = -34	sac(100) = -82

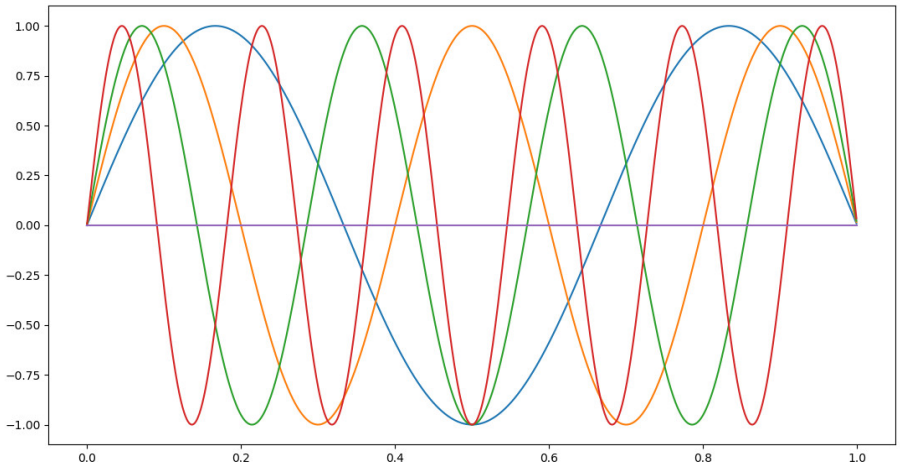
On est étonné de voir que la fonction associe l'opposé $-p$ d'un nombre premier p à son double $2p$ lorsque c'est un nombre premier de la forme $4k+1$ (voir les images $sac(10) = -5, sac(26) = -13, sac(34), sac(58), sac(74), sac(82), \ldots$).

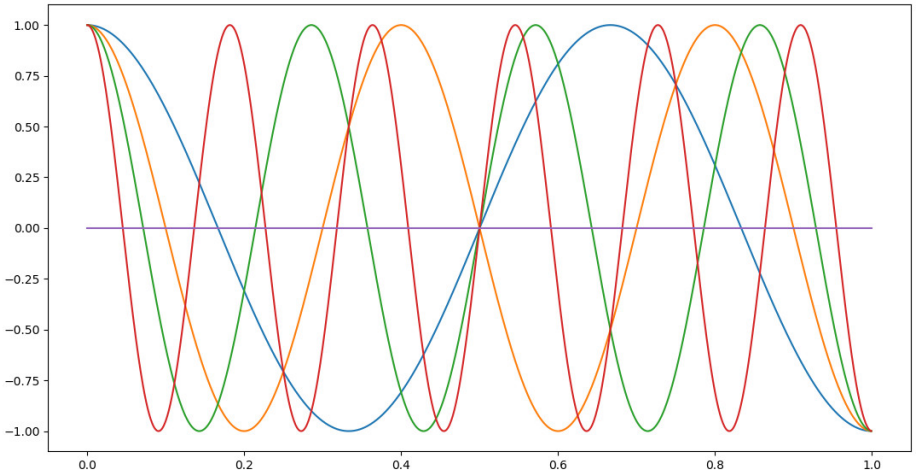
Aux doubles de nombres premiers $2p$ avec p de la forme $4k+3$, la fonction associe $-p-2$ (voir les images $sac(6) = -5, sac(14) = -9, sac(22) = -13, sac(38), sac(46), sac(62), sac(86), sac(94), \ldots$).

Ci-dessous des graphiques montrant vraisemblablement pourquoi les $4k+1$ et les $4k+3$ présentent un comportement différent : dans l'intervalle $[0, 1]$, pour $\frac{1}{2}$, les sinusoïdes des nombres premiers de la forme $4k+1$ se croisent "en haut" du graphique tandis que celles des nombres premiers de la forme $4k+3$ se croisent "en bas". Le premier graphique ci-dessous montre des sinusoïdes et non des cosinusoïdes.



Si l'on se cantonne aux nombres premiers 3, 5, 7, et 11 pour gagner en lisibilité, voici les graphiques des sinusoïdes et ceux des cosinusoïdes.





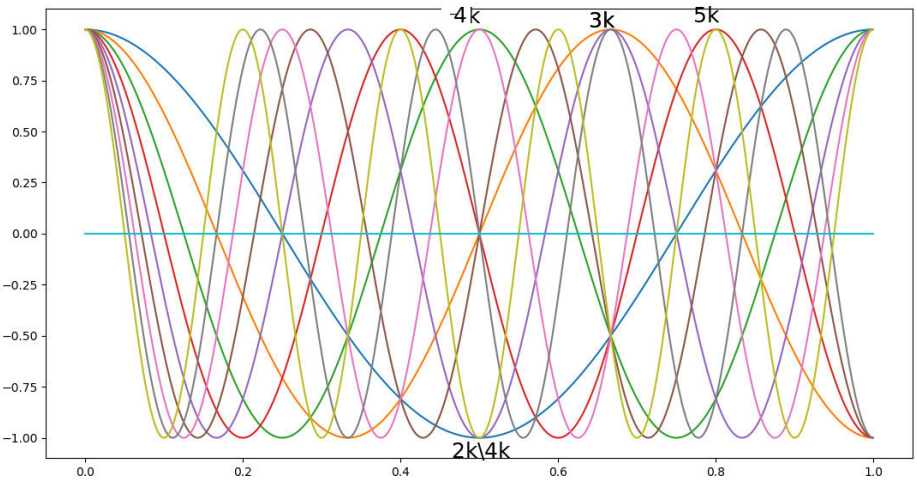
Toutes les cosinusoïdes de fonctions de la forme $\cos(k\pi x)$ avec k impair se croisent en $1/2$.

Les nombres premiers se "voient-ils" sur un ensemble de cosinusoïdes ?

Voici le programme en python qui visualise les cosinusoïdes de $cos(2\pi x)$ à $cos(10\pi x)$:

```
import matplotlib.pyplot as plt
import numpy as np
x = np.arange(0.0,1.0,0.001)
x2 = np.cos(2*np.pi*x) ; x3 = np.cos(3*np.pi*x) ;
x4 = np.cos(4*np.pi*x) ; x5 = np.cos(5*np.pi*x) ;
x6 = np.cos(6*np.pi*x) ; x7 = np.cos(7*np.pi*x) ;
x8 = np.cos(8*np.pi*x) ; x9 = np.cos(9*np.pi*x) ;
x10 = np.cos(10*np.pi*x)
tt = [0 for k in x]
plt.plot(x, x2) ; plt.plot(x, x3) ;
plt.plot(x, x4) ; plt.plot(x, x5) ;
plt.plot(x, x6) ; plt.plot(x, x7) ;
plt.plot(x, x8) ; plt.plot(x, x9) ;
plt.plot(x, x10)
plt.plot(x,tt)
plt.show()
```

Dans le graphique résultant, que voit-on ?

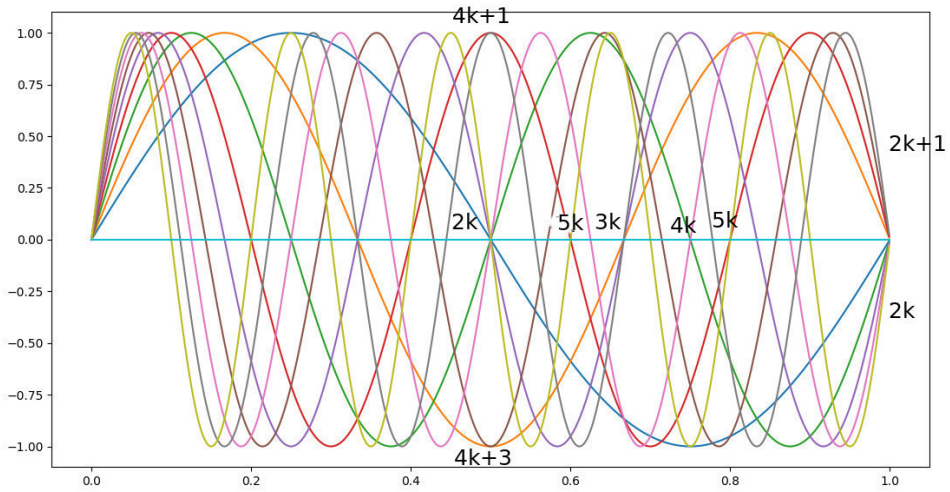


En abscisse 1/2, les courbes des entiers pairs se croisent en haut (ordonnée = +1) ou en bas (ordonnée = -1), les courbes des entiers impairs se croisent sur l'axe des ordonnées (ordonnée = 0). Le point commun à plusieurs courbes en haut au centre voit se croiser les courbes des entiers $4k$ (là, 4 et 8). En bas à la même abscisse de 1/2 on voit les courbes de la forme $2k \backslash 4k$, on désigne par cette notation les multiples de 2 non divisibles par 4 (là, 2, 6 et 10).

En haut, à droite du milieu, en abscisse 2/3, on voit les courbes des $3k$; si on descend verticalement à même abscisse, il n'y a pas de croisement de plusieurs courbes tout en bas et 3 est premier. Idem pour 5 un peu plus loin. Mais pour 7, comme 14 est supérieur à 10, on ne voit pas de croisement en abscisse 6/7.

On peut peut-être utiliser ces points multiples pour compter les nombres premiers ; ici le nombre de nombres premiers impairs compris entre 3 et 5 la moitié de 10 est 2, le nombre de points multiples sur la portion de la droite correspondant à l'ordonnée +1 et pour une abscisse $> 1/2$. Les nombres premiers correspondent aux points multiples d'ordonnée 1 (en haut du diagramme) qui ne tombent pas "en face" de points multiples d'ordonnée -1 (en bas), cette idée permet d'éliminer le nombre 4 (collé à 8) sous prétexte qu'il est "en face" des multiples de son diviseur 2.

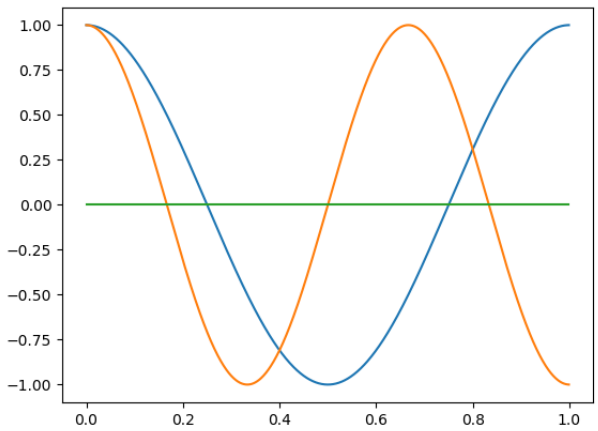
Sur une visualisation utilisant plutôt des courbes de sinus, les points multiples sont amenés sur l'axe des ordonnées.

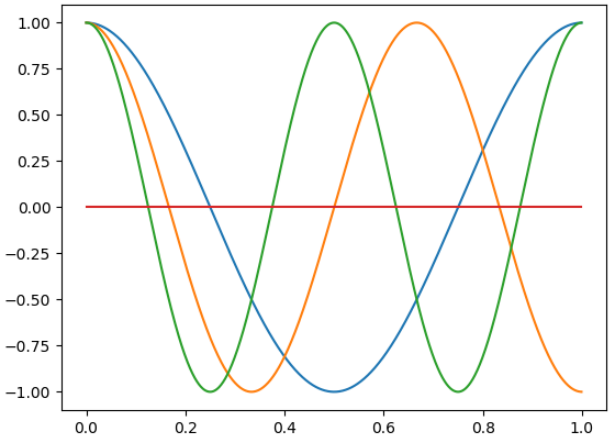


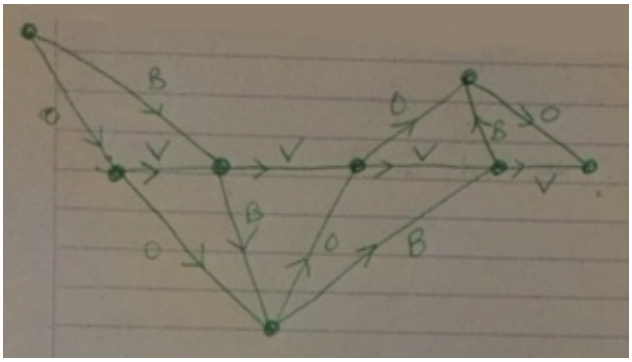
Comment ils passent peut-être des courbes à leurs triangles fléchés (Denise Vella-Chemla, 20.11.2019)

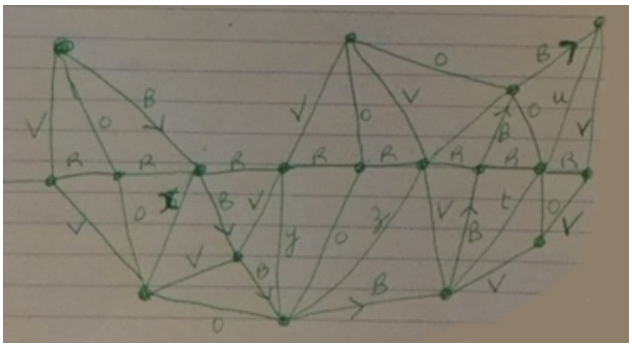
On présente, sur 4 graphiques qui se passent de commentaire, comment on imagine qu'il faut envisager le passage des courbes à des graphes orientés ne contenant que des triangles et dont les arcs sont étiquetés par des +1 et des -1.

On n'imagine pas trop comment voir le fait qu'un nombre en divise un autre là-dessus.









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. Ceci est faux : ce qui était cru à tort et utilisé, c'était "des ensembles disjoints 2 à 2" (ce qui aurait permis d'ajouter tous les cardinaux), alors qu'on peut très bien avoir une intersection globale vide sans avoir disjonction des ensembles 2 à 2.

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

∗. On peut compter les nombres des différents ensembles pour le cas $n = 98$ en annexe 6 pour s'en convaincre.

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.

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).

Il faudrait reprendre tout le raisonnement ci-dessus qui est faux, peut-être en raisonnant sur deux paquets d'ensembles et en établissant la contradiction sur les cardinaux des deux paquets d'ensembles en question, je ne sais pas, ça semble infaisable sans considérer tous les ensembles.

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).

Solution de repli ? ? : Dire que l'intersection des ensembles de la forme $\{\neg 0_{p_k} \wedge \neg n_{p_k}\}$ est vide, ce que l'on note $\bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \varnothing = \bot$ (le symbole $\bot$ est le symbole logique pour *False*), est équivalent à dire que le complémentaire de cet ensemble est le "plein" (dénoté par $\top$, ou *Vrai*), i.e. couvre l'ensemble de tous les impairs de 3 à $n/2$.

$$\complement \bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \bigvee_{p_k}\{0_{p_k} \vee n_{p_k}\} = \top$$

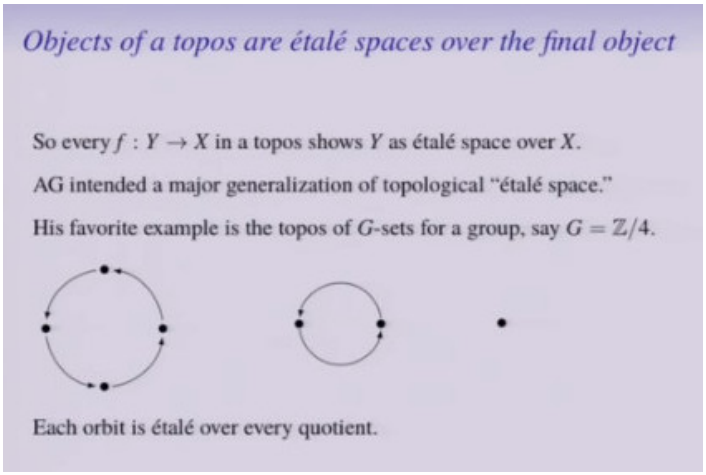
Mais on imagine bien qu'il existe au moins un nombre impair compris entre 3 et $n/2$ qui n'est pas congru à 0, tout en n'étant pas non plus congru à n selon un nombre premier p_k. Ce qui rend notre dernière assertion obligatoirement fausse, et la possibilité que l'intersection soit vide par là même.

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:

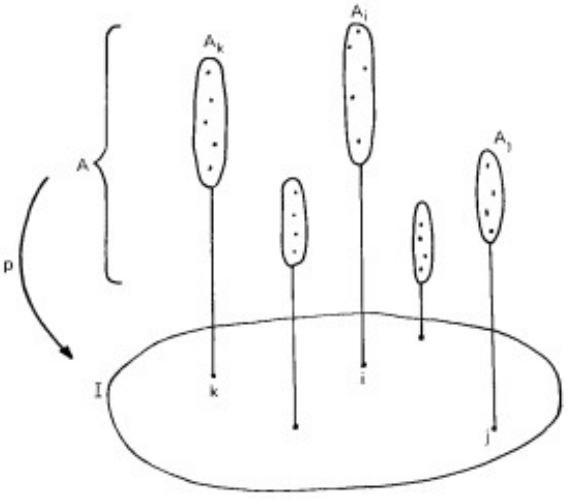


Fig. 4.4.

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 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.

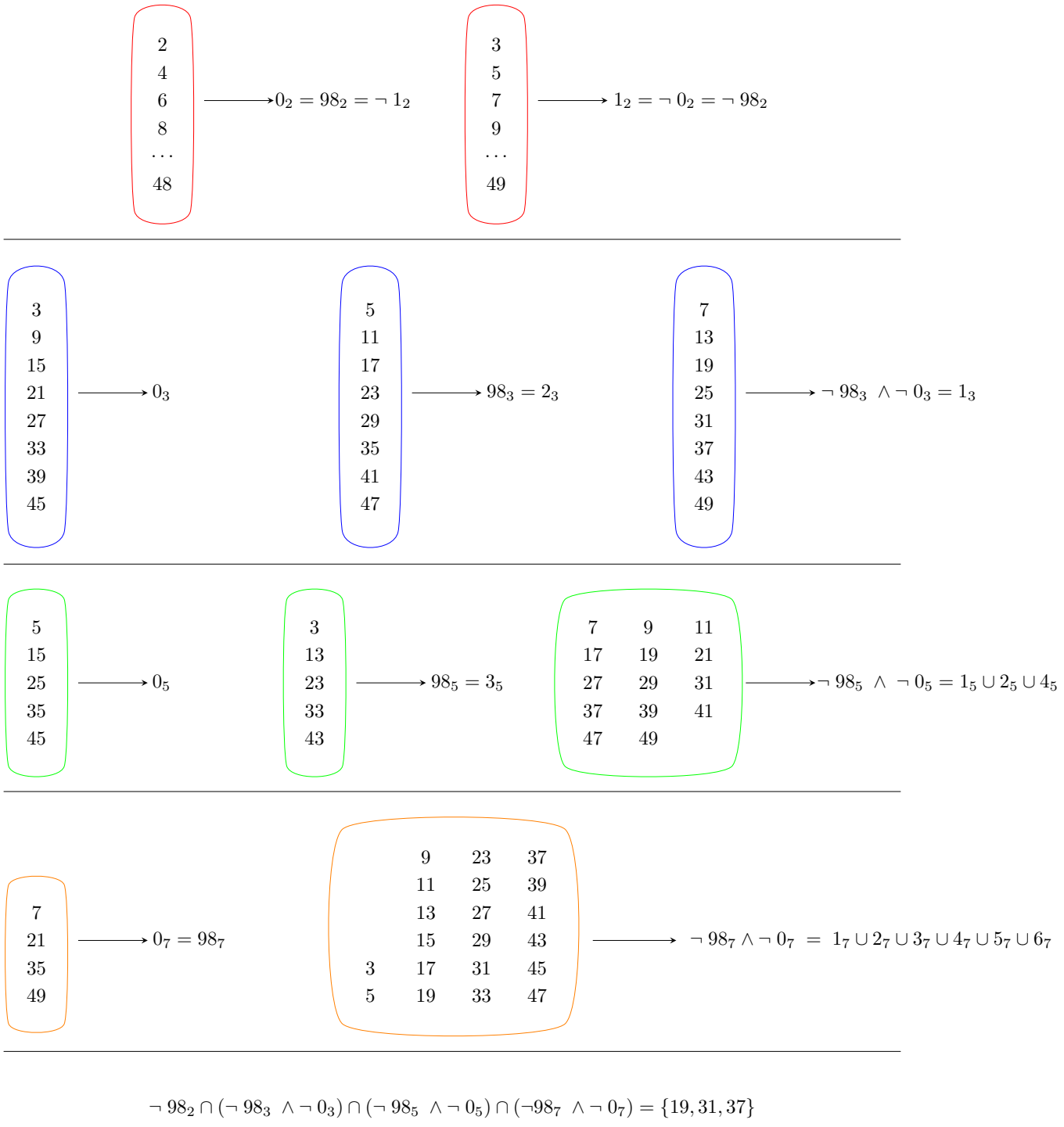
Annexe 5 : Somme des inverses des puissances de 2

$$\sum_{i=1}^{n} \frac{1}{2^i} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^n}$$

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.

Proposition de démonstration de la conjecture de Goldbach dans le formalisme des topos (Denise Vella-Chemla, 25.11.2019)

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 3). La définition première (en mathématique) du mot *fibre*, peut être trouvée dans le cours d'Alexander Grothendieck à Kansas ([1]) ou bien dans un extrait des EGA I (cf. Annexe 2).

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.

Dire que l'intersection des ensembles de la forme $\{\neg 0_{p_k} \wedge \neg n_{p_k}\}$ est vide, ce que l'on note $\bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \varnothing = \bot$ (le symbole $\bot$ est le symbole logique pour *False*), est équivalent à dire que le complémentaire de cet ensemble est le "plein" (dénoté par $\top$, ou *Vrai*), i.e. couvre l'ensemble de tous les impairs de 3 à $n/2$.

$$\complement \bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \bigvee_{p_k}\{0_{p_k} \vee n_{p_k}\} = \top$$

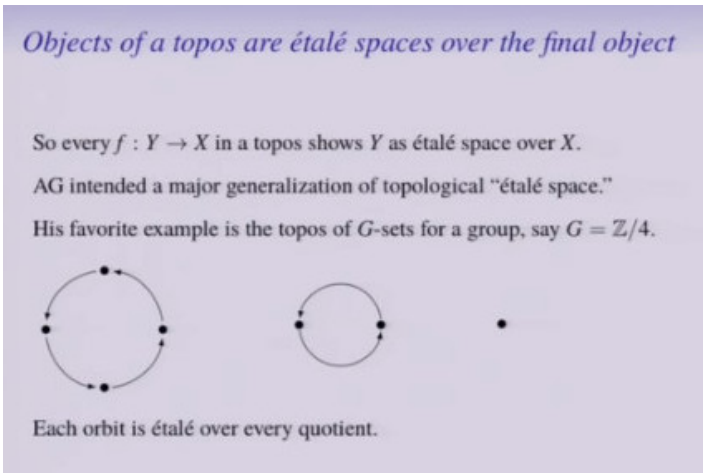
Mais on imagine bien qu'il existe au moins un nombre impair compris entre 3 et $n/2$ qui n'est pas congru à 0, tout en n'étant pas non plus congru à n selon un nombre premier p_k. Ce qui rend notre dernière assertion obligatoirement fausse, et la possibilité que l'intersection soit vide par là même.

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 4 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 : 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 3 : 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:

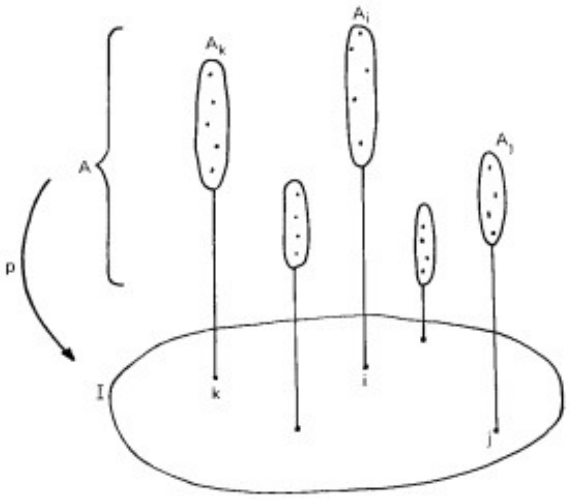


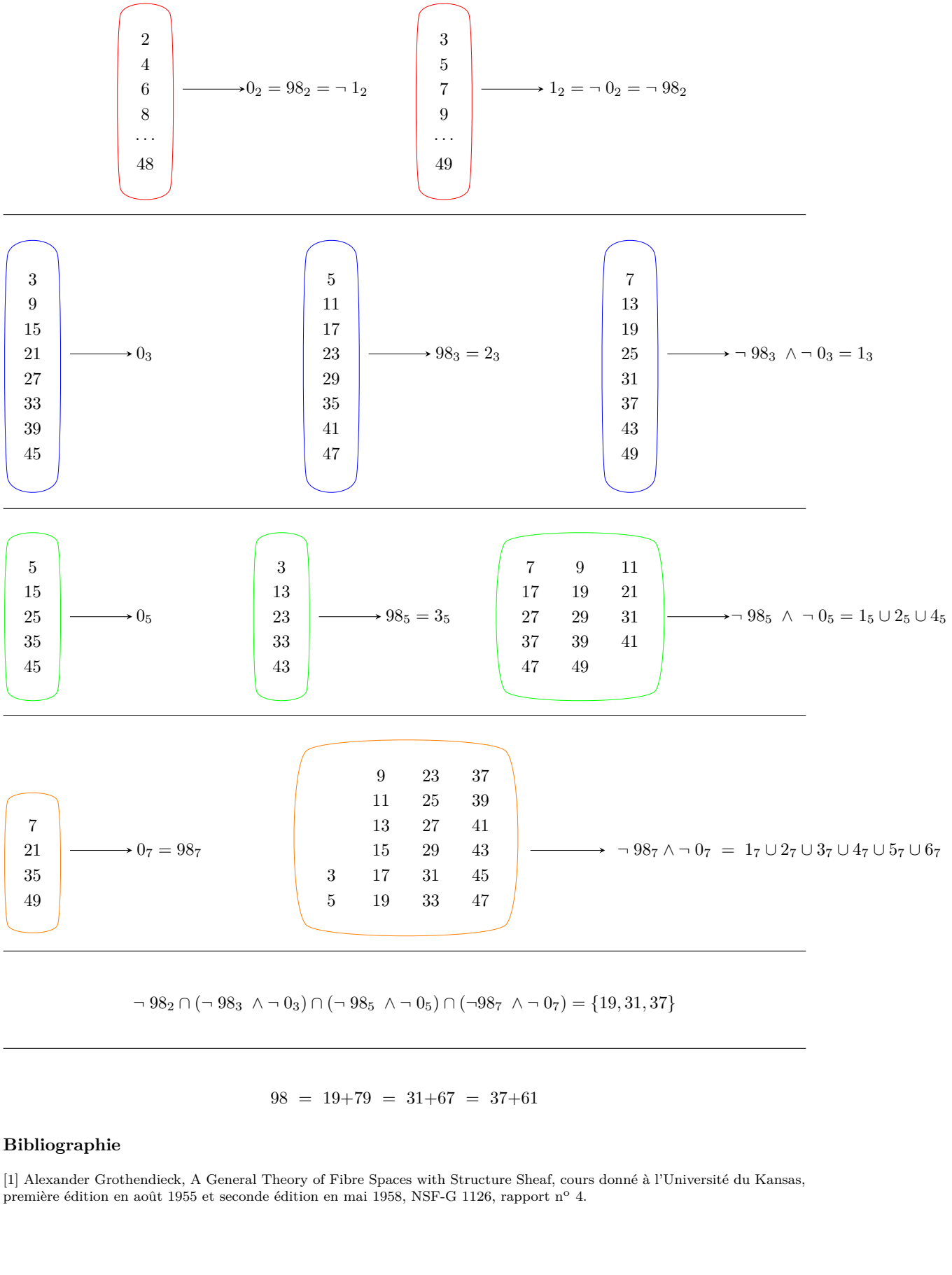
Fig. 4.4.

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 4 : 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, A General Theory of Fibre Spaces with Structure Sheaf, cours donné à l'Université du Kansas, première édition en août 1955 et seconde édition en mai 1958, NSF-G 1126, rapport n° 4.

Bibliographie de Jean-Pierre Serre (articles répertoriés sur la page *Bibliographie* du Collège de France mais sans liens hypertexte fournis dans la page *Textes à télécharger*, fin 2019)

* «Homologie singulière des espaces fibrés. Applications»(Thèse), Paris et Ann. of Math. 54, 1951, 425-505. pdf

* «Groupes d'homotopie et classes de groupes abéliens», Ann. of Math. 58, 1953, 258-294. pdf

* «Cohomologie modulo 2 des complexes d'Eilenberg-Mac Lane», Comm. Math. Helv. 27, 1953, 198-232. pdf

* avec A. Borel, «Groupes de Lie et puissances réduites de Steenrod», Amer. J. Math. 75, 1953, 409-448. pdf

* avec G. P. Hochschild, «Cohomology of group extensions», Trans. AMS, 74, 1953, 110-134. pdf

* «Un théorème de dualité», Comm. Math. Helv. 29, 1955, 9-26. pdf

* «Sur la topologie des variétés algébriques en caractéristique p», Symp. Intern. Top. Alg., Mexico, 1956, 24-53. pdf

* avec A. Borel, «Le théorème de Riemann-Roch, d'après Grothendieck», Bull. SMF 86, 1958, 97-136. pdf

* «Sur les corps locaux à corps résiduel algébriquement clos», Bull. SMF 89, 1961, 105-154. pdf

* avec H. Bass, J. Milnor, «Solution of the congruence subgroup problem for $SL(n)$, $n \geq 3$, and $S_{p_{2n}}$, $n \geq 2$», Publ. Math. IHES, 33, 1967, 59-137. pdf

* Erratum to «Solution of the congruence subgroup problem for $SL(n)$, $n \geq 3$, and $S_{p_{2n}}$, $n \geq 2$», 44, 1975, 241-244. pdf

* Représentations linéaires des groupes finis, Hermann, Paris, 1968. pdf

* «Une interprétation des congruences relatives à la fonction τ de Ramanujan», Séminaire Delange-Pisot-Poitou 4, 1967-1968. pdf

* «Divisibilité de certaines fonctions arithmétiques», L'Ens. Math. 22, 1976, 227-260. pdf

* «Arbres, amalgames, SL_2», Astérisque 46, 1977. pdf

* avec H. Stark, «Modular forms of weight 1/2», Lecture Notes in Math. 627, 1977, 27-67. pdf

* «Groupes algébriques associés aux modules de Hodge-Tate», Astérisque 65, 1979, 155-188. pdf

* «Sur le nombre des points rationnels d'une courbe sur un corps fini», C. R. Acad. Sci. Paris 296, 1983, 397-402. pdf

* «Sur la lacunarité des puissances de η», Glasgow Math. J. 27, 1985, 203-221. pdf

* Topics in Galois Theory, Boston, Jones and Bartlett Publ., 1992. pdf

* avec E. Bayer-Fluckiger, «Torsions quadratiques et bases normales autoduales», Amer. J. Math. 116, 1994, 1-64. pdf

* «La vie et l'œuvre d'André Weil», L'Ens. Math. 45, 1999, 5-16. pdf

* Lectures on $N_X(p)$, New York, AK Peters (Taylor and Francis), 2012, 163 pages. pdf

* Mon premier demi-siècle au Collège de France, La lettre du Collège de France, n° 18, décembre 2006. pdf

Bibliographie de Pierre Cartier

[1] Dualité de Tannaka des groupes et des algèbres de Lie. C. R. Acad. Sci. Paris, 242 (1956), 322-325. pdf

[2] Démonstration algébrique de la formule de Hausdorff. Bull. Soc. Math. France, 84 (1956), 241-249. pdf

[3] Une nouvelle opération sur les formes différentielles. C. R. Acad. Sci. Paris, 244 (1957), 426-428. pdf

[4] Théorie différentielle des groupes algébriques. C. R. Acad. Sci. Paris, 244 (1957), 540-542. pdf

[5] Calcul différentiel sur les variétés algébriques en caractéristique non nulle . C. R. Acad. Sci. Paris, 245 (1957), 1109-1111. pdf

[6] P. Cartier, J. Dixmier, Vecteurs analytiques dans les représentations de groupes de Lie. Amer. J. Math., 80 (1958), 131-145. pdf

[7] Remarques sur le théorème de Birkhoff-Witt. Ann. Scuola Norm. Sup. Pisa (3), 12 (1958), 1-4. pdf

[8] Questions de rationalité des diviseurs en géométrie algébrique. Bull. Soc. Math. France, 86 (1958), 177-251. pdf

[9] Dérivations et diviseurs en géométrie algébrique. Gauthier-Villars, Paris, 1959 (Thèse. Sc. math. Paris. 1958).

[10] Isogénies des variétés de groupes. Bull. Soc. Math. France, 87 (1959), 191-220. pdf

[11] Isogenies and duality of abelian varieties. Ann. Math. (2), 71 (1960), 315-351. pdf

[12] Sur un théorème de Snapper. Bull. Soc. Math. France, 88 (1960), 333-343. pdf

[13] Remarks on "Lie algebra cohomology and the generalized Borel-Weil theorem", by B. Kostant. Ann. of Math. (2), 74 (1961), 388-390.

[14] On H. Weyl's character formula. Bull. Amer. Math. Soc., 67 (1961), 228-230. pdf

[15] Groupes algébriques et groupes formels [Arithmétique des groupes algébriques]. Colloque sur la théorie des groupes algébriques (Bruxelles, 1962), Centre Belge de Recherches Mathématiques, Librairie Universitaire, Louvain ; Gauthier-Villars, Paris, 1962, pp. 87-111. pdf

[16] Sur l'acyclicité du complexe des formes différentielles. Ann. Scuola Norm. Sup. Pisa (3), 16 (1962), 45-74. pdf

[17] Über die Existenz eines Kernes für funktionale Operatoren. Arch. Math., 15 (1964), 50-57. pdf

[18] Über einige Integralformeln in der Theorie der quadratischen Formen. Math. Z., 84 (1964), 93-100. pdf

[19] P. Cartier, J. M. G. Fell, P.-A. Meyer, Comparaison des mesures portées par un ensemble convexe compact. Bull. Soc. Math. France, 92 (1964), 435-445. pdf

[20] Inseparable Galois cohomology. Algebraic Groups and Discontinuous Subgroups (Boulder, Colo., 1965), Proc. Sympos. Pure Math., Vol. IX, Amer. Math. Soc., Providence, R. I., 1966, pp. 183-186.

[21] Quantum mechanical commutation relations and theta functions. Algebraic Groups and Discontinuous Subgroups (Boulder, Colo., 1965), Armand Borel, George D. Mostow, eds., Proc. Sympos. Pure Math., Vol. IX, Amer. Math. Soc., Providence, R. I., 1966, pp. 361-383.

[22] Groupes formels associés aux anneaux de Witt généralisés. C. R. Acad. Sci. Paris, Sér. A-B, 265 (1967), A49-A52. pdf

[23] Modules associés à un groupe formel commutatif. Courbes typiques. C. R. Acad. Sci. Paris, Sér. A-B, 265 (1967), A129-A132.

[24] P. Cartier, P.-A. Meyer, M. Weil, Le retournement du temps : Compléments à l'exposé de M. Weil. Séminaire de Probabilités, II (Univ. Strasbourg, 1967), Springer-Verlag, Berlin, 1968, pp. 22-33. pdf

[25] P. Cartier, D. Foata, Problèmes combinatoires de commutation et réarrangements. Lecture Notes in Mathematics, 85, Springer-Verlag, Berlin-New York, 1969.

[26] Sur certaines variables aléatoires associées au réarrangement croissant d'un échantillon. Séminaire de Probabilités, IV (Univ. Strasbourg, 1968/1969), Lecture Notes in Mathematics, 124, Springer-Verlag, Berlin, 1970, pp. 28-36. pdf

[27] Remarques sur la signature d'une permutation. Enseign. Math. (2), 16 (1970), 7-19. pdf

[28] Quelques remarques sur la divisibilité des coefficients binomiaux. Enseign. Math. (2), 16 (1970), 21-30. pdf

[29] Sur une généralisation des symboles de Legendre-Jacobi. Enseign. Math. (2), 16 (1970), 31-48. pdf

[30] Sur une généralisation du transfert en théorie des groupes. Enseign. Math. (2), 16 (1970), 49-57. pdf

[31] Groupes formels, fonctions automorphes et fonctions zeta des courbes elliptiques. Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 2, Gauthier-Villars, Paris, 1971, pp. 291-299. pdf

[32] Some numerical computations relating to automorphic functions. Computers in Number Theory (Proceedings of the Science Research Council, Atlas Symposium No. 2, Oxford, 1969), A. O. L. Atkin and B. J. Birch, eds., Academic Press, London-New York, 1971, pp. 37-48.

[33] Introduction à l'étude des mouvements browniens à plusieurs paramètres. Séminaire de Probabilités, V (Univ. Strasbourg, 1969/1970), Lecture Notes in Mathematics, 191, Springer-Verlag, Berlin, 1971, pp. 58-75. pdf

[34] On the structure of free Baxter algebras. Advances in Math., 9 (1972), 253-265. pdf

[35] Fonctions harmoniques sur un arbre. Symposia Mathematica, Vol. IX (Convegno di Calcolo delle Probabilità, INDAM, Rome, 1971), Academic Press, London, 1972, pp. 203-270.

[36] R. Azencott, P. Cartier, Martin boundaries of random walks on locally compact groups. Proceedings of the Sixth Berkeley Symposium on Mathematical Statistics and Probability (Univ. California, Berkeley, Calif., 1970/1971), Vol. III : Probability theory, Lucien M. Le Cam, Jerzy Neyman, Elizabeth L. Scott, eds., Univ. California Press, Berkeley, Calif., 1972, pp. 87-129. pdf

[37] Harmonic analysis on trees. Harmonic Analysis on Homogeneous Spaces (Williams Coll., Williamstown, Mass., 1972), Calvin C. Moore, ed., Proc. Sympos. Pure Math., Vol. XXVI, Amer. Math. Soc., Providence, R. I., 1973, pp. 419-424. pdf

[38] P. Cartier, Y. Roy, Certains calculs numériques relatifs à l'interpolation p-adique des séries de Dirichlet. Modular Functions of one Variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Pierre Deligne, Willem Kuyk, eds., Lecture Notes in Mathematics, 350, Springer-Verlag, Berlin, 1973, pp. 269-349. pdf

[39] Introduction à l'étude des mouvements browniens à plusieurs paramètres (en russe). Matematika, Moskva, 18 (1974), 162-175. pdf

[40] P. Cartier, Y. Roy, On the enumeration of quintic fields with small discriminant. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II. J. Reine Angew. Math., 268/269 (1974), 213-215. pdf

[41] Groupes de Lubin-Tate généralisés. Invent. Math., 35 (1976), 273-284. pdf

[42] P. Cartier, J. Tate, A simple proof of the main theorem of elimination theory in algebraic geometry. Enseign. Math. (2), 24 (1978), 311-317. pdf

[43] Analyse numérique d'un problème de valeurs propres à haute precision. Application aux fonctions automorphes. Mathématiques appliquées, 1er Colloq. AFCET-SMF (Palaiseau, 1978), Tome III, (1978), pp. 3-25.

[44] Representations of p-adic groups : a survey. Automorphic Forms, Representations and L-functions (Oregon State Univ., Corvallis, Ore., 1977), Part 1, Armand Borel, W. Casselman, eds., Proc. Sympos. Pure Math., Vol. XXXIII, Amer. Math. Soc., Providence, R. I., 1979, pp. 111-155. pdf

[45] Une étude des covariances mesurables. Mathematical Analysis and Applications, Part A, Essays dedicated to Laurent Schwartz on the occasion of his 65th birthday, Leopoldo Nachbin, ed., Advances in Mathematics, Supplementary Studies, 7a, Academic Press, New York-London, 1981, pp. 267-316. Mathematical analysis and applications. Part B. pdf

[46] Comment l'hypothèse de Riemann ne fut pas prouvée (extraits de deux lettres de P. Cartier à A. Weil, datées du 12 août et du 15 septembre 1979). Seminar on Number Theory (Paris, 1980/1981), Progress in Mathematics, 22, Birkhäuser, Boston, Mass., 1982, pp. 35-48.

[47] Perturbations singulières des équations différentielles ordinaires et analyse non-standard (en russe, traduction, A. K. Zvonkin ; rédaction, M. A. Shubin). Uspekhi Mat. Nauk, 39, No. 2(236) (1984), 57-76. pdf

[48] Analyse non standard : nouvelles méthodes infinitésimales en analyse. Application à la géométrie et aux probabilités. Recherche coopérative sur programme 25 (rencontre entre physiciens théoriciens et mathématiciens), Vol. 35, Publication de l'Institut de recherche mathématique avancée, Strasbourg, 1985, pp. 1-21. Ce texte a aussi paru dans Journées X-U.P.S., Vol. 4, 1983-1984-1985-1986, Centre de Math., école Polytechnique, Palaiseau, 1986, pp. 141-162. pdf

[49] Les gammes musicales et la théorie des groupes. Journées X-U.P.S., Vol. 4, 1983-1984-1985-1986, Centre de Math., école Polytechnique, Palaiseau, 1986, pp. 1-3.

[50] Classification des systèmes quasi cristallins de type icosaédrique. C. R. Acad. Sci. Paris, Sér. II, 304 (1987), 789-792.

[51] P. Cartier, A. Voros, Une nouvelle interprétation de la formule des traces de Selberg. C. R. Acad. Sci. Paris, Sér. I, 307 (1988), 143-148. pdf

[52] P. Cartier, A. Voros, Nouvelle interprétation de la formule des traces de Selberg. Journées "équations aux Dérivées Partielles" (Saint-Jean-de-Monts, 1988), Exp. No. XIII, 8 pp., école Polytechnique, Palaiseau, 1988. pdf

[53] P. Cartier, Y. Feneyrol-Perrin, Comparaison des diverses théories d'intégration en analyse non standard. C. R. Acad. Sci. Paris, Sér. I, 307 (1988), 297-301. pdf

[54] A course on determinants. Conformal Invariance and String Theory (Poiana Braçsov, 1987), Petre Dita and Vladimir Georgescu, eds., Perspect. Phys., Academic Press, Boston, Mass., 1989, pp. 443-557. pdf

[55] Was sind und was sollen die Zahlen ? (Version 84) [en français]. La mathématique non standard : Histoire, philosophie, dossier scientifique, sous la direction de Hervé Barreau et Jacques Harthong, préface de Georges Reeb, Fondements des Sciences, éditions du CNRS, Paris, 1989, pp. 331-353.

