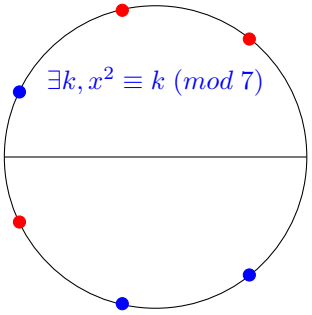
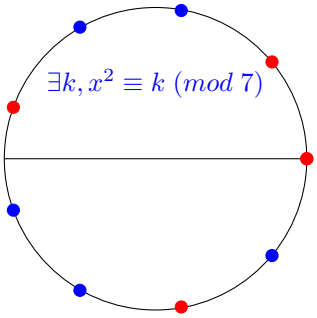
Résidus quadratiques sur colliers (Denise Vella-Chemla, 22.5.2019)

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 $4k+3$.

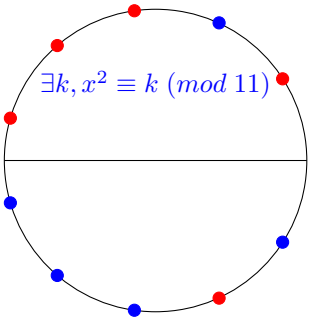
Solutions de $\exists k, x^2 \equiv k \ (mod\ 7)$: 1, 2, 4.
7 est premier.
Il y a 3 solutions.



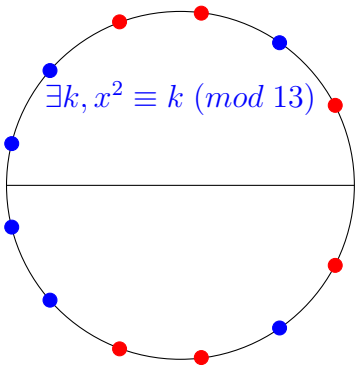
Solutions de $\exists k, x^2 \equiv k \ (mod\ 9)$: 0, 1, 4, 7.
9 est composé.
Il y a 4 solutions.



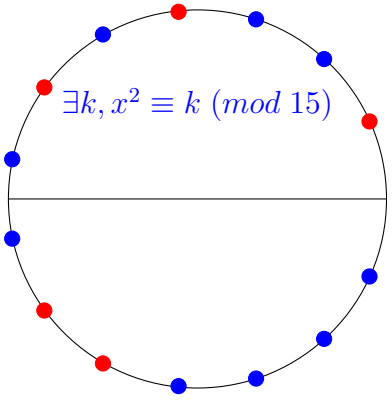
Solutions de $\exists k, x^2 \equiv k \ (mod\ 11)$: 1, 3, 4, 5, 9.
11 est premier.
Il y a 5 solutions.



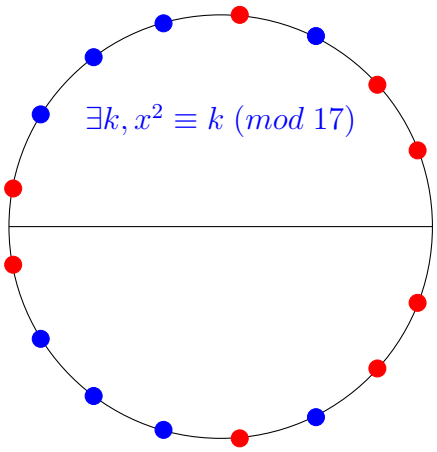
Solutions de $\exists k, x^2 \equiv k \ (mod\ 13)$: 1, 3, 4, 9, 10, 12.
13 est premier.
Il y a 6 solutions.



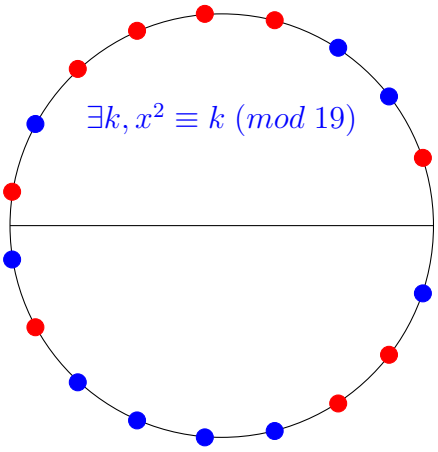
Solutions de $\exists k, x^2 \equiv k \ (mod\ 15)$: 1, 4, 6, 9, 10.
15 est composé.
Il y a 5 solutions.



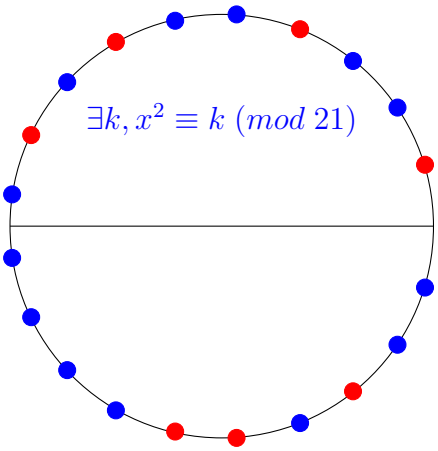
Solutions de $\exists k, x^2 \equiv k \ (mod\ 17)$: 1, 2, 4, 8, 9, 13, 15, 16.
17 est premier.
Il y a 8 solutions.



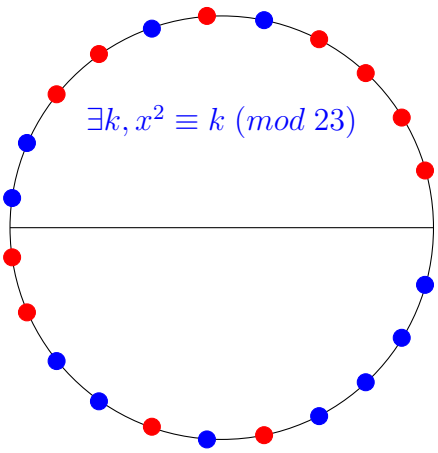
Solutions de $\exists k, x^2 \equiv k \ (mod\ 19)$: 1, 4, 5, 6, 7, 9, 11, 16, 17.
19 est premier.
Il y a 9 solutions.



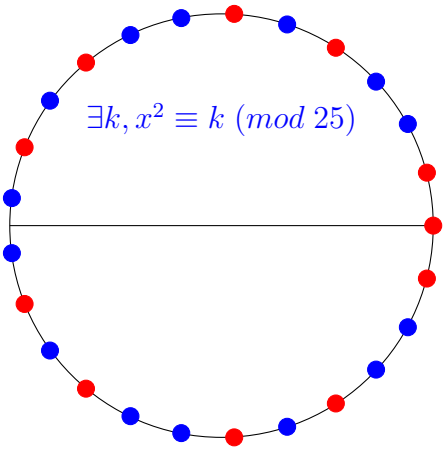
Solutions de $\exists k, x^2 \equiv k \ (mod\ 21)$: 1, 4, 7, 9, 15, 16, 18.
21 est composé.
Il y a 4 solutions.



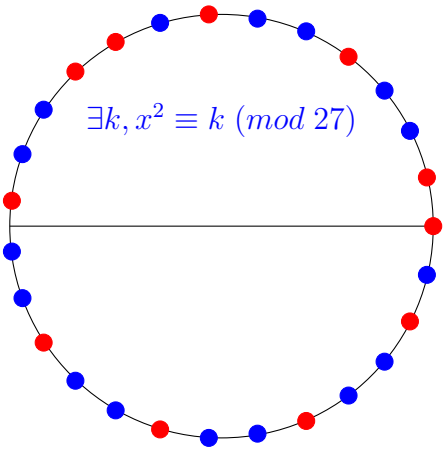
Solutions de $\exists k, x^2 \equiv k \ (mod\ 23)$: 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.
23 est premier.
Il y a 11 solutions.



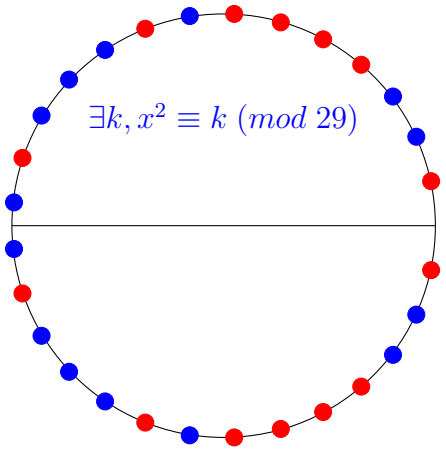
Solutions de $\exists k, x^2 \equiv k \ (mod\ 25)$: 0, 1, 4, 6, 9, 11, 14, 16, 19, 21, 24.
25 est composé.
Il y a 11 solutions.



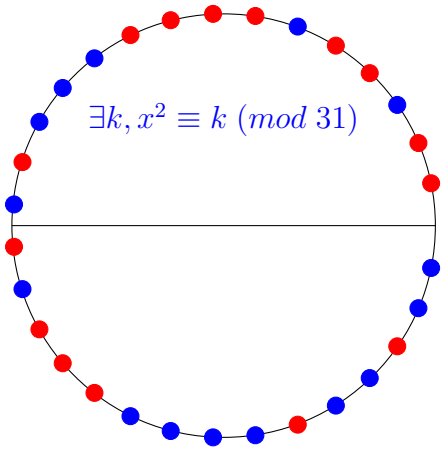
Solutions de $\exists k, x^2 \equiv k \ (mod\ 27)$: 0, 1, 4, 7, 9, 10, 13, 16, 19, 22, 25.
27 est composé.
Il y a 10 solutions.



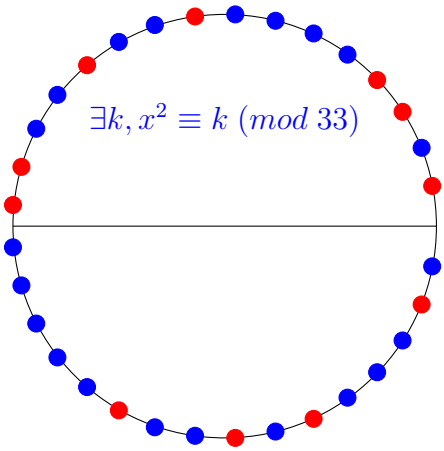
Solutions de $\exists k, x^2 \equiv k \ (mod\ 29)$: 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28.
29 est premier.
Il y a 14 solutions.



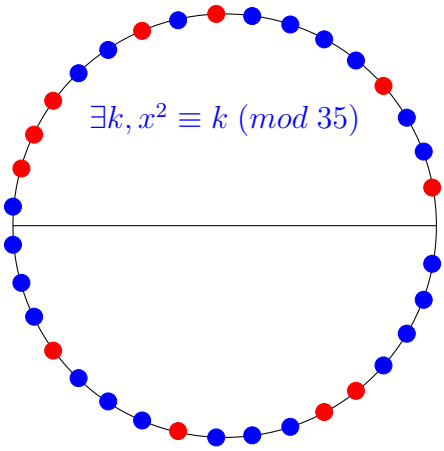
Solutions de $\exists k, x^2 \equiv k \ (mod\ 31)$: 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28.
31 est premier.
Il y a 15 solutions.



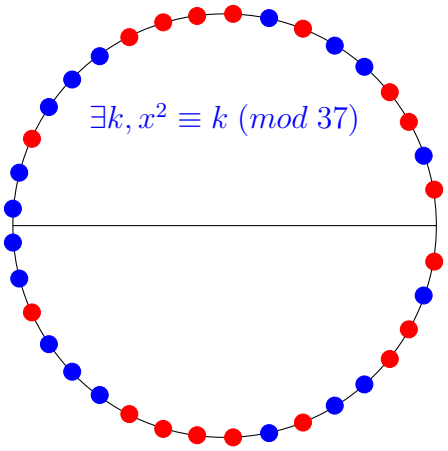
Solutions de $\exists k, x^2 \equiv k \ (mod\ 33)$: 1, 3, 4, 9, 12, 15, 16, 22, 25, 27, 31.
33 est composé.
Il y a 11 solutions.



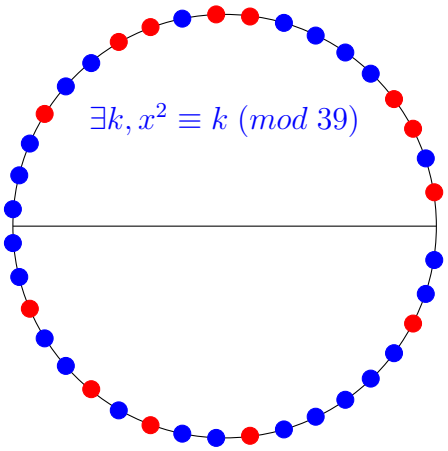
Solutions de $\exists k, x^2 \equiv k \ (mod\ 35)$: 1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30.
35 est composé.
Il y a 11 solutions.



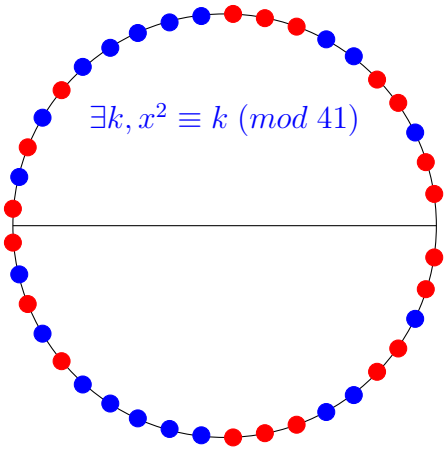
Solutions de $\exists k, x^2 \equiv k \ (mod\ 37)$: 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36.
37 est premier.
Il y a 18 solutions.



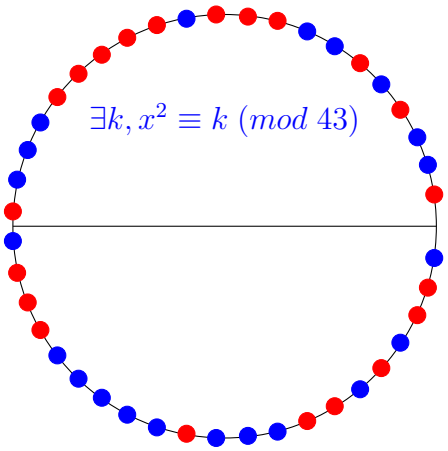
Solutions de $\exists k, x^2 \equiv k \ (mod\ 39)$: 1, 3, 4, 9, 10, 12, 13, 16, 22, 25, 27, 30, 36.
39 est composé.
Il y a 13 solutions.



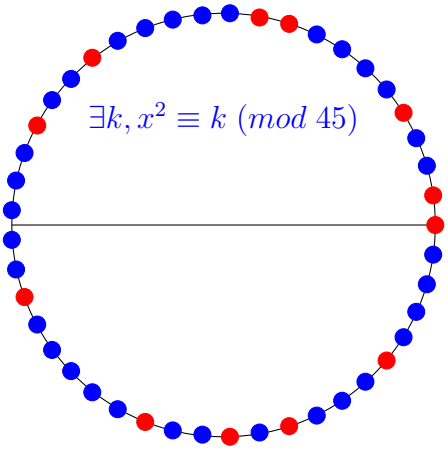
Solutions de $\exists k, x^2 \equiv k \ (mod\ 41)$: 1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40.
41 est premier.
Il y a 20 solutions.



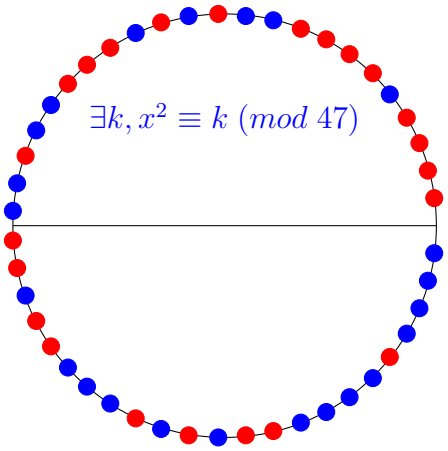
Solutions de $\exists k, x^2 \equiv k \ (mod\ 43)$: 1, 4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23, 24, 25, 31, 35, 36, 38, 40, 41.
43 est premier.
Il y a 21 solutions.



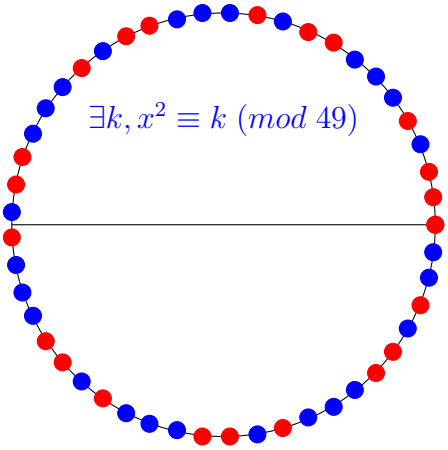
Solutions de $\exists k, x^2 \equiv k \ (mod\ 45)$: 0, 1, 4, 9, 10, 16, 19, 25, 31, 34, 36, 40.
45 est composé.
Il y a 12 solutions.



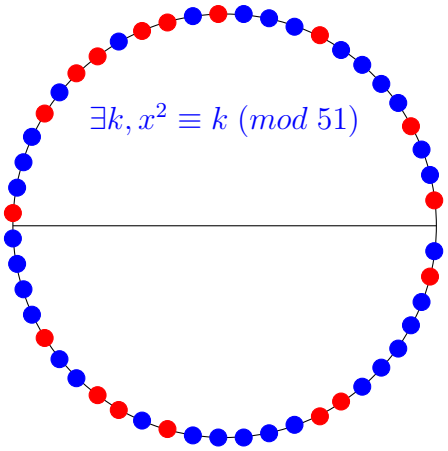
Solutions de $\exists k, x^2 \equiv k \ (mod\ 47)$: 1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42.
47 est premier.
Il y a 23 solutions.



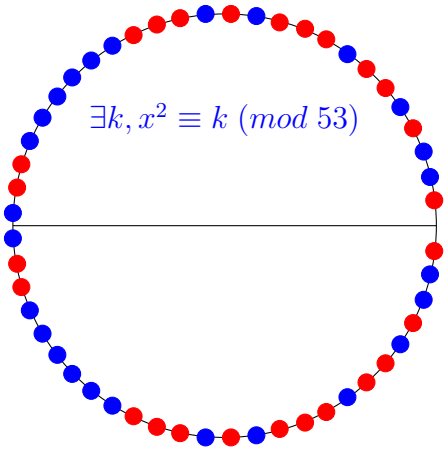
Solutions de $\exists k, x^2 \equiv k \ (mod\ 49)$: 0, 1, 2, 4, 8, 9, 11, 15, 16, 18, 22, 23, 25, 29, 30, 32, 36, 37, 39, 43, 44, 46.
49 est composé.
Il y a 22 solutions.



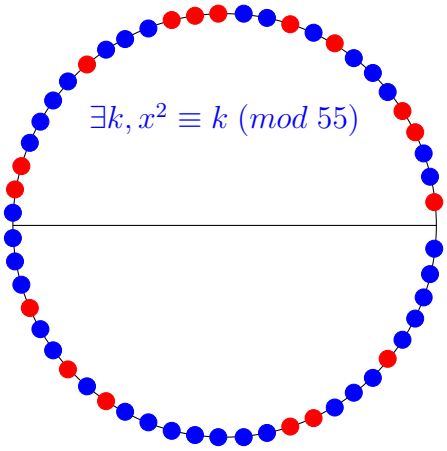
Solutions de $\exists k, x^2 \equiv k \ (mod\ 51)$: 1, 4, 9, 13, 15, 16, 18, 19, 21, 25, 30, 33, 34, 36, 42, 43, 49.
51 est composé.
Il y a 4 solutions.



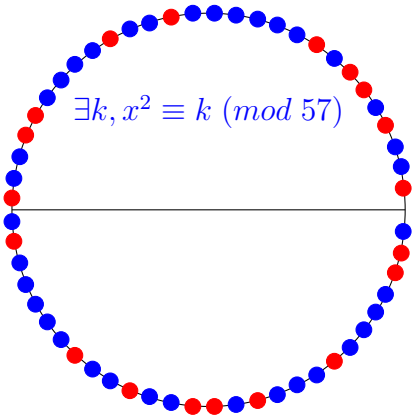
Solutions de $\exists k, x^2 \equiv k \ (mod\ 53)$: 1, 4, 6, 7, 9, 10, 11, 13, 15, 16, 17, 24, 25, 28, 29, 36, 37, 38, 40, 42, 43, 44, 46, 47, 49, 52.
53 est premier.
Il y a 4 solutions.



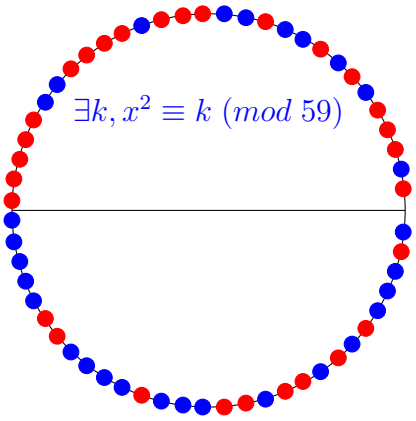
Solutions de $\exists k, x^2 \equiv k \ (mod\ 55)$: 1, 4, 5, 9, 11, 14, 15, 16, 20, 25, 26, 31, 34, 36, 44, 45, 49.
55 est composé.
Il y a 4 solutions.



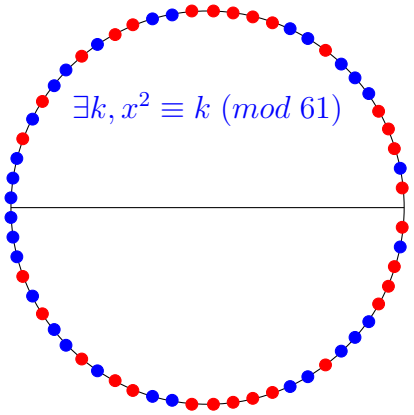
Solutions de $\exists k, x^2 \equiv k \ (mod\ 57)$: 1, 4, 6, 7, 9, 16, 19, 24, 25, 28, 30, 36, 39, 42, 43, 45, 49, 54, 55.
57 est composé.
Il y a 4 solutions.



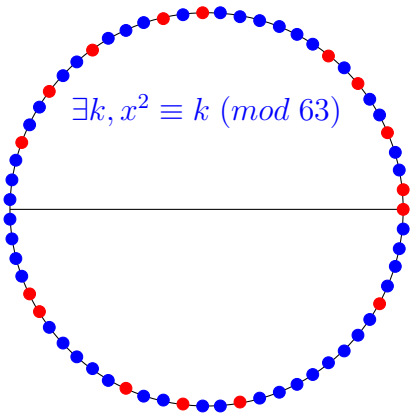
Solutions de $\exists k, x^2 \equiv k \ (mod\ 59)$: 1, 3, 4, 5, 7, 9, 12, 15, 16, 17, 19, 20, 21, 22, 25, 26, 27, 28, 29, 35, 36, 41, 45, 46, 48, 49, 51, 53, 57.
59 est premier.
Il y a 29 solutions.



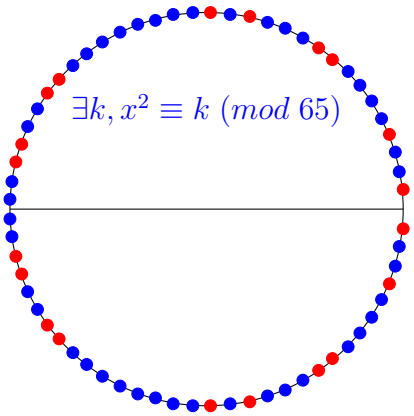
Solutions de $\exists k, x^2 \equiv k \ (mod\ 61)$: 1, 3, 4, 5, 9, 12, 13, 14, 15, 16, 19, 20, 22, 25, 27, 34, 36, 39, 41, 42, 45, 46, 47, 48, 49, 52, 56, 57, 58, 60.
61 est premier.
Il y a 30 solutions.



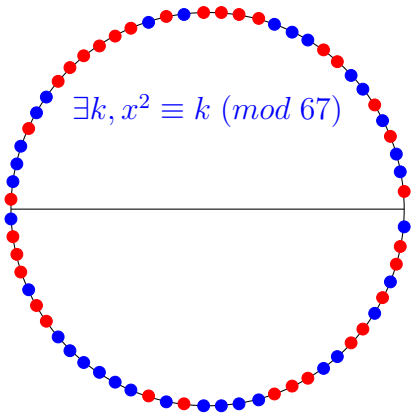
Solutions de $\exists k, x^2 \equiv k \ (mod\ 63)$: 0, 1, 4, 7, 9, 16, 18, 22, 25, 28, 36, 37, 43, 46, 49, 58.
63 est composé.
Il y a 16 solutions.