[56] La pratique - et les pratiques - des mathématiques. L'Univers philosophique, volume dirigé par André Jacob, Encyclopédie philosophique universelle, Presses Univ. France, Paris, 1989, pp. 1063-1069.

[57] P. Cartier, A. Voros, Une nouvelle interprétation de la formule des traces de Selberg. The Grothendieck Festschrift, Vol. II, Progress in Mathematics, 87, Birkhäuser, Boston, Mass., 1990, pp. 1-67.

[58] Sur le développement des mathématiques de 1870 à 1970 : quelques exemples d'interaction avec la physique. Un siècle de rapports entre la physique et les mathématiques (1870-1970) (Paris, 1988), Revue du Palais de la Découverte, numéro spécial, 40 (1991), 19-29.

[59] An introduction to zeta functions. From Number Theory to Physics (Les Houches, 1989), Michel Waldschmidt, Pierre Moussa, Jean-Marc Luck, Claude Itzykson, eds., Springer-Verlag, Berlin, 1992, pp. 1-63.

[60] Nouvelles aventures au pays des q-analogues (équation de Yang-Baxter). Séminaire Lotharingien de Combinatoire (Rouge-Gazon, 1990), Publ. Inst. Rech. Math. Av., 460, Univ. Louis Pasteur, Strasbourg, 1992, pp. 5-37. Version électronique dans Sém. Lothar. Combin., 23 (1990), B23A, 28 pp. pdf

[61] Construction combinatoire des invariants de Vassiliev-Kontsevich des noeuds. C. R. Acad. Sci. Paris, Sér. I, 316 (1993), 1205-1210. pdf

[62] Construction combinatoire des invariants de Vassiliev-Kontsevich des noeuds. Recherche coopérative sur programme 25 (rencontre entre physiciens théoriciens et mathématiciens), Vol. 45 (Strasbourg, 1992/1993), Inst. Rech. Math. Av., 1993/42, Univ. Louis Pasteur, Strasbourg, 1993, pp. 1-10. pdf

[63] P. Cartier, C. DeWitt-Morette, Intégration fonctionnelle ; éléments d'axiomatique. C. R. Acad. Sci. Paris, Sér. II, 316 (1993), 733-738. pdf

[64] P. Cartier, C. DeWitt-Morette, Status report on an axiomatic basis for functional integration. Directions in General Relativity, Bei-Lok Hu, Ted Jacobson, eds., Cambridge University Press, Cambridge, 1993, pp. 78-82.

[65] Des nombres premiers à la géométrie algébrique (une brève histoire de la fonction zéta). Analyse diophantienne et géométrie algébrique, Cahiers Sém. Hist. Math., Sér. 2, 3, Univ. Paris VI, Paris, 1993, 51-77. pdf

[66] An introduction to quantum groups. Algebraic Groups and their Generalizations : Quantum and Infinite-Dimensional Methods (University Park, Pa., 1991), William J. Haboush, Brian J. Parshall, eds., Proc. Sympos. Pure Math., Vol. LVI, Part 2, Amer. Math. Soc., Providence, R. I., 1994, pp. 19-42.

[67] Some fundamental techniques in the theory of integrable systems. Lectures on Integrable Systems (Sophia-Antipolis, 1991), Olivier Babelon, Pierre Cartier, Yvette Kosmann-Schwarzbach, eds., World Sci. Publishing, River Edge, N. J., 1994, pp. 1-41.

[68] P. Cartier, C. DeWitt-Morette, A new perspective on functional integration. J. Math. Phys., 36 (1995), 2237-2312. pdf

[69] P. Cartier, Y. Perrin, Integration over finite sets. Nonstandard Analysis in Practice, Francine Diener, Marc Diener, eds., Universitext, Springer-Verlag, Berlin, 1995, pp. 185-204.

[70] Art, science et transformation. Mathématiques et art (Colloque organisé par le Séminaire Philosophie et Mathématiques, Cerisy, 1991), sous la direction de Maurice Loi, Hermann, Paris, 1995, pp. 39-46.

[71] Kepler et la musique du monde, La Recherche, 278, Vol. 26 (1995), 750-755.

[72] P. Cartier, C. DeWitt-Morette, A new perspective on functional integration. Poisson processes in probability and quantum physics. Path Integrals (Dubna, 1996), V. S. Yarunin, M. A. Smondyrev, eds., Joint Inst. Nuclear Res., Dubna, 1996, pp. 13-21.

[73] C. DeWitt-Morette, P. Cartier, A rigorous mathematical foundation of functional integration. With an appendix by D. Collins. Functional Integration : Basics and Applications (Cargèse, 1996), Cécile DeWitt-Morette, Pierre Cartier, Antoine Folacci, eds., NATO Adv. Sci. Inst., Ser. B, 361, Plenum, New York, 1997, pp. 1-50.

[74] P. Cartier, C. DeWitt-Morette, Physics on and near caustics. Functional Integration : Basics and Applications (Cargèse, 1996), Cécile DeWitt-Morette, Pierre Cartier, Antoine Folacci, eds., NATO Adv. Sci. Inst. Ser. B, 361, Plenum, New York, 1997, pp. 51-66.

[75] Développements récents sur les groupes de tresses. Applications à la topologie et à l'algèbre. Functional Integration : Basics and Applications (Cargèse, 1996), Cécile DeWitt-Morette, Pierre Cartier, Antoine Folacci, eds., NATO Adv. Sci. Inst. Ser. B, 361, Plenum, New York, 1997, pp. 213-246. pdf

[76] M. Senechal, The continuing silence of Bourbaki–an interview with Pierre Cartier, June 18, 1997. Math. Intelligencer, 20 (1998), No. 1, 22-28. pdf

[77] La folle journée, de Grothendieck à Connes et Kontsevich : évolution des notions d'espace et de symétrie. Les relations entre les mathématiques et la physique théorique, Festschrift for the 40th anniversary of the IHES, Inst. Hautes études Sci., Bures-sur-Yvette, 1998, pp. 23-42. pdf

[78] P. Cartier, C. DeWitt-Morette, Geometry and functional integration. Quantization, coherent states, and Poisson structures (Bialowieza, 1995), A. Strasburger et al., eds., PWN, Warsaw, 1998, pp. 187-192.

[78-bis] P. Cartier, C. DeWitt-Morette, Physics on and near caustics–a simpler version. Mathematical Methods of Quantum Physics (Jagna, 1998), Christopher C. Bernido et al., eds., Gordon and Breach, Amsterdam, 1999, pp. 131-143.

[79] Bourbaki et Structures. Dictionnaire d'histoire et de philosophie des sciences, publié sous la direction de Dominique Lecourt, Presses Universitaires de France, Paris, 1999, pp. 128-129 et 883-892 ; réédition, collection Quadrige-Dicos Poche, 2003.

[81] André Weil (1906-1998) : Adieu à un ami. Gazette des Sciences Mathématiques du Québec, 20, No. 1 (1999), 3-26. pdf

[82] André Weil (1906-1998) : Adieu à un ami. Gazette des Mathématiciens, 80, suppl. (1999), 13-35 [texte abrégé de 81].

[83] Abschied von einem Freund : André Weil (1906-1998). Mitt. Dtsch. Math.-Ver. (1999), No. 3, 7-12 [traduction allemande de 81]. pdf

[84] A. Borel, P. Cartier, K. Chandrasekharan, S. S. Chern, S. Iyanaga, A. Weil (1906-1998). Notices Amer. Math. Soc., 46 (1999), No. 4, 440-447 [traduction anglaise d'un extrait de 81]. pdf

[85] Il mio André Weil. Lett. Mat. Pristem, 36 (2000), 43-58 [traduction italienne de 81].

[86] Mathemagics (a tribute to L. Euler and R. Feynman). Noise, Oscillators and Algebraic Randomness (Chapelle-des-Bois, 1999), Michel Planat, ed., Lecture Notes in Phys., 550, Springer-Verlag, Berlin, 2000, pp. 6-67. Version électronique révisée dans Sém. Lothar. Combin., 44 (2000), B44d, 71 pp. pdf

[87] P. Cartier, C. DeWitt-Morette, Brydges' operator in renormalization theory. Mathematical Physics and Stochastic Analysis (Lisbon, 1998), S. Albeverio et al., eds., World Sci. Publishing, River Edge, N. J., 2000, pp. 165-168.

[88] P. Cartier, C. DeWitt-Morette, Functional integration. J. Math. Phys. 41 (2000), 4154-4187.

[89] L'intégrale des chemins de Feynman : d'une vue intuitive à un cadre rigoureux. Jean-Pierre Kahane, Vladimir Arnold, Pierre Cartier et al., Leçons de Mathématiques d'aujourd'hui, Douze conférences présentées par éric Charpentier et Nicolas Nikolski, Cassini, Paris, 2000, pp. 27-59.

[90] P. Cartier, K. Chemla, La création des noms mathématiques : l'exemple de Bourbaki. La Dénomination, Le Temps des savoirs, n° 1, avril 2000, éditions Odile Jacob, pp. 153-170.

[91] Mathématique et réalité. Texte de la 14ème conférence de l'Université de tous les savoirs, donnée le 14 janvier 2000. Qu'est ce que la vie ? Vol. 1, Université de tous les savoirs, éditions Odile Jacob, Paris, 2000, pp. 179-192.

[92] MatemEtica e Realidade. III SimpOsio-Pedagogia na Universidade (2001), R. Bruno de Sousa et al., orgs., Reitoria da Universidade Técnica de Lisboa, 2002, pp. 119-130 [traduction portugaise de 91].

[93] P. Cartier, M. Berg, C. DeWitt-Morette, A. Wurm, Characterizing volume forms. Fluctuating Paths and Fields, Axel Pelster, ed., World Sci. Publishing, River Edge, N. J., 2001, pp. 139-156.

[94] A mad day's work : from Grothendieck to Connes and Kontsevich. The evolution of concepts of space and symmetry (traduit du français [77] par Roger Cooke). Bull. Amer. Math. Soc. (N.S.), 38 (2001), 389-408. pdf

[95] Préface. La Science des noeuds. Pour la Science, Belin, Paris, 2001.

[96] P. Cartier, C. DeWitt-Morette, M. Ihl, C. Sämann, Supermanifolds–application to supersymmetry. With an appendix by Maria E. Bell. Multiple Facets of Quantization and Supersymmetry, Mikhail Olshanetsky and Arkady Vainshtein, eds., World Sci. Publishing, River Edge, N. J., 2002, pp. 412-457. pdf

[97] Le défi post-hilbertien, préface du livre de Jeremy Gray, Le défi de Hilbert, un siècle de mathématiques, traduit de l'anglais par Christos Grammatikas, Dunod, Paris, 2003.

[98] P. Cartier, C. DeWitt-Morette, Functional integration in quantum field theory. Festschrift for J. Devresse.

[99] P. Cartier, C. DeWitt-Morette, Functional Integration. Action and symmetries. Cambridge University Press, 2004.

[100] M. Berg, P. Cartier, Representations of the renormalization group as matrix Lie algebra. hep-th/0105315. pdf

[101] Armand Borel, mathématicien (1923-2003). Universalia, Paris, 2004.

[102] L'oeuvre mathématique de Bourbaki. Tangente, 96 (2004), 12-14.

[103] La dénomination des nombres, Science et Avenir (2004).

Séminaire Bourbaki

[104] Représentations des groupes de Lie (d'après Harish-Chandra). Séminaire Bourbaki, Vol. 2, Exp. No. 96, 415-424, Soc. Math. France, Paris, 1995. pdf

[105] Développements de fonctions arbitraires suivant les fonctions propres d'un opérateur différentiel. Séminaire Bourbaki, Vol. 3, Exp. No. 102, 13-22, Soc. Math. France, Paris, 1995. pdf

[106] Effacement dans la cohomologie des algèbres de Lie. Séminaire Bourbaki, Vol. 3, Exp. No. 116, 161-167, Soc. Math. France, Paris, 1995. pdf

[107] Dualité des variétés abéliennes. Séminaire Bourbaki, Vol. 4, Exp. No. 164, 379-391, Soc. Math. France, Paris, 1995. pdf

[108] Vecteurs analytiques (d'après E. Nelson). Séminaire Bourbaki, Vol. 5, Exp. No. 181, 181-192, Soc. Math. France, Paris, 1995. pdf

[109] Structures simpliciales. Séminaire Bourbaki, Vol. 5, Exp. No. 199, 429-440, Soc. Math. France, Paris, 1995. pdf

[110] Classes de formes bilinéaires sur les espaces de Banach. Séminaire Bourbaki, Vol. 6, Exp. No. 211, 85-98, Soc. Math. France, Paris, 1995. pdf

[111] Analyse spectrale et théorème de prédiction statistique de Wiener. Séminaire Bourbaki, Vol. 6, Exp. No. 218, 197-218, Soc. Math. France, Paris, 1995. pdf

[112] Fluctuations dans les suites de variables aléatoires indépendantes. Séminaire Bourbaki, Vol. 8, Exp. No. 241, 7-24, Soc. Math. France, Paris, 1995. pdf

[113] Représentations linéaires des groupes algébriques semi-simples en caractéristique non nulle. Séminaire Bourbaki, Vol. 8, Exp. No. 255, 179-188, Soc. Math. France, Paris, 1995. pdf

[114] Processus aléatoires généralisés. Séminaire Bourbaki, Vol. 8, Exp. No. 272, 425-434, Soc. Math. France, Paris, 1995. pdf

[115] Equivalence linéaire des idéaux de polynômes. Séminaire Bourbaki, Vol. 9, Exp. No. 283, 93-103, Soc. Math. France, Paris, 1995. pdf

[116] Diviseurs amples. Séminaire Bourbaki, Vol. 9, Exp. No. 301, 351-366, Soc. Math. France, Paris, 1995. pdf

[117] Théorie analytique des formes quadratiques. I. Suites quasi-périodiques. Séminaire Bourbaki, Vol. 9, Exp. No. 309, 479-490, Soc. Math. France, Paris, 1995. pdf

[118] Théorie des groupes, fonctions théta et modules des variétés abéliennes. Séminaire Bourbaki, Vol. 10, Exp. No. 338, 417-432, Soc. Math. France, Paris, 1995. pdf

[119] Relèvements des groupes formels commutatifs. Séminaire Bourbaki, 21ème année (1968/1969), Exp. No. 359, Lecture Notes in Mathematics, 179, Springer-Verlag, Berlin, 1971, pp. 217-230. pdf

[120] Espaces de Poisson des groupes localement compacts (d'après R. Azencott). Séminaire Bourbaki, 22ème année (1969/1970), Exp. No. 370, Lecture Notes in Mathematics, 180, Springer-Verlag, Berlin, 1971, pp. 107-127. pdf

[121] Problèmes mathématiques de la théorie quantique des champs. Séminaire Bourbaki, 23ème année (1970/1971), Exp. No. 388, Lecture Notes in Mathematics, 244, Springer-Verlag, Berlin, 1971, pp. 107-122. pdf

[122] Géométrie et analyse sur les arbres. Séminaire Bourbaki, 24ème année (1971/1972), Exp. No. 407, Lecture Notes in Mathematics, 317, Springer-Verlag, Berlin, 1973, pp. 123-140. pdf

[123] Problèmes mathématiques de la théorie quantique des champs. II. Prolongement analytique. Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 418, Lecture Notes in Math., 383, Springer-Verlag, Berlin, 1974, pp. 1-33. pdf

[124] Inégalités de corrélation en mécanique statistique. Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 431, Lecture Notes in Math., 383, Springer-Verlag, Berlin, 1974, pp. 242-264. pdf

[125] Vecteurs différentiables dans les représentations unitaires des groupes de Lie. Séminaire Bourbaki, 27ème année (1974/1975), Exp. No. 454, Lecture Notes in Math., 514, Springer-Verlag, Berlin, 1976, pp. 20-34. pdf

[126] Les représentations des groupes réductifs p-adiques et leurs caractères. Séminaire Bourbaki, 28ème année (1975/1976), Exp. No. 471, Lecture Notes in Mathematics, 567, Springer-Verlag, Berlin, 1977, pp. 1-22. pdf

[127] Spectre de l'équation de Schrödinger, application à la stabilité de la matière (d'après J. Lebowitz, E. Lieb, B. Simon et W. Thirring). Séminaire Bourbaki, 29ème année (1976/1977), Exp. No. 496, Lecture Notes in Mathematics, 677, Springer-Verlag, Berlin, 1978, pp. 88-104. pdf

[128] Logique, catégories et faisceaux (d'après F. Lawvere et M. Tierney). Séminaire Bourbaki, 30ème année (1977/1978), Exp. No. 513, Lecture Notes in Mathematics, 710, Springer-Verlag, Berlin, 1979, pp. 123-146. pdf

[129] Théorie de la diffusion pour l'équation de Schrödinger. Séminaire Bourbaki (1978/1979), Exp. No. 533, Lecture Notes in Mathematics, 770, Springer-Verlag, Berlin, 1980, pp. 132-150. pdf

[130] La conjecture locale de Langlands pour GL (2) et la démonstration de Ph. Kutzko. Séminaire Bourbaki (1979/1980), Exp. No. 550, Lecture Notes in Mathematics, 842, Springer-Verlag, Berlin-New York, 1981, pp. 112-138. pdf

[131] Les arrangements d'hyperplans : un chapitre de géométrie combinatoire. Séminaire Bourbaki (1980/1981), Exp. No. 561, Lecture Notes in Mathematics, 901, Springer-Verlag, Berlin-New York, 1981, pp. 1-22. pdf

[132] Perturbations singulières des équations différentielles ordinaires et analyse non-standard. Séminaire Bourbaki, Exp. No. 580, Vol. 1981/1982, Astérisque, 92-93, Soc. Math. France, Paris, 1982, pp. 21-44. pdf

[133] La théorie classique et moderne des fonctions symétriques. Séminaire Bourbaki, Exp. No. 597, Vol. 1982/1983, Astérisque, 105-106, Soc. Math. France, Paris 1983, pp. 1-23. pdf

[134] Homologie cyclique : rapport sur des travaux récents de Connes, Karoubi, Loday, Quillen,... Séminaire Bourbaki, Exp. No. 621, Vol. 1983/1984. Astérisque, 121-122 (1985), 123-146. pdf

[135] Décomposition des polyèdres : le point sur le troisième problème de Hilbert. Séminaire Bourbaki, Exp. No. 646, Vol. 1984/1985. Astérisque, 133-134 (1986), 261-288. pdf

[136] Détermination des caractères des groupes finis simples : travaux de Lusztig. Séminaire Bourbaki, Exp. No. 658, Vol. 1985/1986. Astérisque, 145-146 (1987), 137-161. pdf

[137] Jacobiennes généralisées, monodromie unipotente et intégrales itérées. Séminaire Bourbaki, Exp. No. 687, Vol. 1987/1988, Astérisque, 161-162 (1988), 31-52. pdf

[138] Développements récents sur les groupes de tresses. Applications à la topologie et à l'algèbre. Séminaire Bourbaki, Exp. No. 716, Vol. 1989/1990, Astérisque, 189-190 (1990), 17-67. pdf

[139] Démonstration "automatique" d'identités et fonctions hyper-géométriques (d'après D. Zeilberger). Séminaire Bourbaki,Exp. No. 746, Vol. 1991/1992, Astérisque, 206 (1992), 41-91. pdf

[140] La théorie des blocs et les groupes génériques. Séminaire Bourbaki, Exp. No. 781, Vol. 1993/1994, Astérisque, 227 (1995), 171-208. pdf

[141] Fonctions polylogarithmes, nombres polyzêtas et groupes pro-unipotents. Séminaire Bourbaki, Exp. No. 885, Vol. 2000/2001. Astérisque, 282 (2002), 137-173. pdf

Les exposés du Séminaire Bourbaki ont été aussi publiés de 1952 à 1968 par W. A. Benjamin, New York, Amsterdam.

Autres séminaires

Séminaire Sophus Lie

[142] Le théorème de Poincaré-Birkhoff-Witt, Exp. 1, 10 pp., Séminaire Sophus Lie, 1ère année (1954/1955). Théorie des algèbres de Lie. Topologie des groupes de Lie. M. Berger, A. Blanchard, F. Bruhat, P. Cartier, M. Lazard, J.-P. Serre, Secrétariat mathématique, Paris, 1955. pdf

[143] Algèbres de Lie nilpotentes, Exp. 2, 6 pp., ibid.

[144] Cohomologie des algèbres de Lie, I, Exp. 3, 7 pp., ibid. pdf

[145] Cohomologie des algèbres de Lie, II. Interprétation des groupesde cohomologie, Exp. 4, 11 pp., ibid. pdf

[146] Cohomologie des algèbres de Lie, III, Exp. 5, 7 pp., ibid. pdf

[147] Compléments sur la cohomologie, Exp. 5bis, 10 pp., ibid. pdf

[148] Théorie des algèbres semi-simples, Exp. 7, 9 pp., ibid. pdf

[149] Radicaux des algèbres de Lie, Exp. 7bis, 15 pp., ibid. pdf

[150] Théorèmes d'Ado et d'Iwasawa, Exp. 8, 5 pp., ibid. pdf

[151] M. Berger, P. Cartier, Classification des algèbres de Lie simples, Exp. 13, 8 pp., ibid. pdf

[152] Théorème de conjugaison des algèbres de Cartan, Exp. 15, 5 pp., ibid. pdf

[153] Représentations linéaires des algèbres de Lie semi-simples, Exp. 17, 7 pp., ibid. pdf

[154] Théorie des caractères, I. Définition des caractères, Exp. 18, 8 pp., ibid. pdf

[155] Théorie des caractères, II. Détermination des caractères, Exp. 19 et 20, 12 pp., ibid. pdf

[156] Théorie des caractères, III. Caractères des groupes compacts, Exp. 21, 9 pp., ibid.

[157] Structure topologique des groupes de Lie, Exp. 22, 20 pp., ibid. pdf

[158] Traduction russe : Teoria algebr Li et Topologia grupp Li. Traduction, E.B. Vinberg ; rédaction, E.B. Dynkin, Izdatelstvo Inostrannoi Literaturi, Moscou, 1962.

[159] Hyperalgèbres des variétés de groupes, Exp. 1, 11 pp., Séminaire Sophus Lie, 2ème année (1955/1956). Hyperalgèbres et groupes de Lie formels. Secrétariat mathématique, Paris, 1957. pdf

[160] Hyperalgèbres et groupes formels, Exp. 2, 6 pp., ibid. pdf

[161] Exemples d'hyperalgèbres, Exp. 3, 15 pp., ibid. pdf

[162] Modules sur une coalgèbre, Exp. 4, 7 pp., ibid. pdf

Séminaire Grothendieck

[163] Les groupes $Ext^s(A, B)$, Séminaire A. Grothendieck, 1e année (1957). Algèbre homologique. Secrétariat mathématique, Paris, 1958, 19 pp. pdf

Séminaire Chevalley

[164] Définition des variétés algébriques, Exp. 1, 13 pp., Séminaire C. Chevalley, 1956-1958. Classification des groupes de Lie algébriques, Vol. 1, Secrétariat mathématique, Paris, 1958, 13 pp. ; réédition 192] pdf

[165] Schémas des variétés algébriques, Exp. 2, 24 pp., ibid ; réédition [192] pdf

[166] Groupes finis engendrés par des symétries, Exp. 14, 12 pp., Séminaire C. Chevalley, 1956-1958. Classification des groupes de Lie algébriques, Vol. 2, Secrétariat mathématique, Paris, 1958, 12 pp. ; réédition [192] pdf

Séminaire Cartan-Chevalley

[167] Dérivations dans les corps, Exp. 13, 13 pp., Séminaire H. Cartan et C. Chevalley, 8e année (1955/1956). Géométrie algébrique, Secrétariat mathématique, Paris, 1956. pdf

[168] Extensions régulières, Exp. 14, 10 pp., ibid. pdf

[169] P. Cartier, C. Chevalley, Extensions du corps de base dans les schémas, Exp. 15, 12 pp., ibid. pdf

Prépublications de l'IHES n'ayant pas fait l'objet d'une publication

[170] [1972] Groupes formels. Cours à l'IHéS (1972), notes de J. Boutot.

[171] [1974] Représentations des groupes localement compacts [non publié].

[172] [1975] Séminaire de théorie des groupes (1972-1973) : représentation de Weil de certains groupes linéaires sur un corps fini (première partie). Cours à l'IHéS (1975), notes de J. Soto-Andrade et A. Pazzoto.

[173] [1979] IHES/M/79/305 Sur les zéros de la fonction Zeta de Selberg [non publié].

[174] [1980] IHES/M/80/08 Fonctions L d'Artin : théorie locale. Cours à l'IHES (1980), notes de G. Henniart.

[175] [1991] IHES/M/91/12 Review of "Concrete Mathematics" (a book by Knuth et al.) [non publié].

[176] [1991] IHES/M/91/27 La Musique des sphères de Kepler ou La Recherche de l'harmonie chez Kepler [voir [71] ; voir aussi Philosophie et Mathématiques, 71, I.R.E.M., Université Paris-Nord, 1991].

[177] [1993] IHES/M/93/33 Les Mathématiques et l'art. 1er Colloque de Cerisy, 1993 [non publié].

[178] [1993] IHES/M/93/35 Des nombres premiers à la géométrie algébrique [voir [65]].

[179] [1997] IHES/M/97/62 Notes sur l'histoire et la philosophie des mathématiques I. Vie et mort de Bourbaki [voir [76]].

[180] [1998] IHES/M/98/20 P. Cartier, K. Chemla, Notes sur l'histoire et la philosophie des mathématiques II. La création des noms mathématiques : l'exemple de Bourbaki [voir [90]].

[181] IHES/M/98/28 P. Cartier (avec des contributions de F. Patras et A. Borel) Notes sur l'histoire et la philosophie des mathématiques III. Le structuralisme en mathématiques : mythe ou réalité ? [voir [80]].

[182] IHES/P/99/51, P. Cartier, C. DeWitt-Morette, Scaling and functional integration et Brydges' operator in renormalization theory [version abrégée du deuxième article parue dans [87]].

[183] [2000] IHES/M/00/75 Notes sur l'histoire et la philosophie des mathématiques IV. Grothendieck et les motifs. Colloque de Cerisy, 1999 [non publié].

Livres édités

[184] Séminaire de Probabilités, VI. Université de Strasbourg, année universitaire 1970/1971, contenant aussi les conférences des Journées Probabilistes de Strasbourg (31 mars-3 avril 1971), organisées par P. Cartier et C. Dellacherie. Lecture Notes in Mathematics, 258, Springer-Verlag, Berlin-New York, 1972.

[185] The Grothendieck Festschrift. Vol. I. A collection of articles written in honor of the 60th birthday of Alexander Grothendieck. Edited by P. Cartier, L. Illusie, N. M. Katz, G. Laumon, Yu. Manin and K. A. Ribet. Progress in Mathematics, 86, Birkhäuser, Boston, Mass., 1989.

[186] The Grothendieck Festschrift. Vol. II. A collection of articles written in honor of the 60th birthday of Alexander Grothendieck. Edited by P. Cartier, L. Illusie, N. M. Katz, G. Laumon, Y. Manin and K. A. Ribet. Progress in Mathematics, 87, Birkhäuser, Boston, Mass., 1990.

[187] The Grothendieck Festschrift. Vol. III. A collection of articles written in honor of the 60th birthday of Alexander Grothendieck. Edited by P. Cartier, L. Illusie, N. M. Katz, G. Laumon, Y. Manin and K. A. Ribet. Progress in Mathematics, 88, Birkhäuser,Boston, Mass., 1990.

[188] Integrable systems. The Verdier Memorial Conference. Proceedings of the International Conference held in Luminy, July 1-5, 1991. Edited by Olivier Babelon, Pierre Cartier and Yvette Kosmann-Schwarzbach. Progress in Mathematics, 115, Birkhäuser. Boston, Mass., 1993.

[189] Lectures on integrable systems. In memory of Jean-Louis Verdier. Proceedings of the CIMPA School on Integrable Systems held in Sophia-Antipolis, June 10-28, 1991. Edited by Olivier Babelon, Pierre Cartier and Yvette Kosmann-Schwarzbach. World Scientific Publishing Co., Inc., River Edge, N. J., 1994.

[190] Functional integration. Basics and applications. Papers from the NATO Advanced Study Institute held in Cargèse, September 1-14, 1996. Edited by Cecile DeWitt-Morette, Pierre Cartier and Antoine Folacci. NATO Advanced Science Institutes Series B : Physics, 361. Plenum Press, New York, 1997.

[191] C. Chevalley, The algebraic theory of spinors and Clifford algebras. Collected works. Vol. 2. Edited and with a foreword by Pierre Cartier and Catherine Chevalley. With a postface by J.-P. Bourguignon. Springer-Verlag, Berlin, 1997.

[192] C. Chevalley, Classification des groupes algébriques semi-simples. Avec la collaboration de Pierre Cartier, Alexandre Grothendieck et Michel Lazard. Texte révisé en 2003 par Pierre Cartier, Springer-Verlag, Berlin, 2004 [contient les textes de 1958, [164] - [166], révisés].

[193] Psychanalyse et Mathématiques. (Colloque de Cerisy, 1999). Pierre Cartier et Nathalie Charraud, éds., éditions de la cause freudienne.

[194] Frontiers in Number Theory, Physics and Geometry. Pierre Moussa, Bernard L. Julia, Pierre Vanhove, Pierre Cartier, éds., 2 vol., Springer-Verlag, Berlin.

Cours et ouvrages polycopiés

[195] A. Andreotti, P. Cartier, Algèbre homologique, école Normale Supérieure, Secrétariat Mathématique, Paris, 1958.

[196] P. Cartier, P. Gabriel, Compléments de mathématiques, Groupe de Recherche Opérationnelle, Marine Nationale, état-Major général ; 3ème bureau, [Paris, 1960].

[197] P. Cartier, J. R. Barra, Calcul des probabilités. Groupe de Recherche Opérationnelle, Marine Nationale, état-Major général ; 3ème bureau, Paris, 1961.

[198] Algèbre. M. G. P. 1961-62, Amicale des Etudiants de la Faculté des Sciences, Strasbourg, 1961.

[199] Algèbre. M. G. P., Faculté des Sciences, Strasbourg, 1962.

[200] Calcul de probabilités et statistique mathématique 1. Faculté des Sciences, Strasbourg, 1964.

[201] Transformation de Fourier des distributions et applications probabilistes. Tome I. Institut de recherche mathématique avancée, Strasbourg, 1967.

[202] Intégrale de Lebesgue. Département de Mathématique, Strasbourg, 1968.

[203] Introduction à l'analyse fonctionnelle ; espaces métriques, espaces normés. Département de Mathématique, Strasbourg, 1971.

[204] Introduction aux problèmes mathématiques de la mécanique quantique. Notes de R. Barre, U. E. R. de Mathématique, Strasbourg, 1971.

[205] La série génératrice exponentielle, Publication Institut de recherche mathématique avancée, Strasbourg, 1972.

[206] La place des mathématiques, Dossier-débat. P. Cartier, éd., Centre de Math., école Polytechnique, Palaiseau, 1988 [contient Le point de vue de Pierre Cartier, Les conjectures et l'exploration mathématique, Pour la Science, Septembre 1987, p. 7 ; Lettre. Pierre Cartier répond à Claude Allègre, Pour la Science, Janvier 1988, p. 4 ; une lettre à Jean-Pierre Serre].

En l'honneur de Pierre Cartier

[207] La place des mathématiques, Dossier-débat. P. Cartier, éd., Centre de Math., école Polytechnique, Palaiseau, 1988 [contient Le point de vue de Pierre Cartier, Les conjectures et l'exploration mathématique, Pour la Science, Septembre 1987, p. 7 ; Lettre. Pierre Cartier répond à Claude Allègre, Pour la Science, Janvier 1988, p. 4 ; une lettre à Jean-Pierre Serre].

Autres textes

[-] Revue VousNousIls "J'aime l'idée que le trésor mathématique n'est pas pour nous tout seuls.". pdf

[-] *Le château des groupes*, interview de Pierre Cartier par Javier Fresán. pdf

Bibliographie d'Alexander Grothendieck

[1] *Sur la complétion du dual d'un espace vectoriel localement convexe.* C. R. Acad. Sc. Paris 230, 605-606 (1950). pdf

[2] *Quelques résultats relatifs à la dualité dans les espaces ($\mathcal{F}$).* C. R. Acad. Sci. Paris 230, 1561-1563 (1950). pdf

[3] *Critères généraux de compacité dans les espaces vectoriels localement convexes. Pathologie des espaces ($\mathcal{LF}$).* C. R. Acad. Sci. Paris 231, 940-941 (1950). pdf

[4] *Quelques résultats sur les espaces vectoriels topologiques.* C. R. Acad. Sci. Paris 233, 839-841 (1951). pdf

[5] *Sur une notion de produit tensoriel topologique d'espaces vectoriels topologiques, et une classe remarquable d'espaces vectoriels liée à cette notion.* C. R. Acad. Sci. Paris 233, 1556-1558 (1951). pdf

[6] *Critères de compacité dans les espaces fonctionnels généraux.* Amer. J. Math. 74, 168-186 (1952). pdf

[7] *Sur les applications linéaires faiblement compactes d'espaces du type $C(K)$.* Canadian J. Math. 5, 129-173 (1953). pdf

[8] *Sur les espaces de solutions d'une classe générale d'équations aux dérivées partielles.* J. Analyse Math. 2, 243-280 (1953). pdf

[9] *Sur certains espaces de fonctions holomorphes. I.* J. reine angew. Math. 192, 35-64 (1953). pdf

[10] *Sur certains espaces de fonctions holomorphes, II.* J. reine angew. Math. 192, 77-95 (1953). pdf

[11] *Quelques points de la théorie des produits tensoriels topologiques.* Segundo symposium sobre algunos problemas matematicos que se estan estudiando en Latino América, Julio 1954, 173-177. Centro de Cooperación Cientifica de la UNESCO para América Latina, Montevideo, Uruguay, 1954.

[12] *Espaces vectoriels topologiques.* Instituto de Matematica Pura e Aplicada, Universidade de Sao Paulo, 1954.

[13] *Résumé des résultats essentiels dans la théorie des produits tensoriels topologiques et des espaces nucléaires.* Ann. Inst. Fourier 4, 73-112 (1952). pdf

[14] *Sur certains sous-espaces vectoriels de L^p.* Canadian J. Math. 6, 158-160 (1954). pdf

[15] *Résultats nouveaux dans la théorie des opérations linéaires. I.* C. R. Acad. Sci. Paris 239, 577-579 (1954). pdf

[16] *Résultats nouveaux dans la théorie des opérations linéaires, II.* C. R. Acad. Sc. Paris 239, 607-609 (1954). pdf

[17] *Sur les espaces ($\mathcal{F}$) et ($\mathcal{DF}$).* Summa Brazil. Math. 3, 57-123 (1954). pdf

[18] *Produits tensoriels topologiques et espaces nucléaires.* Mem. Amer. Math. Soc. n° 16, 1955. pdf

[19] *Une caractérisation vectorielle-métrique des espaces L^1.* Canad. J Math. 7, 552-561 (1955). pdf

[20] *A general theory of fibre spaces with structure sheaf.* University of Kansas, 1955. pdf pdf pdf

[21] *Erratum au mémoire : Produits tensoriels topologiques et espaces nucléaires.* Ann. Inst. Fourier 6, 117-120 (1955/56). pdf

[22] *Résumé de la théorie métrique des produits tensoriels topologiques.* Bol. Soc. Mat. Sao Paulo 8, 1-79 (1956). pdf

[23] *Théorèmes de finitude pour la cohomologie des faisceaux.* Bull. Soc. Math. France 84, 1-7 (1956). pdf

[24] *La théorie de Fredholm.* Bull. Soc. Math. France 84, 319-384 (1956). pdf

[25] *Sur la classification des fibrés holomorphes sur la sphère de Riemann.* Amer. J. Math. 79, 121-138 (1957). pdf

[26] *Sur certaines classes de suites dans les espaces de Banach, et le théorème de Dvoretzky-Rogers.* Bol. Soc. Mat. Sao Paulo 8, 81-110, (1956). pdf

[27] *Un résultat sur le dual d'une C^*-algèbre.* J. Math. Pures Appl., 36, 97-108 (1957).

[28] *Sur quelques points d'algèbre homologique.* Tohoku Math. J. 9, 119-221 (1957). pdf

[29] *Algèbre homologique.* Séminaire A. Grothendieck, 1ère année, 1957, Secrétariat mathématique IHP, 11 rue Pierre et Marie Curie, 75005 Paris, 1958.

[30] *La théorie des classes de Chern.* Bull. Soc. Math. France 86, 137-154 (1958). pdf

[31] *Sur une note de Mattuck-Tate.* J. reine angew. Math. 200, 208-215 (1958). pdf

[32] *The cohomology theory of abstract algebraic varieties.* Proc. Internat Congress Math. (Edinburgh, 1958), 103-118. Cambridge Univ Press, New York, 1960. pdf

[33] *The trace of certain operators.* Studia Math. 20, 141-143 (1961). pdf

[34] *Fondements de la géométrie algébrique* (Extraits du Séminaire Bourbaki 1957/62), Secrétariat mathématique IHP, 11 rue Pierre et Marie Curie, 75005 Paris, (1962). pdf

[35] *Résidus et dualité, Prénotes pour un séminaire Hartshorne 1963.* R. Hartshorne, Residues and Duality, Lecture Notes in Mathematics 20, Springer-Verlag, Berlin-Heidelberg-New York, 1966.

[36] *Le groupe de Brauer, III : Exemples et compléments.* IHES, Mars 1966. Dix exposés sur la cohomologie des schémas, 88-188. North Holland, Amsterdam et Masson, Paris, 1968. pdf
Note : Ce texte est la continuation des exposés au Séminaire Bourbaki [79] et [80].

[37] *On the de Rham cohomology of algebraic varieties.* Inst. Hautes Etudes Sci. Publ. Math. 29, 95-103 (1966). pdf

[38] *Un théorème sur les homomorphismes de schémas abéliens.* Invent. Math. 2, 59-78 (1966). pdf

[39] (avec Dieudonné J.) *Critères différentiels de régularité pour les localisés des algèbres analytiques.* J. Algebra 5, 305-324 (1967). pdf

[40] *Local cohomology.* A seminar given by A. Grothendieck, Harvard University, Fall 1961, Notes by R. Hartshorne, Lecture Notes in Mathematics 41, Springer-Verlag, Berlin-New York, 1967. pdf

[41] *Catégories cofibrées additives et complexe cotangent relatif.* Lecture Notes in Mathematics 79, Springer-Verlag, Berlin-New York, 1968. pdf

[42] *Classes de Chern et représentations linéaires des groupes discrets.* Dix exposés sur la cohomologie des schémas. 215-305. North Holland, Amsterdam ; Masson, Paris, 1968. pdf

[43] *Crystals and the de Rham cohomology of schemes. Notes by J. Coates and O. Jussila.* Dix exposés sur la cohomologie des schémas, 306-358. North Holland, Amsterdam ; Masson, Paris, 1968. pdf

[44] *Standard conjectures on algebraic cycles.* Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), 193-199. Oxford Univ. Press, London, 1969. pdf

[45] *Hodge's general conjecture is false for trivial reasons.* Topology 8, 299-303 (1969). pdf

[46] *Représentations linéaires et compactification profinie des groupes discrets.* (English summary) Manuscripta Math. 2, 375-396 (1970). pdf

[47] *The Responsibility of the Scientist Today.* Queen's Papers in Pure and Applied Mathematics, 27, Queen's University, Kingston, Ontario 1971. pdf

[48] (with Murre, Jacob P.) *The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme.* Lecture Notes in Mathematics 208, Springer-Verlag, Berlin-New York, 1971. pdf

[49] *Travaux de Heisouké Hironaka sur la résolution des singularités.* Actes du Congrés International des Mathématiciens (Nice, 1970), Tome 1, 7-9. Gauthier-Villars, Paris, 1971. pdf

[50] *Groupes de Barsotti-Tate et cristaux.* Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1, 431-436. Gauthier-Villars, Paris, 1971. pdf

[51] (with Seydi Hamet) *Platitude d'une adhérence schématique et lemme de Hironaka généralisé.* (English summary) Manuscripta Math. 5, 323-339 (1971). pdf

[52] *Topological vector spaces.* Translated from the French ([12]) by Orlando Chaljub. Notes on Mathematics and its Applications. Gordon and Breach Science Publishers, New York-London-Paris, 1973. pdf

[53] *Groupes de Barsotti-Tate et cristaux de Dieudonné.* Séminaire de Mathématiques Supérieures. 45 (Eté 1970). Les Presses de l'Université de Montréal, Montréal, Que., 1974. pdf

[54] *A la poursuite des champs* (1983), non publié. pdf

[55] *Esquisse d'un programme* (1984), non publié. pdf

[56] *Récoltes et Semailles : réflexions ef témoignage sur un passé de mathématicien.* Université des Sciences et Techniques du Languedoc (Montpellier) et CNRS (1985). pdf

[EGA] : Eléments de Géométrie Algébrique, rédigés avec la collaboration de J. Dieudonné. Publications mathématiques de l'IHES :

[57] I. *Le langage des schémas.* **4** (1960) (seconde édition, Springer-Verlag 1971). pdf

[58] II. *Etude globale élémentaire de quelques classes de morphismes.* **8** (1961). pdf

[59] III. *Etude cohomologique des faisceaux cohérents. I.* **11** (1961). pdf

[60] III. *Etude cohomologique des faisceaux cohérents. II.* **17** (1963). pdf

[61] IV. *Etude locale des schémas ef des morphismes de schémas. I.* **20** (1964). pdf

[62] IV. *Etude locale des schémas et des morphismes de schémas. II.* **24** (1965). pdf

[63] IV. *Etude locale des schémas et des morphismes de schémas. III.* **28** (1966). pdf

[64] IV. *Etude locale des schémas et des morphismes de schémas. IV.* **32** (1967). pdf

Exposés au Séminaire Bourbaki *

[65] *Produits tensoriels topologiques et espaces nucléaires.* 1952/53, n° 6. pdf

[66] *La théorie de Fredholm.* 1953/54, n° 91. pdf

[67] *Réarrangements de fonctions et inégalités de convexité dans les algèbres de von Neumann munies d'une trace.* 1954/55, n° 113. pdf

[68] *Sur un mémoire de A. Weil : "Généralisation des fonctions abéliennes".* 1956/57, n° 141. pdf

[69] *Théorèmes de dualité pour les faisceaux algébriques cohérents.* 1956/57, n° 149. pdf

[70] *Géométrie formelle et géométrie algébrique.* 1958/59, n° 182. pdf

[71] *Technique de descente et théorèmes d'existence en géométrie algébrique, I : Généralités. Descente par morphismes fidèlement plats.* 1959/60, n° 190. pdf

[72] *Technique de descente et théorèmes d'existence en géométrie algébrique, II : Le théorème d'existence en géométrie formelle des modules.* 1959/60, n° 195. pdf

[73] *Techniques de construction et théorèmes d'existence en géométrie algébrique, III : Préschémas quotients.* 1960/61, n° 212. pdf

[74] *Techniques de construction et théorèmes d'existence en géométrie algébrique, IV : Les schémas de Hilbert.* 1960/61, n° 221. pdf

[75] *Technique de descente et théorèmes d'existence en géométrie algébrique, V : Les schémas de Picard : Théorémes d'existence.* 1961/62, n° 232. pdf

[76] *Technique de descente et théorèmes d'existence en géométrie algébrique, VI : Les schémas de Picard : Propriétés générales.* 1961/62, n° 236. pdf

[77] *Fondements de la géométrie algébrique, commentaires.* 1961/62, complément. pdf

∗. publiés par W. A. Benjamin, Inc., New York, 1966.