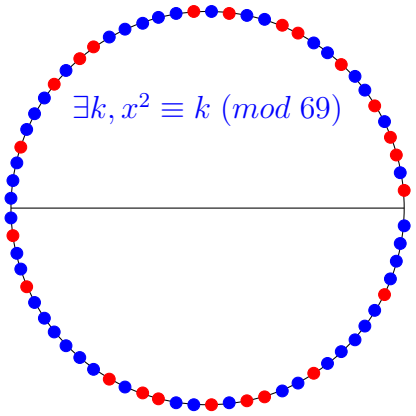
Solutions de $\exists k, x^2 \equiv k \ (mod\ 65)$: 1, 4, 9, 10, 14, 16, 25, 26, 29, 30, 35, 36, 39, 40, 49, 51, 55, 56, 61, 64.
65 est composé.
Il y a 20 solutions.



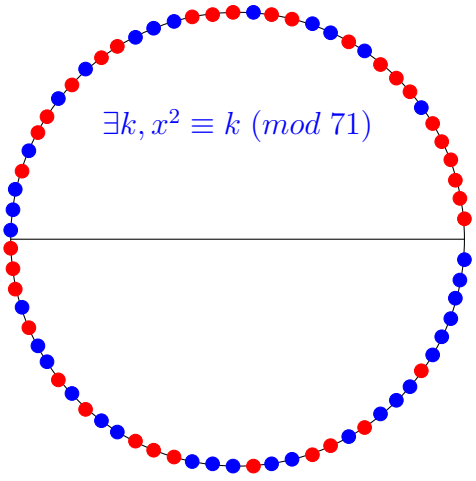
Solutions de $\exists k, x^2 \equiv k \ (mod\ 67)$: 1, 4, 6, 9, 10, 14, 15, 16, 17, 19, 21, 22, 23, 24, 25, 26, 29, 33, 35, 36, 37, 39, 40, 47, 49, 54, 55, 56, 59, 60, 62, 64, 65.
67 est premier.
Il y a 33 solutions.



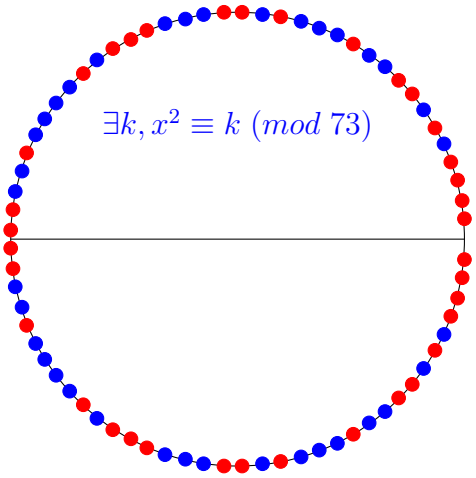
Solutions de $\exists k, x^2 \equiv k \ (mod\ 69)$: 1, 3, 4, 6, 9, 12, 13, 16, 18, 24, 25, 27, 31, 36, 39, 46, 48, 49, 52, 54, 55, 58, 64.
69 est composé.
Il y a 23 solutions.



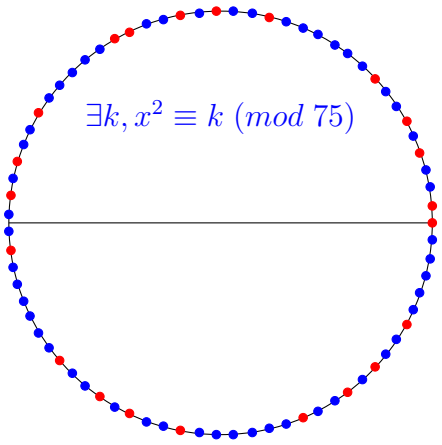
Solutions de $\exists k, x^2 \equiv k \ (mod\ 71)$: 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 19, 20, 24, 25, 27, 29, 30, 32, 36, 37, 38, 40, 43, 45, 48, 49, 50, 54, 57, 58, 60, 64.
71 est premier.
Il y a 35 solutions.



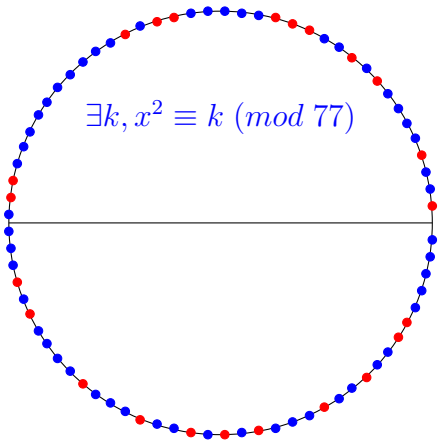
Solutions de $\exists k, x^2 \equiv k \ (mod\ 73)$: 1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 19, 23, 24, 25, 27, 32, 35, 36, 37, 38, 41, 46, 48, 49, 50, 54, 55, 57, 61, 64, 65, 67, 69, 70, 71, 72.
73 est premier.
Il y a 36 solutions.



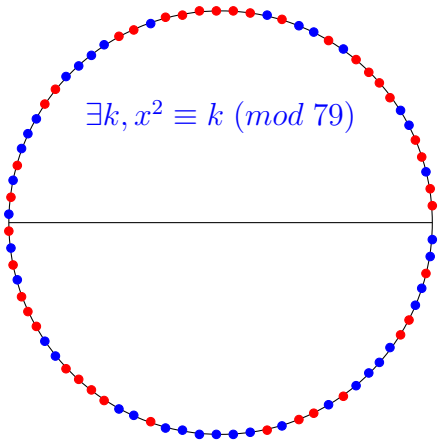
Solutions de $\exists k, x^2 \equiv k \ (mod\ 75)$: 0, 1, 4, 6, 9, 16, 19, 21, 24, 25, 31, 34, 36, 39, 46, 49, 51, 54, 61, 64, 66, 69.
75 est composé.
Il y a 22 solutions.



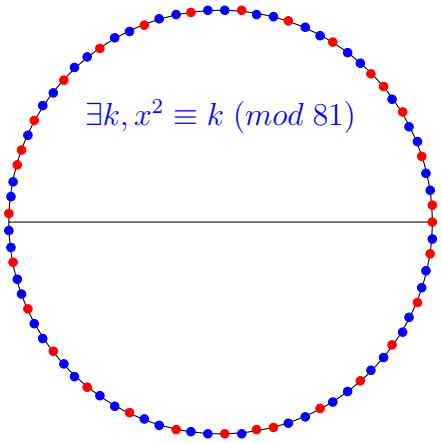
Solutions de $\exists k, x^2 \equiv k \ (mod\ 77)$: 1, 4, 9, 11, 14, 15, 16, 22, 23, 25, 36, 37, 42, 44, 49, 53, 56, 58, 60, 64, 67, 70, 71.
77 est composé.
Il y a 23 solutions.



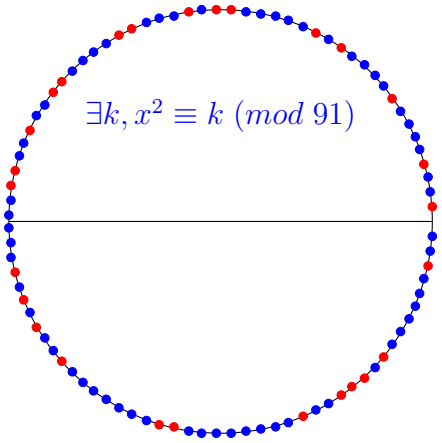
Solutions de $\exists k, x^2 \equiv k \ (mod\ 79)$: 1, 2, 4, 5, 8, 9, 10, 11, 13, 16, 18, 19, 20, 21, 22, 23, 25, 26, 31, 32, 36, 38, 40, 42, 44, 45, 46, 49, 50, 51, 52, 55, 62, 64, 65, 67, 72, 73, 76.
79 est premier.
Il y a 39 solutions.



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.

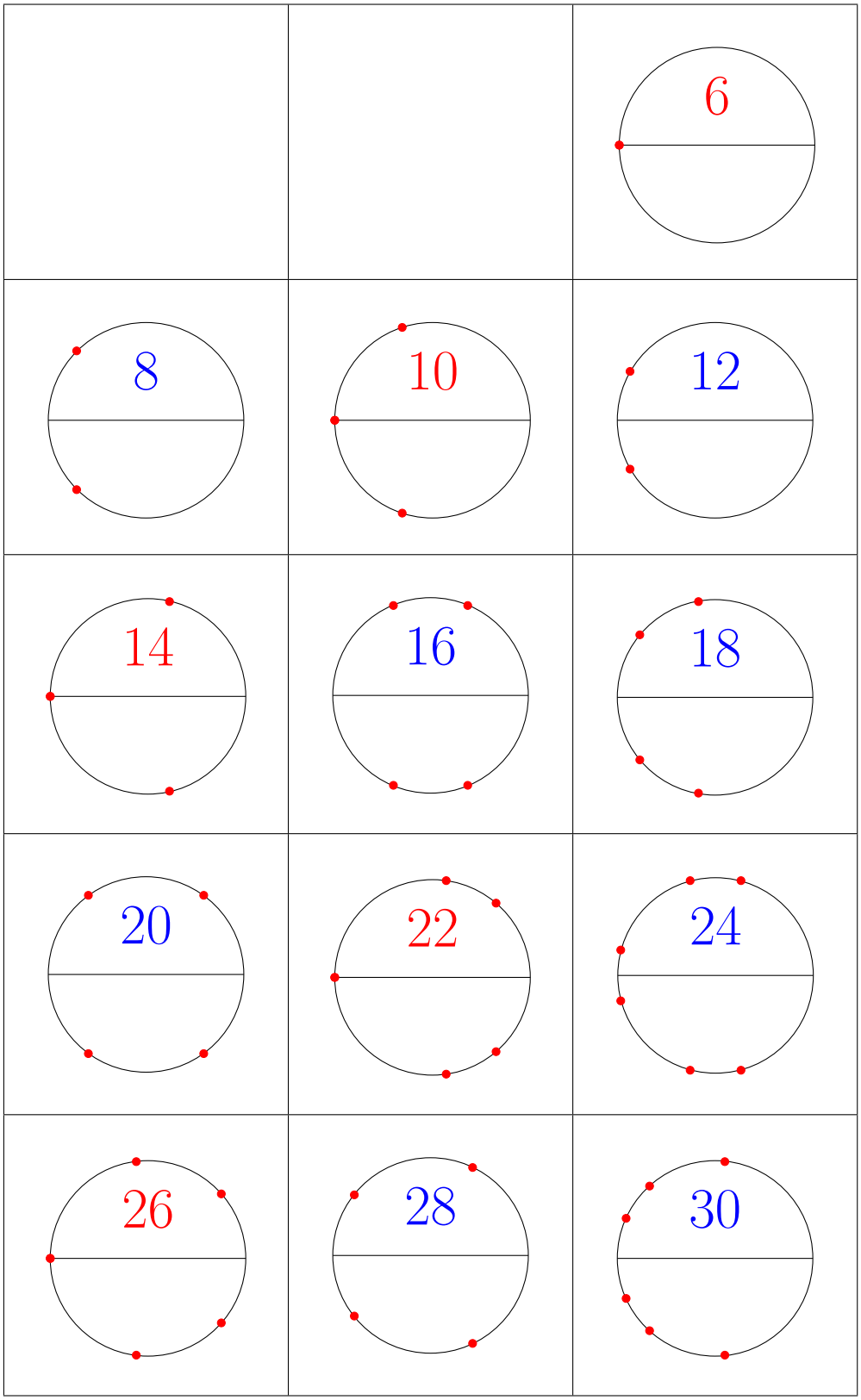


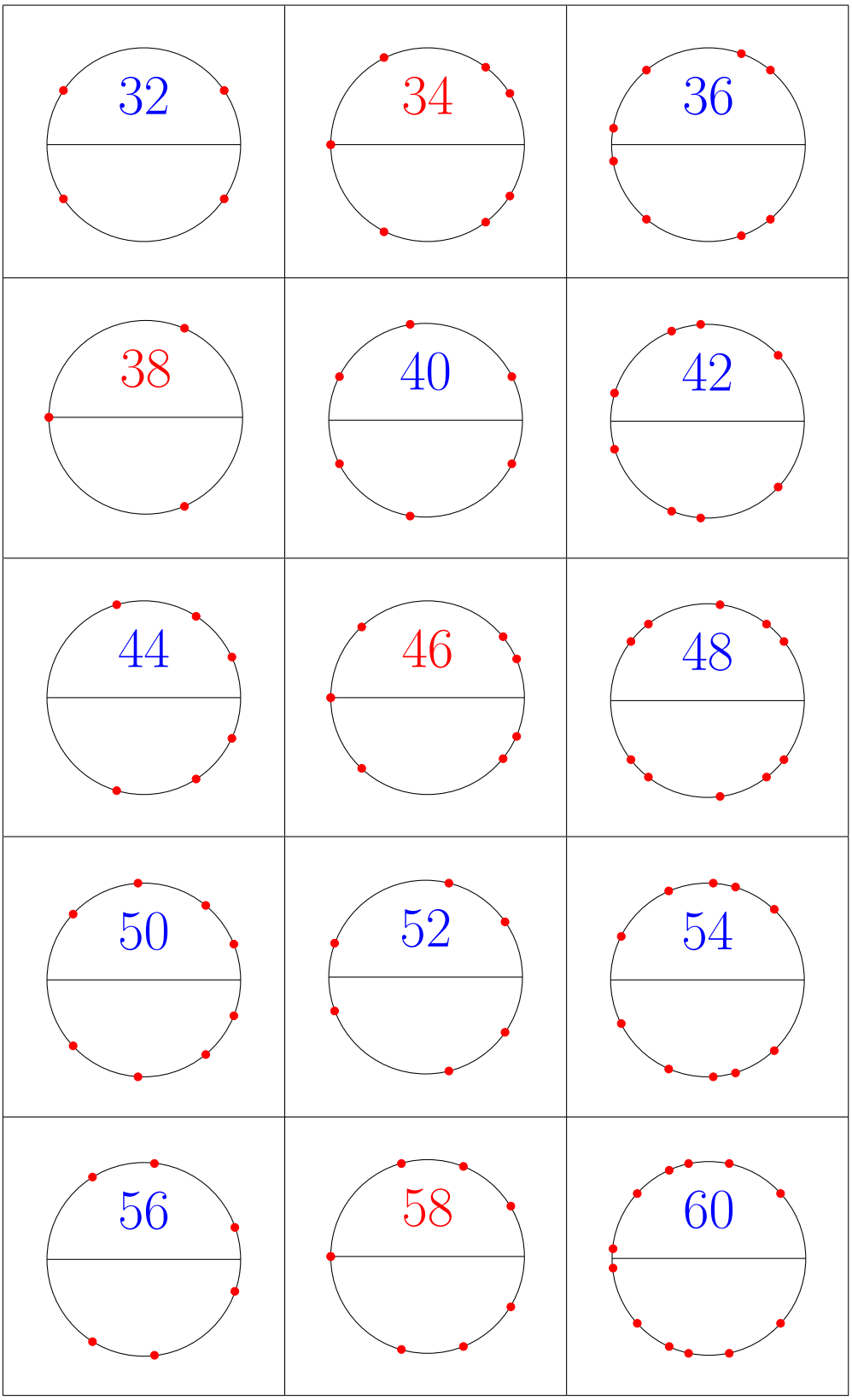
Solutions de $\exists k, x^2 \equiv k \ (mod\ 91)$: 1, 4, 9, 14, 16, 22, 23, 25, 29, 30, 35, 36, 39, 42, 43, 49, 51, 53, 56, 64, 65, 74, 77, 78, 79, 81, 88.
91 est composé.
Il y a 27 solutions.

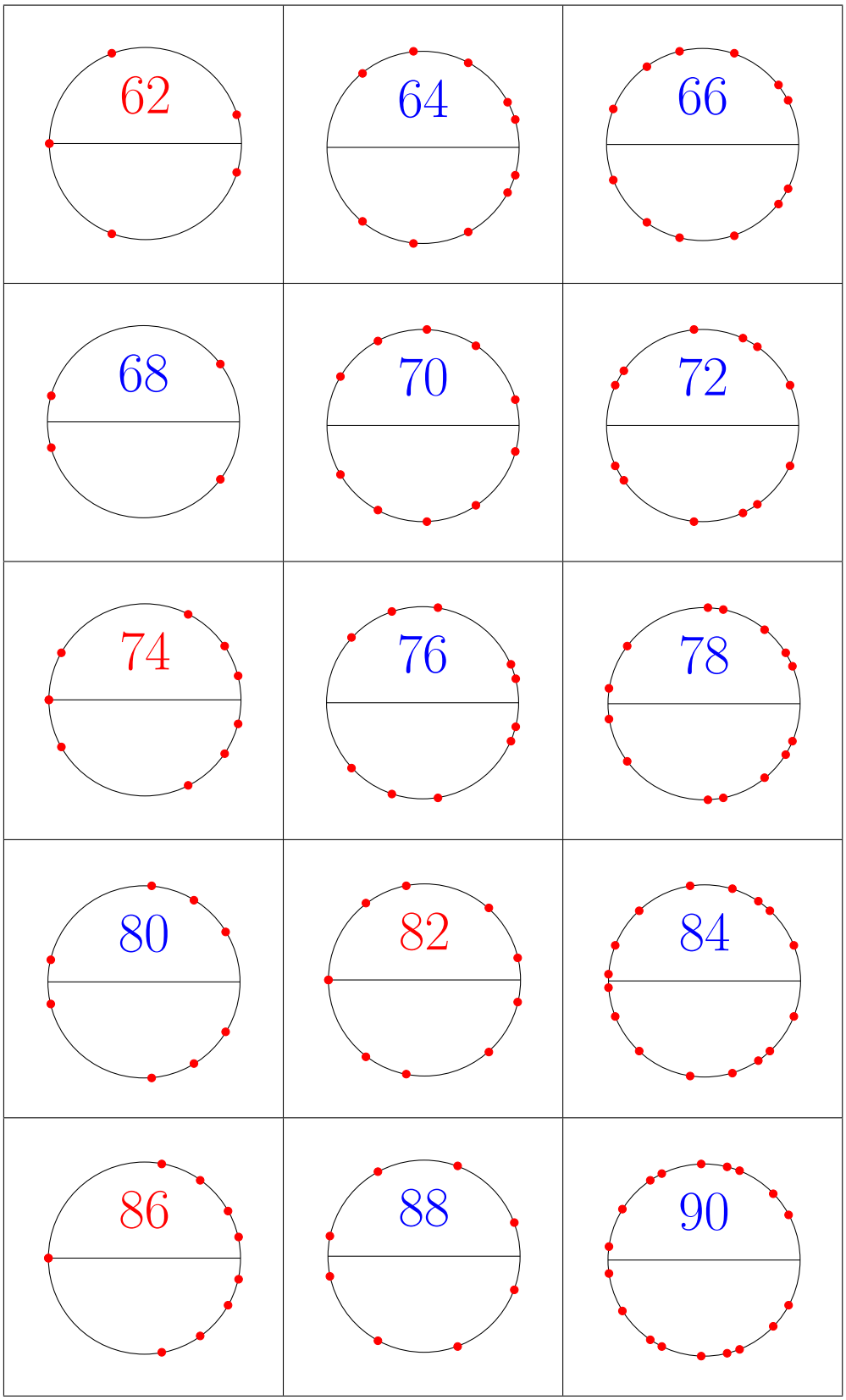


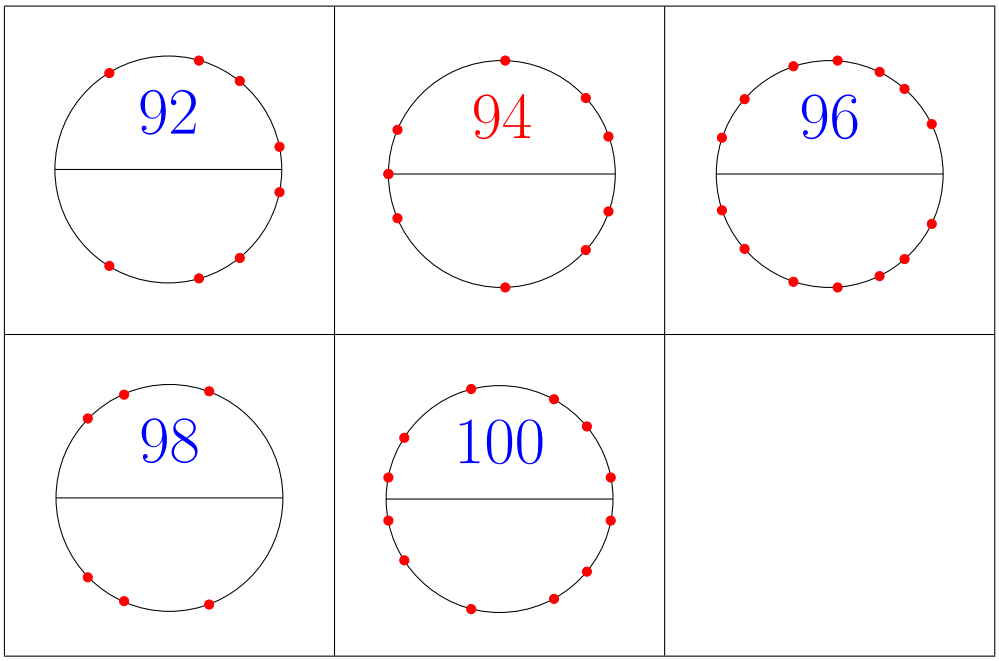
Décomposants de Goldbach sur colliers pour nombres pairs (Denise Vella-Chemla, 23.5.2019)

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.