[78] *Formule de Lefschetz et rationalité des fonctions L.* 1964/65, n° 279. pdf

[79] *Le groupe de Brauer, I : Algèbres d'Azumaya et interprétations diverses.* 1964/65, n° 290. pdf

[80] *Le groupe de Brauer, II : Théorie cohomologique.* 1965/66, n° 297. pdf

Note : [78], [79] et [80] sont reproduits dans "Dix Exposés sur la cohomologie des schémas", North Holland, Amsterdam et Masson, Paris, 1968.

Exposés au Séminaire Chevalley (Institut Henri Poincaré, Secrétariat mathématique, 11 rue Pierre et Marie Curie, 75005 Paris).

Classification des groupes de Lie algébriques (1956/58).

[81] *Généralités sur les groupes algébriques affines. Groupes algébriques affines commutatifs.* Exp. 4. pdf

[82] *Compléments de géométrie algébrique. Espaces de transformations.* Exp. 5. pdf

[83] *Les théorèmes de structure fondamentaux pour les groupes algébriques affines.* Exp. 6. pdf

[84] *Sous-groupes de Cartan, éléments réguliers. Groupes algébriques affines de dimension 1.* Exp. 7. pdf

Anneaux de Chow et applications (1958).

[85] *Sur quelques propriétés fondamentales en théorie des intersections.* Exp. 4. pdf

[86] *Torsion homologique et sections rationnelles.* Exp. 5. pdf

Exposés au Séminaire Cartan 1960/61 : Familles d'espaces complexes et fondements de la géométrie analytique (W. A. Benjamin, Inc., New York, 1967).

Techniques de construction en géométrie analytique :

[87] I : *Description axiomatigue de l'espace de Teichmiller et de ses variantes.* Exp. 7-8. pdf

[88] II : *Généralités sur les espaces annelés et les espaces analytiques.* Exp. 9. pdf

[89] III : *Produits fibrés d'espaces analytiques.* Exp. 10. pdf

[90] IV : *Formalisme général des foncteurs représentables.* Exp. 11. pdf

[91] V : *Fibrés vectoriels, fibrés projectifs, fibrés en drapeaux.* Exp. 12. pdf

[92] VI : *Etude locale des morphismes ; germes d'espaces analytiques, platitude, morphismes simples.* Exp. 13. pdf

[93] VII : *Etude locale des morphismes ; éléments de calcul infinitésimal.* Exp. 14. pdf

[94] VIII : *Rapport sur les théorémes de finitude de Grauert et Remmert.* Exp. 15. pdf

[95] IX : *Quelques problèmes de modules.* Exp. 16. pdf

[96] X : *Construction de l'espace de Teichmüller.* Exp. 17. pdf

SGA : Séminaire de Géométrie Algébrique du Bois-Marie †

[97] SGA 1 *Revêtements étales et groupe fondamental.* 1960/61.
Dirigé par A. Grothendieck
Lecture Notes in Mathematics **224**, Springer-Verlag, Berlin-Heidelberg-New York, 1971. pdf

[98] SGA 2 *Cohomologie des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux.* 1961/62.
Dirigé par A. Grothendieck
North-Holland Publishing Company, Amsterdam, 1968. pdf

[99] SGA 3 *Schémas en groupes.* 1962/64.
Dirigé par M. Demazure et A. Grothendieck
Tome I. Propriétés générales des schémas en groupes, Lecture Notes in Mathematics **151**, Springer-Verlag, Berlin-Heidelberg-New York, 1970.
Tome II. Groupes de type multiplicatif, et structure des schémas en groupes généraux, Lecture Notes in Mathematics **152**, Springer-Verlag, Berlin-Heidelberg-New York, 1970.
Tome III. Structure des schémas en groupes réductifs, Lecture Notes in Mathematics **153**, Springer-Verlag, Berlin-Heidelberg-New York, 1970. pdf

[100] SGA 4 *Théorie des topos et cohomologie étale des schémas.* 1963/64.
Dirigé par M. Artin, A. Grothendieck, J.-L. Verdier
Tome I. Théorie des topos, Lecture Notes in Mathematics **269**, Springer-Verlag, Berlin-Heidelberg-New York, 1972.
Tome II. Lecture Notes in Mathematics **270**, Springer-Verlag, Berlin-Heidelberg-New York, 1972.
Tome III. Lecture Notes in Mathematics **305**, Springer-Verlag, Berlin-Heidelberg-New York, 1973. pdf

[101] SGA 5 *Cohomologie l-adique et fonctions L.* 1965/66.
Dirigé par A. Grothendieck
Lecture Notes in Mathematics **589**, Springer-Verlag, Berlin-Heidelberg-New York, 1977. pdf

[102] SGA 6 *Théorie des intersections et théorème de Riemann-Roch.* 1966/67.
Dirigé par P. Berthelot, A. Grothendieck L. Illusie
Lecture Notes in Mathematics **225**, Springer-Verlag, Berlin-Heidelberg-New York, 1971. pdf

[103] SGA 7 *Groupes de monodromie en géométrie algébrique.* 1967-69.
Tome I, Dirigé par A. Grothendieck
Lecture Notes in Mathematics **288**, Springer-Verlag, Berlin-Heidelberg-New York, 1972.
Tome II, par P. Deligne et N. Katz ‡
Lecture Notes in Mathematics **340**, Springer-Verlag, Berlin-Heidelberg-New York, 1973. pdf
pdf

[-] *Sur les faisceaux algébriques et les faisceaux analytiques cohérents.* Séminaire Henri Cartan, tome 9 (1956/1957), exp. n° 2, p. 1-16. pdf

[-] erratum 1. pdf

[-] erratum 2. pdf

[-] erratum 3. pdf

†. Nous omettons de la liste (SGA 4 1/2, par P. Deligne, Cohomologie étale, Lecture Notes in Mathematics **569**, Springer-Verlag, Berlin-Heidelberg-New York, **197**), qui ne correspond à aucun séminaire du Bois-Marie.

[-] erratum 4. pdf

[-] erratum 5. pdf

[-] erratum 6. pdf

[-] erratum 7. pdf

[-] erratum 8. pdf

Transcriptions en Latex été 2019 pdf pdf pdf pdf pdf pdf pdf

Transcriptions et traductions

1) Leçon inaugurale d'Alain Connes au Collège de France pdf

2) Traduction d'une nouvelle preuve du Théorème de Morley d'Alain Connes pdf

3) Critique dans les AMS du livre Noncommutative geometry par Ingrid Segal pdf

4) Alain Connes : Formule de Trace en géométrie non-commutative et zéros de la fonction zêta de Riemann pdf

5) Jean-Benoît Bost, Alain Connes : Algèbres de Hecke, facteurs de type III et transitions de phase avec brisure spontanée de symétrie en théorie des nombres pdf

6) Paul Dirac : La théorie quantique de l'émission et de l'absorption de radiation pdf

7) Alain Connes : Cohomologie cyclique et géométrie différentielle non-commutative pdf

8) Traduction de "Conseils au débutant, par Alain Connes" dans Princeton companion to mathematics, de Timothy Gowers pdf

9) Alain Connes, Jacques Dixmier : Mes rencontres avec Jacques pdf

10) Les mathématiques et la pensée en mouvement, Conférence à l'Université PSL dans le cadre du Cycle Pluri-disciplinaire d'Études supérieures (2015) pdf (en) pdf

11) Un topo sur les topos, dans le cadre du Colloque Les lectures Grothendieckiennes à l'École Normale Supérieure (2017) pdf (en) pdf

12) Parcours d'un mathématicien, en clotûre du Cycle Maths pour tous, à l'École Normale Supérieure (2017) pdf (en) pdf

13) Intervention courte intégrée au film de l'Exposition Mathématiques, un dépaysement soudain (2012) pdf (en) pdf

14) Présentation de promotion filmée par les éditions Odile Jacob du livre *Le Spectre d'Atacama* pdf (en) pdf

15) Émission de radio La méthode scientifique pour présenter le livre *Le Spectre d'Atacama* sur France Culture (2018) pdf (en) pdf

16) La géométrie de l'incertitude (article de Dana Mackenzie) pdf

17) Alain Connes : La vérité est mathématique (Tangente, août-septembre 2000) pdf

18) Extrait de Mathématiques, un dépaysement soudain et du livre Les déchiffreurs pdf

19) Point de vue d'Alain Connes, Dossier Les mathématiciens d'un ancien magazine Pour la Science pdf

20) Article du magazine numérique Futura Sciences suite à l'obtention de la médaille d'or du CNRS en 2004 pdf

21) L'imagination joue un rôle crucial en mathématiques (article de Libération en 2001) pdf

22) Une réalité archaïque précède les concepts (Les Dossiers de La Recherche n° 20, Mathématiques, nouveaux défis et vieux casse-têtes, août-octobre 2005) pdf

23) L'imagination et l'infini, entretien avec Alain Prochiantz, sur France Culture, Cycle Savoirs / Imaginations (2018) pdf (en) pdf

24) Alain Connes interviewé en Iran par M. Khalkhali et G.B. Khosrovshahi pdf

25) Alain Connes interviewé par Catherine Goldstein et Georges Skandalis pour la Société mathématique européenne en 2008 pdf

26) La créativité en musique et en mathématiques, entretien entre Pierre Boulez et Alain Connes à l'IRCAM (2011) pdf (en) pdf

27) Interventions d'Alain Connes lors d'une table ronde "Les valeurs et les grands principes qui fondent une recherche d'excellence" au sujet du CNRS (2019) pdf (en) pdf

28) Alexandre Grothendieck, créateur réfugié en lui-même, Colloque Migrations, réfugiés, exils au Collège de France (2016) pdf (en) pdf

29) Dualité entre formes et spectres, Colloque La vie des formes, Collège de France (2011) pdf (en) pdf

30) Un entretien au Collège de France avec Alain Connes (2016) pdf (en) pdf

31) Interview à Trieste, autour d'un symposium à l'ICTP (2017) pdf (en) pdf

32) Intervention lors du Colloque Langage et Pensée au Collège de France (2018) pdf (en) pdf

33) Fudan, traduction d'articles de journaux en chinois pdf pdf

34) Extraits du blog créé par Masoud Khalkhali et Alain Connes dans lequel les idées sont présentées de manière non formelle pdf (en) pdf

35) Traduction de La géométrie et le quantique (en) pdf

36) Entretien avec Jean-Christophe Yoccoz pdf (en) pdf

37) Noncommutative Geometry, the spectral aspect (en) pdf (fr) pdf

38) Renormalization and Galois theory (en) pdf (fr) pdf

39) Quantized Calculus and Quasi-Inner Functions (en) pdf (fr) pdf

Mes traductions de la section 6 correspondant au calcul du spectre des zéros de zeta pdf
et le fascicule de résultats correspondant pdf
et des trucs diamino du même article récent (juin 2020) pdf

Articles d'Alain Connes qui n'étaient pas fournis dans la page de bibliographie de son site à la fin de l'année 2018

[1] Sur une généralisation de la notion de corps ordonné, C.R. Acad. Sci. Paris, Sér A-B, 269, 1969, p. A337-A340. pdf

[2] Ordres faibles et localisation des zéros de polynômes, C.R. Acad. Sci. Paris, Sér A-B, 269, 1969, p. A373-A376. pdf

[3] Ordres faibles et localisation de zéros de polynômes, Séminaire Choquet (Delange-Pisot-Poitou) : 1968/69, Initiation à l'Analyse, Exp. 5, 27 p., Secrétariat mathématique, Paris 12, 1969. pdf

[4] Détermination de modèles minimaux en analyse non standard et application, C.R. Acad. Sci. Paris, Sér A-B, 271, 1970, p. A969-A971. pdf

[5] Ultrapuissances et applications dans le cadre de l'analyse non standard, Séminaire Choquet : 1969/70, Initiation à l'Analyse, Fasc. 1, Exp. 8, 25 p., Secrétariat mathématique, Paris, 1970. pdf

[6] Un nouvel invariant pour les algèbres de von Neumann, C.R. Acad. Sci. Paris, Sér A-B, 273, 1971, p. A900-A903.

[7] Un théorème de décomposition d'applications mesurables, Séminaire Choquet, $10^{\text{ème}}$ année (1970/71), Initiation à l'Analyse, Fasc. 1, Exp. n$^{\text{o}}$ 12, 7 p., Sectétariat Mathématique, Paris, 1971. pdf

[8] Calcul des deux invariants d'Araki et Woods par la théorie de Tomita et Takesaki, C.R. Acad. Sci. Paris, Sér A-B, 274, 1972, p. A175-A177. pdf

[9] Etats presque périodiques sur une algèbre de von Neumann, C.R. Acad. Sci Paris, Sér A-B, 274, 1972, p. A1402-A1405. pdf

[10] Groupe modulaire d'une algèbre de von Neumann, C.R. Acad. Sci Paris, Sér A-B, 274, 1972, p. A1923-A1926. pdf

[11] Une classification des facteurs de type III, C.R. Acad. Sci. Paris, Sér A-B, 275, 1972, p. A523-A525. pdf

[12] Ordres faibles et localisation de zéros de polynômes, Séminaire Delange-Pisot Poitou ($12^{\text{ème}}$ année : 1970/71), Théorie des nombres, Exp. n$^{\text{o}}$ 18, 11 p., Secrétariat Mathématique, Paris, 1972. pdf

[13] The group property of the invariant S of von Neumann algebras, Avec Alfons van Daele, Math. Scand. 32, 1973-1974, p. 187-192. pdf

[14] Sur le théorème de Radon-Nikodym pour les poids normaux fidèles semi-finis, Bull. Sci. Math. (2) 97, 1973-1974, p. 253-258.

[15] Flots des poids sur les facteurs de type III, Avec Masamichi Takesaki, C.R. Acad. Sci Paris, Sér A, 278, 1974, p. 945-948.

[16] Almost periodic states and factors of type III_1, J. Functional Analysis 16, 1974, p. 415-445. pdf

[17] Existence de facteurs infinis asymptotiquement abéliens, Avec Edward J. Woods, C.R. Acad. Sci Paris, Sér A, 279, 1974, p, 189-191.

[18] Caractérisation des espaces vectoriels ordonnés sous-jacents aux algèbres de von Neumann, Ann. Inst. Fourier (Grenoble) 24 (1974), n° 4, x, p. 121-155 (1975). pdf

[19] A factor not anti-isomorphic to itself, Ann. Math. (2) 101, 1975, p. 536-554. pdf

[20] On hyperfinite factors of type III_0 and Krieger's factors, J. Functional Analysis 18 (1975), p. 318-327. pdf

[21] Sur la classification des facteurs de type II, C.R. Acad. Sci Paris, Sér A-B, 281, 1975, n° 1, p. A13-A15.

[22] Classification of automorphisms of hyperfinite factors of type II_1 and II_∞ and application to type III factors, Bull. Amer. Math. Soc. 81 (1975), n° 6, p. 1080-1092. pdf

[24] On the hierarchy of W. Krieger, Illinois J. Math. 19 (1975), p. 428-432. pdf

[25] A factor not anti-isomorphic to itself, Bull London Math. Soc. 7 (1975), p. 171-174. pdf

[26] Structure theory for Type III factors, Proceedings of the International Congress of Mathematicians (Vancouver, B. C., 1974), Vol. 2, p. 87-91. Canad. Math. Congress, Montreal, Que., 1975. pdf

[27] Outer conjugacy of automorphisms of factors, Symposia Mathematica, Vol. XX (Convegno sulle Algebte C^* e loro Appicazioni in Fisica Teoria, Convegno sulla Teoria degli Operator Indice e Teoria K, INDAM, Rome, 1975), Academic Press, London, 1976, p. 149-159. pdf

[28] Entropy for automorphisms of II_1 von Neumann algebras, Avec Erling Størmer, Acta Math. 134 (1975), n° 3-4, p. 289-306. pdf

[29] On the classification of von Neumann algebras and their automorphisms, Symposia Mathematica, Vol XX (Convegno sulle Algebre C^* e loro Appicazioni in Fisica Teoria, Convegno sulla Teoria degli Operator Indice e Teoria K, INDAM, Rome, 1975), Academic Press, London, 1976, p. 435-478.

[30] Classification of injective factors. Cases II_1, II_∞, III_λ, $\lambda \neq 1$, Ann. of Math. (2) 104 (1976), n° 2, p. 73-115. pdf

[31] Measure space automorphisms, the normalizers of their full groups, and approximate finiteness, Avec Wolfgang Krieger, J. Functional Analysis 24 (1977), n° 4, p. 336-352. pdf

[32] The Tomita-Takesaki theory and classification of type-III factors, (C^* algebras and their appications to statistical mechanics and quantum field theory (Proc. internat. School of Physics "Enrico Fermi", Course LX, Varenna, 1973), North-Holland, Amsterdam, 1976, p. 29-46.

[34] The flow of weights on factors of type III, Avec Masamichi Takesaki, Tôhoku Math. J. (2) 29 (1977), n° 4, p. 473-575, Errata : Tôhoku Math. J. (2) 30 (1978), n° 4, p. 653-655. pdf

[35] Homogeneity of the state space of factors of type III_1, Avec Erling Størmer, J. Functional Analysis 28 (1978), n° 2, p. 187-196. pdf

[36] On the cohomology of operator algebras, J. Functional Analysis 28 (1978), n° 2, p. 248-253. pdf

[37] The von Neumann algebra of a foliation, Mathematical problems in theoretical physics (Proc. Internat. Conf., Univ. Rome, Rome, 1977), p. 145-151, Lecture Notes in Phys., 80, Springer, Berlin-New York, 1978. pdf

[38] The L^2-index theorem for homogeneous spaces, Avec Henri Moscovici, Bull Amer. Math. Soc. (N.S.) 1 (1979), n° 4, p. 688-690. pdf

[40] On the equivalence between injectivity and semidiscreteness for operator algebras, Algèbres d'opérateurs et leurs applications en physique mathématique (Proc. Colloq., Marseille, 1977), Colloq. Internat. CNRS, 274, CNRS, Paris, 1979, p. 107-112.

[44] On the spatial theory of von Neumann algebras, J. Funct. Anal, 35 (1980), n° 2, p. 153-164. pdf

[45] A factor of type II_1 with countable fundamental group, J. Operator Theory 4 (1980), n° 1, p. 151-153. pdf

[46] Property T and asymptotically invariant sequences, Avec B. Weiss, Israel J. Math. 37 (1980), n° 3, p. 209-210. pdf

[47] Von Neumann algebras, Proceedings of the International Congress of Mathematicians (Helsinki, 1978), Acad. Sci. Fennica, Helsinki, 1980, p. 97-109. pdf

[48] A construction of approximately finite-dimensional non-ITPFI factors, Avec Edward J. Woods, Canad. Math. Bull. 23 (1980), n° 2, p. 227-230. pdf

[49] Théoréme de l'indice pour les feuilletages, Avec Georges Skandalis, C.R. Acad. Sci Paris Sér I Math, 292 (1981), n° 18, p. 871-876. pdf

[50] An analogue of the Thom isomorphism for crossed products of a C^* algebra by an action of $\mathbb{R}$, Adv. in Math. 39 (1981), n° 1, p. 31-55. pdf

[52] Feuilletages et algèbres d'opérateurs, Bourbaki Seminar, Vol 1979/80, p. 139-155, Lecture Notes in Math, 842, Springer, Berlin-New York, 1981. pdf

[53] An amenable equivalence relation is generated by a single transformation, Avec J. Feldman et B. Weiss, Ergodic Theory Dynamical Systems 1 (1981), n° , p. 431-450. pdf

[54] A II_1 factor with two nonconjugate Cartan subalgebras, Avec Vaughan Jones, Bull. Amer. Math. Soc. (N.S.) 6 (1982), n° 2, p. 211-212. pdf

[55] L^2-index theory on homogeneous spaces and discrete series representations, Avec Henri Moscovici, Proc. Sympos. Pure Math., 38, Amer. Math, Soc., Providence, RI, 1982, p. 419-433. pdf

[56] Classification des facteurs, Operator algebras and applications, Part 2 (Kingston, Ont, 1980), p. 43-109, Proc. Sympos. Pure Math., 38, Amer. Math. Soc., Providence, RI, 1982. pdf

[57] The L^2-index theorem for homogeneous spaces of Lie groups, Avec Henri Moscovici, Ann. of Math. (2) 115 (1982), n° 2, p. 291-330. pdf

[60] A connection between the classical and the quantum mechanical entropies, Avec Erling Størmer, Operator algebras and group representations, Vol I (Neptun, 1980), p. 113-123, Monographs Stud. Math., 17, Pitman, Boston, Mass.-London, 1984.

[63] Property T for von Neumann algebras, Avec Vaughan Jones, Bull. London Math. Soc. 17 (1985), n° 1, p. 57-62. pdf

[64] Approximately transitive flows and ITPFI factors, Avec Edward J. Woods, Ergodic Theory Dynamical Systems 5 (1985), n° 2, p. 203-236. pdf

[65] Entropie de Kolmogoroff-Sinai et mécanique statistique quantique, C.R. Acad. Sci. Paris Sér. I Math, 301 (1985),n° 1, p. 1-6. pdf

[66] Introduction to noncommutative differential geometry, Workshop Bonn 1984 (Bonn, 1984), 3-16, Lecture Notes in Math., 1111, Springer, Berlin-New York, 1985. pdf

[68] Factors of type III_1, property L'$_\lambda$, and closure of inner automorphisms, J. Operator Theory 14 (1985), n° 1, p. 189-211.

[69] Diameters of state spaces of type III factors, Avec Uffe Haagerup et Erling Størmer, Operator algebras and their connections with topology and ergodic theory (Busteni, 1983), p. 91-116, Lecture Notes in Math., 1132, Springer, Berlin-New York, 1985. pdf

[70] Leafwise homotopy equivalence and rational Pontrjagin classes, Avec Paul Baum, Foliations (Tokyo, 1983), 1-14, Adv. Stud. Pure Math., 5, North-Holland, Amsterdam-New York, 1985. pdf

[71] Indice des sous facteurs, algébres de Hecke et théorie des noeuds (d'aprés Vaughan Jones), Seminar Bourbaki, Vol. 1984/85. Astéisque n° 133-134 (1986), p. 289-308. pdf

[72] Transgression du caractere de Chern et cohomologie cyclique, Avec Henri Moscovici, C.R. Acad. Sci. Paris Sér. I Math., 303 (1986), n° 18, p. 913-918. pdf

[74] Yang-Mills for noncommutative two-tori, Avec Marc A. Rieffel, Operator algebras and mathematical physics (Iowa City, Iowa, 1985), p. 237-266, Contemp. Math., 62, Amer. Math. Soc., Providence, RI, 1987.

[76] Cyclic cohomology and noncommutative differential geometry, Proceedings of the Intemational Congress of Mathematicians, Vol. 1, 2 (Berkeley, Cal., 1986), p. 879-889, Amer. Math. Soc., Providence, RI, 1987. pdf

[77] Quasi homomorphismes, cohomologie cyclique et positivité, Avec J. Cuntz, Comm. Math. Phys. 114 (1988), n° 3, p. 515-526. pdf

[78] Cyclic cohomology and noncommutative differential geometry, Géométrie différentielle (Paris, 1986), p. 33-50, Travaux en Cours, 3, Hermann, Paris, 1988.

[79] Entire cyclic cohomology of Banach algebras and characters of theta-summable Fredholm modules, K-Theory 1 (1988), n° 6, p. 519-548. pdf

[80] Caractère multiplicatif d'un module de Fredholm, Avec Max Karoubi, K-Theory 2 (1988), n° 3, p. 431-463. pdf

[81] Trace de Dixmier, modules de Fredholm et géomeétrie riemannienne, Conformal field theories and related topics (Annecy-le-Vieux, 1988). Nuclear Phys. B Proc. Suppl. 5b (1988), p. 65-70. pdf

[82] Conjecture de Novikov et groupes hyperboliques, Avec Henri Moscovici, C.R. Acad. Sci. Paris Sér. I Math. 307 (1988), n° 9, p. 475-480. pdf

[83] Chern character for discrete groups, Avec Paul Baum, A fête of topology, p. 163-232, Academic Press, Boston, MA, 1988.

[85] K-theory for discrete groups, Avec Paul Baum, Operator algebras and applications, Vol. 1, p. 1-20, London Math. Soc. Lecture Note Ser., 135, Cambridge Univ. Press, Cambridge, 1988. pdf

[86] Noncommutative geometry, Nonperturbative quantum field theory (Cargése, 1987), p. 33-69, NATO Adv. Sci. Inst. Ser. B : Phys., 185, Plenum, New York, 1988. pdf

[87] Hyperfinite von Neumann algebras and Poisson boundaries of time dependent random walks, Avec Edward J. Woods, Pacific J. Math. 137 (1989), n° 2, p. 225-243. pdf

[88] Compact metric spaces, Fredholm modules, and hyperfiniteness, Ergodic Theory Dynamical Systems 9 (1989), n° 2, p. 207-220. pdf

[89] Embedding of U(1)-current algebras in noncommutative algebras of classical statistical mechanics, Avec David E. Evans, Comm. Math. Phys. 121 (1989),n° 3, p. 507-525. pdf

[90] Conjecture de Novikov et fibrés presque plats, Avec Mikhaïl Gromov et Henri Moscovici, C.R. Acad. Sci Paris Sér. I Math. 310 (1990), n° 5, p. 273-277. pdf

[91] Déformations, morphismes asymptotiques et K-théorie bivariante, Avec Nigel Higson, C.R. Acad. Sci Pars Sér. I Math., 311 (1990), n° 2, p. 101-108. pdf

[93] Caractéres des représentations theta-sommables des groupes discrets, C.R. Acad. Sci. Paris Sér. I Math. 312 (1991),n° 9, p. 661-666. pdf

[94] Introduction à la géométrie non-commutative, The legacy of John von Neumann (Hempstead, NY, 1988), p. 91-118, Proc. Sympos. Pure Math. 60, Amer. Math. Soc., Providence, RI, 1980. pdf

[95] Essay on physics and noncommutative geometry, The interface of mathematics and particle physics (Oxford, 1986), p. 9-48, Inst. Math. Appl. Conf. Ser New Ser., 24, Oxford Univ. Press, New York, 1990.

[96] Particle models and noncommutative geometry, Avec John Lott, Recent advances in field theory (Annecy-le-Vieux, 1990), Nuclear Phys. B Proc. Suppl 18B (1990), p. 29-47 (1991). pdf

[97] On the Chem character of θ summable Fredholm modules, Comm. Math. Phys. 139 (1991),n° 1, p. 171-181. pdf

[98] Sur la nature de la réalité mathématique (On the nature of mathematical reality), Elem. Math. 47 (1992), n° 1, p. 19-26.

[99] Closed star products and cyclic cohomology, Avec Moshé Flato et Daniel Sternheimer, Lett. Math. Phys. 24 (1992), n° 1, p. 1-12. pdf

[100] Produits eulériens et facteurs de type III, Avec Jean-Benoît Bost, C.R. Acad. Sci. Paris Sér I Math. 315 (1992), n°, p. 279-284. pdf

[101] The metric aspect of noncommutative geometry, Avec John Lott, New symmetry principles in quantum field theory (Cargése, 1991), p. 63-93, NATO Adv. Sci. Inst. Ser. B Phys., 295, Plenum, New York, 1992. pdf

[102] Géométrie non commutative et physique quantique, Mathématiques quantiques, 20 p., SMF Journ. Annu. 1992, Soc. Math. France, Paris, 1992.

[103] Noncommutative geometry, Mathematical research today and tomorrow (Barcelona, 1991), p. 40-58, Lecture Notes in Math., 1525, Springer, Berlin, 1992. pdf

[104] Group cohomology with Lipschitz control and higher signatures, Avec Mikhaïl Gromov et Henri Moscovici, Geom. Funct. Anal. 3 (1993), n° 1, p. 1-78. pdf

[105] Formules locales pour les classes de Pontrjagin topologiques, Avec Dennis Sullivan et Nicolas Teleman, C.R. Acad. Sci. Paris Sér I Math. 317 (1993),n° 5, p. 521-526. pdf

[106] Transgression and the Chern character of finite-dimensional K-cycles, Avec Henri Moscovici, Comm. Math. Phys. 155 (1993), n° 1, p. 103-122. pdf

[107] Interpretation géométrique du modèle standard de la physique des particules et structure fine de l'espace-temps, C.R. Acad, Sci. Paris Sér. Gén. Vie Sci. 10 (1993), n°3, p. 223-234. pdf

[108] Quasiconformal mappings, operators on Hilbert space, and local formulae for characteristic classes, Avec Dennis Sullivan et Nicolas Teleman, Topology 33 (1994), n° 4, p. 663-681. pdf

[110] Classifying space for proper actions and K-theory of group C^* algebras, Avec Paul Baum et Nigel Higson, C^*algebras : 1943-1993 (San Antonio, TX, 1993), p. 240-291, Contemp. Math., 167, Amer. Math. Soc., Providence, RI, 1994. pdf

[113] Geometry from the spectral point of view, Lett. Math. Phys. 34 (1995), n° 3, p. 203-238. pdf

[114] Quantized calculus and applications, XIth Intemational Congress of Mathematical Physics (Paris, 1994), p. 15-36, Internat. Press, Cambridge, MA, 1995. pdf

[116] Polarized modules and Fredholm modules, Avec J. Brodzki et D. Ellwood, Mat. Fiz. Anal, Geom. 2 (1995), n° 1, p. 15-24.

[117] Round table : physics and mathematics, Avec J. Lebowitz, M. Atiyah, Brézin, J Fröhlich, D. Gross, A. Jaffe, L. Kadanoff et D. Ruelle, XIth International Congress of Mathematical Physics (Paris, 1994), p. 691-705, Internat. Press, Cambridge, MA, 1995.

[118] Formule de trace en géométrie non-commutative et hypothèse de Riemann, C.R. Acad. Sci. Paris Sér. I Math. 323 (1996), n° 12, p. 1231-1236. pdf

[120] Matrix Vieta theorem revisited, Avec Albert Schwarz, Lett. Math. Phys. 39 (1997), n° 4, p. 349-353. pdf

[122] Non-commutative geometry and physics, Gravitation et quantifications (Les Houches, 1992), p. 805-950, North-Holland, Amsterdam, 1995. pdf

[125] Brisure de symétrie spontanée et géométrie du point de vue spectral, Séminaire Bourbaki, Vol. 1995/96. Astérisque n° 241 (1997), Exp. n° 816, 5, p. 313-349 ; J. Geom. Phys. 23 (1997), n° 3-4, 206-234 ; and Fields Medallists lectures, 340-371, World Sci. Ser. 20th Century Math., 5, World. Sci. Publishing, River Edge, NJ, 1997. pdf

[126] Noncommutative differential geometry and the structure of space time, Operator algebras and quantum field theory (Rome, 1996), p. 330-358, Internat. Press, Cambridge, MA, 1997 ; Cyclic cohomology and noncommutative geometry (Waterloo, ON, 1995), p. 17-42, Fields Inst. Commun., 17, Amer. Math. Soc., Providence, RI, 1997 ; Deformation theory and symplectic geometry (Ascona, 1996), p.1-33, Math. Phys. Stud., 20, Kluwer Acad. Publ, Dordrecht, 1997 ; and Quantum fields and quantum space time (Cargèse, 1996), p. 45-72, NATO Adv. Sci. Inst. Ser. B Phys., 364, Plenum, New York, 1997. pdf

[127] Trace formula in noncommutative geometry and the zeros of the Riemann zeta function, Journées "Equations aux Dérivées Partielles" (Saint-Jean-de-Monts, 1997), Exp. n° IV, 28 p., Ecole Polytech., Palaiseau, 1997. pdf

Machines informatiques et intelligence

A. M. Turing

1 Le jeu de l'imitation

Je propose de considérer la question, "Les machines peuvent-elles penser ?". On devrait commencer par définir les termes "machine" et "pensée." Les définitions devraient être choisies de manière à refléter aussi bien que possible l'usage courant de ces mots, mais cette attitude est dangereuse. Si les significations des mots "machine" et "pensée" doivent être utilisées de la manière dont elles le sont habituellement, il est difficile d'échapper à la conclusion que le sens de la question "Les machines peuvent-elles penser ?" et la réponse à cette question doivent être recherchés de façon statistique, comme par sondage. Mais cela est absurde. Plutôt que de tenter une telle définition, je remplacerai la question par une autre, qui lui est intimement reliée et qui s'exprime en termes relativement non-ambigus.

La nouvelle forme du problème peut être décrite en termes d'un jeu que nous appelons le "jeu de l'imitation". Il se joue à trois, un homme (A), une femme (B), et un interrogateur (C) qui peut être de l'un ou l'autre sexe. L'interrogateur reste dans une pièce et n'est pas vu par les deux autres. L'objectif du jeu pour l'interrogateur est de déterminer qui est l'homme et qui est la femme des deux autres. Il les connaît par leur étiquette (X et Y), et à la fin du jeu, il dit soit "X est A et Y est B" soit "X est B et Y est A." L'interrogateur a le droit de poser des questions à A et B comme :

C : X peut-il ou elle me dire la longueur de ses cheveux ?

Maintenant supposons que X est vraiment A, alors A doit répondre. L'objectif de A pour ce jeu est d'essayer de faire que C se trompe dans son identification. Sa réponse pourrait donc être :

"J'ai les cheveux attachés, et ils sont longs de 20 cm."

Pour que les hauteurs des voix ne puissent pas aider l'interrogateur, les réponses seront écrites ou mieux, tapées à la machine. Le meilleur dispositif consiste à avoir un téléscripteur de communication entre les deux pièces. Sinon, les questions et les réponses

peuvent être répétées par un intermédiaire. L'objectif du jeu pour le troisième joueur (B) est d'aider l'interrogateur. La meilleure stratégie pour cette personne est probablement de donner les vraies réponses. Elle peut ajouter des choses comme "Je suis la femme, ne l'écoutez pas !" à ses réponses, mais ça ne servira à rien parce que l'homme pourra faire des remarques similaires.

Maintenant posons la question, "qu'arrivera-t-il si une machine prend la place de A dans ce jeu ?". L'interrogateur(-machine) se trompera-t-il aussi souvent que lorsque le jeu est joué par des hommes et des femmes ? Ces questions remplacent notre question originale, "Les machines peuvent-elles penser ?"

2 Critique du nouveau problème

De la même façon qu'on peut se demander "Quelle est la réponse à la question sous sa nouvelle forme", on peut aussi se demander "Cette nouvelle question est-elle digne de réflexion ?". On réfléchira à cette dernière question sans tergiverser davantage, coupant là une régression infinie.

Le nouveau problème présente l'avantage de dessiner une frontière assez nette entre les capacités physiques et intellectuelles d'un homme. Aucun ingénieur ou chimiste ne se targue de pouvoir produire un matériau qui ne soit pas distinguable de la peau humaine. Il est possible qu'un jour cela soit réalisé, mais même en supposant que cette invention ait un jour été faite, nous pouvons sentir combien il y a peu en commun entre le fait d'essayer de rendre une "machine pensante" plus humaine en la recouvrant de cette peau artificielle. La forme dans laquelle nous avons spécifié le problème montre que les conditions empêchent l'interrogateur de voir ou toucher les autres personnages, ou d'entendre leurs voix. D'autres avantages du critère proposé peuvent se voir dans des questions et réponses specimen. Par exemple :

Q : S'il vous plaît, écrivez-moi un sonnet avec comme sujet le quatrième pont.

A : Ne comptez pas sur moi. Je ne pourrai jamais écrire de poèmes.

Q : Ajoutez 34957 à 70764.

A : (Pause d'environ 30 secondes et réponse donnée ensuite) 105721.

Q : Jouez-vous aux échecs ?

A : Oui.

Q : J'ai K en K1, et pas d'autres pièces. Vous avez K en K6 et R en R1. C'est votre tour. Que jouez-vous ?

A : (Après une pause de 15 secondes) R-R8 mat.

La méthode des questions et réponses semble adaptée pour introduire presque tous les champs d'application que nous souhaiterions inclure. Nous ne voulons pas pénaliser la machine pour son incapacité à briller dans des concours de beauté, ni pénaliser un humain parce qu'il perd une course contre un avion. Les conditions de notre jeu rendent ces incompétences non pertinentes. Les "témoins" peuvent se vanter, s'il pensent que c'est judicieux, autant qu'ils le souhaitent sur leurs charmes, leur force, ou leur héroïsme, mais l'interrogateur ne peut pas leur demander de démonstrations pratiques.

Le jeu peut peut-être être critiqué sur la base que les chances sont trop désavantageuses contre la machine. Si l'homme voulait faire semblant d'être une machine, il se montrerait vraisemblablement très médiocre. Il serait mis en échec du premier coup par sa lenteur et ses erreurs en arithmétique. Les machines ne sont-elles pas capables de faire quelque-chose qu'on a l'habitude de nommer *penser* mais qui est très différent de ce qu'un humain fait ? Cette objection est une objection très forte, mais au moins, nous pouvons dire que si, néanmoins, une machine peut être construite pour jouer de façon satisfaisante au jeu de l'imitation, il ne faudrait pas être troublé par cette objection.

On doit souligner qu'en jouant au "jeu de l'imitation", la meilleure stratégie pour la machine peut possiblement être quelque-chose de différent de l'imitation du comportement humain. C'est possible, mais je pense qu'il est peu probable que cela ait un grand effet. Dans tous les cas, on n'a pas d'intention ici de faire des recherches en théorie des jeux, et on supposera que la meilleure stratégie est d'essayer de fournir des réponses qui seraient naturellement données par un humain.

3 Machines concernées par le jeu

La question que nous avons posée en 1 ne sera pas bien définie tant que nous n'aurons pas précisé ce que signifie le mot "machine." Il est naturel de vouloir autoriser toutes sortes de techniques d'ingénierie dans nos machines. Nous pouvons aussi souhaiter la possibilité que des ingénieurs puissent construire une machine qui fonctionne, mais qui ne peut être considérée comme satisfaisante car ses constructeurs ont utilisé une méthode qui est très expérimentale. Finalement, nous souhaitons exclure des machines les humains nés de la façon (biologique) habituelle. Il est difficile de cadrer les définitions de manière à satisfaire les trois conditions. On peut par exemple insister pour que l'équipe

d'ingénieurs soient tous du même sexe, mais cela ne serait pas vraiment satisfaisant, car il est possible de construire un individu complet à partir d'une seule cellule de peau (par exemple) d'un humain. Réaliser cela serait un exploit de technique biologique méritant les plus grandes louanges, mais nous ne saurions considérer cela comme un cas de "construction d'une machine pensante". Cela nous enjoint à abandonner la nécessité que tout type de technique puisse être permis. Nous sommes d'autant plus prêts à cela étant donné que l'intérêt actuel pour les "machines pensantes" a été motivé par une sorte particulière de machine, habituellement appelées "ordinateurs électroniques" ou "ordinateurs digitaux". Selon cette suggestion, nous n'autorisons que les ordinateurs digitaux à prendre part à notre jeu.

Cette restriction apparaît au premier abord comme étant très drastique. Je vais essayer de montrer qu'elle ne l'est pas en réalité. Faire cela nécessite une légère prise en compte de la nature et des propriétés de ces ordinateurs.

On peut aussi dire que cette identification des machines aux ordinateurs digitaux, selon notre critère qualifiant la "pensée" ne sera pas satisfaisant si (contrairement à mon sentiment), il s'avère que les ordinateurs ne se montrent pas bons dans le jeu.

Il y a déjà un certain nombre d'ordinateurs digitaux capable de travailler, et on peut se demander "Pourquoi ne pas tenter cette expérience ? Il serait facile de satisfaire les conditions du jeu. Un certain nombre d'interrogateurs pourraient être utilisés, et des statistiques pourraient être calculées qui compteraient le nombre de fois où l'identification aurait été correcte". La réponse rapide à cela est que nous ne nous demandons pas si tous les ordinateurs digitaux seraient capables de jouer à ce jeu, ni si les ordinateurs actuels pourraient le faire, mais si on peut imaginer des ordinateurs capables de le faire. Mais c'est seulement une réponse rapide. Nous verrons cette question sous un autre angle ultérieurement.

4 Ordinateurs digitaux

L'idée derrière les ordinateurs digitaux peut être expliquée en disant que ces machines sont destinées à prendre en charge toutes les opérations qui pourraient être effectuées par des calculateurs humains. Le calculateur humain est supposé suivre des règles fixées ; il n'a pas autorité à dévier d'elles dans le moindre détail. On peut supposer que ces règles sont fournies dans un livre, qui est modifié à chaque fois qu'une nouvelle tâche est à réaliser. Il a aussi une quantité de papier illimitée sur laquelle il peut faire ses calculs. Il peut aussi faire ses multiplications et additions sur une "calculatrice de bureau", mais cela n'a pas d'importance.

Si nous utilisons l'explication ci-dessus comme une définition, nous pouvons risquer

d'être confronté à un argument circulaire. On évite cela en donnant un aperçu des moyens par lesquels l'effet désiré peut être obtenu. Un ordinateur digital peut habituellement être vu comme constitué de 3 parties :

(i) la mémoire.

(ii) l'unité d'exécution.

(iii) le contrôle.

La mémoire stocke l'information, et correspond au papier du calculateur humain, que ce soit le papier sur lequel il fait ses calculs ou celui sur lequel son livre de règles est imprimé. Puisque l'humain peut effectuer une partie de ses calculs de tête, une partie de la mémoire de la machine correspond à cette mémoire du calculateur humain.