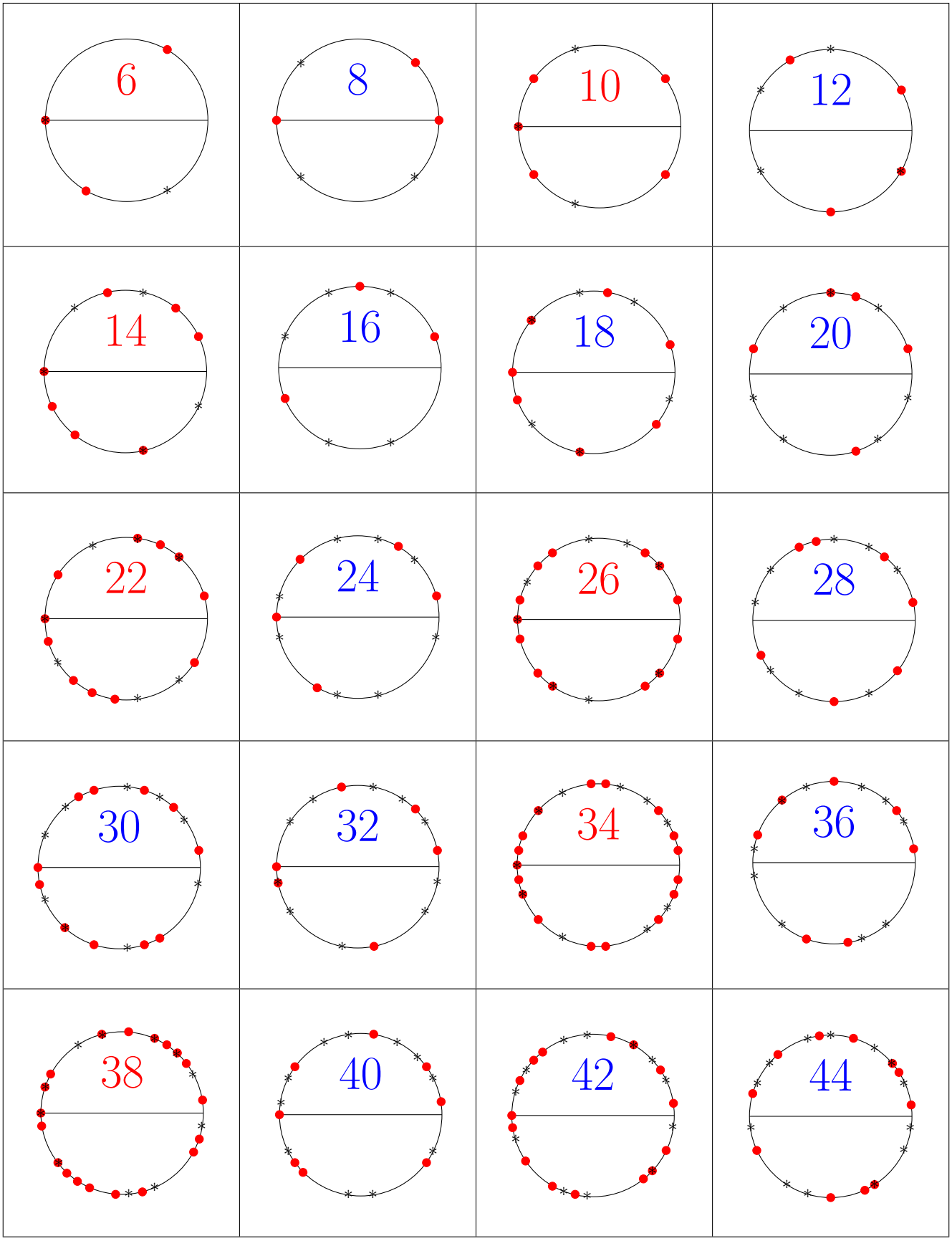

32
34
36
38
40
42
44
46
48
50
52
54
56
58
60

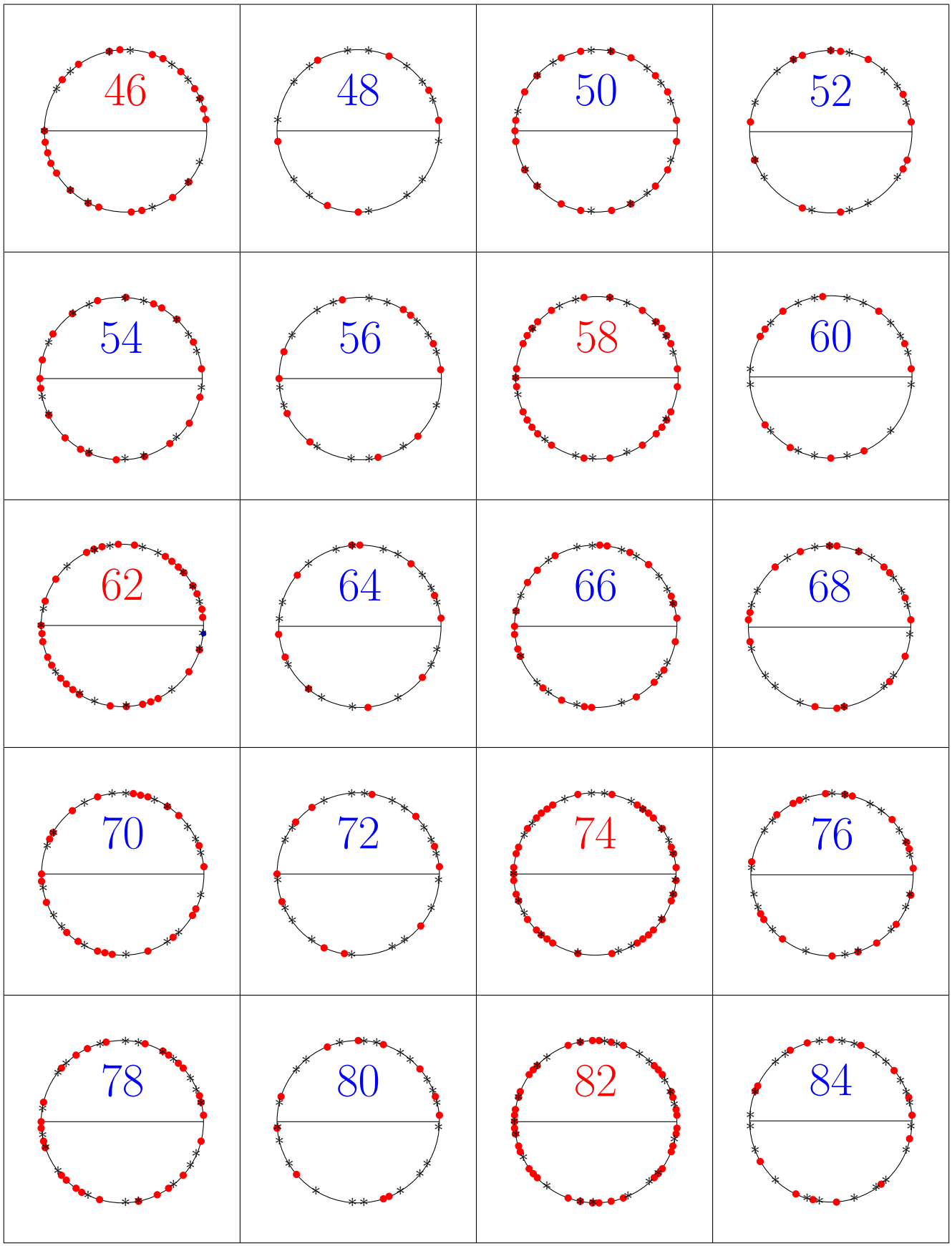

62
64
66
68
70
72
74
76
78
80
82
84
86
88
90

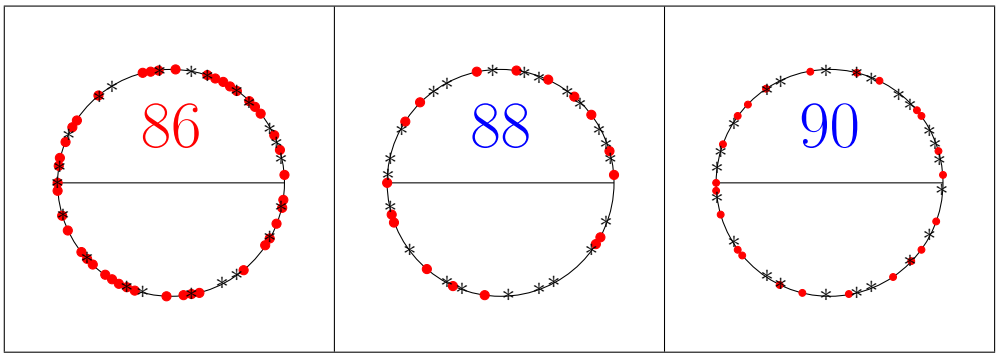

92
94
96
98
100

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

HAL
archives-ouvertes.fr

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

Denise Vella-Chemla

▶ **To cite this version:**

Denise Vella-Chemla. Goldbach's conjecture, where we find ζ in another way. 2019. hal-02145003

HAL Id: hal-02145003
https://hal.archives-ouvertes.fr/hal-02145003

Preprint submitted on 31 May 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Goldbach's conjecture, where we find ζ in another way (Denise Vella-Chemla, 29.5.2019)

One considers here Goldbach's conjecture that asserts that every even number strictly greater than 2 is the sum of two primes.

One recalls that a prime number x lesser than $\frac{n}{2}$, that doesn't share any of its division rest with n an even number strictly greater than 2, in all divisions by a prime number lesser than $\sqrt{n}$, is a Goldbach component of n (i.e. $n - x$ is prime too).

Indeed, if x lesser than $\frac{n}{2}$ doesn't share any of its division rest with n in any division by a prime lesser than $\sqrt{n}$, then $n - x$ is prime.

The asymptotic probability that an integer x lesser than $\frac{n}{2}$ be prime is provided by the prime number theorem ; it equals :

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

The minoration of $\pi(k)$ (the number of prime numbers lesser than k) by $\frac{k}{ln\ k}$ is provided in [1], page 69, for all $x \geq 17$.

Let us suppose now that x is prime. Let us study the probabilities that divisions rests of x and n are equal when one divides them by all the prime numbers lesser than $\sqrt{n}$.

Since we supposed x to be prime, we know at least that x has no rest equal to zero when we divide it by a prime number lesser than $\sqrt{n}$.

n has a certain rest, when we divide it by a prime number lesser than $\sqrt{n}$ and x has to "avoid" the rest in question (it can't have the same).

If we consider a division of n by one of its prime divisors, in which the rest is null, x has only this rest zero (0) to avoid. However x can't have (has yet avoided) the rest 0 since it's prime. It remains $p - 1$ possible rests for x when we divide it by p.

Let us consider now a division of n by a prime number which is not an n's divisor, let us call it d. n has, when we divide it by d a rest that is different from 0 that x must avoid. In this case, x has the choice between $p - 2$ possible rests in its division by p, that it can have with equal probabilities the one or the other but we are going to use the fact that $\frac{1}{p-2} > \frac{1}{p-1}$ to minorate each probability modulo a given prime number p by $\frac{1}{p-1}$, to homogeneize the different possible cases (if we are considering or not a prime divisor of n).

Let us see examples, to fix ideas : in a division by prime number 3, we minorate the number of possibilities by 2 possibilities for the division rests (1 or 2), and x has one chance among two (i.e. 1/2) to obtain one or the other.

In a division by 5, it remains 4 possibilities for x to have some division rest among 1, 2, 3 or 4, and x has one chance among 4 (i.e. 1/4) to obtain the one or the other.

In a division by 7, it remains 6 possibilities for x to have its division rest among 1, 2, 3, 4, 5 or 6, and x has one chance among 6 (i.e. 1/6) to obtain the one or the other.

More generally, in a division by p, one minorates the probability for x and n to have the same division rest in the following way : there are $p - 1$ division rests possibilities at most for x (that are 1, 2, ..., $p - 1$), and x has one chance among $p - 1$ (i.e. $\frac{1}{p-1}$ to obtain the one or the other of those division rests).

All those events (rests sharings) having independent probabilities, the probability to obtain their conjunction is the product of the probabilities of each event alone (the considered events being "x and n have the same rest in a division by 3", or "x and n have the same rest in a division by 5", etc.).

This product of probabilities can be written :

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

We can transform this in :

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

and then in

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

We can extend this product to the set of all primes in infinite number because in fact, it's modulo every prime number that n and x have not to be in the same congruence class (i.e. mustn't share their rest), for the complementary of x to n (i.e. $n-x$) to be prime too. One can recognize then $-\zeta(-1)$ in the calculus of the product for x and n have different rests in a division by whatever prime number. Ramanujan demonstrated that $\zeta(-1) = -\frac{1}{12}$. The note [1] provides a simple demonstration of this fact.

We obtain the cardinal of a set of numbers x that are prime on one side, and that don't have the same division rest than n in a division by any prime number lesser than $\sqrt{n}$ (and in fact by any prime) [2] on the other side :

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

that is :

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

This seems to make Goldbach's conjecture true above $n = 92$ [3].

Attempt to write this reasoning more formally :

We want to demonstrate that $\forall n$ even, $\exists x, 3 \leq x \leq n/2$ odd prime such that $n-x$ is prime too.

$$\begin{array}{lll} (1)\quad x \text{ prime} & \iff \forall p \text{ prime} \leq \sqrt{x}, & x \not\equiv 0\ (mod\ p). \\ (2)\quad n-x \text{ prime} & \iff \forall p \text{ prime} \leq \sqrt{n-x}, & n-x \not\equiv 0\ (mod\ p) \\ & \iff \forall p \text{ prime} \leq \sqrt{n-x}, & x \not\equiv n\ (mod\ p). \end{array}$$

1. Par définition $S = 1+2+3+4+5+....$

One notes than calculating term by term the difference :

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

So $S-4S = B$, i.e. $-3S = B$, d'où $S = -\frac{B}{3} = -\frac{\frac{1}{4}}{3}$ So one finds the expected result : $S = -\frac{1}{12}$.

2. The fact that x doesn't share any division rest with n in divisions by prime numbers lesser than $\sqrt{n}$ is not the same as the fact to be prime to n (to have no common factor greater than 1 with n). This last condition is necessary (i.e. *implied*) but not sufficient (i.e. *implying*). For instance, 17 and 81, that have a sum equal to 98, are both *prime to* 98, but they are not Goldbach'decomponents of 98 since 17 shares its division rest 2 with 98 when we divide them by 3 (Gauss writes this $17 \equiv 98\ (mod\ 3)$, he is the one who drew attention of everyone on the importance to work in prime fields).

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

One can replace in (1) the condition $\forall p$ prime $\leq \sqrt{x}$ by the strongest condition $\forall p$ prime $\leq \sqrt{n/2}$ since we let $x \leq n/2$.

One can minorate the number of prime numbers lesser than $\frac{n}{2}$ by $\frac{\frac{n}{2}}{log\left(\frac{n}{2}\right)}$.