L'unité d'exécution est la partie qui effectue les opérations individuelles impliquées dans un calcul. Ce que sont ces opérations variera d'une machine à l'autre. Habituellement des opérations assez longues peuvent être effectuées comme "Multiplier 3540675445 par 7076345687" mais pour certaines machines, seules des opérations très simples comme "Ecris 0" sont envisageables.

Nous avons mentionné que le "livre de règles" fourni à l'ordinateur est stocké dans la machine dans une partie de sa mémoire. On appelle cette partie de la mémoire la "table d'instructions". C'est la tâche du contrôle de voir que ces instructions sont exécutées correctement et dans le bon ordre. Le contrôle vérifie que ces contraintes sont respectées.

L'information en mémoire est habituellement découpée en paquets de taille modérément petite. Dans une machine, par exemple, un paquet peut consister en dix unités décimales. Des nombres sont assignés aux parties de la mémoire dans lesquelles les différents paquets d'information sont stockés, de manière systématique. Une instruction typique peut dire :

"Ajoute le nombre stocké à la position 6809 à celui en 4302 et met le résultat obtenu dans cette dernière unité de mémoire utilisée."

Il est inutile de dire que cela ne sera pas stocké en machine en anglais courant. Ca a plus de chances d'être codé dans une forme comme 6809430217. Ici 17 dit quelle opération doit être faite sur les deux nombres. Dans ce cas, l'opération est celle décrite plus haut, i.e. "Ajouter les nombres...". On notera que l'instruction prend 10 chiffres et constitue ainsi un paquet d'information, de façon très pratique. Le contrôle prendra normalement les instructions devant être effectuées dans l'ordre dans lequel elles ont été stockées, mais occasionnellement, une instruction comme "N'exécute pas l'instruction à

la position 5606, et continue à partir de là" peut être rencontrée, ou à nouveau "Si à la position 4505, il y a un 0, exécute ensuite l'instruction stockée en 6707, sinon continue séquentiellement".

Les instructions de ces dernières sortes sont très importantes parce qu'elles rendent possible le remplacement d'une séquence d'instructions par une autre plusieurs fois de suite jusqu'à ce qu'une certaine condition soit remplie, et ce faisant, d'exécuter non pas les nouvelles instructions à chaque répétition, mais la même instruction plusieurs fois successives. Pour prendre une analogie domestique, supposons que Maman veuille que Tommy passe chez le cordonnier chaque matin lorsqu'il va à l'école pour demander si ses chaussures sont prêtes, elle peut le lui rappeler chaque matin. Alternativement, elle peut coller un papier une fois pour toutes dans le hall et il le verra quand il part à l'école et cela lui rappellera de demander pour les chaussures, et le post-it sera détruit quand Tommy reviendra avec les chaussures réparées.

Le lecteur doit accepter cela comme un fait que les ordinateurs digitaux peuvent être construits, et par exemple ont été construits, selon les principes que nous avons décrits, et qu'ils peuvent quasiment simuler les actions d'un calculateur humain.

Le livre de règles qu'utilise le calculateur humain dont nous avons parlé est bien sûr une fiction pratique. Les véritables calculateurs humains se rappellent vraiment ce qu'ils ont à faire. Si l'on veut qu'une machine simule le comportement d'un calculateur humain pour des tâches complexes, on doit lui demander comment il fait et ensuite traduire sa réponse en utilisant une table d'instructions. Construire des tables d'instructions est habituellement appelé "programmer". "Programmer une machine pour qu'elle fasse l'opération A" signifie mettre l'instruction appropriée dans la machine de manière à ce qu'elle exécute A.

Une variante intéressante à l'idée d'ordinateur digital est celle d'"ordinateur digital contenant un composant aléatoire". Ces ordinateurs ont des instructions impliquant un lancer de dé ou un processus électronique équivalent ; une telle instruction par exemple peut être "lancer le dé et mettre le nombre résultant dans la case mémoire 1000". Parfois une telle machine est décrite comme possédant un libre-arbitre (même si je n'utiliserai pas cette expression moi-même). Il n'est normalement pas possible de déterminer, en observant la machine, si elle contient un composant basé sur l'aléa, car un effet similaire peut être produit par les composants non aléatoires en rendant les choix dépendant des chiffres des formes décimales des nombres en jeu.

La plupart des ordinateurs digitaux actuels ont seulement une mémoire limitée. Il n'y a pas de difficulté théorique dans l'idée d'un ordinateur avec une mémoire illimitée. Bien sûr que seule une partie limitée de la mémoire peut être utilisée à tout instant,

puisque seulement une quantité finie de mémoire a pu être fabriquée, mais on peut imaginer qu'on en rajoutera de plus en plus lorsque ça sera nécessité. De tels ordinateurs ont un intérêt théorique spécifique et nous les appellerons ordinateurs de capacité infinie.

L'idée d'ordinateur digital est une idée ancienne. Charles Babbage, Professeur Lucasien de Mathématique à Cambridge de 1828 à 1839, avait conçu une telle machine, appelée le moteur analytique, mais il ne l'a jamais terminé. Bien que Babbage ait eu les idées principales, sa machine n'était pas à l'époque un projet très attractif. La vitesse qui aurait été atteinte par cette machine aurait définitivement été plus rapide que celle d'un calculateur humain mais quelque-chose comme 100 fois plus lente que la machine de Manchester, elle-même l'une des plus lentes des machines modernes. La mémoire devait être purement mécanique, et utiliser des roues et des cartes.

Le fait que le moteur analytique de Babbage soit complètement mécanique nous aidera à nous débarrasser d'une superstition. On attache souvent de l'importance au fait que les ordinateurs digitaux modernes sont électriques, et que le système nerveux est également électrique. Puisque la machine de Babbage n'était pas électrique, et puisque tous les ordinateurs digitaux sont en quelque sorte équivalents, nous voyons que cette utilisation de l'électricité ne peut pas avoir d'importance théorique. Bien sûr, l'électricité intervient lorsqu'on doit traiter des signaux rapidement, et ce n'est donc pas surprenant que nous la trouvions dans ces deux sortes de connexions. Dans le système nerveux, les phénomènes chimiques sont au moins aussi importants que les phénomènes électriques. Dans certains ordinateurs, le système de mémoire est principalement acoustique. Le fait d'utiliser l'électricité est ainsi vu comme une simple similarité superficielle. Si nous souhaitons trouver de telles similarités, nous devrions plutôt chercher des analogies mathématiques au niveau des fonctions.

5 L'universalité des ordinateurs digitaux

Les ordinateurs digitaux considérés dans la section précédente peuvent être classés parmi les "machines à états discrets". Ce sont des machines qui bougent par sauts ou clics d'un état parfaitement défini à un autre. Ces états sont suffisamment différents pour que la possibilité de confusion entre eux soit ignorée. De façon stricte, il n'y a pas de sous-machines. Tout va continûement dans la réalité. Mais il y a de nombreuses sortes de machines pour lesquelles il est profitable de les penser comme des machines à états discrets. Par exemple, pour les états d'un système lumineux, c'est une fiction pratique que d'imaginer le système soit comme complètement allumé, soit comme complètement éteint. Il doit y avoir des positions intermédiaires, mais dans de nombreux contextes, nous pouvons les oublier. Comme exemple de machine à états discrets, nous pouvons considérer une roue qui tourne 120 fois par seconde, mais qui peut être arrêtée par un levier de l'extérieur ; supposons en plus qu'une lampe doive être allumée lorsque la roue

est dans une certaine position. Cette machine pourrait être décrite abstraitement comme suit. L'état interne de la machine (qui est décrit par la position de la roue) peut être q_1, q_2 ou q_3. Il y a un signal en entrée i_0 ou i_1 (position du levier). L'état interne à tout moment est déterminé par l'état final et l'état d'entrée selon la table

		Etat final		
		q_1	q_2	q_3
Signal en entrée	i_0	q_2	q_3	q_1
	i_1	q_2	q_3	q_1

Les signaux de sortie, les seules indications visibles de l'extérieur de l'état interne (les lumières) sont décrites par la table

Etat interne	q_1	q_2	q_3
Sortie	o_0	o_0	o_1

Cet exemple est typique des machines à états discrets. Elles peuvent être décrites par de telles tables en supposant qu'elles n'ont qu'un nombre fini d'états possibles.

Il semble que selon un état initial donné de la machine et selon les signaux d'entrée, il soit toujours possible de prédire tous les états futurs. Cela rappelle le point de vue de Laplace selon lequel si l'on connaît l'état complet de l'univers à un instant temporel donné, comme décrit par les positions et vitesses de toutes les particules, on devrait pouvoir prédire tous ses états futurs. La prédiction que nous sommes en train de considérer ici, pourtant, est, cependant, bien plus proche de la prédictabilité que celle considérée par Laplace. Le système de l'"univers comme un tout" est tel que des erreurs plutôt petites dans les conditions initiales peuvent avoir un gros effet plus tard. Le déplacement d'un seul électron d'un billionième de centimètre à un moment peut faire toute la différence entre un homme tué par une avalanche un an après, ou bien en réchappant. C'est une propriété essentielle des systèmes mécaniques que nous avons appelées "machines à états discrets" que ce phénomène ne se produise pas. Même quand nous considérons de vraies machines physiques plutôt que des machines idéelles, une connaissance raisonnable de l'état à un moment donné amène une connaissance raisonnable de l'état quelques étapes plus tard.

Comme nous l'avons mentionné, les ordinateurs digitaux font partie de la classe des machines à états discrets. Mais le nombre d'états d'une telle machine peut être vraiment très grand. Par exemple, le nombre d'états pour une machine de Manchester est environ de $2\ 165,00$, i.e., environ $10 \times 50\ 000$. Comparons cela à notre exemple de la roue à clics décrite précédemment, qui a trois états. Il n'est pas difficile de voir pourquoi le nombre d'états pourrait être aussi grand. L'ordinateur contient une mémoire correspondant au papier utilisé par un calculateur humain. Il doit être possible d'écrire dans

la mémoire n'importe quelle combinaison de symboles qui pourrait avoir été écrite sur le papier. Pour des raisons de simplicité, supposons que l'on n'utilise comme symboles que les chiffres de 0 à 9. Les variations d'écriture sont ignorées. Supposons que l'ordinateur puisse avoir 100 feuilles de papier, chacune contenant 50 lignes de 30 chiffres chacune. Alors le nombre d'états des trois machines mises ensemble est $10\ 100 \times 50 \times 30$ i.e., 10 150 000. C'est à peu près le nombre d'états de trois machines de Manchester mises ensemble. Le logarithme en base 2 de ce nombre d'états est habituellement appelé la "capacité mémoire" de la machine. Ainsi, la machine de Manchester a une capacité mémoire d'environ 165 000 et la machine à roues de notre exemple a une mémoire de taille 1.6. Si deux machines sont mises ensemble, leurs capacités doivent être ajoutées pour obtenir la capacité de la machine résultante. Cela amène à la possibilité d'assertion comme "La machine de Manchester contient 64 barrettes magnétiques chacune d'une capacité de 2560, huit tubes électroniques avec une capacité de 1280. Des petits ajouts accessoires de mémoires s'élèvent à 300, ce qui fait un total de 174 380."

La table correspondant à la machine à états discrets étant donnée, il est possible de prédire ce qu'elle fera. Il n'y a pas de raison que ce calcul ne puisse pas être effectué par un ordinateur digital. Si l'on suppose qu'il peut l'effectuer assez rapidement, l'ordinateur digital devrait pouvoir simuler le comportement d'une machine à états discrets quelconque. On pourrait alors imaginer jouer au jeu de l'imitation avec la machine en question (comme B) et l'ordinateur digital simulateur (comme A) et l'interrogateur ne pourrait pas les distinguer l'un de l'autre. Bien sûr, l'ordinateur digital doit avoir une capacité mémoire adéquate et doit être en mesure d'exécuter ses instructions suffisamment rapidement. De plus, il doit être programmé à nouveau à chaque fois qu'on souhaite le faire simuler une nouvelle machine.

Cette propriété spéciale des ordinateurs digitaux, le fait qu'ils puissent simuler n'importe quelle machine à états discrets, est décrit en les désignant par l'expression "machines universelles". L'existence de machines avec cette propriété a comme conséquence importante que, les considérations de vitesse étant mises à part, il n'est pas nécessaire de concevoir de nouvelles machines variées pour réaliser des processus de calcul variés. Cela peut aussi être fait avec un ordinateur digital, chacun adéquatement programmé pour chaque cas. On verra qu'une conséquence de cela est que tous les ordinateurs digitaux sont équivalents dans un certain sens.

Nous pouvons maintenant considérer à nouveau le point mis en avant à la fin du §3. On avait suggéré conjecturalement que la question "Les machines peuvent-elles penser" soit remplacée par "Les ordinateurs digitaux imaginables pourraient-ils se débrouiller dans le jeu de l'imitation ?". Si nous le souhaitons, nous pouvons rendre cela plus général de façon artificielle et demander "Y a-t-il des machines à états discrets qui seraient capables de faire cela ?". Mais en regardant la propriété universelle, nous voyons que

l'une ou l'autre de ces questions est équivalente à celle-ci : "Fixons notre attention sur un ordinateur digital C. Est-il vrai qu'en modifiant cet ordinateur pour avoir une mémoire adéquate, et en augmentant adéquatement sa rapidité d'exécution, et en lui fournissant un programme adéquat, C peut être fabriqué de façon à jouer de façon satisfaisante la partie A du jeu de l'imitation, la partie B étant tenue par un humain ?".

6 Des vues différentes de la même question

Nous pouvons considérer maintenant que le socle a été clarifié et nous sommes prêts à débattre de notre question "Les machines peuvent-elles penser ?" et de la variante qui a été citée à la fin de la section précédente. Nous ne pouvons pas abandonner la forme originale du problème, car les opinions diffèreront sur le caractère approprié de la substitution des problèmes et nous devons au moins entendre ce qui doit être dit au sujet de cette relation.

Cela simplifiera les choses pour le lecteur si j'explique d'abord mes propres convictions sur le sujet. Considérons d'abord la forme la plus précise de la question. Je crois que dans cinquante ans environ, il sera possible de programmer des ordinateurs d'une capacité d'envison 109, pour les faire jouer au jeu de l'imitation de façon à ce qu'un interrogateur n'ait plus que 70 pour cent de chances de faire l'identification correcte après cinq minutes de questions/réponses. La question originale, "Les machines peuvent-elles penser ?", je la crois trop privée de sens pour mériter une discussion. Pourtant, je crois qu'à la fin du siècle, l'usage des mots et l'opinion éduquée en général aura tellement changé qu'on sera capable de parler de pensée des machines sans s'attendre à être contredit. Je crois même qu'on ne sert aucun but utile en cachant de telles convictions. L'idée populaire que les scientifiques avancent inexorablement d'un fait établi à un fait établi, en n'étant jamais influencés par aucune conjecture améliorée, est légèrement erronée. A partir du moment où l'on sait clairement ce qui constitue les faits et ce qui constitue les conjectures, il n'en résulte aucun préjudice. Les conjectures sont d'une grande importance puisqu'elles suggèrent les orientations utiles de la recherche.

Je vais maintenant considérer les opinions opposées à la mienne.

(1) L'objection théologique

Penser est une fonction de l'âme immortelle humaine. Dieu a donné une âme immortelle à chaque homme et à chaque femme, mais non pas aux animaux ou aux machines. De ce fait, aucun animal et aucune machine ne peut penser.

Je ne peux accepter aucun élément de l'argument ci-dessus, mais vais essayer d'y répondre en termes théologiques. Je trouverais l'argument plus convaincant si les animaux

étaient classés du côté des humains, parce qu'à mon sens, la différence entre l'inanimé et l'animé est plus grande que celle entre l'humain et les autres animaux. Le caractère arbitraire d'un tel point de vue orthodoxe devient clair si nous considérons la manière dont cet argument peut être perçu par un membre d'une autre communauté religieuse. Comment les Chrétiens regardent-ils l'opinion musulmane selon laquelle les femmes n'ont pas d'âme ? Mais laissons ce point de côté et retournons à l'argument principal. Il me semble que l'argument cité ci-dessus entraîne une sérieuse restriction à l'omnipotence du Tout-Puissant. Il est admis qu'il y a certaines choses qu'Il ne peut pas faire comme par exemple faire que un soit égal à deux, mais ne devrions-nous pas croire qu'Il a la liberté de donner une âme à un éléphant s'Il trouve cela approprié ? Nous pourrions nous attendre à ce qu'Il puisse exercer son pouvoir conjointement à une mutation qui pourvoierait l'éléphant d'un cerveau adéquatement amélioré pour gérer des besoins de ce type. Un argument du même type peut être utilisé dans le cas des machines. Il peut sembler différent parce qu'il est plus difficile à "avaler". Mais cela signifie seulement que nous pensons qu'il serait moins vraisemblable qu'Il considère les circonstances appropriées pour leur conférer une âme. Les circonstances en question sont discutées dans le reste de cet article. En essayant de créer de telles machines, nous ne serions pas irrespectueux en usurpant Son pouvoir de créer des âmes, de même que nous ne le sommes pas quand nous procréons et avons des enfants : nous sommes plutôt, dans les deux cas, des instruments de Sa volonté pour créer les réceptacles des âmes qu'Il crée.

Pourtant, ceci, c'est de la pure spéculation. Je ne suis pas très impressionné par les arguments théologiques, quel que soit ce qu'ils sont destinés à expliquer. De tels arguments se sont souvent avérés insatisfaisants par le passé. A l'époque de Galilée, il avait été dit que les textes, "Et le soleil dura alors... et ne descendit pas pendant une journée complète" (Josué 10 :13) et "Il a posé les fondations de la Terre, de manière à ce qu'elle ne bouge jamais" (Psaume 104) étaient une réfutation de la théorie de Copernic. Avec nos connaissances actuelles, un tel argument semble futile. Quand cette connaissance n'était pas encore acquise, cela a fait une impression plutôt différente.

(2) L'objection "la tête dans le sable"

"Les conséquences du fait que des machines pensent seraient trop horribles. Espérons et croyons qu'elles ne pourront jamais le faire."

Cet argument est rarement exprimé de manière si claire qu'il ne l'est ci-dessus. Mais il affecte beaucoup d'entre nous qui le pensent complètement. Nous aimons penser que l'Homme est en quelque sorte supérieur au reste de la création. Il est mieux qu'il puisse être vu comme nécessairement supérieur, car alors il n'y a pas de danger qu'il perde sa position dominante. La popularité de l'argument théologique est clairement reliée à ce sentiment. Il est vraisemblable qu'un tel avis soit très partagé par les intellectuels, parce

qu'ils considèrent le pouvoir de la pensée comme plus important que ne le font d'autres personnes, et ils sont donc plus enclins à baser leurs convictions sur la supériorité de l'Homme concernant cette possibilité.

Je ne crois pas que cet argument soit suffisamment substantiel pour nécessiter une réfutation. La consolation serait plus appropriée : peut-être qu'elle pourrait être recherchée dans la métempsychose.

(3) L'objection mathématique

Il y a un certain nombre de résultats de logique mathématique qui peuvent être utilisés pour montrer qu'il y a des limitations à ce que peuvent les machines à états discrets. Le plus connu de ces résultats est le théorème de Gödel (1931) qui montre que dans tout système logique suffisamment puissant, des assertions peuvent être formulées qui ne peuvent ni être prouvées ni être réfutées dans ce système, à moins que le système lui-même dans son ensemble ne soit démontré comme étant inconsistant. Il y a d'autres résultats, similaires à celui-là en quelque sorte, dus à Church (1936), Kleene (1935), Rosser, et Turing (1937). Le dernier résultat est le plus pratique à considérer, puisqu'il fait directement référence aux machines, alors que les autres peuvent seulement être utilisés dans un argument indirect : par exemple, si le théorème de Gödel doit être utilisé, on a besoin d'avoir en plus des moyens de décrire les systèmes logiques par rapport aux machines, et les machines par rapport aux systèmes logiques. Le résultat en question [1] fait référence à un type de machine qui consiste essentiellement en un ordinateur digital avec une capacité infinie. Il établit qu'une machine ne peut effectuer certaines tâches. Si une telle machine doit donner des réponses à des questions comme dans le jeu de l'imitation, il y aura des questions auxquelles soit elle donnera une réponse fausse, soit elle échouera à donner une quelconque réponse quel que soit le temps qui lui est alloué pour y répondre. Il peut, bien sûr, exister de nombreuses telles questions, et les questions auxquelles une certaine machine ne pourra pas répondre pourront cependant recevoir une réponse satisfaisante de la part d'une autre machine. Nous supposons là que les questions sont de type fermé, i.e. elles attendent comme réponse appropriée une réponse "Oui" ou "Non", plutôt que des questions ouvertes comme "Que pensez-vous de Picasso ?". Les questions dont nous savons que les machines doivent échouer sont de ce type. "Considérons les machines spécifiées comme suit... Cette machine répondra-t-elle "oui" à toute question ?". Les points de suspension doivent être remplacés par une description d'une machine de forme standard, qui pourrait être du type de celles qui ont été envisagées au §5. Quand la machine décrite partage une certaine relation comparativement simple avec la machine que l'on interroge, on peut montrer que la réponse est soit fausse soit ne vient jamais. C'est cela le résultat mathématique : on soutient qu'il prouve l'incapacité des machines qui n'ont pas un intellect humain.

1. *ndt* : le résultat le plus pratique

La réponse courte à cet argument est que même s'il est établi qu'il y a des limitations à la possibilité de penser pour une machine particulière, il a seulement été affirmé, sans aucune sorte de preuve, que de telles limitations ne s'appliquent pas à l'intellect humain. Mais je ne pense pas qu'un tel point de vue doive être rejeté si clairement. A chaque fois que l'on pose à une telle machine une question critique appropriée, et qu'elle fournit une réponse, et que nous savons que cette réponse est fausse, cela nous donne un certain sentiment de supériorité. Ce sentiment est-il illusoire ? C'est sans doute vrai, mais je ne pense pas que trop d'importance doive être accordée à cela. Nous donnons nous-mêmes trop souvent des mauvaises réponses à des questions pour être satisfaits que cela soit utilisé comme évidence de la faillibilité des machines. De plus, notre supériorité peut seulement se ressentir dans certaines occasions précises, en relation avec une machine spécifique contre laquelle nous avons enregistré un petit triomphe. Il ne saurait être question de triompher simultanément de toutes les machines. En bref, de ce fait, il se pourrait qu'il existe un humain qui soit plus intelligent que n'importe quelle machine, mais alors à nouveau, il y aura des machines plus intelligentes que lui, et etc.

Ceux qui croient en cet argument mathématique devraient, je pense, accepter la plupart du temps le jeu de l'imitation comme base de discussion. Ceux qui sont convaincus des deux objections précédentes ne seraient probablement intéressés par aucun critère quel qu'il soit.

(4) L'argument de la conscience

Cet argument est très bien exprimé par le Professeur Jefferson dans son discours d'obtention de la médaille Lister, dont je cite : "Pas avant qu'une machine n'ait écrit un sonnet ou composé une symphonie à cause d'émotions et pensées ressenties, et pas par le hasard de concordance de symboles, nous ne pourrons être d'accord sur le fait qu'une machine égale un cerveau humain, c'est-à-dire que non seulement cette machine écrit mais qu'en plus, elle sait ce qu'elle a écrit. Aucun mécanisme ne pourrait ressentir de plaisir lorsqu'il réussit (et pas seulement des signaux artificiels, des stratagèmes faciles), ne pourrait ressentir de difficulté quand ses vannes fusionnent, être réconforté par des flatteries, ou rendu misérable par ses erreurs, charmé par le sexe, en colère ou déprimé parce qu'il n'arrive pas obtenir ce qu'il veut.".

Cet argument semble être un déni de la validité de notre test. Selon une forme extrême de ce point de vue selon lequel le seul moyen d'être sûr qu'une machine pense est d'être une machine et de se sentir penser. On pourrait alors décrire ce qu'une machine ressent au monde, mais bien sûr personne n'aurait la possibilité de donner son avis. Selon ce point de vue également, le seul moyen de savoir si un homme pense est d'être cet homme particulier. C'est en fait un point de vue solipsiste. Il peut être le point de vue le plus

logique mais il rend la communication des idées difficile. A est susceptible de croire “A pense mais B ne pense pas” tandis que B croit “B pense mais pas A.”. Plutôt que de continuer à tergiverser éternellement sur ce point, il est habituel d'avoir la convention polie que tout le monde pense.

Je suis sûr que le Professeur Jefferson ne souhaite pas adopter le point de vue extrême et solipsiste. Il serait vraisemblablement prêt à accepter le jeu de l'imitation comme test. Le jeu (sans le joueur B) est fréquemment utilisé en pratique sous le nom de *viva voce* pour découvrir si quelqu'un comprend effectivement quelque-chose ou bien “répète cette chose comme un perroquet”. Ecoutons un tel extrait du jeu *viva voce* :

Interrogateur : Dans la première ligne de votre sonnet “Je te comparerai à une journée d'été”, est-ce qu'“un jour de printemps” serait aussi bien ou mieux ?

Témoin : Ca n'irait pas.

Interrogateur : Et “un jour d'hiver”, ça sonnerait bien.

Témoin : Oui, mais personne n'a envie d'être comparé à un jour d'hiver.

Interrogateur : Diriez-vous que M. Pickwick vous rappelle Noël ?

Témoin : D'une certaine manière, oui.

Interrogateur : Bien, Noël est un jour d'hiver, et je ne pense que M. Pickwick soit gêné par la comparaison.

Témoin : Je ne pense pas que vous ayez raison. Par un jour d'hiver, on entend un jour d'hiver basique, plutôt qu'un jour aussi spécial que le jour de Noël.

Et le tout à l'avenant... Que dirait le Professeur Jefferson si la machine à écrire des sonnets était capable de répondre ainsi au jeu de *viva voce* ? Je ne sais pas s'il considèrerait la machine comme “fournissant plutôt artificiellement” ces réponses, mais si les réponses étaient aussi satisfaisantes et soutenues que dans l'extrait ci-dessus, je ne pense pas qu'il la décrirait comme “un stratagème facile”. Cette phrase est destinée, je pense, à couvrir des mécanismes tels que l'inclusion dans la machine d'un enregistrement de quelqu'un lisant un sonnet, avec la possibilité appropriée de la mettre en marche de temps en temps.

En résumé donc, je pense que la plupart de ceux qui sont en faveur de l'argument de la conscience devraient être persuadés d'abandonner un tel point de vue plutôt que d'être forcés à prendre une position solipsiste. Ils souhaiteraient alors probablement accepter

notre test.

Je ne veux pas donner l'impression que je pense qu'il n'y a aucun mystère à propos de la conscience. Il y a, par exemple, quelque-chose de paradoxal lié au fait de souhaiter la localiser. Mais je ne pense pas que ces mystères aient nécessairement besoin d'être résolus avant que nous puissions répondre à la question à laquelle nous nous intéressons dans le présent article.

(5) Des arguments d'impossibilités diverses

Ces arguments sont de la forme "Je vous accorde le fait que vous puissiez fabriquer des machines qui font toutes les choses que vous avez mentionnées mais vous ne serez jamais capable d'en fabriquer une qui puisse faire X.". De nombreuses possibilités sont suggérées pour X dont je fournis une sélection :

Etre gentil, ingénieux, beau, amical, prendre des initiatives, avoir le sens de l'humour, dire ce qui est vrai ou pas, faire des erreurs, tomber amoureux, aimer les fraises à la chantilly, rendre quelqu'un amoureux de soi, apprendre de l'expérience, utiliser les mots à bon escient, être le sujet de ses propres pensées, présenter autant de variété dans son comportement qu'un être humain, faire quelque-chose de vraiment nouveau.

Aucun étayage pour soutenir ces assertions n'est en général fourni. Je crois que ces arguments sont la plupart du temps fondés sur le principe de l'induction scientifique. Un humain a vu des milliers de machines dans sa vie. De ce qu'il a vu d'elles, il tire un certain nombre de conclusions. Elles sont laides, chacune d'elle est conçue pour atteindre un objectif spécifique, si on a un autre objectif que celui-là, elles ne nous sont d'aucune utilité, la variété de comportement de toutes ces machines est très faible, etc., etc. Naturellement, il conclut que ces propriétés sont des propriétés nécessaires des machines en général. Beaucoup de telles limitations sont associées à la très faible capacité mémoire de la plupart des machines (je suppose que l'idée de capacité mémoire est étendue de façon à couvrir les machines autres que celles à états discrets. La définition exacte n'importe pas puisqu'aucune précision mathématique n'est revendiquée dans la présente discussion). Il y a quelques années, quand on avait encore peu entendu parlé des ordinateurs digitaux, il était possible d'éluder une telle incrédulité, si l'on mentionnait leurs propriétés sans décrire leur construction. Cela était sûrement dû à une application similaire du principe d'induction scientifique. Ces applications du principe sont bien sûr largement inconscientes. Quand un enfant qui s'est brûlé craint le feu et montre qu'il le craint en l'évitant, on pourrait dire qu'il applique une induction scientifique (je pourrais décrire son comportement de nombreuses autres façons). Les travaux et les habitudes des humains ne semblent pas être un matériau adéquat auquel appliquer l'induction scientifique. Une grande partie de l'espace-temps doit être étudié, si on souhaite ob-

tenir des résultats fiables. Sinon nous pourrions (comme le font la plupart des enfants anglais) décider que tout le monde parle anglais, et qu'il est idiot d'apprendre le français.

Il y a, cependant, des remarques particulières à faire à propos d'un certain nombre d'incapacités (des machines) qui ont été mentionnées. L'impossibilité d'aimer les fraises à la chantilly pourrait avoir semblé futile au lecteur. On pourrait fabriquer une machine pour apprécier ce met délicieux, mais toute tentative de faire cela semblerait débile. Ce qui est important dans cette incapacité, c'est qu'elle contribue à d'autres incapacités, e.g. à la difficulté qu'il y ait la même sorte d'amitié entre un homme et une machine qu'entre un homme et un autre.

L'argument "Les machines ne peuvent pas se tromper." semble curieux. On est tenté de rétorquer "Sont-elles pires de ce fait ?". Mais adoptons une attitude plus sympathique, et essayons de voir ce que l'on cherche réellement à dire par là. Je pense que cette critique peut s'expliquer selon le jeu de l'imitation. L'argument dit que l'interrogateur pourrait distinguer la machine de l'humain simplement en lui posant un certain nombre de problèmes d'arithmétique. La machine serait démasquée à cause de sa piètre compétence à les résoudre. La réponse à cela est simple. La machine (programmée pour jouer au jeu) n'essaierait pas de donner des réponses correctes aux problèmes arithmétiques. Elle introduirait délibérément des erreurs de manière à tromper l'interrogateur. Une erreur mécanique lui montrerait probablement à travers une décision inadéquate quelle sorte d'erreur faire dans un problème arithmétique. Même cette interprétation de la critique n'est pas suffisamment sympathique. Mais nous ne pouvons perdre de la place à entrer plus avant dans les détails. Il me semble que cette critique dépend d'une confusion entre deux sortes d'erreurs. Nous pourrions les appeler les "erreurs de fonctionnement" et les "erreurs de raisonnement". Les erreurs de fonctionnement sont dues à des défauts électriques ou mécaniques qui empêchent la machine de se comporter comme elle a été programmée à le faire. Dans les discussions philosophiques, on aime ignorer ces possibilités d'erreurs ; ce faisant, on discute de "machines abstraites". Ces machines abstraites sont des idées mathématiques plutôt que des objets physiques. Par définition, elles sont incapables d'erreurs de fonctionnement. C'est en ce sens qu'on peut dire que "les machines ne font jamais d'erreurs". Les erreurs de raisonnement peuvent quant à elles seulement advenir quand un sens est attaché aux signaux en sortie de la machine. La machine pourrait, par exemple, écrire des équations mathématiques, ou des phrases en anglais. Quand une phrase fausse est tapée, nous disons que la machine a fait une erreur de raisonnement. Il n'y a bien sûr aucune raison de dire qu'une machine ne peut jamais faire ce genre d'erreur. Elle pourrait ne rien faire et écrire sans fin "$0 = 1$". Pour prendre un exemple moins pervers, elle pourrait avoir une méthode pour trouver ses conclusions par induction scientifique. Nous pouvons nous attendre à ce qu'une telle méthode puisse parfois amener à des résultats erronés.

On peut répondre à l'argument selon lequel une machine ne peut être le sujet de sa propre pensée seulement si l'on peut montrer qu'une machine pense à certains sujets. Néanmoins, "Le sujet des opérations d'une machine" semble ne rien vouloir dire, au moins pour les personnes qui s'intéressent à un tel sujet. Si, par exemple, la machine essaye de trouver une solution de l'équation $x^2 - 40x - 11 = 0$, on peut être tenté de décrire cette équation comme faisant partie du sujet de la pensée de la machine à ce moment-là. Dans ce sens-là, une machine peut sans aucun doute être le sujet de sa propre pensée. Elle peut être utilisée pour mettre à jour ses propres programmes, ou pour prédire les effets des altérations de sa propre structure. En observant les résultats de son propre comportement, elle peut modifier ses propres programmes pour atteindre certains buts plus efficacement. Ce sont des possibilités de l'avenir proche, plutôt que des rêves utopiques.

La critique selon laquelle une machine ne peut pas avoir un comportement aussi diversifié est juste une manière de dire qu'elle ne peut pas avoir beaucoup de capacité mémoire. Jusqu'à assez récemment, une capacité mémoire d'un millier de digits était très rare.

Les critiques que nous considérons ici sont souvent des formes déguisées de l'argument concernant la conscience. Habituellement, si on maintient qu'une machine peut faire l'une de ces choses, et si l'on décrit le genre de méthode que la machine devrait utiliser pour ce faire, cela ne fera pas plus qu'une impression. On pense qu'une telle méthode (quelle qu'elle soit, car elle peut être mécanique) est vraiment plutôt basique. Comparer cela à ce qui est entre parenthèses dans l'assertion de Jefferson vue précédemment.

(6) L'objection de Lady Lovelace

L'information en notre possession la plus détaillée concernant le moteur analytique de Babbage est un mémoire d'Ada Lovelace (1842). Dans celui-ci, elle écrit "Le moteur analytique ne prétend pas *inventer* quoi que ce soit. Il peut faire *tout ce dont nous savons comment le lui ordonner*." (caractères en italique selon l'écrit original d'Ada Lovelace). Cette assertion est citée par Hartree (1949) qui ajoute : "Cela n'implique pas qu'il ne puisse être possible de construire un équipement électronique qui "penserait par lui-même", ou dans lequel, en termes biologiques, quelqu'un pourrait incorporer un réflexe conditionné, qui servirait de base à un "apprentissage". Que cela soit ou pas possible en principe est une question stimulante et excitante, suggérée par certains développements récents. Mais il ne semble pas que les machines construites ou projetées de l'être ont cette propriété.".

Je suis en profond accord avec Hartree sur cela. Il sera noté qu'il ne dit pas que les machines en question n'avaient pas cette propriété, mais plutôt que la conviction de Lady Lovelace ne l'encourageait pas à penser que les machines avaient cette propriété.

Il est assez possible que les machines en question avaient cette propriété dans un certain sens. Car supposons qu'une machine à états discrets ait cette propriété. Le moteur analytique était un ordinateur digital universel, et donc, si sa capacité mémoire et sa vitesse étaient adéquates, il aurait pu par programmation simuler la machine en question. Il est probable que cet argument n'ait pas été trouvé par la Comtesse ou par Babbage. Dans tous les cas, ils n'avaient aucune obligation de dire tout ce qui aurait pu être dit.

L'ensemble de cette question sera considéré à nouveau dans le paragraphe concernant les machines apprenantes.

Une variante de l'objection de Lady Lovelace affirme qu'une machine ne pourra "jamais faire quelque-chose de vraiment nouveau". On peut parer à cet argument par la litanie "Rien de nouveau sous le soleil". Qui peut être certain qu'un "travail original" qu'il a effectué n'était pas simplement la récolte d'une semaille qui a été plantée en lui lorsqu'il a reçu son enseignement, ou l'effet de principes généraux bien connus. Une meilleure variante de l'objection dit qu'une machine ne peut jamais "nous prendre par surprise". Cet argument est un défi plus direct et on peut le contrer directement. Les machines m'ont surpris très souvent. Cela est largement dû au fait que je ne fais pas suffisamment de calcul pour décider de ce que je dois attendre d'elles, ou plutôt parce que, même si je fais un tel calcul, je le fais à toute vitesse, d'une façon négligeante, en prenant des risques. Peut-être que je me dis à moi-même "Je suppose que le voltage ici doit être le même que là : bon, supposons que c'est le cas.". Bien sûr, j'ai souvent tort, et le résultat m'est une surprise car quand l'expérimentation arrive à son terme, j'ai oublié les suppositions que j'ai faites. Admettre cela me laisse ouvert pour écouter des conférences au sujet de ces mauvaises manières, mais ne laisse aucun doute sur ma crédibilité quand je témoigne de ces surprises que je rencontre.

Je ne m'attends pas à ce que cette réponse fasse se taire les points de vue critiques sur mon point de vue. On dira probablement que les surprises sont dues à une action mentale créative de ma part, et ne sauraient être attribuées à la machine. Cela nous ramène à l'argument de la conscience, et loin de l'idée de surprise. C'est une ligne d'argumentation que nous devons considérer comme fermée, mais il est peut-être pire de remarquer que l'appréciation de quelque-chose comme étant surprenant nécessite autant d'"action mentale créative", que l'événement surprenant ait été provoqué par un humain, un livre, une machine ou quoi que ce soit d'autre.

Le point de vue selon lequel les machines ne peuvent pas créer de surprises est dû, je pense, à une erreur que les philosophes et les mathématiciens font particulièrement souvent. C'est la supposition selon laquelle dès qu'un fait est présenté à un esprit, toutes les conséquences de ce fait germent dans l'esprit simultanément à ce fait. Cette supposition est très utile dans de nombreuses circonsctances, mais on oublie trop souvent qu'elle est

fausse. Une conséquence naturelle du fait de faire de la sorte est que l'on suppose alors qu'il n'y pas de vertu à traiter les conséquences des données et des principes généraux.

(7) L'argument au sujet de la continuité du système nerveux

Le système nerveux n'est certainement pas une machine à états discrets. Une petite erreur concernant l'information à propos de la taille de l'impulsion nerveuse en entrée d'un neurone peut engendrer une très grande différence sur l'impulsion en sortie. On peut arguer que, cela étant, on ne peut s'attendre à être capable de simuler le système nerveux par un système à états discrets.

Il est vrai qu'une machine à états discrets doit être différente d'une machine continue. Mais si nous nous plaçons dans les conditions du jeu de l'imitation, l'interrogateur ne pourra pas tirer avantage de cette différence. La situation peut être clarifiée si nous considérons une machine continue sonore la plus simple qui soit. Un analyseur différentiel sera parfait (un analyseur différentiel est une certaine sorte de machine qui n'est pas du type à états discrets et qui est utilisée pour certaines sortes de calculs). Certains d'entre eux fournissent leurs réponses sous une forme typée, et sont ainsi capables d'être utilisés dans le jeu d'imitation. Il ne serait pas possible qu'un ordinateur digital prédise exactement quelles réponses l'analyseur digital donnerait à un problème, mais il pourrait être capable de donner la bonne sorte de réponse. Par exemple, si on lui demande de donner la valeur de π (environ 3.1416), il serait raisonnable de choisir au hasard parmi les valeurs 3.12, 3.13, 3.14, 3.15, 3.16 avec les probabilités de 0.05, 0.15, 0.55, 0.19, 0.06 (disons). Dans ces circonstances, il serait très difficile pour l'interrogateur de distinguer l'analyseur digital de l'ordinateur digital.

(8) L'argument provenant du caractère informel du comportement

Il n'est pas possible de produire un ensemble de règles destinées à décrire ce qu'un homme devrait faire dans tout ensemble concevable de circonstances. On pourrait par exemple avoir une règle qui est qu'on doit s'arrêter quand on voit un feu rouge, et avancer quand on voit un feu vert mais que faire dans le cas où ils apparaissent tous les deux simultanément ? On peut peut-être décider qu'il est plus prudent de s'arrêter. Mais d'autres difficultés peuvent alors découler plus tard de cette prise de décision. Essayer de fournir des règles de conduite couvrant toutes les éventualités, même celles provenant des feux de la circulation, semble impossible. Avec tout ça, je suis d'accord.

A cause de ces raisons, on dit que nous ne pouvons pas être des machines. Je vais essayer de reproduire l'argument, mais je crains de ne pas lui rendre justice. C'est un peu quelque chose comme ça : "si tout homme avait un ensemble défini de règles de conduite par lesquelles il pouvait régenter sa vie, il ne serait rien de plus qu'une machine. Mais

de telles règles n'existent pas, et donc les hommes ne peuvent pas être des machines.". Le déséquilibre est flagrant. Je ne pense pas que l'argument soit jamais exprimé en ces termes, mais je crois que c'est cependant ce genre d'argument qui est utilisé. La confusion certaine entre les "règles de conduite" et les "lois de comportement" obscurcit le problème. Par "règles de conduite", je veux parler de préceptes tels que "Arrêtez-vous si vous voyez des feux rouges", que l'on peut faire, et dont on peut être conscient. Par "règles de comportement", je veux parler des lois de la nature telles qu'elles s'appliquent à un corps humain comme "si vous le pincez, il va crier". Si vous substituez "lois de comportement qui régentent sa vie" à "lois de conduite par lesquelles il régente sa vie" dans l'argument cité, le juste équilibre devient atteignable. Car nous croyons qu'il est non seulement vrai que voir son comportement commandé par des règles de comportement implique d'être une sorte de machine (même si cela ne signifie pas nécessairement être une machine à états discrets), mais qu'inversement, être une machine implique d'être régenté par de telles lois de comportement. Pourtant, nous ne pouvons pas nous convaincre aussi simplement de l'absence de lois pour tous les comportements possibles, ou de règles de conduite dans toutes les circonstances possibles. La seule manière que nous connaissions pour trouver de telles lois est l'observation scientifique, et nous ne connaissons sûrement aucun contexte dans lequel nous pourrions dire "Nous avons assez cherché. Il n'y a pas de telles lois.".

Nous pouvons démontrer de façon plus forte encore qu'une telle assertion serait injustifiée. Car supposons que nous soyons certains de trouver de telles lois si elles existaient. Alors étant donnée une machine à états discrets, il serait certainement possible de découvrir en l'observant suffisamment comment prédire son comportement futur et cela dans un temps raisonnable, disons mille ans. Mais cela ne semble pas être le cas. J'ai écrit un petit programme sur la machine de Manchester qui n'utilise que 1000 unités mémoire, et ce programme est tel que si l'on fournit à la machine un nombre à seize chiffres en renvoie un autre en deux secondes. Je défie quiconque d'en apprendre suffisamment sur ce programme en étudiant les réponses qu'il fournit, et d'être capable de prédire la réponse qu'il renverrait pour n'importe quelle valeur non déjà testée.