It matters then to find how many numbers in this set of prime numbers lesser than $\frac{n}{2}$, set whose we know the cardinal, share their division rest with n ; sharing a rest with n, the even number considered, consists in "fixing" the possible rest and so to make decrease by 1 the number of possible rests for each module ; we must multiply the cardinal $\pi\left(\frac{n}{2}\right)$ minorated by $\frac{\frac{n}{2}}{log\left(\frac{n}{2}\right)}$ (that corresponds to the condition (1) above) by the probability there would be a rest sharing modulo each prime number independently (that corresponds to the condition (2) above) and this probability has as value $-\zeta(-1) = \frac{1}{12}$. It's a set cardinal one obtains by this process of multiplying a set cardinal by a probability. Such a calculus seems to make sense and seems to ensure a cardinal equal at least to 1 above 92.

Bibliography

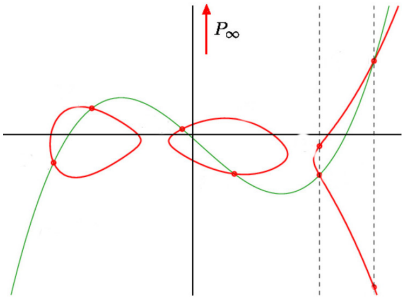
[1] J. B. Rosser et L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, dedicated to Hans Rademacher for his seventieth birthday, Illinois J. Math., Volume 6, Issue 1 (1962), 64-94.

Ô stop ! (Denise Vella-Chemla, 31.5.2019)

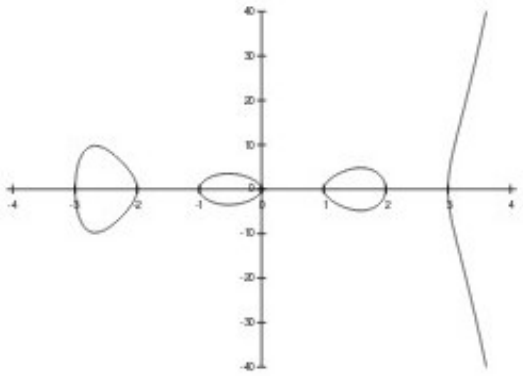
Il s'agit de garder en mémoire le fait qu'en calculant les indices de la section 53 des Recherches arithmétiques de Gauss (consultables ici http://denise.vella.chemla.free.fr/indices-RA53.pdf), on a réalisé à nouveau que la caractéristique des nombres premiers est d'avoir une solution au moins à l'équation $x^{\frac{p-1}{2}} \equiv 1 \ (mod \ p)$ (on peut réécrire cette congruence $x^{\frac{p-1}{2}} - kp - 1 = 0$), alors que cette équation n'a pas de solution pour p composé.

Cela permet d'associer à chaque nombre premier une courbe hyperelliptique de genre $\frac{p-1}{2}$ (ou une surface de Riemann à $\frac{p-1}{2}$ trous), selon les exemples ci-dessous.

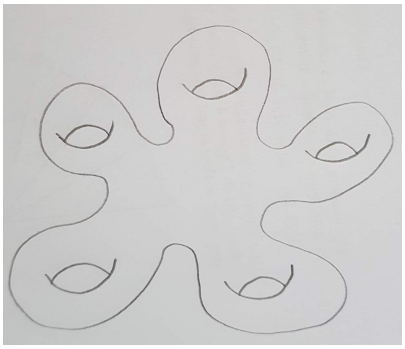
Exemple d'une courbe hyperelliptique de genre 2 associable au nombre premier 5



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



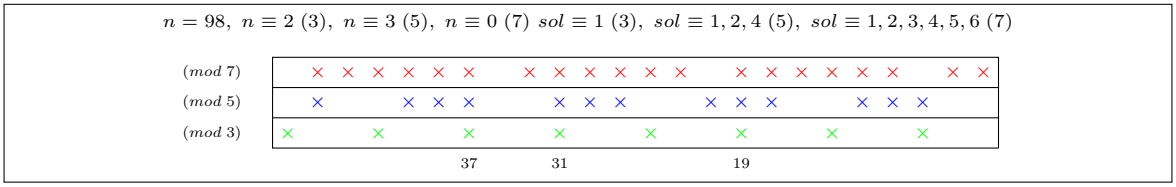
Exemple d'une surface de Riemann à 5 trous associable au nombre premier 11



Conjecture de Goldbach et les impairs (Denise Vella-Chemla, 2.6.2019)

Après avoir écouté une conférence de Timothy Gowers, présentant les leçons de Pólya pour résoudre un problème (ici https://vimeo.com/331192239), ainsi qu'un interview qu'il a donné dans le cadre des Heidelberg Laureate Forum (ici https://www.youtube.com/watch?v=7F97Q1DGOkE), on a l'idée d'appliquer des éléments de connaissance qui nous ont été utiles pour comprendre la conjecture de Goldbach forte (tout nombre pair supérieur à 6 est la somme de deux nombres premiers impairs) aux cas des nombres impairs et cela nous amène à une curieuse découverte. La conjecture de Goldbach pour les nombres impairs exprime que tout nombre impair est la somme de 3 nombres premiers. Harald Helfgott a proposé une démonstration de la conjecture de Goldbach pour les impairs en 2013. La conjecture de Goldbach pour les impairs découlerait trivialement de la conjecture de Goldbach forte (en effet, tout nombre impair étant la somme d'un nombre pair et de 3, si tout nombre pair était la somme de deux nombres premiers, alors tout nombre impair serait la somme de ces deux nombres premiers et de 3, et donc la somme de trois nombres premiers). Ce n'est pas à cela qu'on s'intéresse ici. Il s'agit plutôt d'étudier quel est le complémentaire à un nombre impair n d'un nombre premier qui n'a aucun reste commun avec n (dans les divisions par les nombres premiers inférieurs à $\sqrt{n}$).

Précisons l'idée : pour trouver les décomposants de Goldbach d'un nombre pair n, on a pris l'habitude d'utiliser un crible particulier : le crible d'élimination des restes modulaires de n ; par exemple, si on cherche les décomposants de Goldbach de 98, qui est égal à 2 modulo 3, à 3 modulo 5 et à 0 modulo 7, on va éliminer tous les nombres impairs qui sont égaux soit à 0 soit à 98, modulo 3 ou bien modulo 5 ou bien modulo 7. Ce faisant, on obtiendra tous les décomposants de Goldbach de 98 compris entre la partie entière de la racine carrée de 98 et la moitié de 98. On a symbolisé ceci par des petits dessins tels que celui ci-dessous, dans lequel les croix montrent les nombres impairs qui ne sont pas égaux à 0 ou bien à 98, modulo 3, modulo 5 et modulo 7.



On décide de réappliquer le même crible aux nombres impairs n, pour voir si le complémentaire d'un nombre premier p qui ne partagerait aucun de ses restes avec n impair aurait des propriétés particulières.

On utilise le programme suivant :

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

int tabfacteurs[2021], tabpuiss[2021], tabexpo[2021], residfacteurs[2021] ;

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

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

```
int factorise(int i) {
  int k, p, nbdiv, tempo, expo ;
  int tab[2018] ;

  std::cout << i << "\n" ;
  tab[i] = 1 ;
  tabfacteurs[i] = 1 ;
  tabpuiss[i] = 1 ;
  tabexpo[i] = 1 ;
  tempo = i ; p = i/2 ; nbdiv = 1 ;
  if (prime(tempo)) {
      tabfacteurs[1] = tempo ;
      tabpuiss[1] = tempo ;
      tabexpo[1] = 1 ;
  }
  else while ((tempo > 1) && (p > 1)) {
           if ((prime(p)) && ((tempo%p) == 0)) {
               tabfacteurs[nbdiv] = p ;
               nbdiv = nbdiv+1 ;
               tempo = tempo/p ;
           }
           p=p-1 ;
  }
  if (not(prime(i))) nbdiv=nbdiv-1 ;
  if ((nbdiv == 1) && (prime(i))) {
      tabpuiss[1] = i ;
      tabexpo[1] = 1 ;
  }
  else if ((nbdiv == 1) && (not(prime(i)))) {
      tempo = tabfacteurs[1] ;
      tabpuiss[1] = i ;
      expo = 1 ;
      while (tempo < i) {
          tempo=tempo*tabfacteurs[1] ;
          expo = expo+1 ;
      }
      tabexpo[1] = expo ;
  }
  else if (nbdiv > 1) {
      for (k = 1 ; k <= nbdiv ; ++k) {
          tempo = tabfacteurs[k] ;
          expo = 1 ;
          while (((i % tempo) == 0) && (tempo < i)) {
              tempo=tempo*tabfacteurs[k] ;
              expo = expo+1 ;
          }
          tabpuiss[k] = tempo/tabfacteurs[k] ;
          tabexpo[k] = expo-1 ;
      }
  }
  for (k = nbdiv ; k >= 1 ; --k) {
      std::cout << tabfacteurs[k] << "^" ;
      std::cout << tabexpo[k] << "." ;
  }
}

int main (int argc, char* argv[]) {
  int x, y, module ;
  bool restesdifferents ;

  for (x = 7 ; x <= 2020 ; x = x+2) {
      std::cout << "\n\n" << x << "␣-->␣\n" ;
      for (y = sqrt(x) ; y <= x/2 ; ++y)
        if (prime(y)) {
            restesdifferents = true ;
            for (module = 3 ; module <= sqrt(x) ; module = module+2) {
                if (prime(module))
                  restesdifferents = restesdifferents && ((x % module) != (y % module)) ;
            }
            if (restesdifferents) {
                std::cout << "\n" << y << "␣+␣" ;
                factorise(x-y) ;
                std::cout << "\n" ;
            }
        }
  }
}
```

Le résultat de ce programme est consultable ici : http://denise.vella.chemla.free.fr/resetlesimpairs.pdf.

On constate avec surprise qu'il semblerait qu'un nombre impair puisse toujours s'écrire $p_1 + 2^k p_2$ avec $k \geq 1$ et p_1 et p_2 premiers. Cette constatation est peut-être aussi difficile à démontrer que la conjecture de Goldbach.

L'intérêt cependant d'une telle découverte, si elle s'avérait juste, est simplement qu'elle fournit une généralisation de la conjecture de Goldbach, la conjecture forte pour les pairs pouvant être vue comme une réécriture de la formule proposée pour les impairs, avec $k = 0$, i.e. pouvant s'écrire pour tout n pair supérieur ou égal à 6, selon une écriture de la forme $n = p_1 + 2^0 p_2$.

Tentative de démonstration du fait que s'il existe, pour un nombre impair donné n, un nombre premier $p_1 \leq \frac{n}{2}$ qui lui est incongru selon tout module inférieur à sa racine carrée, alors le complémentaire à n de p_1 est un nombre de la forme $2^k p_2$ avec p_2 premier et $k \geq 1$

Soit n un nombre impair et supposons qu'il existe une décomposition additive de n de la forme $p_1 + n'$ avec $p_1 \not\equiv n \ (mod\ m)$ pour tout m premier tel que $3 \leq m \leq \sqrt{n}$. Montrons qu'n' est alors nécessairement de la forme $2^k p_2$ avec $k \geq 1$ et p_2 premier.

n étant impair, n' est forcément pair. Voyons pourquoi, sous la condition que p_1 existe, alors n' ne contient dans sa factorisation qu'un seul nombre premier (qu'on appellera p_2), en plus d'un certain nombre d'occurrences du facteur premier 2. On a :

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

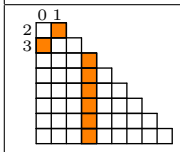
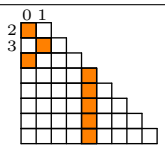
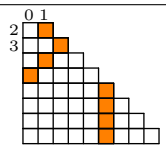
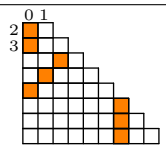
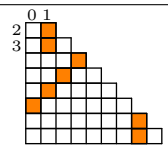
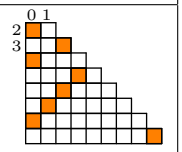
et

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

Cela a pour conséquence que les deux diviseurs premiers autres que 2 de n' devraient être supérieurs à $\sqrt{n}$ (car (1) $\iff$ $n - p_1 \not\equiv 0 \ mod\ m$ avec les mêmes conditions) ; mais si tel était le cas, i.e. si $n' = 2p'p''$ avec $p' > \sqrt{n}$ et $p'' > \sqrt{n}$ alors n' serait supérieur à $2n$, ce qui est en contradiction avec l'hypothèse $\frac{n}{2} \leq n' \leq n$. Le complémentaire de p_1 à n est alors forcément de la forme $2^k p_2$ avec $k \geq 1$ et p_2 premier impair. On n'est cependant pas assuré de l'existence obligatoire de p_1.