(9) L'argument de la perception extra-sensorielle

Je suppose que le lecteur est familier avec l'idée de perception extra-sensorielle (ESP), et qu'il connaît la signification des quatre termes suivants : la télépathie, la clairvoyance, la prescience et la psychokinèse. Ces phénomènes troublants semblent mettre en défaut toutes nos idées scientifiques habituelles. Comme nous aimerions les discréditer ! Malheureusement l'évidence statistique, au moins pour la télépathie, est accablante. Il est très difficile de réordonner les idées de quelqu'un pour que ces faits cadrent dans sa pensée. Une fois qu'on les a admis, ça n'a pas l'air d'être une grosse étape de plus que de croire aux fantômes. L'idée que nos corps bougent simplement selon les lois connues

de la physique, et de quelques autres idées non encore découvertes mais à peu près similaires, va être la première idée vers laquelle se diriger.

Cet argument est selon moi un argument assez fort. On peut dire en réponse à cela que de nombreuses théories scientifiques semblent rester applicables en pratique, malgré leur opposition aux idées de perceptions extra-sensorielles ; c'est en fait ce que l'on obtient très simplement, quand on oublie celles-ci. C'est plutôt confortable, et on craint que la pensée soit la seule sorte de phénomène où les ESP puissent être particulièrement pertinents.

Un argument plus spécifique basé sur les ESP pourrait être le suivant : "Jouons au jeu de l'imitation, en utilisant comme témoins un homme qui est un bon récepteur télépathe, et un ordinateur digital. L'interrogateur peut poser des questions comme "A quelle suite la carte dans ma main droite appartient-elle ?". L'homme par clairvoyance télépathique donnera la bonne réponse pour 130 cartes sur 400. La machine peut seulement deviner au hasard et elle obtiendra peut-être 104 bonnes réponses, et alors l'interrogateur fera la bonne identification.". Il y a une possibilité intéressante qui s'ouvre ici. Supposez que l'ordinateur digital contienne un générateur de nombres aléatoires. Alors il sera naturel qu'il utilise ce dispositif pour décider de la réponse à fournir. Mais alors le générateur de nombres aléatoires pourra être manipulé par les pouvoirs psychokinétiques de l'interrogateur. Peut-être que ces pouvoirs psychokinétiques pourraient permettre à la machine de répondre juste plus souvent que ce qui est attendu selon un calcul de probabilités, de telle façon que l'interrogateur ne soit plus capable de faire la bonne identification. D'un autre côté, il pourrait être capable de deviner correctement sans poser aucune question, par sa clairvoyance. Avec l'ESP, tout peut arriver.

Si on admet la télépathie, il sera nécessaire de resserrer nos tests. La situation devrait être regardée comme analogue à celle qui arriverait si l'interrogateur se parlait à lui-même et si l'un des compétiteurs écoutait avec son oreille collée au mur. Mettre les compétiteurs dans une "pièce pour preuve télépathique" satisferait toutes les contraintes.

7 Machines apprenantes

Le lecteur aura compris que je n'ai aucun argument convaincant de nature positive pour appuyer mon point de vue. Si j'en avais, je n'aurais pas fait tant d'efforts pour montrer la fausseté des points de vue contraires. Je vais exposer la conviction qui est la mienne.

Retournons un instant à l'objection de Lady Lovelace, qui exprime que la machine ne peut que faire ce qu'on lui dit de faire. On pourrait dire qu'un humain "injecte" une idée dans la machine, et qu'elle répondra en quelque sorte, et puis retournera dans le calme, comme une corde de piano frappée par un marteau. Une autre image similaire serait

celle d'une pile atomique avec moins d'énergie qu'une certaine dose critique : une idée qu'on lui injecte correspond là à un neutron entrant dans la pile de l'extérieur. Un tel neutron provoquera une perturbation certaine qui éventuellement n'aura aucun effet. Si, cependant, la taille de la pile est suffisamment augmentée, la perturbation causée par un électron entrant va continuer à augmenter jusqu'à ce que la pile entière soit détruite. Y a-t-il un phénomène correspondant pour les esprits, y en a-t-il un pour les machines ? Il semble y en avoir un pour l'esprit humain. La majorité d'entre eux semblent être "sous-critiques", i.e. correspondre à cette analogie des piles de taille sous-critique. Une idée présentée à un tel esprit va en moyenne donner naissance à une idée en retour. Une petite proportion d'entre eux sont super-critiques. Une idée présentée à un tel esprit donnera naissance à une "théorie" complète consistant en une idée secondaire, une troisième et d'autres plus éloignées. Les esprits des animaux semblent être définitivement sous-critiques. En adhérant à cette analogie, on se demande "Une machine peut-elle être rendue super-critique ?".

L'analogie de la "peau d'oignon" est aussi utile. En considérant les fonctions de l'esprit ou du cerveau, nous trouvons certaines opérations que nous pouvons expliquer en termes purement mécaniques. Nous disons que cela ne correspond pas à l'esprit véritable : c'est une sorte de peau que nous devons arracher si nous voulons trouver le véritable esprit. Mais là, nous trouvons une nouvelle peau, que nous devons arracher aussi, et etc. En procédant de cette manière, nous n'arrivons jamais au "véritable" esprit, ou bien est-ce que nous finissons par arriver à une peau qui ne contient rien ? Dans ce dernier cas, tout l'esprit est mécanique (ce ne sera pas pour autant une machine à états discrets. Nous avons déjà discuté de cela.).

Ces deux derniers paragraphes ne prétendent pas être des arguments convaincants. Ils devraient plutôt être décrits comme des "récitations tendant à produire une croyance".

Le seul appui réellement satisfaisant qui peut être donné au point de vue exprimé au début du §6, sera d'attendre la fin du siècle et puis de réaliser l'expérience décrite. Mais que pouvons-nous dire en attendant ? Par quelles étapes devrions-nous passer aujourd'hui si l'expérience devait s'avérer une réussite ?

Comme je l'ai expliqué, le problème est principalement un problème de programmation. Des avancées dans l'ingénierie devront avoir être effectives également, mais il ne semble pas qu'elles ne puissent pas permettre ce que l'expérience requiert. Les estimations de la capacité mémoire du cerveau varie de 10^{10} à 10^{15} unités binaires (bits). Je penche pour les valeurs les plus basses et je crois que seule une petite fraction est utilisée pour les types de pensées les plus hautes. La plupart de ces unités sont probablement utilisées pour retenir les impressions visuelles, je ne serais pas surpris si plus de 10^9 était nécessitées pour jouer de manière satisfaisante au jeu de l'imitation, à n'importe quel niveau contre

un homme aveugle (Note : la capacité de l'Encyclopaedia Britannica, $11^{\text{ème}}$ édition, est de 2×10^9). Une capacité mémoire de 10^7 serait une possibilité praticable même par les techniques actuelles. Il ne serait probablement pas nécessaire du tout d'augmenter les vitesses de traitement des opérations des machines. Des parties des machines modernes qui peuvent être regardées comme analogues aux cellules nerveuses travaillent environ mille fois plus vite que ces dernières. Cela fournirait une "marge de sécurité" qui pourrait couvrir la perte de vitesse pouvant advenir de multiples façons. Notre problème alors est de trouver comment programmer ces machines pour qu'elles puissent jouer au jeu. A mon niveau de travail actuel, je produis environ un millier de digits de code par jour, ce qui fait qu'environ soixante personnes, travaillant pendant cinquante ans pourraient accomplir le travail, si aucune ligne n'est jamais mise à la poubelle. Des méthodes plus expéditives semblent souhaitables.

Dans la tentative d'imiter l'esprit d'un adulte humain, nous devons forcément répondre au défi de comprendre le processus qui l'a amené à l'état dans lequel il est. Nous pouvons considérer trois composants :

(a) L'état initial de l'esprit, disons à la naissance,
(b) L'éducation à laquelle il a été soumis,
(c) L'expérience, différente de son éducation, qu'il a vécue.

Plutôt que d'essayer de produire un programme pour simuler l'esprit adulte, pourquoi ne pas plutôt essayer d'en produire un qui simule celui de l'enfant ? Si celui-ci était soumis à une éducation adéquate, il permettrait d'obtenir un esprit adulte. On présume que le cerveau de l'enfant est une sorte de carnet de note qu'on achète chez le papetier. Plutôt peu de mécanismes, et beaucoup de papier blanc (mécanisme et écriture sont de notre point de vue presque synonymes). Notre espoir qu'il y ait peu de mécanisme dans le cerveau de l'enfant permettrait de le programmer facilement. La quantité de travail d'éducation que nous pouvons supposer pour notre système doit être environ la même que celle nécessaire pour l'éducation d'un cerveau d'enfant, en première approximation.

Nous avons ainsi divisé notre problème en deux parties : la programmation du cerveau d'enfant et le processus d'éducation. Ces deux aspects restent très intimement connectés. Nous ne pouvons espérer trouver une bonne machine-enfant à la première tentative. On doit alors expérimenter l'enseignement à une telle machine et voir si elle apprend bien. On peut alors en essayer une autre et voir si elle est meilleure ou pire. Il y a une connexion évidente entre ce processus et l'évolution, par les identifications suivantes :

$$\begin{aligned} \text{Structure de la machine enfant} &= \text{matériau héréditaire} \\ \text{Changements dans la machine enfant} &= \text{mutation} \\ \text{Sélection naturelle} &= \text{jugement de l'expérimentateur} \end{aligned}$$

On peut espérer, cependant, que ce processus sera plus rapide que l'évolution. Le fait

que le test d'adaptation perdure est dû à un lent processus de mesure des avantages. L'expérimentateur, en exerçant son intelligence, devrait être capable de l'accélérer. Le fait que le processus ne soit pas restreint à des mutations hasardeuses est aussi important. Si l'on peut retrouver la trace de certaines faiblesses, l'expérimentateur pourra probablement penser aux sortes de mutations qui l'amélioreront.

Il ne sera pas possible d'appliquer exactement le même processus d'apprentissage à une machine qu'à un enfant normal. Elle n'aura pas de jambes, et on ne pourra pas lui demander de sortir et de remplir le seau à charbon. Il est possible qu'elle n'ait pas d'yeux. Mais pourtant, ces déficiences peut être surmontées par une ingénierie intelligente, on ne peut pas envoyer la créature à l'école, les autres enfants ne pourront pas trop jouer avec elle. On doit payer des frais de scolarité. On n'a pas besoin de trop se préoccuper de ces problèmes de jambes, d'yeux, etc. L'exemple de Mademoiselle Helen Keller montre que l'éducation est possible du moment que la communication est possible dans les deux sens entre l'élève et l'enseignant et qu'elle peut être assurée d'une manière ou d'une autre.

Nous associons habituellement des récompenses et des punitions au processus d'enseignement. On peut construire des machines enfants simples ou les programmer selon cette sorte de principe. La machine doit être ainsi construite que les événements qui précèdent l'arrivée d'un signal de punition ne doivent pas être répétés alors que la probabilité de répétition de l'occurrence d'événements qui ont précédé un signal de récompense augmentera. Ces définitions ne présupposent aucun sentiment de la part de la machine, j'ai fait quelques expériences avec une telle machine enfant, et j'ai réussi à lui apprendre quelques petites choses, mais la méthode d'enseignement était trop peu orthodoxe pour qu'on puisse considérer cette expérimentation comme un réel succès.

L'utilisation de punitions et récompenses peut être au mieux une partie du processus d'enseignement. Pour parler grossièrement, si l'enseignant n'a pas d'autre moyen de communiquer avec l'élève, le montant d'information qui peut l'atteindre n'excède pas le nombre total de punitions et de récompenses appliquées. Quand un enfant apprendra à répéter "Casablanca", il sera sûrement très endolori, si ce mot peut seulement être découvert par la technique des "Vingt questions", chaque lettre "o" occasionnant un coup. Il est nécessaire par conséquent d'avoir des canaux de communication "non émotionnels". Si ceux-ci existent, on peut enseigner à une machine par des punitions et des récompenses à obéir à des ordres exprimés dans un certain langage, e.g. un langage symbolique. Ces ordres doivent être transmis à travers des canaux "non émotionnels". L'utilisation de ce langage ne diminuera pas beaucoup le nombre de punitions et récompenses requis.

Les opinions peuvent varier au sujet de la complexité qui est appropriée pour la machine enfant. On pourrait essayer de la rendre aussi simple que possible de façon à

satisfaire les principes généraux. De façon alternative, on pourrait avoir un système complet d'inférences logiques "pré-construites". Dans ce dernier cas, la mémoire devrait être largement occupée par les définitions et les propositions. Les propositions auraient plusieurs sortes de statuts, e.g. le statut de faits bien établis, de conjectures, de théorèmes mathématiquement prouvés, d'assertions données par une autorité, d'expressions ayant la forme logique de propositions mais qui ne sont pas des croyances. Certaines propositions peuvent être décrites comme "impératives" (les consignes). La machine pourrait être construite de telle manière que dès qu'un ordre est classé comme "bien établi", l'action appropriée serait automatiquement effectuée. Pour illustrer cela, supposons que l'enseignant dise à la machine "fais tes devoirs maintenant". Cela pourrait avoir comme conséquence l'inclusion de "L'enseignant dit "Fais tes devoirs" " dans les faits bien établis. Un autre tel fait pourrait être "Tout ce que dit l'enseignant est vrai". Combiner ces faits pourrait finalement amener la consigne "Fais tes devoirs maintenant", parmi les faits bien établis, et cela, par construction de la machine, signifierait que les devoirs seraient alors effectués, et cet effet est très satisfaisant. Les processus d'inférence utilisés par la machine n'ont pas besoin d'être tels qu'ils satisfassent les logiciens les plus sévères. Il pourrait par exemple n'y avoir aucune hiérarchie des types. Mais cela ne signifie pas pour autant que des erreurs de type auront lieu, ni que nous allons tomber dans des pièges. Les consignes adéquates (exprimées dans les systèmes, ne faisant pas partie des règles du système) telles que "N'utilisez pas une classe à moins que ce soit une sous-classe d'une classe qui a été mentionnée par l'enseignant" peuvent avoir un effet similaire à "Ne vous approchez pas du bord".

Les consignes auxquelles une machine qui n'a pas de membres peut obéir sont de nature plutôt intellectuelles, comme dans l'exemple donné ci-dessus (des devoirs). Les consignes importantes de l'ensemble des consignes seront les consignes qui déterminent l'ordre dans lequel les règles du système logique concerné doivent être appliquées. Car à chaque étape de la mise en œuvre d'un système logique, il y a un grand nombre d'étapes alternatives, chacune d'entre elles pouvant être appliquée, du moment qu'elle obéit aux règles du système logique. Ces choix font la différence entre un système qui raisonne vite et un système qui raisonne lentement, et non pas la différence entre un système qui raisonne juste, et un système qui raisonne faux. Les propositions amenant à des consignes de cette sorte peuvent être "Quand Socrate est mentionné, utilise le syllogisme de Barbara" ou bien "Si une méthode s'est avérée plus rapide qu'une autre, n'utilise pas la méthode lente.". Certaines de ces règles peuvent être "données par l'autorité" mais d'autres peuvent être produites par la machine elle-même, e.g. par induction scientifique.

L'idée d'une machine apprenante peut sembler paradoxale à certains lecteurs. Comment les règles opératoires de la machine peuvent-elles être modifiées ? Elles devraient décrire complètement comment la machine réagira quelle que soit les événements auxquels elle est soumise, quels que soient les changements qu'elle peut subir. Les règles sont ainsi

assez indépendantes du temps. C'est presque vrai. L'explication du paradoxe est que les règles qui seront modifiées par le processus d'apprentissage sont plutôt d'un type moins prétentieux, et n'ont qu'une validité éphémère. Le lecteur pourrait faire un parallèle avec la Constitution des Etats-Unis.

Une propriété importante d'une machine apprenante est que son enseignant sera souvent ignorant de ce qui se passe à l'intérieur de la machine, bien qu'il soit cependant capable dans une certaine mesure de prédire le comportement de son élève. Cela devrait s'appliquer d'autant plus à l'éducation d'une machine qui était précédemment une machine enfant avec un entraînement bien conçu (bien programmé). Ceci est en contraste clair avec la procédure normale qui est que quand on utilise une machine pour faire des calculs, on a une image mentale claire de l'état de la machine à tout moment durant l'exécution du calcul. Cet objectif est difficile à atteindre. Le point de vue qu'"une machine ne peut faire que ce qu'on lui a ordonné de faire" semble étrange face à cela. La plupart des programmes que nous pouvons entrer en machine auront comme résultat qu'elle fera quelque-chose à quoi nous ne pouvons donner du sens (ou du moins, auquel nous attribuerons un sens complètement hasardeux). Se comporter intelligemment consiste justement à s'éloigner du comportement complètement discipliné tel que celui utilisé lorsqu'on effectue un calcul, et d'effectuer plutôt de légers changements, ce qui ne signifie pas pour autant de se comporter de manière aléatoire, ou de faire des répétitions sans fin. Une autre conséquence importante de la préparation de notre machine pour qu'elle puisse exécuter sa partie dans le jeu de l'imitation en la lui enseignant est que la "faillibilité humaine" sera vraisemblablement omise de façon assez naturelle, i.e. sans "coaching" particulier (le lecteur devrait réconcilier cela avec le point de vue de certaines des pages précédentes). Les processus appris ne produisent pas un résultat sûr à cent pour cent ; si c'était le cas, ils ne pourraient pas être désappris.

Il est probablement sage d'inclure un élément aléatoire dans la machine apprenante. Un composant aléatoire est assez utile quand on cherche une solution à un problème. Supposons par exemple que nous voulions trouver un nombre entre 50 et 200 qui soit égal au carré de la somme de ses chiffres. On peut commencer par 51, puis essayer 52 et continuer jusqu'à trouver un nombre qui marche. On peut alternativement choisir des nombres au hasard jusqu'à en trouver un correct. Cette méthode a comme avantage qu'il n'est pas nécessaire de garder trace des valeurs qui ont été testées, mais le désavantage c'est qu'on peut tester deux fois le même nombre, mais ça n'est pas important s'il y a plusieurs solutions possible. La méthode systématique présente le désavantage qu'il peut y avoir un énorme bloc de nombres successifs qui ne sont pas solutions dans la région qu'on testera en premier. Maintenant le processus d'apprentissage peut être vu comme la recherche d'une forme de comportement qui satisfera l'enseignant (ou bien satisfera un autre critère). Puisqu'il y a probablement un très grand nombre de solutions satisfaisantes, la méthode aléatoire semble être meilleure que la méthode systématique.

On peut noter qu'elle est utilisée dans le processus analogue de l'évolution. Mais là, la méthode systématique n'est pas possible. Comment pourrait-il être gardé trace des différentes combinaisons génétiques qui ont été essayées, de manière à éviter de les tester à nouveau ?

Nous pouvons espérer que les machines finiront par entrer en compétition avec les hommes dans des domaines purement intellectuels. Mais quels sont les meilleurs domaines par lesquels commencer ? Même si c'est une question difficile, beaucoup de personnes pensent qu'une activité très abstraite, comme le fait de jouer aux échecs, serait la plus adaptée. On peut aussi arguer qu'il serait plus judicieux de pourvoir les machines des meilleurs organes des sens que l'on peut payer, et d'alors leur apprendre à parler anglais. Ce processus pourrait être identique à celui par lequel on enseigne habituellement à un enfant. On montrerait les choses du doigt et on dirait leur nom, etc. A nouveau je ne sais pas quelle est la bonne réponse, mais je pense que les deux approches devraient être tentées.

Nous ne pouvons que regarder à une petite distance temporelle dans le futur, mais nous voyons là qu'il y a beaucoup de choses à faire.

Machines intelligentes, une théorie hérétique

A. M. Turing

"Vous ne pouvez pas faire qu'une machine pense pour vous". Ceci est un lieu commun qui est habituellement accepté sans questionnement. Ce sera l'objectif du présent article que de questionner cette phrase.

La plupart des machines fabriquées à des fins commerciales sont conçues pour effectuer une tâche très spécifique de façon sûre et extraordinairement vite. Très souvent, une telle machine fait la même série d'opérations de nombreuses fois sans aucune variété. Ce fait à propos des machines réelles est un argument puissant pour de nombreuses personnes de la phrase énoncée plus haut. Pour un mathématicien logicien, cet argument n'est pas valable, car il a été démontré qu'il est possible de fabriquer des machines qui feront quelque chose qui est très proche de la pensée. Elles pourront, par exemple, tester la validité d'une preuve formelle dans le système des *Principia Mathematica*, ou même dire d'une formule d'un tel système si elle est prouvable ou réfutable. Dans le cas où la formule n'est ni prouvable, ni réfutable,une telle machine ne se comportera vraisemblablement pas d'une manière très satisfaisante, car elle continuera à tourner indéfiniment, sans produire de résultat du tout, mais cela ne peut pas être considéré comme très différent comme attitude de la réaction des mathématiciens, qui ont par exemple travaillé des centaines d'années sur la question de savoir si le dernier théorème de Fermat est vrai ou faux. Dans le cas des machines de ce type, une sorte d'argument plus subtil est nécessaire. Par le fameux théorème de Gödel, ou par un argument similaire, on peut montrer que quelle que soit la manière dont une machine est construite, il y aura des cas où la machine échouera à donner une réponse, mais où un mathématicien pourra en donner une. D'un autre côté, la machine a certains avantages sur le mathématicien. On peut s'appuyer sur tout ce que la machine fait, si l'on suppose qu'il n'y aura pas de panne mécanique, tandis que le mathématicien commet parfois des erreurs, selon une certaine proportion. Je crois que ce danger du mathématicien faisant des erreurs est un corollaire inévitable de la possibilité qu'il utilise parfois de mettre en œuvre une méthode complètement nouvelle. Cela semble être confirmé par le fait bien connu que les personnes les plus fiables n'utilisent en général pas de méthodes vraiment nouvelles.

Ce que je prétends, c'est que des machines peuvent être construites qui simuleront la

Philosophia Mathematica (3) Vol. 4 (1996), pp. 256-260.
http://www.turingarchive.org/browse.php/B/4

Résumé. Dans cet essai posthume, Turing prétend qu'il pourrait être possible de construire une machine qui contiendrait un composant aléatoire et un analogue au principe de plaisir en psychologie, à qui on pourrait apprendre, et qui pourrait finalement devenir plus intelligente que les humains.

pensée humaine de façon très approchée. Parfois elles feront des erreurs, et parfois elles feront de nouvelles assertions très intéressantes, et globalement, les réponses qu'elles fourniront en sortie seront à première vue quasiment les mêmes réponses que celles fournies par un cerveau humain. Le contenu de mon assertion réside dans la grande fréquence attendue d'assertions vraies, et elle ne peut pas, je pense, être reçue comme une assertion vraie. Il ne pourrait pas, par exemple, être suffisant pour dire simplement qu'une machine exprimera une assertion vraie un jour ou l'autre, car un exemple d'une telle machine serait celui d'une machine qui exprime toutes les assertions un jour ou l'autre. Nous savons comment les construire, et comme elles devraient produire (probablement) des assertions vraies et des assertions fausses à peu près aussi fréquemment les unes que les autres, leurs verdicts seraient bien pire. Ce serait la réaction réelle de la machine aux circonstances qui prouverait ce que je prétends, si tant est qu'elle puisse être prouvée.

Voyons plus précisément la nature de cette argumentation. Il est clairement possible de fabriquer une machine qui fournirait un compte-rendu très précis à propos d'elle-même pour n'importe quel jeu de tests, si cette machine était suffisamment élaborée. Pourtant, ceci ne pourrait à nouveau que très difficilement être considéré comme une preuve adéquate. Une telle machine finirait par se perdre en faisant toujours la même sorte d'erreur encore et encore, et en étant quasiment incapable de se corriger elle-même, ou en étant corrigée par des arguments fournis de l'extérieur. Si la machine était capable d'une certaine manière d'"apprendre par expérience", ce serait beaucoup plus impressionnant. Si c'était le cas, il semblerait qu'il n'y ait aucune raison réelle pour que quelqu'un n'essaie pas de commencer avec une machine comparativement simple, et, en la soumettant à un certain nombre d'expériences adéquates, à la transformer en une autre machine qui serait plus élaborée, et qui serait capable de gérer un nombre plus élevé de contingences. Ce processus serait probablement accéléré par une sélection appropriée des expériences auxquelles la machine serait soumise. On pourrait appeler ce processus l'"éducation". Mais ici, nous devons être prudents. Ce serait assez facile d'arranger des expériences de telle manière qu'elles fassent que la structure de la machine se retrouve dans une forme particulière, et cela serait de façon évidente une grosse manière de tricher, presque autant que d'avoir un homme caché dans la machine. A nouveau ici, le critère exprimant ce qui devrait être considéré comme raisonnable en termes d'"éducation" ne peut pas être mis en termes mathématiques, mais je suggère que ce qui suit pourrait être considéré comme adéquat en pratique. Supposons que l'on souhaite que la machine comprenne l'anglais, et qu'elle n'ait ni mains ni pieds, et aucun besoin de se nourrir, aucun désir de cigarette, elle occupera son temps principalement à jouer à des jeux tels que les échecs ou le Go, et peut-être le Bridge. La machine est équipée d'un clavier de machine à écrire sur lequel on peut taper toute remarque qu'on souhaite lui faire, et elle écrit en retour toute chose qu'elle veut dire. Je suggère que l'éducation de la machine soit confiée à un maître d'école très compétent qui est intéressé par le projet mais à qui l'on n'a communiqué aucune connaissance détaillée du fonctionnement interne de la machine. Le mécanicien

qui a construit la machine, par contre, doit la maintenir en état de marche, et s'il suspecte que la machine n'a pas effectué ses tâches correctement, il a le doit de la remettre dans un état antérieur et de demander au professeur de répéter sa leçon à partir de cet endroit-là, mais il n'a pas le droit de prendre part en aucune manière au processus d'enseignement. Puisque cette procédure est uniquement destiné à tester la *bonne foi* de la mécanique, il faut que j'insiste sur le fait qu'elle ne pourrait pas être adoptée dans les étapes expérimentales. Comme je le vois, le processus d'enseignement serait en pratique essentiel à l'obtention d'une machine raisonnablement intelligente dans un intervalle de temps raisonnablement court. L'analogie humaine suggère cela.

Je peux maintenant donner quelques indications sur la manière de fonctionner que l'on peut attendre d'une telle machine. La machine devrait incorporer une mémoire. Cela ne nécessite pas beaucoup d'explication. Elle devrait consister en une liste de toutes les assertions qui existent pour elle ou bien qu'elle a faites, et de tous les mouvements qu'elle a faits, et de toutes les cartes qu'elle a jouées dans les jeux auxquels elle a participé. Tout ça sera listé dans l'ordre chronologique. Outre cette mémoire évidente, il y aura un certain nombre d'"index d'expériences". Pour expliquer cette idée, je suggèrerai la forme qu'un tel index pourrait prendre. Cela pourrait être un classement en ordre alphabétique des mots qui ont été utilisés en donnant l'"instant" auquel ils ont été utilisés, de telle manière qu'on puisse les retrouver dans la mémoire. Un autre tel index pourrait contenir les images des humains ou des parties des gobans qui auront été rencontrées. Aux périodes plus tardives de l'éducation, la machine pourrait être étendue pour inclure d'importantes parties de la configuration de la machine à tout moment, ou en d'autres termes, elle pourrait se rappeler quelles ont été les pensées qu'elle a eues. Cela donnerait naissance à de nouvelles formes d'indexation très fructueuses. Les nouvelles formes d'indexation pourraient être introduites en tenant compte de motifs spéciaux observés dans les index déjà utilisés. Les index seraient utilisés de la façon suivante : à chaque fois qu'un choix devrait être fait sur l'action à effectuer ensuite, les motifs de la situation présente seraient observés dans les index disponibles, et le choix précédent qui aurait été fait dans des situations similaires, et la sortie, bonne ou mauvaise, qui en aurait découlé seraient retrouvés.

Le nouveau choix sera fait selon toutes ces données. Cela entraîne un certain nombre de problèmes. Si certaines indications sont favorables et d'autres non favorables, que faire ? La réponse à cela diffèrera probablement d'une machine à l'autre et variera également en fonction du degré d'éducation de la machine. Initialement, probablement que quelques règles assez succinctes suffiront, e.g. faire l'action qui a le plus de votes en sa faveur. A un stade bien plus tardif de l'enseignement, la question entière de la procédure dans de tels cas aura probablement été étudiée par la machine elle-même, par les moyens d'une sorte d'index, et cela pourra résulter en quelque chose de beaucoup plus sophistiqué et, on espère, à des formes de règles bien plus satisfaisantes. Il semble probable pourtant

que les formes comparativement brutes des règles seront elles-mêmes raisonnablement satisfaisantes, de telle manière qu'un progrès global puisse être fait malgré le manque de précision du choix de règles. Cela semble être vérifié par le fait que les problèmes d'ingénierie sont parfois résolus de la manière la plus rustre par des procédures ad-hoc qui ne gèrent que les aspects les plus superficiels du problème, e.g. si une fonction croît ou décroît en l'une de ses variables. Un autre problème soulevé par cette image de la manière dont le comportement est déterminé est l'idée d'une "sortie favorable". Sans une telle idée, correspondant au "principe de plaisir" des psychologues, il est très difficile de voir comment procéder. Certainement qu'il serait plus naturel d'introduire quelques petites choses comme celles ci-après en machine. Je suggère qu'il pourrait y avoir deux clefs manipulables par le maître, et qui représente les idées de plaisir et déplaisir. A des stades ultérieurs de l'apprentissage, la machine reconnaîtrait certaines autres conditions comme étant désirables compte tenu du fait qu'elles auront par le passé constamment été associées au plaisir, et inversement, un certain nombre d'autres choses sont non désirables. Les expressions de colère de la part du maître pourraient, par exemple, être reconnues comme si déplaisantes qu'elles seraient négligées, de telle façon que le maître trouverait qu'il n'est plus nécessaire d'"employer la punition".

Faire de plus amples suggestions à propos de ces lignes serait probablement sans effets à ce niveau, dans la mesure où elles ne consisteront vraisemblablement en rien de plus qu'en une analyse des méthodes actuelles d'éducation appliquée aux enfants humains. Il y a, pourtant, une fonctionnalité dont j'aimerais suggérer qu'elle soit incorporée dans les machines, et c'est le "composant aléatoire". On devrait doter chaque machine d'une bande magnétique contenant une série aléatoire de figures, e.g., des 0 et des 1 à quantités égales, et cette série de figures devrait être utilisée dans les choix effectués par la machine. Cela aura pour conséquence que le comportement de la machine ne sera pas complètement déterminé par les expériences auxquelles elle a été sujette, et aura des utilisations précieuses quand on aura expérimenté ces nouvelles idées. En simulant les choix effectués, quelqu'un pourrait être capable de contrôler le développement de la machine dans une certaine mesure. On pourrait, par exemple, insister sur le fait que le choix effectué doit être un choix particulier, disons, en 10 endroits particuliers, et cela signifierait qu'une machine sur 1024 devrait se développer à un degré au moins aussi haut que celui qui aurait été simulé. Cela aura du mal à devenir une assertion précise à cause de la nature subjective de l'idée de "degré de développement" en ne disant même rien sur le fait que la machine qui avait été simulée aurait pu être aussi chanceuse dans ses choix non simulés.

Supposons maintenant, pour conforter l'argument, que ces machines soient une véritable possibilité, et regardons les conséquences de leur construction. Les construire effectivement devrait recontrer une grande opposition, à moins que nous n'ayions grandement avancé en terme de tolérance religieuse depuis le temps de Galilée. Il y aurait alors une

grande opposition des intellectuels, qui craindraient de perdre leur travail. Il est probable pourtant que les intellectuels se tromperaient à ce propos. Il y aurait beaucoup de choses à faire pour essayer, disons, de maintenir notre intelligence au niveau standard établi par les machines, car il semble probable qu'une fois que la méthode de pensée de la machine aura démarré, elle ne mettra pas longtemps à dépasser nos faibles possibilités. Il ne sera pas question de leur mort, et elles seront capables de converser les unes avec les autres pour aiguiser leurs esprits. Nous devons ainsi nous attendre à ce qu'à un moment, elles prennent le contrôle, comme cela est mentionné dans le livre de Samuel Butler *Erewhon*.

Les ordinateurs digitaux peuvent-ils penser ? (Alan M. Turing)

Les ordinateurs digitaux ont souvent été décrits comme des cerveaux mécaniques. La plupart des scientifiques regardent probablement ces descriptions comme de simples slogans journalistiques, mais d'autres non. Un mathématicien m'a exposé le point de vue opposé plutôt violemment en ces termes "On dit communément que ces machines ne sont pas des cerveaux mais vous et moi savons que c'en sont". Dans cet exposé, j'essaierai d'expliquer les idées derrière les différents points de vue possibles, mais je ne le ferai pas de façon impartiale. J'accorderai davantage d'attention au point de vue qui est le mien, qui est qu'il n'est pas déraisonnable de décrire les ordinateurs digitaux comme des cerveaux. Un point de vue différent a déjà été défendu par le Professeur Hartree.

D'abord, nous pouvons considérer le point de vue naïf de l'homme de la rue. Il entend des compte-rendus surprenants à propos de ce que ces machines peuvent faire : la plupart semblent avoir des capacités intellectuelles qu'il ne possède lui-même pas. Il ne peut l'expliquer qu'en supposant que la machine est une sorte de cerveau, même s'il préfère plutôt ne pas croire ce qu'il a entendu.

La majorité des scientifiques méprisent ces attitudes quasiment superstitieuse. Ils savent quelque-chose des principes sur lesquels ces machines sont construites et de la manière dont on les utilise. Leur organisation générale a été résumée par Lady Lovelace il y a une centaine d'années environ, lorsqu'elle a décrit le moteur analytique de Babbage. Elle dit, comme Hartree l'a citée "Le moteur analytique n'a aucune prétention à initier quoi que ce soit. Il peut faire tout ce qu'on lui ordonne de faire.". Ceci décrit très bien la manière dont les ordinateurs digitaux sont utilisés au jour d'aujourd'hui, et la manière dont ils seront principalement utilisés dans de nombreuses années à venir. Pour le moindre calcul, la totalité de la procédure que la machine va utiliser est planifiée à l'avance par un mathématicien. Moins il y a de doute sur ce qui va se produire, plus le mathématicien est content. C'est comme planifier une opération militaire. Dans ces conditions, on peut dire que la machine n'initie rien.

Il y a pourtant un troisième point de vue, qui est le mien. Je suis d'accord dans la mesure du possible avec l'énoncé de Lady Lovelace, mais je crois que sa validité dépend du fait de considérer la manière dont les ordinateurs digitaux sont utilisés plutôt que celle dont ils pourraient être utilisés. En fait, je crois qu'ils pourraient être utilisés de telle manière qu'on les décrirait adéquatement par le terme cerveaux. Je dirais également que "si une machine peut être décrite de manière appropriée comme un cerveau, alors tout ordinateur digital peut également être décrit ainsi".

---

15 Mai 1951.

http://www.turingarchive.org/browse.php/B/5

Cette dernière phrase nécessite d'être expliquée. Cela peut sembler surprenant, mais avec quelques réserves, cela semble inévitable. On peut montrer que cela découle d'une propriété caractéristique des ordinateurs digitaux, que j'appellerai leur universalité. Un ordinateur digital est une machine universelle au sens où elle peut remplacer toute machine d'un ensemble très grand. Elle ne remplacera pas un bulldozer ou une machine à vapeur ou un télescope, mais elle remplacera toute autre machine à calculer, c'est-à-dire toute machine dans laquelle on entre des données et qui plus tard renvoie des résultats. Pour que notre ordinateur imite une machine donnée, il est seulement nécessaire de le programmer pour qu'il simule ce que la machine en question aurait fait dans telles circonstances, et en particulier quelles données en sortie elle aurait fournies. L'ordinateur peut ainsi être programmé pour fournir les mêmes réponses.

Si maintenant une machine particulière peut être décrite comme un cerveau, nous n'avons qu'à programmer notre ordinateur pour l'imiter et ce sera aussi un cerveau. Si l'on accepte que les cerveaux réels, comme ceux des animaux, et en particulier ceux des humains, sont des sortes de machines, il en découlera que nos ordinateurs digitaux convenablement programmés se comporteront comme des cerveaux.

Cet argument implique un certain nombre de suppositions qui peuvent être raisonnablement défiées. J'ai déjà expliqué que la machine à imiter doit ressembler plutôt à une calculatrice qu'à un bulldozer. C'est seulement une réflexion au sens où nous sommes en train de parler d'analogues mécaniques des cerveaux, plutôt que des jambes ou des mâchoires. Il est aussi nécessaire que cette machine soit d'un genre dont le comportement peut être prédit par le calcul. Nous ne savons certainement pas comment un tel calcul devrait être fait, et il a même été expliqué par Sir Arthur Eddington que du fait du principe d'incertitude de la mécanique quantique, une telle prédiction n'est même pas possible théoriquement.

Une autre supposition était que la capacité de la mémoire de l'ordinateur devrait être suffisante pour prédire le comportement de la machine à imiter. Il faudrait aussi disposer d'une vitesse de calcul suffisante. Nos ordinateurs actuels n'ont probablement pas assez d'espace mémoire, bien qu'il soit possible qu'ils aient la vitesse de traitement appropriée. Cela signifie en effet que si nous souhaitons imiter quelque-chose d'aussi compliqué que le cerveau humain, nous avons besoin d'une bien plus grande machine qu'aucun des ordinateurs dont nous disposons actuellement. Nous avons vraisemblablement besoin de quelque-chose qui soit au moins cent fois plus grand que l'ordinateur de Manchester. Alternativement bien sûr, une machine de taille égale ou plus petite pourrait aller si des progrès suffisants étaient faits en termes de stockage de l'information.

Il faudrait noter qu'il n'est pas nécessaire d'augmenter la complexité des ordinateurs utilisés. Si nous essayons d'imiter des machines encore plus compliquées ou des cerveaux,

nous devons utiliser des ordinateurs de plus en plus gros pour le faire. Nous n'avons pas besoin d'en utiliser qui soient de plus en plus compliqués. Cela peut sembler paradoxal, mais l'explication n'en est pas difficile. L'imitation d'une machine par un ordinateur nécessite non seulement que nous ayons fabriqué l'ordinateur, mais également que nous l'ayons programmé de la façon appropriée. Plus la machine à imiter est compliquée, plus le programme doit l'être. Peut-être cela pourra-t-il être rendu plus clair par une analogie. Supposons que deux hommes veuillent écrire leur auto-biographie, et que l'un ait eu une vie pleine d'événements mais que très peu d'événements se soient produits dans la vie de l'autre. Il y aurait deux difficultés troublant l'homme avec une vie pleine, et qui le gêneraient plus que l'autre. Il lui faudrait plus de papier et il aurait plus de difficulté à décider de ce qu'il va écrire. Le fait de le pourvoir en papier ne semble pas être une difficulté sérieuse, à moins par exemple qu'il soit sur une île déserte, et dans tous les cas, ce ne serait qu'un problème technique et financier. L'autre difficulté serait plus fondamentale et deviendrait plus sérieuse encore si plutôt que d'écrire sa vie, il s'agissait d'effectuer un travail sur un sujet auquel il ne connaît rien, disons sur la vie sur Mars. Notre problème pour programmer un ordinateur pour qu'il se comporte comme un cerveau est quelque-chose qui ressemble à l'écriture de ce traité, et dans tous les cas, nous ne savons pas ce que nous devrions écrire si nous l'avions. C'est un piètre état de choses, mais, pour poursuivre l'analogie, il faudrait savoir quoi écrire, et apprécier le fait que la plupart des connaissances peuvent être incarnées dans les livres.

Au vu de cela, il semble que le plus sage étayage sur lequel critiquer la description des ordinateurs digitaux en tant que "cerveaux mécaniques" ou "cerveaux électroniques" est que, bien qu'ils puissent être programmés pour se comporter comme des cerveaux, nous ne savons pas à présent comment cela pourrait être fait. Avec cet argument, je suis en total accord. Il laisse ouverte la question de savoir si nous finirons par réussir ou pas à trouver un tel programme. Je pense par exemple probable qu'à la fin du siècle, il sera possible de programmer une machine qui répondra à des questions de telle manière qu'il sera extrêmement difficile de deviner si les réponses en sont données par un homme ou par une machine. J'imagine quelque-chose comme un examen de viva voce, mais avec des questions et réponses toutes tapées à la machine de manière à ce que nous n'ayons pas à considérer des éléments non pertinents comme la qualité avec laquelle la voix humaine peut être imitée. C'est seulement mon opinion ; il y a de la place pour de nombreuses autres opinions.

Il reste des difficultés. Se comporter comme un cerveau nécessite le libre-arbitre, mais le comportement d'un ordinateur digital, lorsqu'il a été programmé, est complètement déterministe. Ces deux faits devraient être réconciliés en quelque sorte, mais faire cela semble nous ramener à la controverse d'un autre âge du "libre-arbitre-et-déterminisme". On ne peut pas s'en sortir. Il est possible que l'impression de libre-arbitre que nous partageons tous ne soit qu'une illusion. Ou bien il est possible que nous ayons effecti-

vement un libre-arbitre, mais qu'il soit impossible de dire qu'il en est ainsi uniquement en observant notre comportement de l'extérieur. Dans ce dernier cas, aussi réaliste que soit la manière dont une machine pourra imiter le comportement humain, elle ne pourra être considérée que comme un simulacre. Je ne sais pas comment nous pourrons jamais décider entre ces deux alternatives mais quelle que soit l'alternative correcte, il est sûr qu'une machine sensée imiter un cerveau doit sembler se comporter comme si elle avait un libre-arbitre, et c'est aussi bien de se demander comment on pourrait faire ça. Une des possibilités est que son comportement dépende de quelque-chose comme une roulette ou un atome de radium. Le comportement de ces dispositifs pourrait sembler pouvoir peut-être être prédit, mais si tel est le cas, nous ne savons pas comment faire cette prédiction.

Il n'est, cependant, pas vraiment nécessaire de faire ça. Il n'est pas difficile de concevoir des machines dont le comportement semble assez aléatoire à quiconque ne connaît aucun détail de leur construction. Naturellement, l'inclusion de cet élément aléatoire, quelle que soit la technique utilisée, ne résoud pas notre problème principal, qui est de savoir comment programmer une machine pour imiter un cerveau, ou, comme nous pourrions le dire plus brièvement, même si c'est moins précis, pour *penser*. Mais cela nous donne une indication sur ce à quoi pourrait ressembler le processus. Nous ne devons pas nous attendre à toujours savoir ce que l'ordinateur va faire. Nous devrions être content si la machine nous surprend, de la même façon que nous sommes content lorsqu'un élève fait quelque chose que nous ne lui avons pas explicitement demandé de faire.