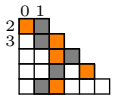
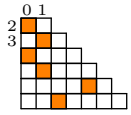
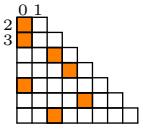
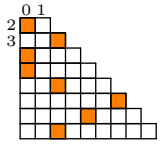
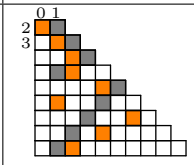
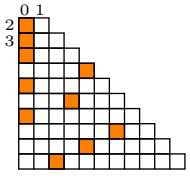
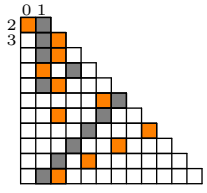
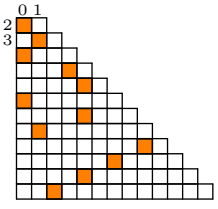
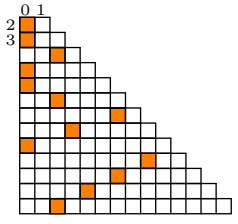
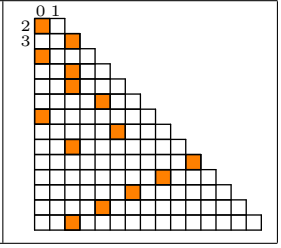
Tores trapézoïdaux (Denise Vella-Chemla, 9.6.2019)

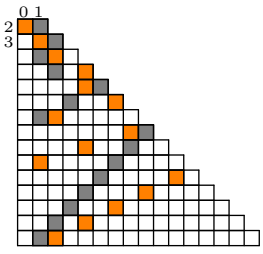
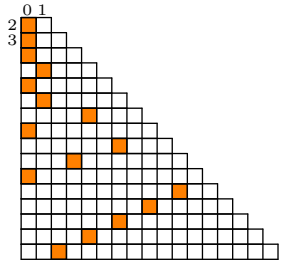
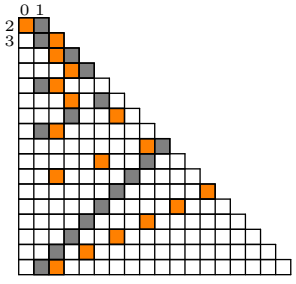
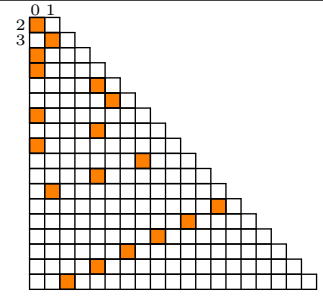
On observe d'abord des pixels qui avancent dans un tore trapézoïdal de taille donnée (utile par exemple si on cherche les décomposants de Goldbach de 20).
Les indices des colonnes de chaque tore trapézoïdal représenté par une matrice triangulaire basse de pixels sont égaux à 0, 1, 2, etc.
Les indices des lignes sont égaux à 2, 3, etc.
Le pixel $[i, j]$ de la matrice de n est orange si $n \equiv i \ (mod\ j)$.
Chaque pixel arrivant au bout d'une ligne à droite est ramené à l'extrémité gauche de la ligne et se remet à parcourir la ligne de gauche à droite.

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

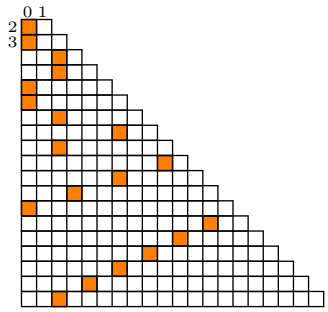
On fournit ci-dessous les tores associés aux seuls nombres pairs. Pour voir le mouvement d'un pixel d'un tore à l'autre, rappelons-nous qu'il saute une case de nombre pair en nombre pair. On montre pour les nombres pairs $2p$ (en orange) doubles d'un nombres premier p (en gris) ce dcomposant de Goldbach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

Sont décomposants de Goldbach d'un nombre pair n les nombres premiers dont le tore coupé à $n/2$ n'a aucun pixel commun avec celui de n. Un nombre premier est caractérisé par le fait que la colonne d'indice 0 de ses tores (quelle que soit leur taille) ne contient qu'un seul pixel à 1. Dans les trapèzes de pixels ci-dessous, on a également détaillé que 11 est décomposant de Goldbach de 54, que 47 est un décomposant trivial de 94 (pour montrer la diagonale de pixels d'un nombre premier, là 47, dans le bas du graphique).

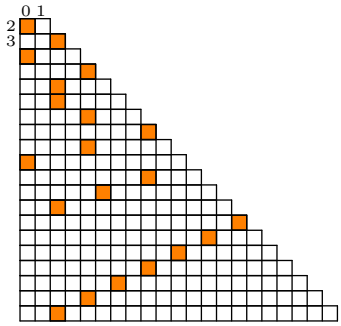
14 : 3, 7	16 : 3, 5	18 : 5, 7	20 : 3, 7	22 : 3, 5, 11
				