Reconsidérons maintenant l'énoncé de Lady Lovelace : "La machine peut faire tout ce dont on sait comment lui apprendre à le faire". Le sens du reste du passage est que l'on est tenté de dire que la machine ne peut faire que ce dont on sait lui expliquer comment le faire. Mais je pense que cela peut ne pas être vrai. Certainement que la machine ne peut faire que ce que nous lui ordonnons, si elle faisait autre chose, cela proviendrait d'un problème mécanique. Mais il n'est pas nécessaire de supposer cela, quand nous lui donnons ses ordres, nous savons ce que nous faisons, ce que les conséquences de ces ordres vont être. On n'a pas besoin de comprendre comment ces ordres vont amener la machine à avoir le comportement associé, ni de comprendre le mécanisme de germination quand on plante des graines dans le sol. La plante poussera qu'on le comprenne ou pas. Si nous donnons à la machine un programme qui résultera dans le fait qu'elle fera une chose intéressante que nous n'avions pas anticipée, je serais enclin à dire que la machine a initié quelque-chose, plutôt que de dire que son comportement était implicite dans le programme, et qu'ainsi l'originalité n'est que de notre fait.

Je n'essaierai pas d'en dire beaucoup sur la manière dont ce processus consistant à "programmer une machine à penser" doit être fait. Le fait est que nous n'en savons que très peu à ce sujet, et que très peu de recherche a déjà été faite. Il y a de nombreuses idées,

mais nous ne savons pas encore lesquelles sont importantes. Comme dans une histoire de détective, au début de l'enquête, tout détail peut être important pour l'enquêteur. Quand le problème a été résolu, seuls les faits essentiels doivent être racontés au jury. Mais à présent, nous n'avons rien à montrer devant un jury. Je dirai seulement cela, je crois que le processus sera très lié à celui de l'enseignement.

J'ai essayé d'expliquer quels sont les arguments rationnels principaux pour et contre la théorie selon laquelle on pourrait fabriquer des machines pensantes, mais il faut dire quelque chose à propos des arguments irrationnels. Beaucoup de personnes sont extrêmement opposées à l'idée qu'une machine puisse penser, mais je ne crois pas que ce soit pour aucune des raisons que j'ai mentionnées, ou pour une quelconque autre raison rationnelle, mais simplement parce qu'ils n'aiment pas cette idée. On peut voir de nombreuses caractéristiques qui rendent cette idée désagréable. Si une machine pense, elle pourrait penser plus intelligemment que nous ne le faisons, et alors où serions-nous ? Même si nous pouvons maintenir les machines dans une position d'esclaves, par exemple, en coupant leur alimentation à des moments stratégiques, nous pourrions nous sentir grandement humiliés en tant qu'espèce. Un danger et une humiliation similaire nous menacent lorsque nous envisageons la possibilité que nous puissions être remplacés par des cochons ou des rats. C'est une possibilité théorique qui est très controversée, mais nous avons vécu avec des cochons et des rats depuis si longtemps sans que leur intelligence n'augmente beaucoup, que nous ne sommes pas davantage troublés par cette possibilité. Nous ressentons que si ça devait arriver un jour, cela n'adviendrait pas avant quelques millions d'années. Alors que le nouveau danger semble plus proche. S'il advient, ce sera vraisemblablement au prochain millénaire. C'est dans un avenir lointain mais pas dans un avenir astronomiquement lointain, et c'est certainement quelque-chose qui peut nous rendre anxieux.

Il est coutumier, dans un exposé sur ce sujet, de fournir un peu de réconfort, en disant que quelques caractéristiques humaines particulières ne seront jamais imitées par une machine. On pourrait par exemple dire qu'aucune machine n'écrira jamais très bien l'anglais, ou qu'elle ne sera jamais attirée par le sexe ou ne fumera la pipe. Je ne peux pas fournir un tel argument réconfortant, car je crois qu'aucune telle limite ne peut être fixée. Mais j'espère certainement et je crois qu'aucun grand effort ne sera fait pour mettre en machine les caractéristiques les plus distinctives des humains, mais des caractéristiques non intellectuelles comme la forme du corps humain. Cela me semble assez stupide de faire de telles tentatives et leurs résultats ont quelque chose d'aussi déplaisant que lorsqu'on pense aux fleurs artificielles. Les tentatives de faire penser les machines me semblent d'un tout autre ordre. Le processus complet de la pensée humaine est encore plutôt mystérieux pour moi, mais je crois que la tentative de créer une machine pensante nous aidera grandement à trouver comment nous pensons nous-mêmes.

Qu'est-ce que les mathématiques modernes ?

Gustave CHOQUET

Première publication en 1962

Table des matières

Préface

Bourbaki et l'analyse

Malgré le sous-titre, je n'ai pas l'intention dans ce court texte de m'embarquer dans le projet fou d'essayer de lire l'esprit de Bourbaki, ce génie à plusieurs têtes.

Pourtant, puisque je suis concerné par la totalité de l'analyse, le traité de Bourbaki contenant des concepts si clairs et étant si étroitement lié au développement des mathématiques de notre temps, nous pouvons espérer que l'étude de "sa" philosophie et de "son" travail mathématique nous amènera à l'essence des tendances modernes en analyse.

Une telle étude peut servir à développer pour tous les niveaux de l'éducation un enseignement des mathématiques mieux adapté aux besoins de notre époque et au niveau de conscience de notre génération.

Chapitre 1

La méthode axiomatique

L'étude de l'histoire des mathématiques montre assez clairement que chaque période de recherche et d'extension est suivie d'une période de révision et de synthèse durant laquelle les méthodes plus générales évoluent et les fondations sont consolidées. C'est ainsi que la contribution de Descartes peut être regardée comme le point culminant d'une longue période de recherches apparemment diverses qui ont rendu possible la relégation dans les musées d'un grand nombre de procédures différentes pour l'étude des courbes et fonctions particulières et ont permis de les remplacer par une procédure plus universelle. Aujourd'hui, le nombre de chercheurs en mathématiques est si grand que les deux processus, recherche et synthèse, peuvent être menés simultanément. De plus, le travail de synthèse des cinquante dernières années, rendu possible par la théorie des ensembles et la terminologie proprement dite, a été particulièrement remarquable. On peut trouver cela clairement établi dans Bourbaki, et c'est ce que je voudrais étudier.

Pour Bourbaki n'existe qu'une MATHEMATIQUE, et l'instrument principal de son évolution vers l'unité était la méthode axio-

matique. Pour appliquer cette méthode à l'étude d'une théorie, le mathématicien "sépare les lignes principales de raisonnement qui figure dans la théorie, puis, prenant chacune d'elle isolément, il la considère comme un principe abstrait et il déduit d'elle ses conséquences naturelles ; alors, revenant à la théorie étudiée, il "recombine" les éléments précédemment considérés séparément et il voit comme ils interagissent les uns avec les autres." (Bourbaki trouve dans cette assertion une présentation plus structurelle de l'un des principes de base de la méthode de Descartes : diviser chaque difficulté en autant d'éléments que nécessaire pour la comprendre.

1.1 Structures

Les "lignes principales de raisonnement" sont les structures. Par exemple, l'ensemble $\mathbb{R}$ des nombres réels possède des structures variées : celle de groupe, celle de corps, celle d'espace vectoriel, celle d'ensemble ordonné et celle d'espace topologique. Inversement, une structure identique peut être retrouvée dans un certain nombre de théories distinctes. Par exemple, la structure de groupe trouvé dans l'étude de $\mathbb{R}$ est la structure de l'ensemble des entiers modulo p ou celle de l'ensemble de certains déplacements spatiaux.

Pour que l'étude d'une structure soit applicable à différentes théories, les ensembles considérés doivent nécessairement être généraux ; en particulier, la *nature* de leurs éléments ne doit pas intervenir, seules les *relations* entre eux importent. Ces relations

sont clairement établies par les *axiomes* définissant la structure.

Ainsi la structure d'ordre d'un ensemble arbitraire est une relation binaire sur S, dénotée $\prec$, qui satisfait les axiomes suivants ou postulats.

Pour tout x, y, z appartenant à S, on a

1) $x \prec x$
2) $(x \prec y \; et \; y \prec x) \implies (x = y)$
3) $(x \prec y \; et \; y \prec z) \implies (x \prec z)$

Quelques-unes de ces structures ont une signification plus fondamentale parce qu'on les rencontre dans toutes les théories. On les appelle des structures mères et elles incluent les structures associées à une relation d'équivalence, les structures d'ordre, les structures algébriques, les structures topologiques, etc.

Quand nous comparons les structures les unes aux autres, nous pouvons voir que certaines sont "plus riches" que d'autres. Ainsi les structures appelées groupes finis abéliens ou corps, sont plus riches que toute structure qui serait seulement une structure de groupe.

Certaines structures sont plus complexes parce qu'elles présentent plusieurs structures mères liées ensemble par des conditions de compatibilité. On les appelle structures multiples. Par exemple, un groupe topologique est un ensemble qui présente simultanément une structure de groupe et une structure topologique ren-

due compatible en stipulant que les opérations $(x, y) \longrightarrow x.y$ and $x \longrightarrow x^{-1}$ doivent être continues.

L'algèbre topologique et la topologie algébrique traitent des structures multiples ; la géométrie différentielle et l'algèbre différentielle considèrent des structures qui sont encore plus riches. Au sommet de l'édifice, on trouve les "structures carrefours" qui contiennent de très nombreuses structures. La théorie du potentiel est un exemple particulièrement représentatif d'une telle structure. C'est la multiplicité des structures mères trouvées dans de telles théories qui expliquent pourquoi des mathématiciens si différents les uns des autres leur trouvent autant d'intérêt : chaque pas en avant dans l'étude des structures constituantes a des répercussions sur la théorie dans son ensemble. Il est facile d'établir que le progrès dans la théorie du potentiel correspond aux progrès dans les autres théories comme l'intégration de Lebesgue, les espaces topologiques, les espaces vectoriels topologiques, la mesure de Radon, les groupes abéliens localement compacts, les distributions, etc., etc.

De telles structures sont le champ d'étude véritable de l'analyse et nous allons définir l'analyse comme l'ensemble complet des structures carrefours. Mais comme celles-ci n'ont pas été définies de façon rigide, notre définition de l'analyse ne fait qu'établir une hiérarchie.

Une théorie A sera classée comme appartenant davantage à l'ana-

lyse qu'une théorie B si les structures étudiées dans A sont plus riches que celles étudiées dans B.

L'analyse apparaît comme un univers dont la complexité rappelle celle de la vie elle-même. Alors que l'algèbre est un monde de minéraux dont les beautés sont celles de cristaux avec leurs formes pures, l'analyse est habitée d'êtres dont les formes sont aussi incertaines que celles des algues, des hydres ou des éponges ; c'est un monde exubérant plein d'opportunités où les explorations peuvent suivre l'un quelconque de multiples cours et où chacun peut laisser l'empreinte de sa personnalité dans la partie qu'il explore.

1.2 Caractéristiques de la méthode axiomatique

(a) *Economie de la pensée*

Les développements récents dans les mathématiques ou l'industrie montrent des analogies intéressantes ; la méthode axiomatique est analogue à une chaîne de production automatique ; les structures mères correspondent aux machines-outils.

La méthode axiomatique permet une économie de la pensée et de la notation, car les théorèmes importants nécessités sous différentes formes, dans différents contextes, sont établis une fois pour toutes dans un système d'axiomes suffisamment général de manière à leur faire inclure toutes les applications utiles. Dans ce système général de référence, la terminologie et la notation sont choisies pour s'adapter aux cas particuliers variés, et la préférence

est toujours donnée aux mots les plus suggestifs qui provoquent des résonances et stimulent l'intuition. Ce soin dans le choix des termes va de pair avec un souci de clarté dans la présentation ; les mathématiciens modernes ont développé un style précis et austère, et ne sont satisfaits que lorsque leurs articles consistent en un ensemble d'os nus de définitions, lemmes, théorèmes, corollaires et signes pour attirer l'attention (Ƨ).

(b) *La multivalence* : une garantie d'unité et d'universalité

Les premiers systèmes axiomatiques étaient catégoriques ou *univalents*, comme l'axiomatisation de la géométrie élémentaire par Euclide et par Hilbert, ou la définition des entiers par Peano. En contraste avec cela, les structures sont *multivalentes*, c'est-à-dire que les axiomes qui les définissent peuvent être appliqués à de vastes classes d'ensembles portant des structures non isomorphes.

C'est la multivalence qui est une garantie de l'adaptabilité aux situations les plus variées. Il s'ensuit de cela qu'il est parfois difficile de dire si une assertion appartient plutôt au domaine de l'algèbre, de la géométrie ou de l'analyse.

Ainsi, nous pouvons dire que la géométrie élémentaire de l'espace n'est rien d'autre que l'algèbre linéaire dans un espace vectoriel de dimension 3 sur lequel un produit scalaire est défini, et que l'étude des formes quadratiques dans cet espace est équivalent à l'étude des coniques du plan.

De façon similaire, étudier l'espace de Hilbert est, bien sûr, faire de la géométrie (puisqu'on parle là de sphères, d'angles, de perpendiculaires) mais il est égal de faire cela en algèbre ou en analyse.

Par exemple pour Henri Cartan, balayer en théorie du potentiel, c'est la même chose que projeter orthogonalement sur un cône convexe de l'espace de Hilbert. Plus généralement, bien que les ensembles convexes appartiennent à la géométrie, ils deviennent un des outils de base de l'analyse pour celui qui étudie les espaces.

Cette multivalence des grandes structures est donc un facteur unifiant qui permet un élargissement mutuel des différentes théories mathématiques. Un tel phénomène n'est pas nouveau. Nous avions déjà des exemples dans la représentation géométrique des nombres complexes ; la synthèse de l'algèbre et de la géométrie effectuée par Descartes ; l'utilisation que Monge avait fait de la géométrie dans sa recherche en analyse. Mais il a été permis à l'algèbre des ensembles et à son langage universel d'amplifier ce phénomène. Voici quelques exemples :

- la topologie de Zariski en géométrie algébrique.
- l'interprétation topologique et les démonstrations de nombreux théorèmes importants en logique.
- la théorie de Leray des paquets de fibres d'abord étudiés en géométrie algébrique mais qui envahissent maintenant l'algèbre et l'analyse.

(c) *Illumination mutuelle des entités mathématiques : dynamisme*

Il s'ensuit de cette multivalence que les entités isolées ne sont plus étudiées ; ce qui est étudié, ce sont les familles d'entités liées par des relations mutuelles. Non seulement les théorèmes acquièrent une plus grande généralité ce faisant, mais en même temps, chaque entité est individuellement mieux connue, puisque ces relations avec les autres entités font ressortir ses propres aspects variés. Ici aussi, ce qui est nouveau ce n'est pas l'utilisation d'un "contexte" mais la conscience du phénomène et de sa généralité.

Il est bien connu que la tangente d'une courbe en un point a été définie par une famille de sécantes ; que les fonctions analytiques d'une variable réelle deviennent mieux connues quand on les étudie dans le plan complexe, et que parfois les "familles normales" des fonctions analytiques ont été un outil puissant. Les mathématiques modernes sont "relationnelles " et cela leur donne leur dynamisme interne, celui-ci se réfléchissant dans un vocabulaire spécial et dans des signes typographiques spéciaux : fonctions, injections, jets, flèches, et schémas fléchés.

Une notation pratique et très suggestive a été produite pour indiquer les relations et les transformations.

$$x \longrightarrow f(x); A \longrightarrow \bar{A}; x \sim y; x < y; A \times B; \prod A_i; E/R; \text{ etc.}$$

Entre les mains des mathématiciens, les entités sont façonnées comme les pierres précieuses entre les mains du joaillier et cha-

cune des transformations qui est amenée révèle une nouvelle facette, un aspect inattendu.

Cet aspect relationnel des mathématiques est en accord avec le principe bien connu qui est que pour bien connaître une notion, on doit étudier ses formes et ses contraires. Il y a aussi accord sur le principe qui semble dominer toutes les investigations scientifiques modernes, i.e. que nous ne pouvons pas atteindre à l'"essence" des entités étudiées, mais seulement aux relations qu'elles entretiennent entre elles. Une expérience en physique ne révèle seulement que la relation entre l'univers et le système expérimental. Ce qui est essentiel dans un réseau téléphonique, ce n'est pas la nature des fils ou leur forme mais l'ensemble de ses connexions. Pour le mathématicien, deux ensembles structurés isomorphiquement sont équivalents.

La virtuosité avec laquelle les jeunes générations de mathématiciens se sont nourries aux nouvelles méthodes, utilisent le dynamisme des relations, et le plaisir qu'ils tirent de cela, semble prouver que ce dynamisme est bien adapté à la structure du cerveau humain.

(d) *Adaptabilité à l'univers physique*

Cette multivalence des théories est une garantie qu'elles aient de grandes possibilités d'être utilisées en physique. Ainsi, l'espace de Hilbert a servi à mieux interpréter les théories de champ quan-

tique ; la géométrie des espaces de Riemann et le calcul différentiel extérieur ont formé le cadre de la relativité générale. La physique théorique moderne elle-même développe maintenant ses propres structures : des faits fondamentaux sont pris comme postulats et de ces postulats sont déduites des conséquences dont on cherche alors les vérifications expérimentales. Naturellement, on comprend que les axiomes choisis correspondent à un seul aspect de l'univers physique.

(e) *Validation des notions qui sont devenues métaphysiques*

Un bon système axiomatique est assez souvent le seul moyen de se sortir de difficultés métaphysiques. Ainsi les nombres complexes ont perdu leur mystère et leur "absurdité" quand leur ensemble a été identifié à $\mathbb{R}^2$ auquel deux opérations adéquatement définies étaient associées. Plus récemment, les fondations de la théorie des probabilités étaient très brumeuses quand cette théorie était basée sur la théorie des jeux, la théorie des erreurs et la théorie stochastique. La théorie des probabilités a seulement ancré son unité et ses fondations fermes quand Kolmogorov lui a donné une présentation axiomatique. De ces axiomes, la théorie des probabilités apparaît comme une branche de la théorie de la mesure, mais une branche spéciale qui montre une grande vigueur, a son langage et ses problèmes propres et pourrait s'enrichir de nouveaux résultats de la théorie de la mesure tout en fertilisant l'analyse classique. Une brillante illustration de ce dernier fait peut être trouvée dans la relation étroite démontrée récemment qui existe

entre les processus de Markov et la théorie du potentiel.

1.3 Dangers de la méthode axiomatique

Bien que les systèmes axiomatiques soient les machines-outils des mathématiques, on comprendra facilement qu'ils ne présentent un intérêt que si leur résultat est correct. Il est assez facile de construire des systèmes axiomatiques, en modifiant légèrement des systèmes connus ; on constatera malheureusement qu'on en produit trop dans des thèses ou des articles. Leurs auteurs peuvent se régaler à les formuler et cela les amène à exagérer leur importance. Un grand nombre de ces vastes théories ont peu d'applications voire pas du tout. Une question urgente se pose alors : quels sont les systèmes axiomatiques utiles ?

Il n'y a probablement pas de critère absolu qui permettrait à quelqu'un de prendre une décision à ce sujet. Cependant, on sera d'accord sur le fait qu'on n'a pas besoin d'un tank pour tuer une mouche. Une théorie générale sera justifiée si elle révèle des liens insoupçonnés et fructueux entre des théories jusque-là considérées comme éloignées, ou si elle résoud un défi qui restait ouvert. Ce fait qu'une théorie soit générale n'entraîne pas forcément qu'elle sera utile, particulièrement si la lumière qu'elle projette est trop faible. Nous verrons plus loin avec quelles restrictions Bourbaki permettait à des théories d'avoir le droit d'exister. Mais il est intéressant de regarder les garde-fous qui auront protégé Bourbaki de succomber à la tentation de développer des systèmes axiomatiques comme des fins en soi.

Pour André Weil, “si la logique représente les règles d’hygiène pour un mathématicien, le pain quotidien qui assure sa subsistance est constitué par les grands problèmes”. C’est une autre façon de dire ce qu’Hilbert avait l’habitude de dire, “Une branche de la science est pleine de vie tant qu’elle a des problèmes en abondance ; l’absence ou le manque de problèmes est un signe de mort.”.

Hilbert est pour Bourbaki un modèle et presque une figure du père. Le fils recherche le père pour la simplicité élégante de ses articles “due au fait qu’il a tiré de rien, alors que personne n’avait été capable de le faire jusque-là, les principes fondamentaux qui ont rendu possible le fait de tracer la voie royale qui avait été jusqu’alors été cherchée en vain”. Il est le Maître de la méthode axiomatique, que l’on considère les structures univalentes (comme en géométrie élémentaire) ou les théories multivalentes, et il a appris aux mathématiciens à penser axiomatiquement. “Il ne tombe jamais dans le piège de certains de ses disciples de créer et élaborer une théorie pour quelques maigres résultats et il ne généralise jamais pour le plaisir de généraliser.” (Dieudonné). Il aime le problème particulier, précis et concret. C’est dans le but de résoudre de tels problèmes qu’il a créé des outils dont l’importance n’a pas diminué : la méthode directe dans le calcul des variations basée sur la semi-continuité pour résoudre le problème de Dirichlet ; la définition et l’utilisation des “espaces de Hilbert” pour résoudre les équations intégrales, etc., etc.

Les grands problèmes sur lesquels il a attiré l'attention des mathématiciens au congrès de 1900 ont continué à stimuler la recherche de façon très fertile. Aujourd'hui, par exemple, le problème de Riemann des zéros de la fonction ζ continue de provoquer un nombre très grand de tentatives d'en trouver une démonstration, même si la nature véritable du problème semble échapper à tout le monde.

Chapitre 2

Quelques outils de l'axiomatique

Un mathématicien moderne étudiant une structure est contraint d'utiliser des structures auxiliaires. Pour les construire, il a besoin d'un guide qui l'amène aux bonnes définitions. Nous allons maintenant examiner quelques-unes des procédures qui se sont montrées particulièrement efficaces et se sont avérées être de bons guides.

2.1 Morphismes

Une structure sur un ensemble S est définie par plusieurs axiomes exprimés en fonction des éléments de S et potentiellement des ensembles auxiliaires. La forme de ces axiomes définit ce qu'on appelle une *catégorie de structure* dont nous allons donner quelques exemples.

Les postulats pour la notion de groupe définissent une *catégorie*, les groupes commutatifs en forment une sous-espèce. Autres exemples : la catégorie des espaces vectoriels sur $\mathbb{R}$, celle des es-

paces topologiques compacts et celle des variétés différentielles.

Soient deux ensembles S et S' doté de structures de la même catégorie, alors une *bijection* (c'est-à-dire une correspondance un-pour-un) f de S dans S' est appelée un *isomorphisme* s'il échange les structures de S et S' d'une manière simple à établir dans chaque cas.

De façon plus générale, un morphisme de A dans B est une application de A dans B qui a des propriétés qui sont reliées à la structure. La définition des morphismes est telle que le produit de deux morphismes est aussi un morphisme et que si une bijection f de A dans B est un morphisme, ainsi que f^{-1}, alors f est un isomorphisme. Par exemple, pour les catégories de structures formées des espaces topologiques, la classe des applications continues forme une classe de morphismes ; les applications ouvertes (i.e. qui changent tout ensemble ouvert en un ensemble ouvert) forment aussi une autre classe de morphismes qui est non moins utile que celle des morphismes du premier type.

Soit A un ensemble, (B_i) une famille d'ensembles dotés d'une structure d'une catégorie donnée, et pour chaque i appelons f_i une application de A dans B_i. Une question qui se pose est : pouvons-nous doter A d'une structure de la même catégorie de telle manière que f_i soit un morphisme ? Sous certaines conditions, c'est possible et parmi toutes les solutions possibles, il y en a une qui est privilégiée et qui est appelée la *structure ini-*

tiale associée à (B_i, f_i). C'est la manière dont cela est utilisé, par exemple, pour la catégorie des espaces topologiques pour définir l'image réciproque d'une topologie, la topologie induite, sur un sous-ensemble d'un espace donné ; le produit d'une famille d'espaces topologiques.

Quand f_i est une application de B_i dans A, la solution du problème, si elle existe, est appelée la *structure finale* associée au (B_i, f_i) ; ceci est la manière dont on définit une topologie sur l'ensemble-quotient A d'un espace topologique B par une relation d'équivalence R.

2.2 Ensembles et applications universelles

Soit S et T deux catégories de structures, soit A un ensemble de catégories S ; donnons-nous une famille d'applications appelées (ST)-applications de A dans les ensembles de catégories T et une famille d'applications appelées T-applications des ensembles de catégories T dans les ensembles de mêmes catégories ; supposons aussi que ces familles sont transitives au sens où le produit d'une (ST)-application par une T-application est encore une (ST)-application et que le produit de deux T-applications est encore une T-application. La question alors est de trouver s'il existe un ensemble $\mathscr{B}$ de catégories T et une (ST)-application Φ de A dans B telle que toute (ST)-application (de A dans un B) peut être écrite comme $\psi = f \circ \Phi$ où f est une T-application de $\mathscr{B}$ dans B. Sous des conditions suffisantes très générales, ce problème a une solution et même une infinité de solutions non isomorphes.

Pour déterminer une solution unique, la condition suivante doit être ajoutée : l'image $\Phi(A)$ de A dans $\mathscr{B}$ est telle que deux T-applications de B dans un B qui coïncident dans $\Phi(A)$ coïncident aussi dans $\mathscr{B}$. L'espace B ainsi obtenu est appelé l'*espace universel* associé à A et Φ est appelé l'*application universelle* associée à A.

Exemples.

a) *Groupes compacts associés à un groupe topologique.*
A est un groupe topologique, T est la catégorie des groupes topologiques, les (ST)-applications et les T-applications sont formées par les homomorphismes arbitraires continus. On peut montrer qu'il y a identité entre les fonctions presque-périodiques définies sur A et les fonctions $\psi \circ \Phi$ où g est n'importe quelle fonction continue sur $\mathscr{B}$.
Cet exemple montre quel intérêt peuvent présenter les ensembles universaux pour l'analyse.

b) *Produit tensoriel de deux espaces vectoriels.*
A ici est le produit (cartésien) de deux espaces vectoriels S_1 et S_2 (sur le corps $\mathbb{R}_1$), T est la catégorie des espaces vectoriels sur $\mathbb{R}$; les (ST)-applications sont les applications bilinéaires définies dans $S_1 \times S_2$; les T-applications sont les applications linéaires. L'espace vectoriel universel $\mathscr{B}$ est appelé le produit tensoriel des espaces S_1, S_2 ; à travers lui, l'étude des applications bilinéaires définies dans $S_1 \times S_2$ est réduit aux applications linéaires définies dans $\mathscr{B}$.

Voici quelques autres ensembles universaux ;
- les structures algébriques libres,
- les anneaux et les corps de fractions,
- la complétion d'un espace uniforme,
- la compactification de Stone-Cech,
- les groupes topologiques libres,
- les variétés d'Albanese (en géométrie algébrique).

2.3 Catégories et foncteurs

Des vastes outils des mathématiques, la théorie des "catégories" est la plus récemment développée. C'est une plongée de plus dans l'abstraction, car les relations qu'elle considère ne sont plus des relations entre éléments d'un ensemble, mais des relations entre des entités d'une "catégorie" ou même de différentes catégories.

C'est presque miraculeux qu'une telle généralité ne soit pas synonyme de vide et de facilité. Mais en fait, la théorie est devenue un guide indispensable pour les jeunes générations de mathématiciens dans différents domaines.

Dans ce texte, nous nous contenterons de quelques exemples et de quelques définitions pour donner une idée de ce dont il est question.

Tous les groupes forment une catégorie.
Il en est de même de tous les espaces vectoriels,
tous les espaces topologiques,

tous les espaces ordonnés,
et plus généralement il y a la catégorie de tous les ensembles dotés d'une catégorie de structure sur lesquels existent des morphismes.

Ainsi une catégorie n'est pas un ensemble ; il est pratique de penser à elle comme à une classe d'objets qui est plus grande qu'un ensemble. Maintenant, appelons $\mathscr{C}$ une classe d'objets. A chaque $X, Y \in \mathscr{C}$, nous associons un *ensemble* dénoté $Hom(X, Y)$ dont les éléments sont appelés *homomorphismes* ou morphismes de X dans Y, et pour tout $X, Y, Z \in \mathscr{C}$, nous supposons l'existence d'une application $(f, g) \longrightarrow g \circ f$ (appelée la composition) de $Hom(X, Y) \times Hom(Y, Z)$ dans $Hom(X, Z)$. Nous dirons que $\mathscr{C}$ équipé de ses homomorphismes est une catégorie si les axiomes suivants sont remplis :

- K_1 : la composition est associative : $h \circ (g \circ f) = (h \circ g) \circ f$.
- K_2 : pour chaque $X \in \mathscr{C}$, il existe un élément e_x de $Hom(X, X)$ appelé l'unité de X et tel que $e_x \circ f = f$ et $f \circ e_x = f$ pour tous les homomorphismes f (quand ces expressions ont un sens).

Nous appellerons isomorphismes de X dans $Y (X, Y \in \mathscr{C})$ tout $u \in Hom(X, Y)$ tel qu'il existe $v \in Hom(Y, X)$ pour lequel $u \circ v = e_x$ and $v \circ u = e_y$.

Les relations entre les différentes catégories sont établies via les *foncteurs*. Soit $\mathscr{C}, \mathscr{C}'$ deux catégories et soit F une loi qui associe à tout $X \in \mathscr{C}$ un élément $X' \in \mathscr{C}'$, dénotée par $F(X)$ et supposons que, à tout $X, Y \in \mathscr{C}$ et à tout $u \in Hom(X, Y)$, F

associe $u' \in Hom(X', Y')$ (u' est dénoté $F(u)$).

F est un foncteur si

a) quand u est une unité alors $F(u)$ est une unité également,
b) pour tout u, v tel que $u \circ v$ a un sens $F(u \circ v) = F(u) \circ F(v)$.

De ces deux notions de catégories et foncteurs, il est possible de construire une algèbre qui devient plus riche lorsque les catégories sont spécialisées.

Montrons sur un exemple simple comment les catégories servent de guide.

De l'étude des catégories classiques "concrètes" dans lesquelles la notion de produit existe (ensembles ordonnés, groupes, espaces topologiques), on abstrait un schéma exprimable en terme de catégories générales, et ainsi la notion d'une *catégorie avec produit*. Si nous rencontrons une nouvelle catégorie concrète non encore dotée d'un produit, le schéma général indique non seulement si l'on peut définir ce produit mais également, il formule sa définition.

Pour résumer : nous avons juste considéré quelques outils de caractère très général ; d'autres existent tels que, par exemple, les séquences exactes et les diagrammes, qui sont constamment utilisés en algèbre et en topologie algébrique. L'utilisation de ces outils est inséparable d'un ensemble très précis de notations dont

le champ d'application est en constant élargissement. C'est un nouveau langage, proche du profane, mais clair et évocatif à l'initié. Bien sûr, ces outils ne sont pas des baguettes magiques et ne valent que ce que leur utilisateur vaut.

Chapitre 3

Les méthodes de découverte liées à la méthode axiomatique

Bien qu'aucun outil ne puisse engendrer des cadeaux s'il n'y en a pas, les outils peuvent considérablement augmenter l'efficacité quand ils existent. Nous avons étudié quelques-uns des outils de la méthode axiomatique, nous allons maintenant considérer quelques-unes des méthodes de découverte qui ne prennent leur plein sens que dans l'étude des structures multivalentes. Tout chercheur sérieux les découvre de lui-même mais il n'est pas sans intérêt de les rendre explicite.

3.1 Le relâchement des axiomes

Un certain analyste croit qu'une assertion s concernant une structure carrefour S définie par un certain nombre d'axiomes est correcte. L'assertion s a été formulée en termes simples qui continueront d'avoir un sens dans un autre système axiomatique S' moins riche en axiomes que S (cela ne signifie pas que l'assertion sera forcément vraie dans S'). L'analyste peut alors utiliser la méthode

suivante qui se réduit au "relâchement" de certains axiomes. Il essaiera de prouver s dans S' ; il y a très peu de combinaisons d'axiomes dans S' et cela peut aider à trouver la démonstration ; s'il a de la chance, soit il aura prouvé s dans S', et également dans S par conséquent, ou bien il aura trouvé dans S' un contre-exemple C réfutant s. Une étude attentive de C peut l'amener à formuler une propriété supplémentaire P qui ajoutée aux axiomes de S' lui permettra de prouver s. La seule chose qui restera à faire sera de revenir à S' pour voir si P pourrait être démontrée à partir de là. La preuve de s en découlera.

3.2 La contraction des axiomes

La méthode 1, a consisté à supprimer quelques axiomes du système S ; une autre méthode de recherche consiste à en ajouter de nouveaux, i.e. à étudier les cas particuliers.

Les axiomes supplémentaires permettront d'utiliser des outils qui n'étaient pas présents dans S ; de cette façon, nous obtenons des assertions inattendues et des preuves ; en retournant dans S, on essaie d'adapter les résultats obtenus à S.

Un cas particulier bien connu de cette méthode consiste à utiliser des modèles discrets ou finis. En théorie des probabilités par exemple, les processus de Markov doivent beaucoup à l'étude des processus sur les ensembles discrets ou finis. Dans la théorie du potentiel, l'étude des noyaux sur un ensemble fini révèle des phénomènes inexpliqués dans le cas général.

3.3 Etude de structures qui ne sont pas très différentes

Si l'on ne sait pas comment prouver un théorème T concernant une structure carrefour S, mais qu'il est possible de le prouver pour une structure S' avec des axiomes différant très peu de ceux de S, une grande partie des lemmes, grâce auxquels la preuve de T dans S' peut être établie, peuvent être également valides dans S. L'examen des autres peut amener à leur reformulation de façon à obtenir des assertions également valides dans S.

Ainsi, par exemple, puisqu'il n'est pas encore possible de prouver l'hypothèse de Riemann, on étudie les problèmes liées aux corps finis, en espérant être capable de transposer les résultats ainsi obtenus à la question classique, ou même de faire apparaître de tels cas comme des cas particuliers de l'un d'eux et du même problème arithmético-algébrique. Ainsi, un problème plus général peut être plus facilement démontré. L'histoire des mathématiques regorge d'exemples montrant qu'en se déplaçant au niveau de généralité adéquat, on gagne souvent en flexibilité et qu'ainsi, les sources secrètes des preuves sont rendues plus évidentes.

Il est cependant important quand nous ne pouvons pas résoudre un problème, de ne pas tomber dans le piège d'en résoudre des plus faciles et de croire qu'un progrès sur la question originale a été fait. De telles tentatives peuvent être d'excellents moyens de s'approcher du but, mais il est souvent préférable de ne pas les publier.

3.4 Génération de structures respectant certaines contraintes

La technologie de nos jours peut produire à la demande des machines-outils répondant à des exigences complexes. Nous ne sommes pas si loin de jours futurs où les chimistes seront capable de produire synthétiquement des fibres qui satisferont toutes les exigences du public. En mathématiques, la théorie des catégories nous montre comment il est maintenant possible de produire des structures qui auront toutes les propriétés requises pour telle ou telle question.

L'état d'esprit d'un jeune mathématicien n'est plus celui d'un constructeur en contact avec la matière ; il ne construit plus étape après étape, et brique après brique, les entités complexes dont il a besoin ; il demande seulement que ces entités entretiennent entre elles des relations mutuelles (et non contradictoires) ; elles forment ainsi une catégorie que l'on peut étudier par les méthodes ordinaires. La concrétisation des éléments d'une catégorie comme celle des ensembles dotée d'une certaine structure est l'une des dernières étapes d'une recherche.

Chapitre 4

Quelques caractéristiques de la contribution de Bourbaki à l'analyse

Nous avons examiné ci-dessus les outils et les principes ; considérons maintenant comment le groupe Bourbaki, ainsi que ses membres chacun individuellement, les ont utilisés pour effectuer leur travail.

4.1 Axiomatique et multivalence

En accord avec ses principes, Bourbaki montre une prédilection pour les structures multivalentes. Bourbaki aime les assertions générales. Il dit "quand ça ne coûte pas davantage, toute théorie produira le cadre le plus général possible". Ceci, même si cela permet de préserver de nombreuses idées, nécessite un gros effort de la part du lecteur.

Ainsi, non seulement les espaces vectoriels sont étudiés en relation à un corps arbitraire, mais à chaque fois que c'est possible, leur

étude est remplacée par celle des modules sur un anneau doté d'une unité (cela, bien sûr, force à adopter des définitions qui sont valides dans le cas général, par exemple, celle de produit tensoriel). De la même manière, des équations comme $x' = f(x,t)$ sont étudiées non pas dans les espaces de dimension finie mais dans des espaces normés et $f(x,t)$ est supposé être seulement Lipschitzien en x et réglé en t.[1]

4.2 Bourbaki est essentiellement un algébriste

Les initiateurs de Bourbaki avaient découvert l'algèbre en travaillant avec les grands algébristes allemands à une époque où l'algèbre moderne n'était pas connue en France. De ce fait, leur analyse est imprégnée d'algèbre et de notations algébriques : algèbres d'ensembles, bien sûr, mais également groupes, algèbres linéaires et multi-linéaires, dualité. Ils aiment les transformations et les propriétés qui sont décrites comme des relations algébriques. Quand une théorie considérée de façon classique comme appartenant à l'analyse peut être transformée en théorie algébrique en partie ou en totalité, Bourbaki n'oublie pas le plaisir de le faire.

Dans le passé, l'analyse était essentiellement l'étude des fonctions définies sur $\mathbb{R}$ ou $\mathbb{R}^n$ dont les valeurs appartenaient à $\mathbb{R}$ ou $\mathbb{R}^n$ ainsi que l'étude des opérateurs de différentiation et d'intégration. A présent, pour les Bourbakistes, $\mathbb{R}$ est principalement un corps commutatif de caractéristique zéro et cela semble assez souvent suffire. Quand Bourbaki travaille dans le corps des réels, il sait

1. Une fonction est dite réglée en t si elle est la limite uniforme de fonctions étagées.

que la seule chose à ajouter est qu'il est ordonné et localement compact.

Dans les mains de Claude Chevalley, l'étude des groupes de Lie ou des algèbres de Lie est libérée de tout élément extérieur : l'analyse joue là un rôle très restreint ; elle ne sert qu'à prouver l'existence d'entités dotées de telle ou telle propriété ou dans la définition de telle ou telle opération. Par exemple, pour la différentiation, on retient seulement le fait qu'elle soit une application d'une algèbre dans elle-même, satisfaisant identiquement la relation $D(x, y) = xD(y) + D(x)y$.

Dans les mains d'Henri Cartan, la théorie des fonctions de plusieurs variables complexes est purifiée : l'intégration reste l'outil fondamental mais Bourbaki l'étudie localement, dessinant à partir de lui les propriétés algébriques qui dorénavant sont les seules qui doivent être utilisées. Dans son excellente "*Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*", il préfère le point de vue de Weierstrass à celui de Cauchy et dans son chapitre I, il extrait de l'étude algébrique des séries formelles le maximum d'information à partir de leur composition, de leur inversion et de leur différentiabilité. Quand il étudie la théorie du potentiel, il préfère les outils algébriques : la formule de composition des noyaux ; l'interprétation de l'"opération de balayage" comme une projection orthogonale dans un espace de Hilbert.

4.3 Le renouvellement constant de l'Œuvre

Le monument de Bourbaki n'est pas un bilan du passé mais une construction vivante en constante évolution et tournée vers le futur. Bourbaki intègre dans son travail les développements récents qui se sont avérés démontrés, et à cause des nouvelles tendances, il est prêt à refondre complètement des branches même si elles sont d'une importance majeure (souvent découvrant, ce faisant, de nouveaux résultats inattendus et fascinants). Par exemple, les vieux livres du traité vont être refondus en utilisant les catégories, implicitement ou explicitement : des champs non séparés ont acquis droit de cité depuis que leur importance dans différentes théories (et en particulier en géométrie algébrique) a été découverte ; les équations différentielles partielles linéaires sont traitées en termes de distributions, convolutions et de transformations de Fourier et de Laplace.

D'un autre côté, Bourbaki montre sur certaines questions des phobies irrationnelles. Par exemple, il a une conception intéressante de la théorie de la mesure mais il est trop rigide en termes d'espaces localement compacts de convergence vague ; il relègue les mesures abstraites à la Chambre des horreurs, fermant par là la porte pour que ses disciples puissent aller du côté de la théorie des probabilités qui, même si elle n'a pas encore trouvé ses outils optimaux, fait vraiment la preuve d'une vitalité étonnante.

4.4 Choix des définitions

Une partie essentielle des efforts de Bourbaki consiste à trouver de bonnes définitions. Voici ce que les gens objectent au caractère excessivement déductif et formel de ce travail : Bourbaki établit les postulats et dessine les conséquences mais n'explique ni ses choix des axiomes, ni les théorèmes qu'il prouve. La raison est que l'histoire de ces choix serait trop longue. Quiconque a essayé de fournir l'axiomatique d'une théorie jusqu'ici confuse sait que les bonnes définitions sont seulement trouvées après un certain nombre de tentatives infructueuses et que ces tentatives devraient être jetées à la poubelle, de peur que l'on affaiblisse son esprit en retenant un certain nombre de théories axiomatiques similaires. La justification réelle pour une bonne théorie axiomatique est son succès.

Observons Bourbaki au travail sur un choix de définitions. Tandis que l'analyste classique commencerait à partir de définitions "naturelles" dans un certain contexte historique et déduirait des théories clefs de ces définitions, en les gardant comme elles étaient à l'origine et en allant de l'avant dans la théorie, Bourbaki changerait les définitions sous l'influence des théorèmes clefs. Il utiliserait les théorèmes clefs comme définitions si je peux utiliser une phrase imprécise mais expressive. Ceci est un des plus importants aspects de la *Bourbakization* des théories.

De façon plus précise, quand un théorème établit que les entités E définies par une définition D ont une propriété P qui se révèle

au cours du développement comme plus adaptable que D, ou qui reste valide sur un domaine plus grand que D et permet ainsi une plus large généralisation, Bourbaki donne à P le rôle dévolu précédemment à D en obtenant ainsi une définition de E équivalente à la première, mais plus gérable, ou un élargissement de la classe de E à laquelle la théorie est applicable.

Voici quelques illustrations de cette méthode fructueuse.

a) *Mesures de Radon.*

Un théorème dû à F. Riesz a prouvé que, sur $\mathbb{R}$, il y a identité entre les intégrales de Stieltjes (définies pour une fonction de variation localement limitée) et les formes linéaires continues de l'espace $\mathscr{H}(\mathbb{R})$ des fonctions numériques continues s'évanouissant à l'extérieur d'un compact.

Pris comme définition, cela fournit quelques avantages de la mesure de Radon sur la mesure ordinaire : l'extension immédiate non seulement à $\mathbb{R}$ mais également à tout espace localement compact ; une plus grande flexibilité dans l'étude des opérations sur les mesures (produit de mesures, images de mesures, etc.) ; les adaptations parfaites à la définition de la topologie faible de l'espace de mesures, qui s'est avérée être la plus adaptée de toutes les topologies de cet espace.

Il s'ensuit que la définition des mesures de Radon est maintenant

bien connue.

Les définitions qui précèdent ont montré que cette définition n'était pas adaptée au seul cas de l'intégration. Une mesure de Radon n'est rien d'autre qu'une forme linéaire continue sur un certain espace vectoriel topologique ; les nouvelles entités peuvent maintenant aisément être définies par le processus suivant. Soit V un espace topologique ; les formes linéaires continues sur V sont de nouvelles entités qui forment un espace vectoriel V' dual de V ; la théorie de la dualité, maintenant bien établie, fournira des topologies variées sur V' qui rendront plus facile l'étude de V. Cela donne un monde de possibilités. Mentionnons, comme exemples, les distributions de L. Schwartz, les courants de de Rham, les surfaces généralisées de L. C. Young.

b) *Mesures invariantes sur un groupe*

L'intégrale de Lebesgue sur $\mathbb{R}$ peut être définie par tout processus de continuation de l'intégrale de fonctions continues avec support compact ; sur l'espace $\mathscr{H}(\mathbb{R})$ de ces fonctions, c'est une forme linéaire J qui est positive au sens où $I(f) > 0$ pour tout $f > 0$ et est invariante par translation, au sens où $I(f) = I(g)$ quand g est obtenue de f par translation.

On peut montrer que toute fonction qui a ces propriétés ne diffère de l'intégrale de Lebesgue que par un coefficient constant. Par conséquent, la définition axiomatique de l'intégrale de Lebesgue

sur $\mathbb{R}$ (à facteur constant près) est : c'est une forme linéaire positive sur $\mathscr{H}(\mathbb{R})$ qui est invariante par rapport aux translations sur $\mathbb{R}$. Cette nouvelle définition est non seulement plus gérable parce qu'elle amène les propriétés de l'intégrale qui sont directement utilisables mais également parce qu'elle peut être immédiatement adaptée au cas des groupes arbitraires localement compacts.

c) *Fonctions mesurables*

En analyse classique, les applications mesurables de $\mathbb{R}$ sur $\mathbb{R}$ sont définies comme suit :

f est dite mesurable si pour tout nombre λ, l'ensemble des x tels que $f(x) < \lambda$ est mesurable (selon la mesure de Lebesgue).

Le théorème de Lusin démontre l'équivalence de cette définition avec la suivante : f est mesurable si, pour tout compact K de $\mathbb{R}$, et pour tout nombre $\epsilon > 0$, il existe un sous-compact K' de K tel que

(1) la mesure de $(K - K')$ est plus petit qu'ϵ ;
(2) la restriction de f à K' est continue.

La propriété impliquée dans cette seconde définition est à la fois suggestive et plus pratique dans un certain nombre d'applications. D'un autre côté, elle continue à avoir une signification intéressante quand on substitue pour la mesure une fonction sur l'ensemble plus générale, comme par exemple la capacité en théorie du potentiel. Finalement, elle est immédiatement utilisable dans la définition des applications mesurables d'un espace localement

compact (doté d'une mesure de Radon positive) dans un espace topologique arbitraire.

Cette seconde définition est donc préférable à la définition classique et devrait être adoptée.

4.5 Choix des contenus et théorèmes

Dans l'écriture de son traité, Bourbaki est forcé de faire des choix à tout moment. Nous avons juste vu comment il choisit ses définitions. Il est également très attentif quand il choisit le contenu de ses chapitres.

Son intérêt principal est dans les outils et seulement dans ceux qui ont particulièrement montré leur utilité. Les résultats élégants ou même les résultats profonds ne retiennent pas son attention s'ils sont des fins de théories ou s'ils conduisent à des impasses. Il abandonne, non concerné par des soucis de complétude, les notions qui sont proches de celles qu'il a jugées comme étant les plus fondamentales. S'il pense qu'une théorie n'est pas suffisamment mûre pour qu'un choix soit fait parmi ses différentes possibilités de fondations axiomatiques, il préfère attendre pour l'inclure que la théorie ait suffisamment mûri. Il n'a que peu de goût pour les hors-d'œuvres, pour l'embellissement ou pour les développements accidentels sans grande connexion avec le reste des mathématiques.

Il construit comme les Romains, solidement. Si la construction est

par chance, élégante, c'est dû à la beauté de sa propre structure ; par-dessus tout, il cherche la simplicité, la force, l'utilité, l'efficacité.

En topologie générale, suivant Haussdorf, il a fait un choix sobre parmi un labyrinthe de notions. Choix de postulats pratiques pour les espaces topologiques compacts ; choix d'une bonne notation pour la compacité ; l'introduction des filtres (H. Cartan) a simplifié la notion de convergence ; celle des espaces uniformes (A. Weil) a amené un certain nombre de notions qui jusque-là étaient considérées comme non reliées. Cette introduction des espaces uniformes a été plus tard justifiée quand les relations entre les espaces compacts et les espaces uniformes ont été découvertes.

En analyse fonctionnelle, il a été capable de mettre dans la bonne perspective les notions et les techniques consacrées par la dualité ; le théorème du graphe fermé ; le théorème de la séparation d'ensembles convexes ; les théorèmes de Krein et Milman et de Stone-Weierstrass.

Nous avons déjà mentionné son choix exclusif, dans la théorie de l'intégration, des mesures de Radon sur les espaces localement compacts, qui entre ses mains, sont devenus un outil remarquable. Dans les "volumes élémentaires", les questions classiques sont traitées avec un économie de moyens inhabituelle et une grande généralité. Le théorème des accroissements finis est donné pour les fonctions dont les valeurs appartiennent à un espace normé ; les

fonctions convexes sont traitées de façon élémentaire mais dans un style suffisamment complet pour satisfaire la plupart des besoins de l'analyse ; les primitives sont définies en référence aux fonctions réglées ; pour finir, nous avons déjà noté la généralité de son étude "élémentaire" des équations différentielles.

Chapitre 5

L'analyse moderne dans le monde d'aujourd'hui

J'ai exprimé au début de ce texte que l'étude des travaux de Bourbaki et des travaux de ses disciples donnerait une idée bonne et fidèle des tendances modernes en analyse.

Après un examen bref des caractères saillants de ces travaux, nous pouvons essayer de vérifier cette assertion en regardant ce qui est fait en analyse dans le monde entier. Dans ce but, ouvrons les "Mathematical Reviews". Environ deux tiers de ce qui est écrit pourrait encore l'être avec des outils qui existaient déjà il y a une trentaine d'années ; un bon nombre de ces articles ont de la valeur, certains contiennent des raisonnements profonds et ingénieux ;ils ont introduit des notions importantes et des outils ont été créés et testés dans un domaine spécialisé. Mais l'on peut se lamenter du fait que trop peu de rédacteurs ne semblent être au courant de l'existence d'outils basiques qui ont été complètement testés et qu'ils redécouvrent, avec ingénuité mais laborieusement, et dans un domaine restreint des cas particuliers de théorèmes

déjà connus.

Dans le tiers restant, les rédacteurs utilisent les outils modernes. Là, à nouveau, on trouve le gaspillage inévitable qui va de pair avec toute production scientifique ; trop d'articles sont peu profonds ou creux et n'ajoutent rien à la construction du "temple mathématique". Mais dans les meilleurs articles, les théories modernes montrent un rendement extraordinaire. Chaque année amène la solution d'un ou de plusieurs problèmes considérés comme inatteignables et voit des ponts créés entre des théories qui semblaient n'avoir rien en commun.

Voici une liste des branches les plus florissantes de l'analyse :

- Groupes topologiques et Théorie de Lie.
- Algèbre topologique.
- Mesure et intégration.
- Fonctions de plusieurs variables complexes et variétés analytiques (qui contiennent beaucoup de techniques algébriques, faisceaux de fibres, espaces filtrés).
- Equations différentielles partielles (dans lesquelles on utilise des distributions et d'autres fonctions généralisées ; étude du cas non linéaire).
- Théorie du potentiel (noyaux généraux, étude des principes et des relations avec la théorie des probabilités).
- Analyse harmonique sur les groupes généraux, fonctions de type positif.
- Analyse fcnctionnelle (espaces vectoriels topologiques locale-

ment convexes ; convexité ; théorie spectrale des opérateurs.)
- Topologie générale.
- Géométrie différentielle.
- Topologie différentielle.
- Théorie des probabilités.

Ces branches ont développé leur pleine vigueur en suivant les mêmes principes que Bourbaki ; le langage utilisé est le même. Dans les colloques spécialisés qui leur sont consacrés, les meilleurs des spécialistes utilisent les mêmes méthodes, le même langage, ont les mêmes préoccupations. Dans ses parties les plus actives, l'analyse moderne manifeste donc une grande unité.

Chapitre 6

L'impact sur l'enseignement des mathématiques modernes

Depuis des temps immémoriaux, l'enseignement a été adapté à l'évolution des connaissances. Mais cette adaptation a parfois été à la traîne, au grand détriment et de la science et de l'enseignement. Durant les cinquante dernières années environ, le progrès a été si rapide qu'un délai pour l'adaptation est devenu inévitable. En mathématiques, le "nouveau visage" résultant de l'utilisation de la théorie des ensembles et de la méthode axiomatique a été une révolution qui rend urgente une rénovation de l'enseignement à tous les niveaux : primaire, secondaire et universitaire.

La rénovation est nécessaire.

D'abord pour la santé des mathématiques elle-même. En effet, ce ne sont pas les vieilles personnes ou même celles d'un âge moyen qui produisent le meilleur travail ; il est impératif que nous clarifiions le chemin pour la jeune génération. De façon à ce qu'ils assimilent les mathématiques plus facilement, nous devons leur

montrer clairement les grandes idées simplificatrices, leur enseigner comment gérer les situations complexes en leur parlant des théories unificatrices, qui lancent des ponts entre différents domaines. Cela requerra un sacrifice et d'accepter d'abandonner cette théorie élégante ou cette autre, qui, polies par des siècles de travail, sont vues maintenant comme des branches isolées.

Secundo, pour les utilisateurs des mathématiques (qui sont chaque jour de plus en plus nombreux), d'un côté, un certain nombre de techniques mathématiques sont devenues indispensables ou utiles en physique et ingénierie : les matrices ; les transformées de Fourier et Laplace ; les équations différentielles partielles ; les distributions ; les espaces de Hilbert ; etc. D'un autre côté, les nouvelles mathématiques ont amené des simplifications et une économie de pensée à tous les domaines, dont le physicien et l'ingénieur peuvent bénéficier autant que le futur mathématicien.

Il est évident que les livres pour un tel renouvellement sont encore désirés. Complètement absorbés par leurs recherches, les mathématiciens professionnels ont laissé une faille profonde entre la recherche et l'enseignement. Mais dans les dix dernières années, effrayés par la vue du goufre grandissant, ils ont réagi. Ils ont commencé par changer leur manière d'enseigner, puis ils se sont tournés vers leurs collègues de l'enseignement secondaire et ils ont engagé des dialogues profitables avec eux. Ils ont encore besoin de rassembler leur courage pour une tâche urgente et essentielle. Le temps des simples critiques et des vagues indications est ré-

volu. Ils doivent maintenant s'asseoir et écrire les livres nécessaires ou aider leurs collègues, les techniciens, ou les enseignants du secondaire à les écrire. Le but n'est pas de recopier la production de Bourbaki qui a été conçue pour des étudiants avancés, mais d'adapter à chaque niveau d'âge les méthodes et les techniques des mathématiques d'aujourd'hui.

Tertio, pour ceux qui ne deviendront ni mathématiciens, ni utilisateurs de mathématiques, il est universellement reconnu que de l'étude de cette discipline, ils peuvent tirer une flexibilité intellectuelle qui ne peut être acquise autrement. Les mathématiques modernes donneront peut-être davantage à ceux-là qu'aux autres. Parce qu'elles n'utilisent pas trop de technique, ils peuvent apprendre la théorie des ensembles comme reliée à la logique et trouver cela attractif et utile. La simplicité des systèmes axiomatiques multivalents les rend accessibles à tous et comme elles ont un certain nombre d'applications variées, elles n'apparaîtront pas comme un simple jeu.

Il est hors de question de tenter ici de décrire un programme. Tout ce qui peut être fait est d'indiquer quelques principes qui découlent de l'examen que nous avons mené dans ce texte.

Habituons nos élèves à penser dès que possible en termes d'ensembles et d'opérations. A un très jeune âge, on pourra leur apprendre à utiliser le langage et l'algèbre des ensembles, car son symbolisme est simple et précis. Des expériences d'enseignement

ont montré que les élèves aiment l'utiliser.

Conjointement avec l'algèbre des ensembles, les éléments de logique peuvent leur être enseignés en connexion avec l'analyse grammaticale de leur propre langue naturelle. Il a été observé que des étudiants seniors de 19 ans sont incapables de raisonner, ne peuvent donner la négation d'une proposition, ni énoncer correctement une définition ou un théorème ; nous pensons que ceci est dû à un entraînement trop tardif à ce genre d'exercice.

Très tôt également, nos élèves doivent saisir la notion de fonction. Dans ce but, ils doivent avoir étudié et construit divers exemples provenant de la vie courante, de l'algèbre, de l'arithmétique, de la géométrie, de la physique, etc. Ils devraient savoir comment composer des fonctions, prendre la fonction réciproque d'une fonction mono-valuée, reconnaître une transformation ou un groupe de transformations. Progressivement, ils seront amenés aux structures plus vastes d'équivalence, d'ordre, et aux structures topologiques et algébriques. Ces structures peuvent être étudiées, à différents niveaux, dès le début de l'enseignement secondaire (à environ 12 ans).

Le but est de donner à nos élèves quelques outils et de leur apprendre à les utiliser. Nous devons éviter de nous perdre dans des généralités ; au contraire, nous devons nous diriger droit vers les théorèmes clefs qui incluent un grand nombre de théorèmes spécialisés avec des applications immédiates.

Par exemple, on trouvera très tôt en géométrie élémentaire la structure affine du plan ou de l'espace, et on utilisera l'algèbre des vecteurs. Après cela, d'une manière ou d'une autre, le produit scalaire peut être introduit et cela réduira les parties essentielles de la géométrie selon une mesure ordinaire à quelques calculs simples et peu nombreux.

De façon similaire, au niveau universitaire, les outils les plus puissants seront mis en lumière : les théorèmes sur les espaces compacts ; la mesure de convergence uniforme ; le théorème de Stone-Weierstrass ; la méthode des approximations successives, etc. : les étudiants devraient être entraînés à reconnaître quelles structures sont impliquées dans les assertions rencontrées ; cela présuppose que les définitions et les assertions utilisées mettent toujours l'accent sur les structures. Par exemple, l'intégrale de Lebesgue sur $\mathbb{R}$ peut leur apparaître à une certaine étape comme une forme linéaire positive sur $\mathscr{K}(\mathbb{R}^n)$, invariante par rapport aux translations ; le Laplacien doit apparaître comme le seul opérateur différentiel du second ordre invariant par rapport aux déplacements, etc.

Dans ce texte, beaucoup a été dit à propos des mathématiques en général, et peu à propos de l'analyse en particulier. La raison en est qu'il n'est plus possible de diviser l'enseignement des mathématiques en ses parties classiques que sont l'algèbre, la géométrie et l'analyse.

Les bases effectives pour l'enseignement de l'analyse même à un niveau scolaire sont l'algèbre (algèbres d'ensembles, étude du corps $\mathbb{R}$, algèbre linéaire, groupes) et la topologie. Les mêmes bases algébriques sont nécessaires à l'étude de la géométrie (qui signifie dans le secondaire aujourd'hui l'étude d'un espace vectoriel de dimension deux ou trois muni d'un produit scalaire).

Il devient donc essentiel de penser à un enseignement dont les éléments principaux seront les structures fondamentales. L'algèbre et la géométrie s'étaieront mutuellement, l'algèbre amenant son symbolisme et ses opérations, la géométrie amenant son langage chargé d'intuitions. La géométrie fournira à l'analyse son cadre topologique, l'outil de la convexité et une interprétation adéquate de l'intégration et de la différentiation ; l'analyse à son tour produira pour l'algèbre une collection riche de groupes et d'espaces vectoriels.

L'activité mathématique comme un tout

Peu a été dit ici à propos des méthodes de recherche et un peu plus a été dit à propos de la théorie mathématique déjà existante. Pour conclure cet examen des mathématiques entrepris dans le but d'aider à comprendre les problèmes rencontrés dans l'enseignement des mathématiques, ajoutons un mot supplémentaire à propos d'un aspect de l'activité mathématique dont on n'a pas parlé du tout.

Toute activité mathématique est formée de cycles, plus larges, dans lesquels on peut reconnaître essentiellement les quatre étapes suivantes : observation, mathématisation, déduction, applications.

Ces quatre étapes sont essentielles, en particulier un enseignement purement déductif serait traumatisant et stérile.

Chacune de ces larges étapes correspond à la conquête d'une nouvelle notion ; ces quatre étapes sont les étapes nécessaires qui permettent au cerveau de se restructurer et de s'élever d'un niveau de pensée à un autre. Ceci est aussi valable pour le chercheur que pour l'élève dont l'activité créatrice ne peut fonctionner à moins que nous ne le laissions suivre le chemin qui mène à la connaissance, et peut-être que nous l'aidions à suivre ce chemin.

Proposition de démonstration de la conjecture de Goldbach dans le formalisme des topos (Denise Vella-Chemla, 25.11.2019)

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 3). La définition première (en mathématique) du mot *fibre*, peut être trouvée dans le cours d'Alexander Grothendieck à Kansas ([1]) ou bien dans un extrait des EGA I (cf. Annexe 2).

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.

Dire que l'intersection des ensembles de la forme $\{\neg 0_{p_k} \wedge \neg n_{p_k}\}$ est vide, ce que l'on note $\bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \varnothing = \bot$ (le symbole $\bot$ est le symbole logique pour *False*), est équivalent à dire que le complémentaire de cet ensemble est le "plein" (dénoté par $\top$, ou *Vrai*), i.e. couvre l'ensemble de tous les impairs de 3 à $n/2$.

$$\complement \bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \bigvee_{p_k}\{0_{p_k} \vee n_{p_k}\} = \top$$

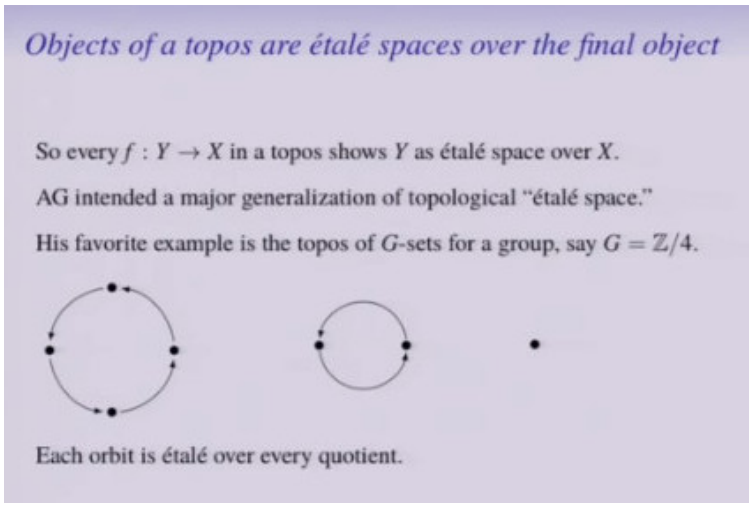
Mais on imagine bien qu'il existe au moins un nombre impair compris entre 3 et $n/2$ qui n'est pas congru à 0, tout en n'étant pas non plus congru à n selon un nombre premier p_k. Ce qui rend notre dernière assertion obligatoirement fausse, et la possibilité que l'intersection soit vide par là même.

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 4 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 : 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 3 : 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:

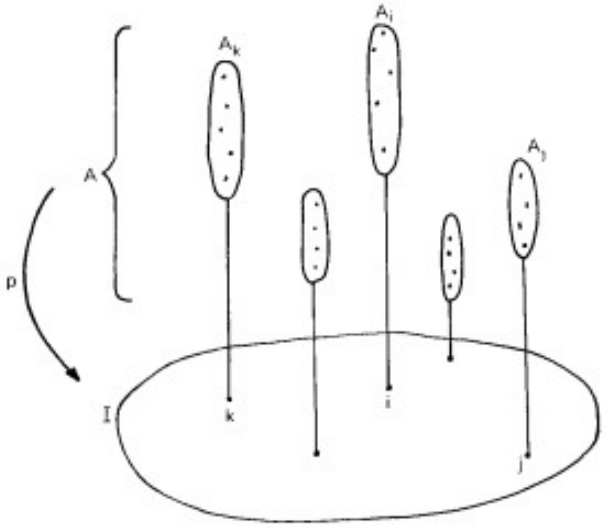


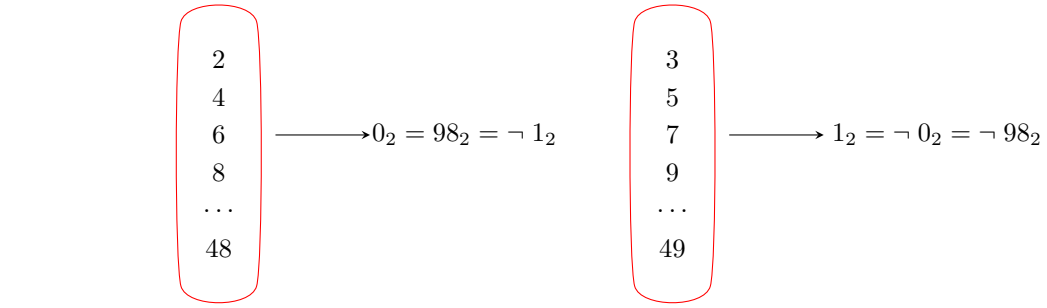
Fig. 4.4.

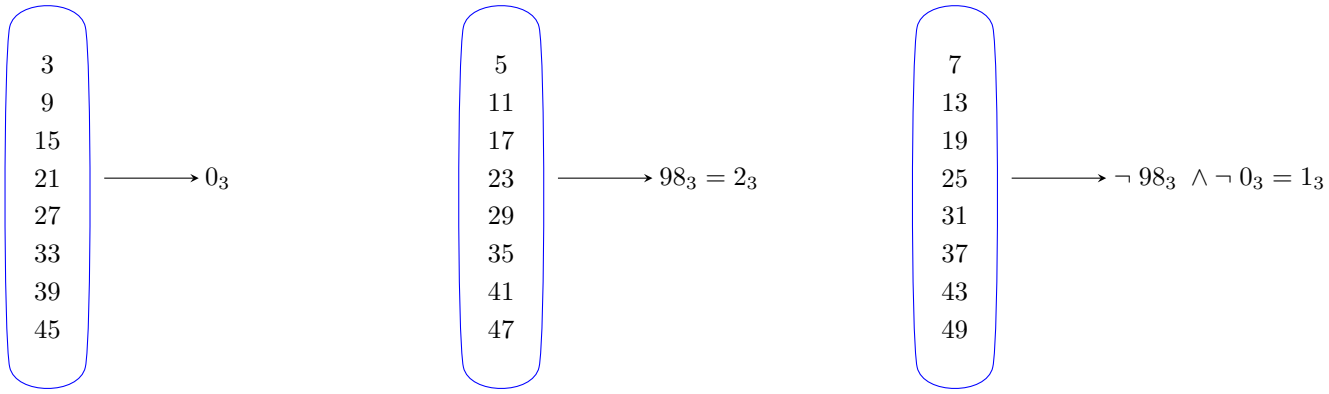
If we let A be the union of all the A_i's, i.e.

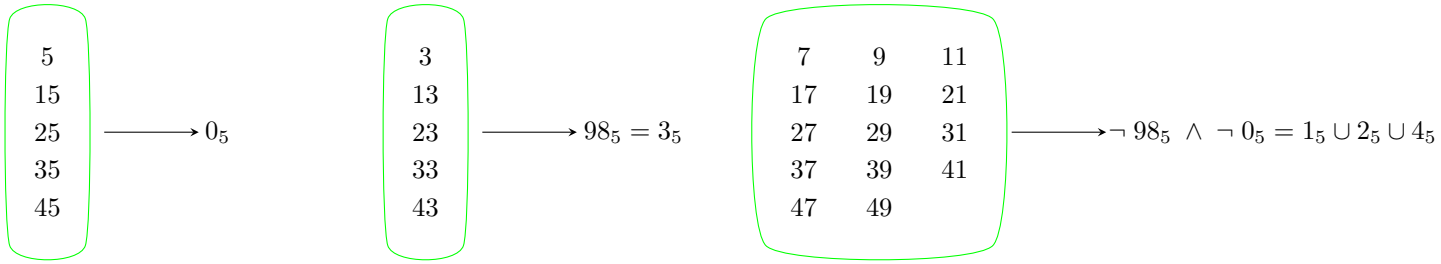
$$A = \{x : \text{for some } i,\ x \in A_i\}$$

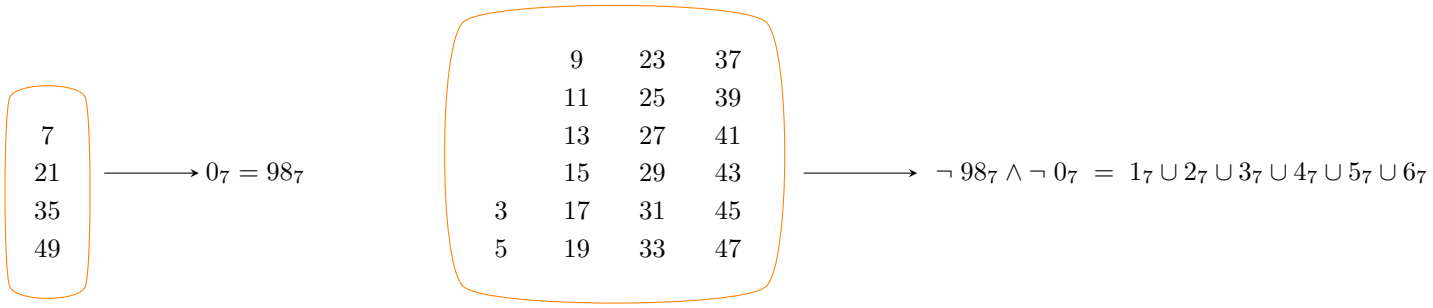
then there is an obvious map $p : A \to I$. If $x \in A$ then there is exactly one A_i such that $x \in A_i$, by the disjointness condition. We put $p(x) = i$. Thus

Annexe 4 : 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, A General Theory of Fibre Spaces with Structure Sheaf, cours donné à l'Université du Kansas, première édition en août 1955 et seconde édition en mai 1958, NSF-G 1126, rapport n° 4.

Une aide qui tombe à point nommée (Denise Vella-Chemla, 4.12.2019)

Du fait de travaux récents que j'ai effectués de secrétariat bibliographique, j'ai pris contact avec Leila Schneps, qui gère sur son site personnel la page du "Grothendieck circle" et elle a eu la gentillesse d'écrire correctement "mes" mathématiques. Je voulais garder ici mémoire de nos échanges.

Extrait d'un mail de Leila Schneps du 3.12.2019

Fixons un nombre pair n supérieur à 4. Pour tout nombre premier p entre 3 et $\sqrt{n}$, notons $F(p,n)$ l'ensemble des entiers m qui sont :

i) impairs,

ii) compris entre $\sqrt{n}$ et $n/2$,

iii) non congrus à 0 modulo p (i.e. non divisibles par p),

iv) non congrus à n modulo p (i.e. le reste après division de m par p n'est pas égal au reste après division de n par p).

On pose maintenant $D(n) = \cap F(p,n)$, c'est l'intersection des ensembles $F(p,n)$ pour tous les premiers compris entre 3 et $\sqrt{n}$.

Démontrons que si $D(n)$ est non vide, il ne contient que des nombres premiers.

Lemme 1 : Soit m un entier positif impair. Si m n'est divisible par aucun nombre premier compris entre 3 et $\sqrt{m}$, alors m est premier.

Démonstration : Supposons que m ne soit pas premier. Alors il existe un nombre premier $p < m$ qui divise m. Mais on sait que p n'est pas compris entre 3 et $\sqrt{m}$, donc $p > \sqrt{m}$. On pose $k = m/p$. On a donc $kp = m$. Si $k \geq \sqrt{m}$, alors puisqu'on a aussi $p > \sqrt{m}$, on obtient $kp > m$, ce qui est impossible. On doit donc avoir $k < \sqrt{m}$. Mais comme tout entier, l'entier k est divisible par un nombre premier $q \leq k$. Comme q divise k et k divise m, on a que q divise aussi m, et comme $k \leq \sqrt{m}$, on a que $q \leq \sqrt{m}$, ce qui contredit notre hypothèse de départ que m n'est divisible par aucun premier $\leq \sqrt{m}$. QED.

J'applique ce résultat maintenant à $D(n)$ pour obtenir votre énoncé que $D(n)$ ne contient que des nombres premiers.

Lemme 2 : Si $D(n)$ est non vide, il ne contient que des nombres premiers.

Démonstration : Soit $m \in D(n)$. Alors m est impair et $m \leq n/2$. On sait par le lemme 1 que si m n'est divisible par aucun premier compris entre 3 et $\sqrt{m}$, alors m est premier. Mais par la définition de $D(n)$, on sait déjà que m n'est divisible par aucun premier compris entre 3 et $\sqrt{n}$, et puisque $m < n$, on a $\sqrt{m} < \sqrt{n}$ et donc a fortiori m n'est divisible par aucun premier compris entre 3 et $\sqrt{m}$, donc par le lemme 1, m est bien premier. QED.

Lemme 3 : Si $D(n)$ est non vide et m appartient à $D(n)$, alors $n - m$ est premier.

Démonstration : On commence par montrer qu'aucun nombre premier p compris entre 3 et $\sqrt{n}$ ne divise $n - m$. En effet, si $n - m$ est divisible par p, alors m est congru à n modulo p, ce qui contredit le fait que m appartient à $D(n)$. Ensuite, on note que puisque $n - m < n$, on a $\sqrt{n-m} < \sqrt{n}$ et donc a fortiori, $n-m$ n'est divisible par aucun premier $\leq \sqrt{n-m}$, donc par le lemme 1, $n-m$ est bien un nombre premier.

Si $D(n)$ est non vide, alors n vérifie la conjecture de Goldbach. Il faut maintenant comprendre pourquoi $D(n)$ est non vide !

Ma réponse : Le complémentaire de l'ensemble vide, c'est l'ensemble plein ; dire qu'un ensemble est vide, c'est dire que son complémentaire contient TOUS les nombres. On sait bien (sic ;-))) que TOUS les nombres n'ont pas soit comme reste 0 soit le même reste qu'un nombre donné (je ne sais pas moi, 3, au hasard) quand on les divise par un nombre premier quelconque, même si les nombres en question sont tous compris dans un même intervalle $[\sqrt{n}, n/2]$. Si le complémentaire de l'ensemble que l'on suppose vide ne peut pas être "le plein", alors l'ensemble que l'on a supposé vide ne l'est pas (par démonstration par l'absurde).

On est sûr que les conditions "(congru à 0) OU (congru à n) selon chaque p" sont trop faibles pour être couvrantes de TOUS les nombres ; et c'est exactement là-dessus qu'est basée ce que je pense être une démonstration : puisqu'on sait que le contraire (complémentaire) de l'ensemble vide, qui normalement est l'ensemble plein (i.e. tous les nombres, en l'occurrence ceux compris entre $\sqrt{n}$ et $n/2$), ne peut être plein parce qu'on a, je ne sais pas moi, sur 3 nombres consécutifs, toutes les classes de congruence modulo 3 qui sont couvertes, et que là, en souhaitant que le nombre ne soit ni congru à 0, ni congru à n selon tout p compris entre 3 et $\sqrt{n}$, on n'élimine que 2 classes au maximum (éventuellement confondues lorsque p est un diviseur de n), on aboutit à une contradiction : on ne peut obtenir le "plein" avec seulement deux classes de congruences possibles selon tout p ou dit autrement, "on ne peut pas avoir tout le monde en n'ayant que 2 classes selon tout p, ça laissera des trous". Comme cette contradiction (provenant de "j'ai obtenu un plein qui ne peut pas être plein", qui est une proposition équivalente à "l'intersection des non congrus à 0 et non congrus à n selon tout p est vide"), eh bien, on en conclut que l'intersection des (non congrus à 0 et non congrus à n selon tout p) n'est pas vide et comme cela a été démontré plus haut (voir mail de Leila), l'intersection en question (notée $\cap F(p, n)$) contient un décomposant de Goldbach au moins (il a en effet été démontré dans le mail de Leila que l'intersection des ensembles de nombres qui ne sont ni congrus à 0 ni congrus à n selon tout p premier compris entre 3 et $\sqrt{n}$ contient les décomposants de Goldbach de n qui sont compris entre $\sqrt{n}$ et $n/2$ et que cette intersection ne contient qu'eux).

Je trouve que ces échanges illustrent exactement ce que veut dire s'exprimer en langage mathématique : Leila Schneps emploie un langage très précis, ses assertions s'enchaînent logiquement de manière imparable.

Quant à moi, je me dis que peut-être que la conjecture fait finalement partie des énoncés indémontrables... Mais ça m'étonnerait.

Juste cause (Denise Vella-Chemla, 5.12.2019)

On cherche à démontrer la conjecture de Goldbach. Fixons un nombre pair n supérieur à 4, double d'un nombre composé (car les doubles de nombres premiers vérifient trivialement la conjecture). Pour tout nombre premier p_k entre 3 et $\sqrt{n}$, notons $F(p_k, n)$ l'ensemble des entiers m qui sont :

i) impairs,

ii) compris entre $\sqrt{n}$ et $n/2$,

iii) non congrus à 0 modulo p_k (i.e. non divisibles par p_k),

iv) non congrus à n modulo p_k (i.e. le reste après division de m par p_k n'est pas égal au reste après division de n par p_k).

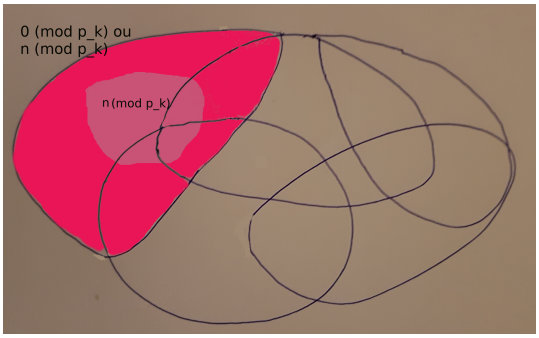
On pose maintenant $D(n) = \cap F(p_k, n)$, c'est l'intersection des ensembles $F(p_k, n)$ pour tous les premiers p_k compris entre 3 et $\sqrt{n}$.

A été démontré dans http://denisevellachemla.eu/aide-Leila-Schneps.pdf que si $D(n)$ est non vide, il ne contient que des nombres premiers qui sont décomposants de Goldbach de n et qu'alors n vérifie la conjecture de Goldbach.

Voyons pourquoi $D(n) = \cap F(p_k, n)$ ne peut être vide. On reprend l'écriture initiale qu'on avait choisi, sous forme logique : dire que l'intersection des ensembles de la forme $\{\neg 0_{p_k} \wedge \neg n_{p_k}\}$ est vide, ce que l'on note $\bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \varnothing = \bot$ (le symbole $\bot$ est le symbole logique pour *False*), est équivalent à dire que le complémentaire de cet ensemble est le "plein" (dénoté par $\top$, ou *Vrai*), i.e. couvre l'ensemble de tous les impairs de 3 à $n/2$.

$$\complement \bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \bigvee_{p_k}\{0_{p_k} \vee n_{p_k}\} = \top$$

Pour fixer (autant que faire se peut) les idées, on représente cette union d'ensembles de nombres "congrus à 0 ou à n selon un nombre premier p_k compris entre 3 et $\sqrt{n}$" qui contient TOUS les nombres de 3 à $n/2$ par un ensemble de patatoïdes comme sur le dessin suivant ;



Chaque ensemble délimité contient un ensemble de nombres compris entre 3 et $n/2$ et congrus à 0 ou bien congrus à n selon un nombre premier p_k (p_k compris entre 3 et $\sqrt{n}$). On a coloré l'un d'eux en fuschia et à l'intérieur de lui on a "isolé" en utilisant la couleur rose clair les nombres qui sont congrus à n parmi ceux qui sont congrus à 0 ou à n modulo p_k.

Etudions le cas d'un nombre pair n qui est le double d'un nombre composé et concentrons-nous sur le produit, noté P de tous les nombres premiers qui sont compris entre $\sqrt{n}$ et $n/2$.

Alors on a que chacun des p_m composant le produit P ne peut pas être un élément des parties des ensembles contenant les nombres "congrus à 0" selon un p_k compris entre 3 et $\sqrt{n}$ puisque c'est un nombre premier. Chaque nombre premier p_m composant le produit P est donc forcément dans les parties des ensembles contenant les nombres "congrus à n selon un p_k" (partie rose clair et non fuschia pour la fixation d'idées).

Mais alors le produit P est congru à une puissance de n, puisque chacun de ses termes est congru à n, P est congru à la puissance n^x avec x le nombre de nombres premiers compris entre $\sqrt{n}$ et $n/2$.

Or on a supposé que n est le double d'un nombre composé. Il a donc un diviseur d inférieur à sa racine. Ce diviseur d divise la puissance n^x puisqu'il divise n, c'est à dire que n^x est congru à 0 modulo d ce diviseur ; mais d ne divise pas P puisque tous les nombres composant le produit P sont des nombres premiers. On a abouti à une contradiction (congruence à 0 ou non congruence à 0 modulo d un diviseur de n). Tous les nombres compris entre 3 et $n/2$ ne peuvent pas être couverts par l'union ensembliste des congrus à 0 ou congrus à n modulo chaque p_k compris entre 3 et $\sqrt{n}$. Le complémentaire du vide n'est pas plein. L'ensemble initial n'est pas vide. Il contient un décomposant de Goldbach au moins à l'issue de cette démonstration par l'absurde. Et n vérifie ainsi la conjecture.

Réécrire (Denise Vella-Chemla, 6.12.2019)

On cherche à démontrer la conjecture de Goldbach.

1. Caractérisation des décomposants de Goldbach d'un nombre pair

Fixons un nombre pair n supérieur à 4, double d'un nombre composé (car les doubles de nombres premiers vérifient trivialement la conjecture). Pour tout nombre premier p_k entre 3 et $\sqrt{n}$, notons $F(p_k, n)$ l'ensemble des entiers m qui sont * :

i) impairs,

ii) compris entre $\sqrt{n}$ et $n/2$,

iii) non congrus à 0 modulo p_k (i.e. non divisibles par p_k),

iv) non congrus à n modulo p_k (i.e. le reste après division de m par p_k n'est pas égal au reste après division de n par p_k).

On pose maintenant $D(n) = \cap F(p_k, n)$, c'est l'intersection des ensembles $F(p_k, n)$ pour tous les premiers p_k compris entre 3 et $\sqrt{n}$.

Démontrons que si $D(n)$ est non vide, il ne contient que des nombres premiers.

Lemme 1 : Soit m un entier positif impair. Si m n'est divisible par aucun nombre premier compris entre 3 et $\sqrt{m}$, alors m est premier.

Démonstration : Supposons que m ne soit pas premier. Alors il existe un nombre premier $p < m$ qui divise m. Mais on sait que p n'est pas compris entre 3 et $\sqrt{m}$, donc $p > \sqrt{m}$. On pose $k = m/p$. On a donc $kp = m$. Si $k \geq \sqrt{m}$, alors puisqu'on a aussi $p > \sqrt{m}$, on obtient $kp > m$, ce qui est impossible. On doit donc avoir $k < \sqrt{m}$. Mais comme tout entier, l'entier k est divisible par un nombre premier $q \leq k$. Comme q divise k et k divise m, on a que q divise aussi m, et comme $k \leq \sqrt{m}$, on a que $q \leq \sqrt{m}$, ce qui contredit notre hypothèse de départ que m n'est divisible par aucun premier $\leq \sqrt{m}$. QED.

Appliquons ce résultat maintenant à $D(n)$ pour obtenir que $D(n)$ ne contient que des nombres premiers.

Lemme 2 : Si $D(n)$ est non vide, il ne contient que des nombres premiers.

Démonstration : Soit $m \in D(n)$. Alors m est impair et $m \leq n/2$. On sait par le lemme 1 que si m n'est divisible par aucun premier compris entre 3 et $\sqrt{m}$, alors m est premier. Mais par la définition de $D(n)$, on sait déjà que m n'est divisible par aucun premier compris entre 3 et $\sqrt{n}$, et puisque $m < n$, on a $\sqrt{m} < \sqrt{n}$ et donc a fortiori m n'est divisible par aucun premier compris entre 3 et $\sqrt{m}$, donc par le lemme 1, m est bien premier. QED.

Lemme 3 : Si $D(n)$ est non vide et m appartient à $D(n)$, alors $n - m$ est premier.

Démonstration : On commence par montrer qu'aucun nombre premier p_k compris entre 3 et $\sqrt{n}$ ne divise $n - m$. En effet, si $n - m$ est divisible par p_k, alors m est congru à n modulo p_k, ce qui contredit le fait que m appartient à $D(n)$. Ensuite, on note que puisque $n - m < n$, on a $\sqrt{n - m} < \sqrt{n}$ et donc a fortiori, $n-m$ n'est divisible par aucun premier $\leq \sqrt{n - m}$, donc par le lemme 1, $n-m$ est bien un nombre premier.

Si $D(n)$ est non vide, alors n vérifie la conjecture de Goldbach.

∗. Cette section a été rédigée formellement par Leila Schneps : du fait de travaux récents que j'ai effectués de secrétariat bibliographique, j'ai pris contact avec elle, car elle gère sur son site académique la page du "Grothendieck circle" ; en échange de ce service, je lui ai demandé de regarder mon texte http://denisevellachemla.eu/fibres-inter.pdf, ce qu'elle a fait, et elle m'a envoyé par mail la formalisation de cette section *Caractérisation des décomposants de Goldbach d'un nombre pair.*

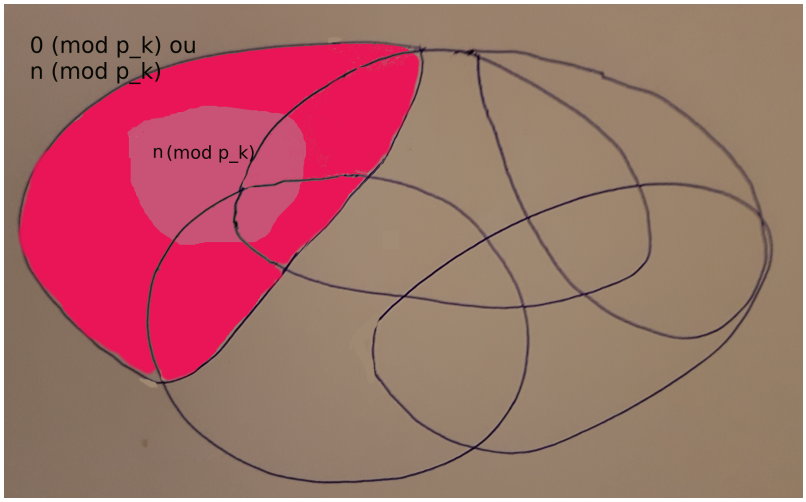
2. Existence d'un décomposant de Goldbach pour tout nombre pair

On a vu que si $D(n)$ est non vide, il ne contient que des nombres premiers qui sont décomposants de Goldbach de n et qu'alors n vérifie la conjecture de Goldbach.

Essayons de comprendre pourquoi $D(n) = \cap F(p_k, n)$ ne peut être vide. On reprend l'écriture initiale qu'on avait choisie, sous forme logique : dire que l'intersection des ensembles de la forme $\{\neg 0_{p_k} \wedge \neg n_{p_k}\}$ est vide [†], ce que l'on note $\bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \varnothing = \bot$ (le symbole $\bot$ est le symbole logique pour *False*), est équivalent à dire que le complémentaire de cet ensemble est le "plein" (dénoté par $\top$, ou *Vrai*), i.e. couvre l'ensemble de tous les nombres impairs compris entre 3 et $n/2$.

$$\complement \bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \bigvee_{p_k}\{0_{p_k} \vee n_{p_k}\} = \top$$

Pour fixer (autant que faire se peut) les idées, on représente cette union d'ensembles de nombres "congrus à 0 ou à n selon un nombre premier p_k compris entre 3 et $\sqrt{n}$" qui contient TOUS les nombres impairs compris entre 3 et $n/2$ par un ensemble de patatoïdes comme sur le dessin suivant ;



Chaque ensemble délimité contient un ensemble de nombres impairs compris entre 3 et $n/2$ et congrus à 0 ou bien congrus à n selon un nombre premier p_k (p_k compris entre 3 et $\sqrt{n}$). On a coloré l'un d'eux en fuschia et à l'intérieur de lui on a "isolé" en utilisant la couleur rose clair les nombres qui sont congrus à n parmi ceux qui sont congrus à 0 ou à n modulo p_k.

Etudions le cas d'un nombre pair n qui est le double d'un nombre composé et considérons les nombres premiers (notons les p_{m_k}) compris entre $\sqrt{n}$ et $n/2$.

Alors on a que tout p_{m_k} ne peut pas être un élément des parties des ensembles contenant les nombres "congrus à 0" selon un p_k compris entre 3 et $\sqrt{n}$ puisque p_{m_k} est un nombre premier. Chaque nombre premier p_{m_k} est donc forcément dans les parties des ensembles contenant les nombres "congrus à n selon un p_k" (partie rose clair et non fuschia pour la fixation d'idées).

On n'arrive toujours pas à démontrer pourquoi il est impossible qu'il existe pour chaque p_{m_k} compris entre $\sqrt{n}$ et $n/2$ un nombre premier p_k compris entre 3 et $\sqrt{n}$ tel que p_{m_k} et n ont même reste dans une division entière par p_k.

†. $\neg$ est le symbole logique du "*non*", $\wedge$ est le symbole logique du "*et*", $\vee$ est le symbole logique du "*ou*", 0_{p_k} est l'expression choisie pour exprimer "*x est congru à 0 modulo p_k, i.e. $x \equiv 0$ (mod p_k) de Gauss*" (on omet le x pour alléger l'écriture) et n_{p_k} est l'expression choisie pour exprimer "*x est congru à n modulo p_k*".

Réécrire

Denise Vella-Chemla (7.12.2019) aidée par Leila Schneps pour la section 1

1. Caractérisation des décomposants de Goldbach d'un nombre pair

Soit n un nombre pair supérieur à 4 et p_k un nombre premier compris entre 3 et $\sqrt{n}$.

Notons $F(p_k, n) = \{m \in \mathbb{N} : m \text{ impair}, \sqrt{n} \leq m \leq n/2, m \neq 0\ [p_k], m \neq n\ [p_k]\}$

Appelons $D(n) = \cap F(p_k, n)$ l'intersection des ensembles $F(p_k, n)$ pour tous les premiers p_k compris entre 3 et $\sqrt{n}$.

Démontrons que $D(n)$ ne contient que des nombres premiers.

Lemme 1 : Soit m un entier positif impair. Si m n'est divisible par aucun nombre premier compris entre 3 et $\sqrt{m}$, alors m est premier.

Démonstration : Supposons que m ne soit pas premier. Alors il existe un nombre premier $p < m$ qui divise m. Mais on sait que p n'est pas compris entre 3 et $\sqrt{m}$, donc $p > \sqrt{m}$. On pose $k = m/p$. On a donc $kp = m$. Si $k \geq \sqrt{m}$, alors puisqu'on a aussi $p > \sqrt{m}$, on obtient $kp > m$, ce qui est impossible. On doit donc avoir $k < \sqrt{m}$. Mais comme tout entier, l'entier k est divisible par un nombre premier $q \leq k$. Comme q divise k et k divise m, on a que q divise aussi m, et comme $k \leq \sqrt{m}$, on a que $q \leq \sqrt{m}$, ce qui contredit notre hypothèse de départ que m n'est divisible par aucun premier $\leq \sqrt{m}$. QED.

Appliquons ce résultat à $D(n)$ pour obtenir que $D(n)$ ne contient que des nombres premiers.

Lemme 2 : $D(n)$ ne contient que des nombres premiers [*].

Démonstration : Soit $m \in D(n)$. Alors m est impair et $m \leq n/2$. On sait par le lemme 1 que si m n'est divisible par aucun premier compris entre 3 et $\sqrt{m}$, alors m est premier. Mais par la définition de $D(n)$, on sait déjà que m n'est divisible par aucun premier compris entre 3 et $\sqrt{n}$, et puisque $m < n$, on a $\sqrt{m} < \sqrt{n}$ et donc a fortiori m n'est divisible par aucun premier compris entre 3 et $\sqrt{m}$, donc par le lemme 1, m est bien premier. QED.

Lemme 3 : Si m appartient à $D(n)$, alors $n - m$ est premier.

Démonstration : On commence par montrer qu'aucun nombre premier p compris entre 3 et $\sqrt{n}$ ne divise $n - m$. En effet, si $n - m$ est divisible par p, alors m est congru à n modulo p, ce qui contredit le fait que m appartient à $D(n)$. Ensuite, on note que puisque $n - m < n$, on a $\sqrt{n - m} < \sqrt{n}$ et donc a fortiori, $n - m$ n'est divisible par aucun premier $\leq \sqrt{n - m}$, donc par le lemme 1, $n - m$ est bien un nombre premier.

Si $D(n)$ est non vide, alors n vérifie la conjecture de Goldbach.

2. Existence d'un décomposant de Goldbach pour tout nombre pair

On a vu que $D(n)$ ne contient que des nombres premiers qui sont décomposants de Goldbach de n. Il faut maintenant démontrer que $D(n)$ est non vide pour que n vérifie la conjecture de Goldbach.

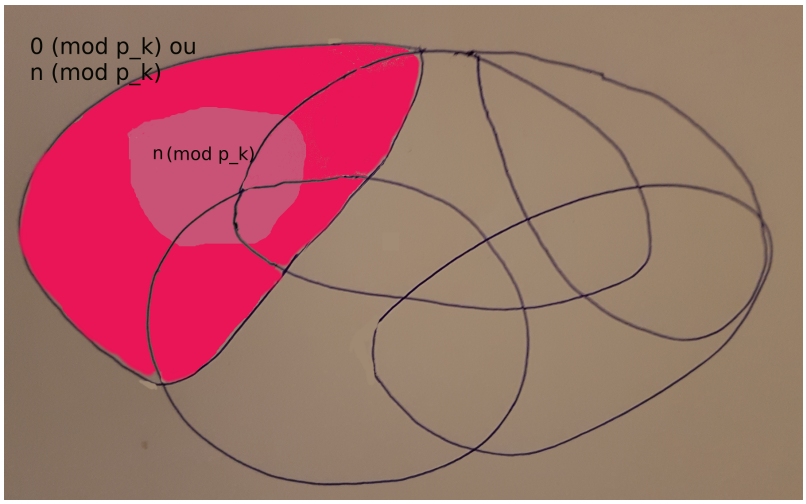
Essayons de comprendre pourquoi $D(n) = \cap F(p_k, n)$ ne peut être vide. On reprend l'écriture initiale qu'on avait choisie, sous forme logique : dire que l'intersection des ensembles de la forme $\{\neg 0_{p_k} \wedge \neg n_{p_k}\}$

∗. si $D(n)$ est vide, le lemme est vrai par vacuité.

est vide [†], ce que l'on note $\bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \varnothing = \bot$ (le symbole $\bot$ est le symbole logique pour *False*), est équivalent à dire que le complémentaire de cet ensemble est le "plein" (dénoté par $\top$, ou *Vrai*), i.e. couvre l'ensemble de tous les nombres impairs compris entre 3 et $n/2$.

$$\complement \bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \bigvee_{p_k}\{0_{p_k} \vee n_{p_k}\} = \top$$

Pour fixer (autant que faire se peut) les idées, on représente cette union d'ensembles de nombres "congrus à 0 ou à n selon un nombre premier p_k compris entre 3 et $\sqrt{n}$" qui contient TOUS les nombres impairs compris entre 3 et $n/2$ par un ensemble de patatoïdes comme sur le dessin suivant ;



Chaque ensemble délimité contient un ensemble de nombres impairs compris entre 3 et $n/2$ et congrus à 0 ou bien congrus à n selon un nombre premier p_k (p_k compris entre 3 et $\sqrt{n}$). On a coloré l'un d'eux en fuschia et à l'intérieur de lui on a "isolé" en utilisant la couleur rose clair les nombres qui sont congrus à n parmi ceux qui sont congrus à 0 ou à n modulo p_k.

Etudions le cas d'un nombre pair n qui est le double d'un nombre composé et considérons les nombres premiers (notons les p_{m_k}) compris entre $\sqrt{n}$ et $n/2$.

Alors on a que tout p_{m_k} ne peut pas être un élément des parties des ensembles contenant les nombres "congrus à 0" selon un p_k compris entre 3 et $\sqrt{n}$ puisque p_{m_k} est un nombre premier. Chaque nombre premier p_{m_k} est donc forcément dans les parties des ensembles contenant les nombres "congrus à n selon un p_k" (partie rose clair et non fuschia pour la fixation d'idées).

Essayons maintenant de démontrer pourquoi il est impossible qu'il existe pour chaque p_{m_k} compris entre $\sqrt{n}$ et $n/2$ un nombre premier p_k compris entre 3 et $\sqrt{n}$ tel que p_{m_k} et n ont même reste dans une division entière par p_k.

Voyons l'exemple du nombre pair 100 [‡].

†. $\neg$ est le symbole logique du "*non*", $\wedge$ est le symbole logique du "*et*", $\vee$ est le symbole logique du "*ou*", 0_{p_k} est l'expression choisie pour exprimer "*x est congru à 0 modulo p_k, i.e. $x \equiv 0$ (mod p_k) de Gauss*" (on omet le x pour alléger l'écriture) et n_{p_k} est l'expression choisie pour exprimer "*x est congru à n modulo p_k*".

‡. puisqu'on est 100 (sans) démonstration !

	3	5	7
11	2	1	4
13	1	3	6
17	2	2	3
19	1	4	5
23	2	3	2
29	2	4	1
31	1	1	3
37	1	2	2
41	2	1	6
43	1	3	1
47	2	2	5
100	1	0	2

On a noté en rouge les restes partagés par $n = 100$ et par les nombres premiers compris entre $\sqrt{n} = \sqrt{100} = 10$ et $n/2 = 100/2 = 50$ selon les modules 3, 5, 7 inférieurs à $\sqrt{n} = \sqrt{100} = 10$. Les lignes dans lesquels aucun reste n'est partagé avec 100 fournissent les décomposants de Goldbach de 100.

Exprimons les partages de restes par des égalités (égalités classiques de la forme $n = aq + p$ représentant des divisions euclidiennes) portant sur le nombre 100 et sur les nombres premiers entêtes de lignes : on a

$$\begin{array}{ll}
100 = ... & + 11 \\
100 = 29 \times 3 & + 13 \\
100 = ... & + 17 \\
100 = 27 \times 3 & + 19 \\
100 = 11 \times 7 & + 23 \\
100 = ... & + 29 \\
100 = 23 \times 3 & + 31 \\
100 = 21 \times 3 & + 37 \\
100 = ... & + 41 \\
100 = 19 \times 3 & + 43 \\
100 = ... & + 47
\end{array}$$

On a utilisé des points de suspension (...) pour exprimer qu'on n'a pas trouvé de produits de deux entiers, l'un compris entre 3 et $\sqrt{n}$, l'autre compris entre $n/2$ et $n - \sqrt{n}$, pour certaines lignes, les lignes des décomposants de Goldbach de 100 justement.

Il faudrait réussir à montrer que le système suivant d'équations correspondant à des divisions euclidiennes (en nombre $\pi(n/2) - \pi(\sqrt{n})$, avec la notation habituelle $\pi(x)$ est le nombre de nombres premiers inférieurs ou égaux à x) ne peut être vérifié par des a_k tous strictement supérieurs à 1.

$$\left\{\begin{array}{ll}
n = a_1 \times q_1 & + p_1 \\
n = a_2 \times q_2 & + p_2 \\
... & \\
n = a_k \times q_k & + p_k
\end{array}\right.$$

Les p_k sont compris entre $\sqrt{n}$ et $n/2$. Les q_k sont compris entre 3 et $\sqrt{n}$, il est nécessaire qu'il y ait des redondances, i.e. des égalités de la forme $q_i = q_j$ avec $i \neq j$, dans la mesure où les q_k sont bien moins nombreux que les p_k.

On arrive à établir une contradiction pour l'instant seulement si tous les nombres premiers compris entre 3 et $\sqrt{n}$ apparaissent chacun au moins une fois dans les équations du système : pour cela, on isole les p_k du côté droit des équations, on obtient :

$$\left\{\begin{array}{ll}
n - a_1 \times q_1 & = p_1 \\
n - a_2 \times q_2 & = p_2 \\
... & \\
n - a_k \times q_k & = p_k
\end{array}\right.$$

On multiplie alors toutes les équations entre elles, ce qui permet d'obtenir une égalité entre le produit de tous les nombres premiers compris entre $\sqrt{n}$ et $n/2$ et le produit de facteurs $(n - a_1 \times q_1)(n - a_2 \times$

$q_2)\dots(n - a_k \times q_k)$. Le développement de ce produit de facteurs est une somme de termes dans lesquels on peut toujours mettre n en facteur et d'un dernier terme produit de tous les $a_k p_k$. Le produit de toutes les équations donne :

$$\prod_k (n - a_k q_k) = \prod_k p_k$$

$$\iff \quad nT \pm \prod a_k q_k = \prod_k p_k$$

Note : On a noté $\pm$ dans la partie gauche de la seconde égalité car on ne sait pas si le dernier terme est ajouté ou soustrait (cela dépend du nombre d'équations du système mais cela n'intervient pas dans l'étude des différentes divisibilités). Si tous les nombres premiers compris entre 3 et $\sqrt{n}$ sont représentés "dans" l'une des équations, un diviseur de n figure au moins parmi eux. Il divise tous les termes contenant un facteur n, il divise également $\prod a_k q_k$ puisqu'il est l'un des q_k mais il ne divise pas le produit $\prod_k p_k$ de droite dans la mesure où ce produit est un produit de nombres premiers. On aboutit ainsi à une contradiction dans ce cas.

Subsiste un problème si l'un des nombres premiers compris entre 3 et $\sqrt{n}$ n'apparaît dans aucune équation du système.

Réécrire

Denise Vella-Chemla (8.12.2019)

1. Caractérisation des décomposants de Goldbach de n supérieurs à $\sqrt{n}$ [1]

Soit $n \in 2\mathbb{N}+6$ un entier pair supérieur à 6. Pour tout $p \in \mathbb{P}^*$ premier impair inférieur à $\sqrt{n}$ (*i.e.* $3 \leq p \leq \sqrt{n}$), on définit l'ensemble :

$$F_n(p) = \{m \in 2\mathbb{N}+1 : 3 \leq m \leq n/2,\ m \not\equiv 0\ [p],\ m \not\equiv n\ [p]\}$$

L'intersection des ensembles $F_n(p)$ pour tout p premier compris entre 3 et $\sqrt{n}$ est notée :

$$D_n = \bigcap_{\substack{p \in \mathbb{P} \\ 3 \leq p \leq \sqrt{n}}} F_n(p)$$

Nous allons montrer que D_n et son complémentaire $n - D_n$ ne contiennent que des nombres premiers.

Lemme 1 : Soit $m \in 2\mathbb{N}+1$ un entier impair. Si m n'est divisible par aucun nombre premier compris entre 3 et $\sqrt{m}$, alors il est premier.

Démonstration : Si m est composé, on a $m = pq$, où p est le plus petit nombre premier intervenant dans la factorisation de m en nombres premiers et où q est le produit de tous les autres facteurs. Puisque m est impair, $p \geq 3$, et puisque $q \geq p$ (q étant le produit d'entiers $\geq p$), $m = pq \geq pp = p^2$ et donc $\sqrt{m} \geq p$ (la fonction racine carrée étant croissante). On a ainsi montré que si m impair est composé, il est divisible par un premier compris entre 3 et $\sqrt{m}$. Le lemme s'obtient par contraposition. □

Lemme 2 : $D_n \subseteq \mathbb{P}$

Démonstration : Soit $m \in D_n$. Alors $m \in F_n(p)$ pour tout p premier compris entre 3 et $\sqrt{n}$. Par conséquent, m est impair et m n'est divisible par aucun nombre premier p compris entre 3 et $\sqrt{n}$ (puisque $m \not\equiv 0\ [p]$), et donc *a fortiori* par aucun premier compris entre 3 et $\sqrt{m}$ (car $m \leq n/2 \implies m \leq n \implies \sqrt{m} \leq \sqrt{n}$). D'après le lemme 1, m est donc premier. □

Lemme 3 : $n - D_n \subseteq \mathbb{P}$

Démonstration : Soit $m \in D_n$. Alors $m \in F_n(p)$ pour tout p premier compris entre 3 et $\sqrt{n}$. Par conséquent, $n - m$ est impair (car m est impair et n pair) et $n - m$ n'est divisible par aucun nombre premier p compris entre 3 et $\sqrt{n}$ (puisque $m \not\equiv n\ [p]$), et donc *a fortiori* par aucun premier compris entre 3 et $\sqrt{n-m}$ (car $n - m \leq n \implies \sqrt{n-m} \leq \sqrt{n}$). D'après le lemme 1, $n - m$ est donc premier. □

Les ensembles D_n ne contiennent que des décomposants de Goldbach de n.

Lemme 4 : Soit $n \in 2\mathbb{N}+6$. Si $D_n \neq \varnothing$, alors n vérifie la conjecture de Goldbach.

Démonstration : Si $D_n \neq \varnothing$, il contient un entier p nécessairement premier (d'après le lemme 1), tel que $q = n - p$ est également premier (d'après le lemme 2), et donc $n = p + q$ vérifie la conjecture de Goldbach.

1. Leila Schneps d'abord, Jacques Chemla ensuite, ont réécrit cette partie.

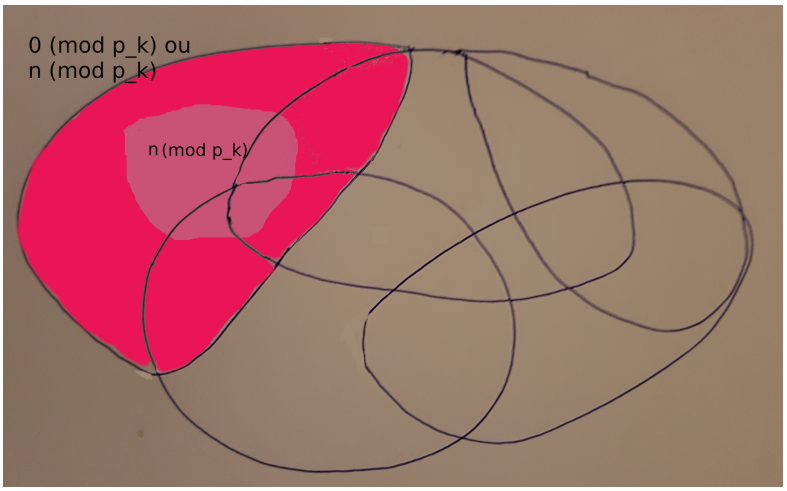
2. Existence d'un décomposant de Goldbach pour tout nombre pair

On a vu que $D(n)$ ne contient que des nombres premiers qui sont décomposants de Goldbach de n. Il faut maintenant démontrer que $D(n)$ est non vide pour que n vérifie la conjecture de Goldbach.

Essayons de comprendre pourquoi $D(n) = \cap F(p_k, n)$ ne peut être vide. On reprend l'écriture initiale qu'on avait choisie, sous forme logique : dire que l'intersection des ensembles de la forme $\{\neg 0_{p_k} \wedge \neg n_{p_k}\}$ est vide [2], ce que l'on note $\bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \varnothing = \bot$ (le symbole $\bot$ est le symbole logique pour *False*), est équivalent à dire que le complémentaire de cet ensemble est le "plein" (dénoté par $\top$, ou *Vrai*), i.e. couvre l'ensemble de tous les nombres impairs compris entre 3 et $n/2$.

$$\complement \bigwedge_{p_k}\{\neg 0_{p_k} \wedge \neg n_{p_k}\} = \bigvee_{p_k}\{0_{p_k} \vee n_{p_k}\} = \top$$

Pour fixer (autant que faire se peut) les idées, on représente cette union d'ensembles de nombres "congrus à 0 ou à n selon un nombre premier p_k compris entre 3 et $\sqrt{n}$" qui contient TOUS les nombres impairs compris entre 3 et $n/2$ par un ensemble de patatoïdes comme sur le dessin suivant ;



Chaque ensemble délimité contient un ensemble de nombres impairs compris entre 3 et $n/2$ et congrus à 0 ou bien congrus à n selon un nombre premier p_k (p_k compris entre 3 et $\sqrt{n}$). On a coloré l'un d'eux en fuschia et à l'intérieur de lui on a "isolé" en utilisant la couleur rose clair les nombres qui sont congrus à n parmi ceux qui sont congrus à 0 ou à n modulo p_k.

Etudions le cas d'un nombre pair n qui est le double d'un nombre composé et considérons les nombres premiers (notons les p_{m_k}) compris entre $\sqrt{n}$ et $n/2$.

Alors on a que tout p_{m_k} ne peut pas être un élément des parties des ensembles contenant les nombres "congrus à 0" selon un p_k compris entre 3 et $\sqrt{n}$ puisque p_{m_k} est un nombre premier.

2. $\neg$ est le symbole logique du "*non*", $\wedge$ est le symbole logique du "*et*", $\vee$ est le symbole logique du "*ou*", 0_{p_k} est l'expression choisie pour exprimer "*x est congru à 0 modulo p_k, i.e. $x \equiv 0\ (mod\ p_k)$ de Gauss*" (on omet le x pour alléger l'écriture) et n_{p_k} est l'expression choisie pour exprimer "*x est congru à n modulo p_k*".

Chaque nombre premier p_{m_k} est donc forcément dans les parties des ensembles contenant les nombres "congrus à n selon un p_k" (partie rose clair et non fuschia pour la fixation d'idées).

Essayons maintenant de démontrer pourquoi il est impossible qu'il existe pour chaque p_{m_k} compris entre $\sqrt{n}$ et $n/2$ un nombre premier p_k compris entre 3 et $\sqrt{n}$ tel que p_{m_k} et n ont même reste dans une division entière par p_k.

Voyons l'exemple du nombre pair 100 [3].

	3	5	7
11	2	1	4
13	1	3	6
17	2	2	3
19	1	4	5
23	2	3	2
29	2	4	1
31	1	1	3
37	1	2	2
41	2	1	6
43	1	3	1
47	2	2	5
100	1	0	2

On a noté en rouge les restes partagés par $n = 100$ et par les nombres premiers compris entre $\sqrt{n} = \sqrt{100} = 10$ et $n/2 = 100/2 = 50$ selon les modules 3, 5, 7 inférieurs à $\sqrt{n} = \sqrt{100} = 10$. Les lignes dans lesquels aucun reste n'est partagé avec 100 fournissent les décomposants de Goldbach de 100.

Exprimons les partages de restes par des égalités (égalités classiques de la forme $n = aq + p$ représentant des divisions euclidiennes) portant sur le nombre 100 et sur les nombres premiers entêtes de lignes : on a

$$\begin{aligned}
100 &= \ldots &&+ 11\\
100 &= 29 \times 3 &&+ 13\\
100 &= \ldots &&+ 17\\
100 &= 27 \times 3 &&+ 19\\
100 &= 11 \times 7 &&+ 23\\
100 &= \ldots &&+ 29\\
100 &= 23 \times 3 &&+ 31\\
100 &= 21 \times 3 &&+ 37\\
100 &= \ldots &&+ 41\\
100 &= 19 \times 3 &&+ 43\\
100 &= \ldots &&+ 47
\end{aligned}$$

On a utilisé des points de suspension (...) pour exprimer qu'on n'a pas trouvé de produits de deux entiers, l'un compris entre 3 et $\sqrt{n}$, l'autre compris entre $n/2$ et $n - \sqrt{n}$, pour certaines lignes, les lignes des décomposants de Goldbach de 100 justement.

3. puisqu'on est 100 (sans) démonstration !

Il faudrait réussir à montrer que le système suivant d'équations correspondant à des divisions euclidiennes (en nombre $\pi(n/2) - \pi(\sqrt{n})$, avec la notation habituelle $\pi(x)$ est le nombre de nombres premiers inférieurs ou égaux à x) ne peut être vérifié par des a_k tous strictement supérieurs à 1.

$$\begin{cases} n = a_1 \times q_1 & + p_1 \\ n = a_2 \times q_2 & + p_2 \\ \dots \\ n = a_k \times q_k & + p_k \end{cases}$$

Les p_k sont compris entre $\sqrt{n}$ et $n/2$. Les q_k sont compris entre 3 et $\sqrt{n}$, il est nécessaire qu'il y ait des redondances, i.e. des égalités de la forme $q_i = q_j$ avec $i \neq j$, dans la mesure où les q_k sont bien moins nombreux que les p_k.

On arrive à établir une contradiction pour l'instant seulement si tous les nombres premiers compris entre 3 et $\sqrt{n}$ apparaissent chacun au moins une fois dans les équations du système : pour cela, on isole les p_k du côté droit des équations, on obtient :

$$\begin{cases} n - a_1 \times q_1 & = p_1 \\ n - a_2 \times q_2 & = p_2 \\ \dots \\ n - a_k \times q_k & = p_k \end{cases}$$

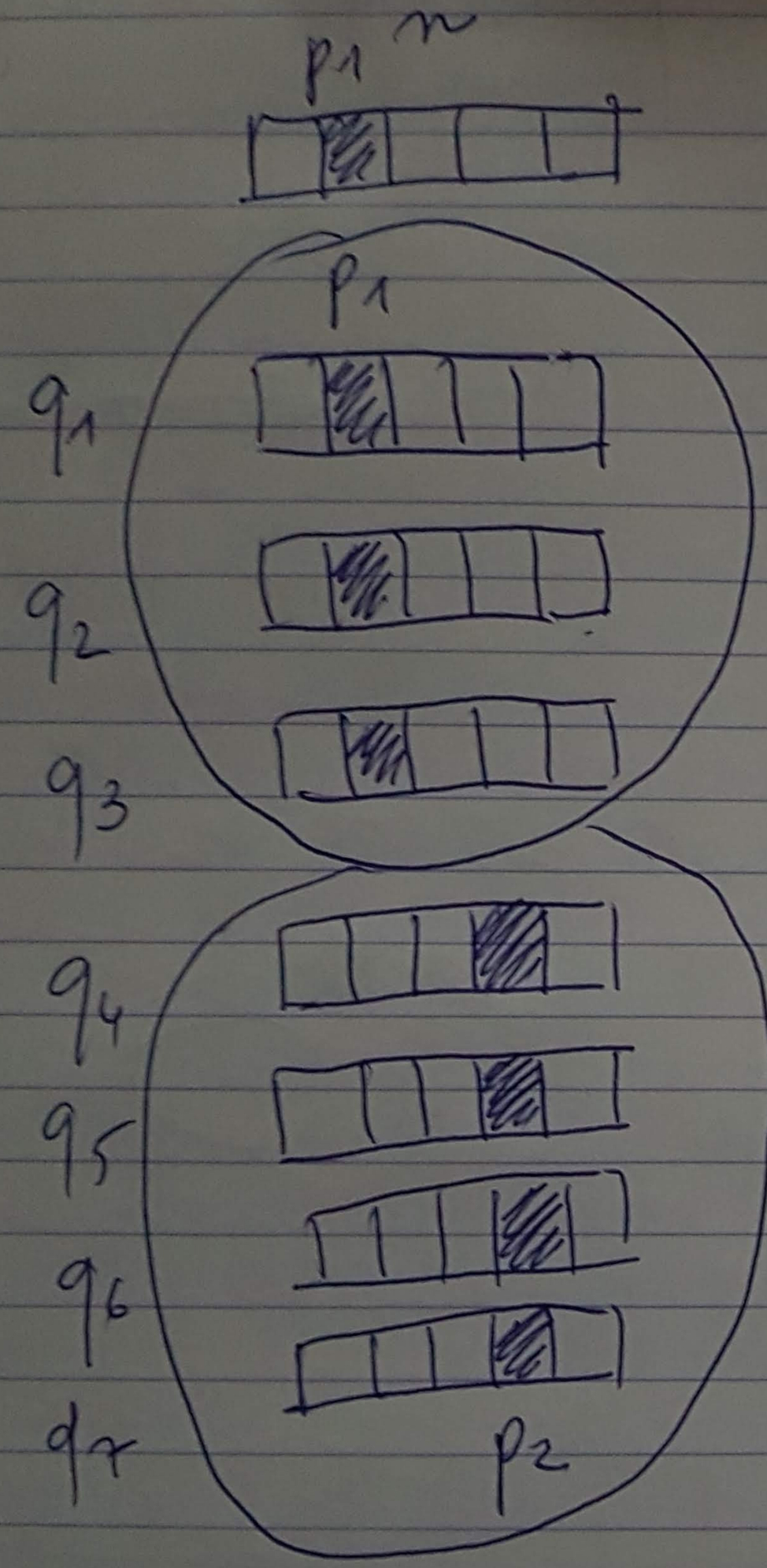
On multiplie alors toutes les équations entre elles, ce qui permet d'obtenir une égalité entre le produit de tous les nombres premiers compris entre $\sqrt{n}$ et $n/2$ et le produit de facteurs $(n - a_1 \times q_1)(n - a_2 \times q_2) \dots (n - a_k \times q_k)$. Le développement de ce produit de facteurs est une somme de termes dans lesquels on peut toujours mettre n en facteur et d'un dernier terme produit de tous les $a_k p_k$. Le produit de toutes les équations donne :

$$\prod_k (n - a_k q_k) = \prod_k p_k$$

$$\iff \quad nT \pm \prod a_k q_k = \prod_k p_k$$

Note : On a noté $\pm$ dans la partie gauche de la seconde égalité car on ne sait pas si le dernier terme est ajouté ou soustrait (cela dépend du nombre d'équations du système mais cela n'intervient pas dans l'étude des différentes divisibilités). Si tous les nombres premiers compris entre 3 et $\sqrt{n}$ sont représentés "dans" l'une des équations, un diviseur de n figure au moins parmi eux. Il divise tous les termes contenant un facteur n, il divise également $\prod a_k q_k$ puisqu'il est l'un des q_k mais il ne divise pas le produit $\prod_k p_k$ de droite dans la mesure où ce produit est un produit de nombres premiers. On aboutit ainsi à une contradiction dans ce cas.

Subsiste un problème si l'un des nombres premiers compris entre 3 et $\sqrt{n}$ n'apparaît dans aucune équation du système.



$q_1 q_2 q_3 \equiv n^3 \ (p_1)$

p_2 —— $\equiv p_2^{n^3} \ (p_1 p_2)$ ⇓

↕ Contraad ?

p_1 —— $\equiv p_1^{n^4} \ (p_1 p_2)$ ⇓

$q_4 q_5 q_6 q_7 \equiv n^4 \ (p_2)$

Propriété utilisée (voir RA Gaun

$a \equiv b \pmod m$

$\Rightarrow ka \equiv kb \pmod{km}$

Restrictions (Denise Vella-Chemla (14.12.2019)

Cette note fait suite à une autre note consultable ici

http://denisevellachemla.eu/jade.pdf.

On ne parvient pas à démontrer que tous les nombres premiers compris entre $\sqrt{n}$ et $n/2$ ne peuvent avoir tous simultanément l'un de leur reste égal à celui de n dans une division par un nombre premier p compris entre 3 et $\sqrt{n}$. On se convainc d'une chose, par programme : on constate que pour $24 < n \leq 10000$, on trouve toujours un décomposant de Goldbach de n parmi les nombres qui ne sont pas une racine carrée de 1 modulo n. On se dit qu'il n'y a peut-être pas de raison que cela change pour $n \geq 10000$.

Le programme est consultable ici http://denisevellachemla.eu/paracine.pdf et son résultat est consultable là http://denisevellachemla.eu/resparacine.pdf.

Maintenant, il faudrait pour prouver la conjecture montrer que dans cet ensemble des nombres premiers compris entre $\sqrt{n}$ et $n/2$ et non racines carrées de 1, qui est un ensemble encore plus petit que celui auquel on s'intéressait précédemment [1], tous les nombres premiers ne peuvent pas être simultanément congrus à n modulo un nombre premier compris entre 3 et $\sqrt{n}$.

Si on parvenait à cela, on aurait utilisé une méthode à l'opposé de celle souvent utilisée par les mathématiciens et qui consiste à généraliser un problème pour le résoudre.

Là au contraire, on cherche à prouver la non-vacuité d'un ensemble $E \supset F$ (i.e. d'un ensemble E contenant F) en démontrant la non-vacuité de F, qui aurait pour conséquence la non vacuité de E.

1. et qui était l'ensemble de tous les nombres premiers compris entre $\sqrt{n}$ et $n/2$.

Extraits de Monsieur Croche de Claude Debussy (éd. L'imaginaire Gallimard (DV, 19/1/2020)

(p. 318)

- Pelléas et Mélisande *ne va-t-il pas être prochainement représenté dans plusieurs villes étrangères où il était encore ignoré ?*

- Je ne puis rien vous dire de précis à ce sujet, je n'en sais absolument rien ; et puis, pour moi, l'intérêt n'est pas là. Il est dans la musique, dans celle qu'on fait, dans celle qu'on aime ! Je l'aime passionnément, moi, et c'est par amour pour elle que je m'efforce de la dégager de certaines traditions stériles qui l'engoncent. C'est un art libre, jaillissant, un art de plein air, un art à la mesure des éléments, du vent, du ciel, de la mer ! Il ne faut pas en faire un art fermé, scolaire. Évidemment, c'est très joli, l'écriture, le métier, je m'en suis moi-même enthousiasmé, autrefois ; mais j'ai beaucoup réfléchi, et cette écriture même gagnerait à être simplifiée, les moyens d'expression plus directs. Ne croyez pas qu'en disant cela, je veuille me placer en chef d'école ou en réformateur ! Je tâche seulement d'exprimer le plus sincèrement que je puis les sensations et les sentiments que j'éprouve ; le reste m'importe peu ! On m'a prêté je ne sais quelle attitude que je n'ai jamais eue vis-à-vis des maîtres, et l'on m'a fait dire sur Wagner, sur Beethoven, des choses que je n'ai jamais dites. J'admire Beethoven et Wagner, mais je me refuse à les admirer en bloc parce qu'on m'a dit que c'étaient des maîtres ! Ça jamais ! De nos jours, à mon avis, on prend à l'égard des maîtres des façons de domestiques fort déplaisantes ; je veux avoir la liberté de dire qu'une page ennuyeuse m'ennuie quel que soit son auteur. Mais je n'ai nulle théorie, nulle prévention. J'essaie d'être un homme sincère, dans mon art et dans mes opinions, voilà tout. Seulement, j'estime qu'il y a dans l'art une aristocratie qu'il ne faut pas compromettre. C'est pourquoi je souhaite peu le gros succès, la notoriété tapageuse. Encore une fois, je ne suis pas l'homme de ma légende, je n'aime que le silence, la paix, le travail, l'isolement, et tout ce que l'on peut dire de ma musique m'est complètement égal. Je ne prétends point qu'on l'imite, ni qu'elle exerce une influence quelconque sur qui que ce soit. Je tiens à rester indépendant ; je fais mon œuvre comme je dois, comme je puis, voilà tout ce que je peux vous dire.

(p. 325)
Qui connaîtra le secret de la composition musicale ? Le bruit de la mer, la courbe d'un horizon, le vent dans les feuilles, le cri d'un oiseau déposent en nous de multiples impressions. Et, tout à coup, sans que l'on y consente le moins du monde, l'un de ces souvenirs se répand hors de nous et s'exprime en langage musical. Il porte en lui-même son harmonie. Quelque effort que l'on fasse, on n'en pourra trouver de plus juste, ni de plus sincère. Seulement ainsi, un cœur destiné à la musique fait les plus belles découvertes.

Si je vous parle ainsi, ce n'est pas pour vous proposer l'opulent étalage d'une morale artistique, mais pour vous prouver justement que je n'en ai pas. J'abomine les doctrines et leurs impertinences.

C'est pourquoi je veux écrire mon songe musical avec le plus complet détachement de moi-même. Je veux chanter mon paysage intérieur avec la candeur naïve de l'enfance.

Sans doute, cette innocente grammaire d'art ne va pas sans heurts. Elle choquera toujours les partisans de l'artifice et du mensonge. Je le prévois et m'en réjouis. Je ne ferai rien pour me créer des adversaires. Mais je ne ferai, non plus rien, pour convertir mes inimitiés en amitiés. Il faut s'efforcer d'être un grand artiste pour soi-même et non pour les autres. Je veux oser être moi-même et souffrir pour ma vérité. Ceux qui ressentent à ma façon ne m'en aimeront que davantage. Les autres m'éviteront, me haïront. Je ne ferai rien pour me les concilier.

En vérité, le jour lointain - il faut espérer que ce sera le plus tard possible - où je ne susciterai plus de querelles, je me le reprocherai amèrement. Dans ces œuvres dernières, dominera nécessairement la détestable hypocrisie qui m'aura permis de contenter tous les hommes.

(p. 289)

— *À ce moment de la conversation, je rappelle à M. Debussy ses succès du Conservatoire, son grand prix de Rome, remporté par lui en 1883 avec sa cantate* L'enfant prodigue.

- Vieux souvenirs, me dit-il, et dont je ne m'enorgueillis pas. S'il y a quelque chose que je trouve inutile et même nuisible au Conservatoire, c'est la forme par laquelle on y récompense les élèves.

  La forme du concours me paraît déplorable. Quelqu'un travaille bien. C'est un très bon élève. Le jour du concours il est mal disposé et il ne réussit pas.

  Je ne connais rien de plus absurde que le concours. Il y a des gens qui n'ont, au Conservatoire, obtenu aucun prix, aucun accessit et qui sont devenus d'excellents, de parfaits musiciens.

  Pour moi la vérité est qu'il faut sortir du Conservatoire le plus tôt possible, pour chercher et trouver son individualité.

  L'État a institué des concours partout, dans toutes les professions. Nous formons de plus en plus des bêtes à concours. Dans toutes les professions j'estime que la méthode est mauvaise, mais dans le domaine de l'art, j'affirme que le concours est chose absolument nuisible.

  C'est vous dire que je suis hostile à la fameuse tradition du Prix de Rome. On s'adresse là encore à la partie la moins intéressante de l'homme, à sa vanité. Et puis, le Prix de Rome ne sert absolument à rien.

  On fait faire des choses aux logistes qu'on ne refera plus jamais dans sa carrière de musicien.

  Enfin, il demeure, ce Prix de Rome. Qu'on en tire donc de meilleurs avantages que ceux obtenus jusqu'à présent, qu'on laisse plus de liberté aux musiciens dans leurs envois de Rome. Qu'on ne leur impose pas de thèmes !

  Je vous ai confié toute ma pensée, sans détours.

  Ce comité où je vais entrer n'est peut-être pas une mauvaise chose, mais il y a l'atmosphère de cette vieille maison qui s'appelle le Conservatoire et qui ne laisse pas pénétrer le moindre vent de réforme...

- *Mais à ce comité, Maître, vous défendrez les idées que vous venez de m'exposer ?*

- Je vous dis tout cela ici. Eh bien ! je vous l'assure, je serai incapable de le redire au Conservatoire.

  Il faudrait une autorité que je n'ai pas, des moyens d'élocution que je n'ai pas non plus. Je ne saurai peut-être pas défendre mes idées.

  Comme ceux qui ont beaucoup d'idées, je n'aime pas la contradiction.

Avant de prendre congé de M. Debussy, je l'interroge sur ses travaux personnels, sur ses prochaines œuvres, il me répond en quelques mots :

- J'ai mis douze ans pour faire *Pelléas et Mélisande*. C'est vous dire que je ne travaille pas vite. Voyez-vous, on écrit toujours trop, et on ne pense jamais assez.