24 : 5, 7, 11	**26 : 3, 7, 13**	**28 : 5, 11**	**30 : 7, 11, 13**	**32 : 3, 13**
				

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

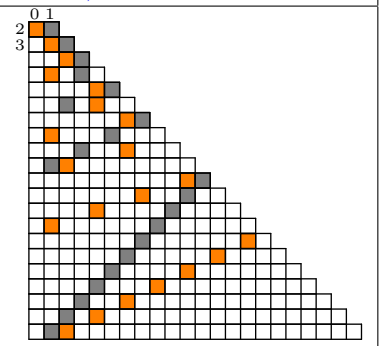
42 : 5, 11, 13, 19



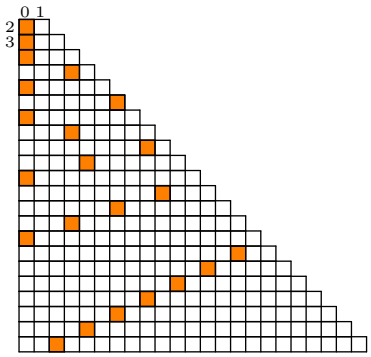
44 : 7, 13



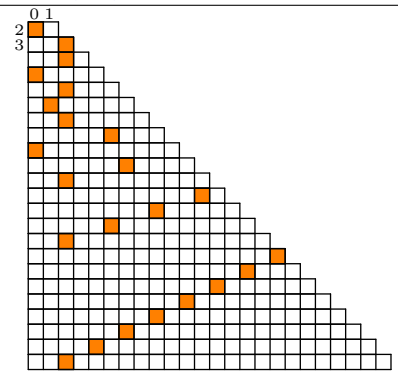
46 : 17, 23



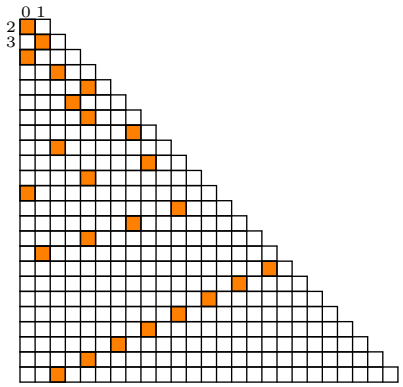
48 : 7, 11, 17, 19



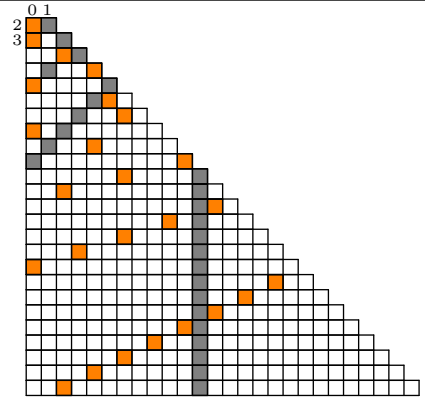
50 : 7, 13, 19



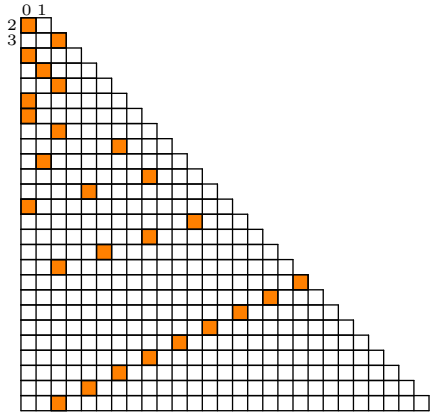
52 : 11, 23



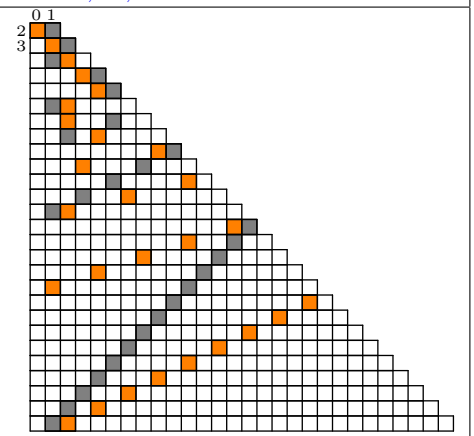
54 : 7, 11, 13, 17, 23



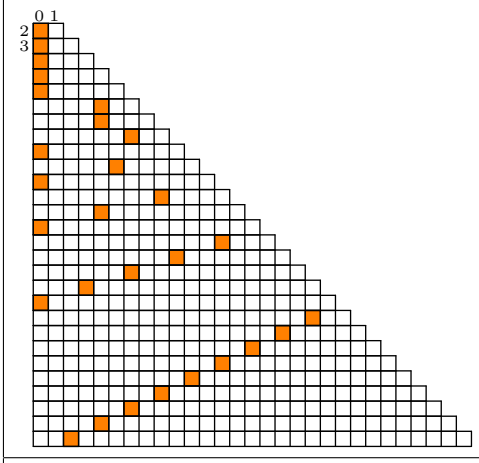
56 : 13, 19



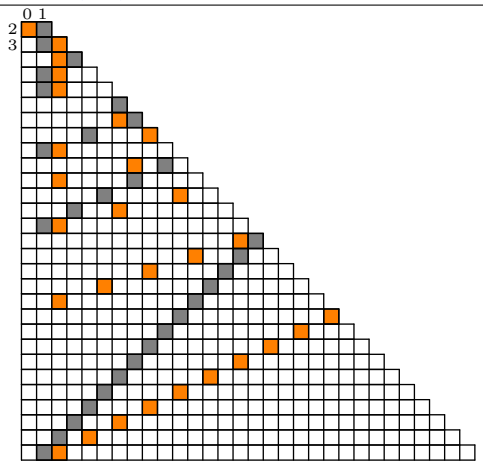
58 : 11, 17, 29



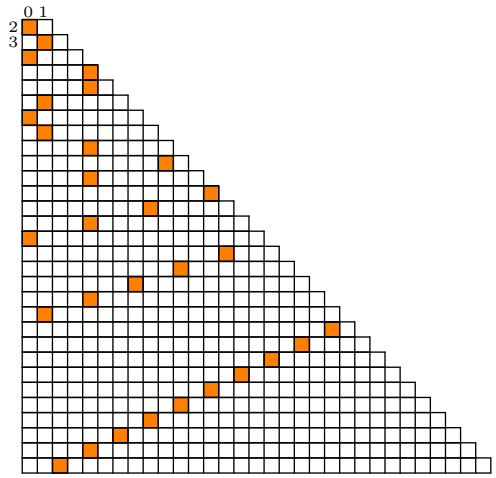
60 : 7, 11, 13, 17, 19, 23, 29



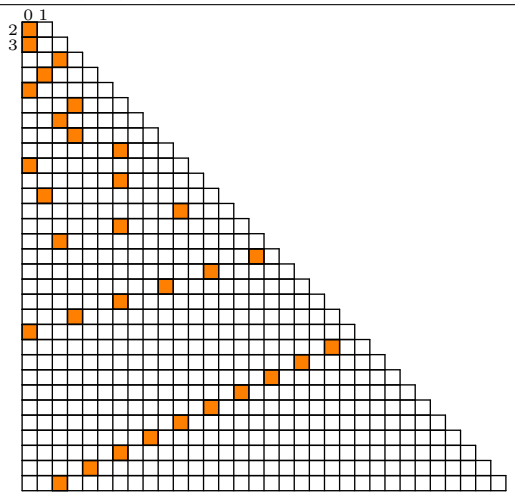
62 : 13, 19, 31



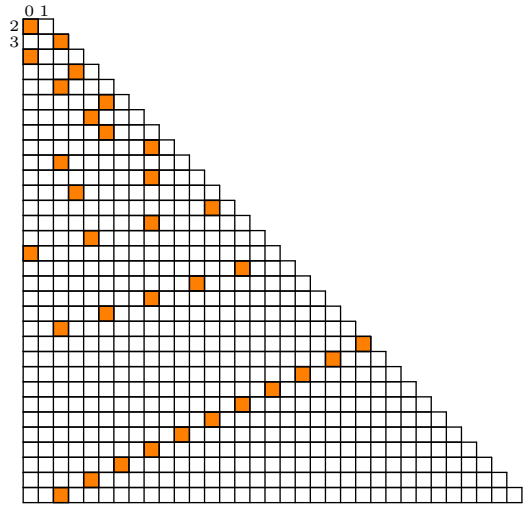
64 : 11, 17, 23



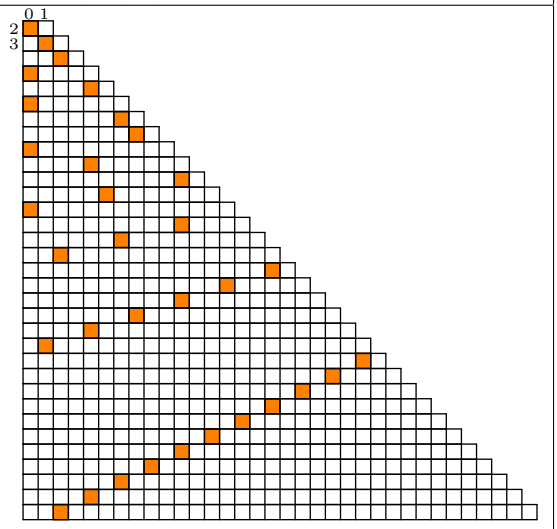
66 : 13, 19, 23, 29

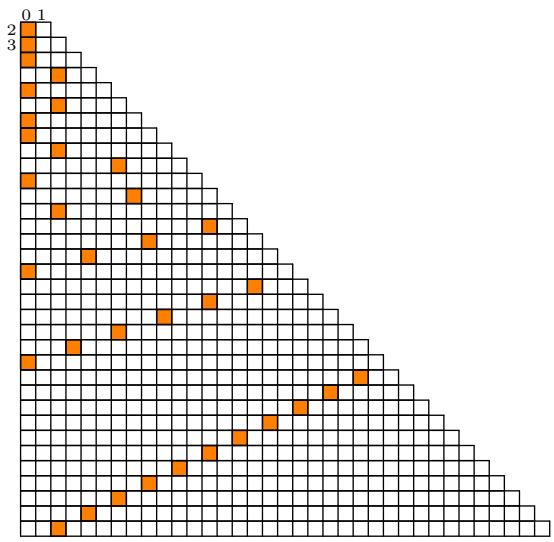
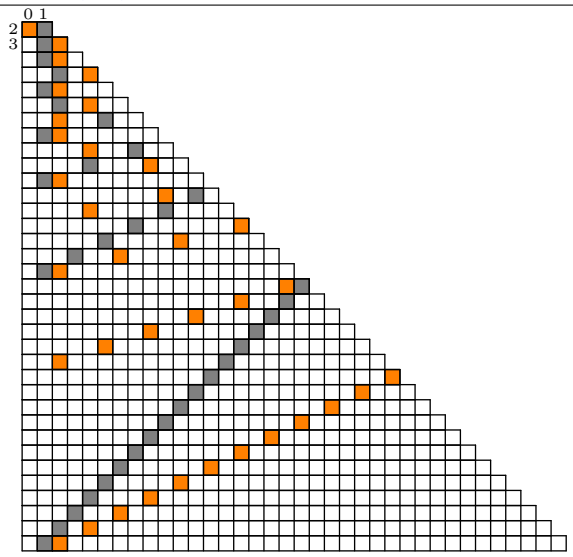
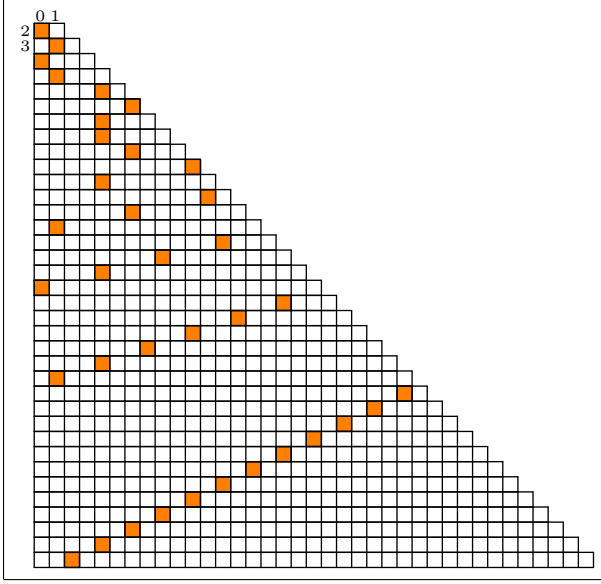
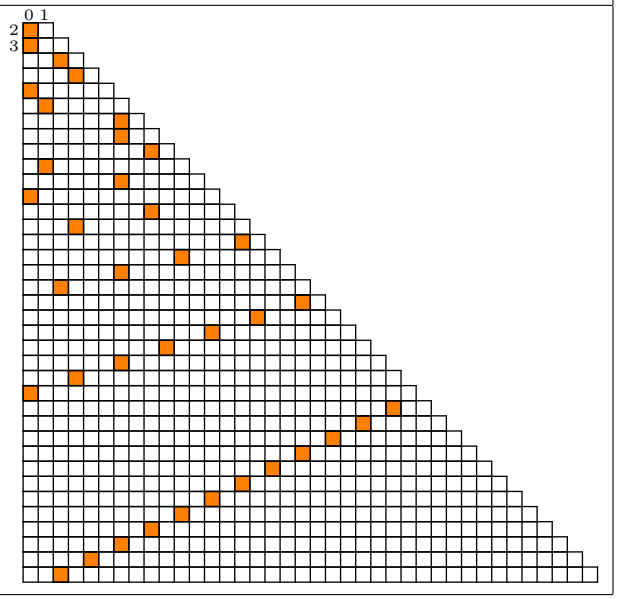


68 : 31

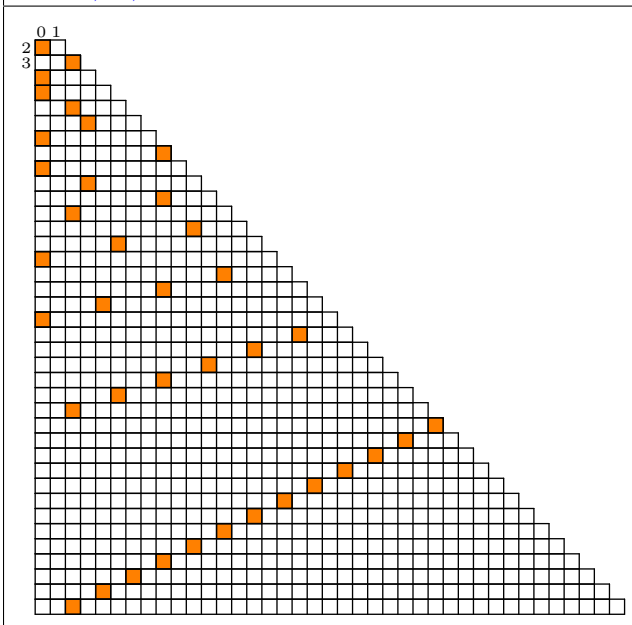


70 : 11, 17, 23, 29

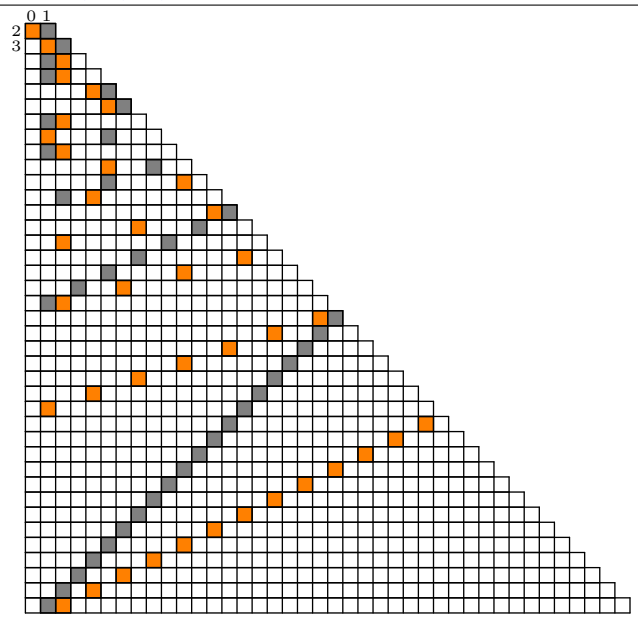


$72 : 11, 13, 19, 29, 31$	$74 : 13, 31, 37$
	
$76 : 17, 23, 29$	$78 : 11, 17, 19, 31, 37$
	

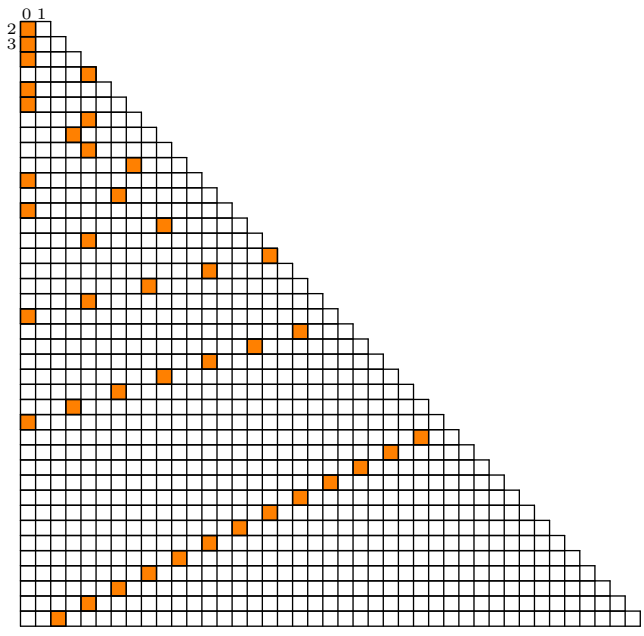
80 : 13, 19, 37



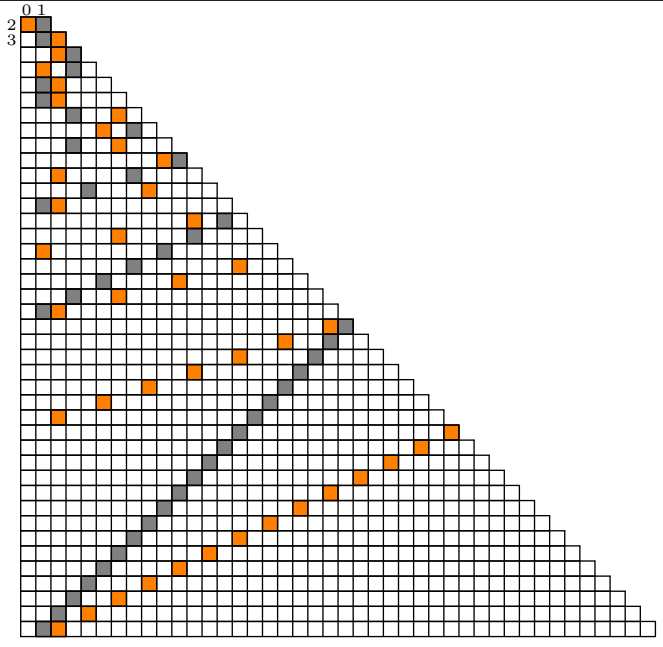
82 : 11, 23, 29, 41



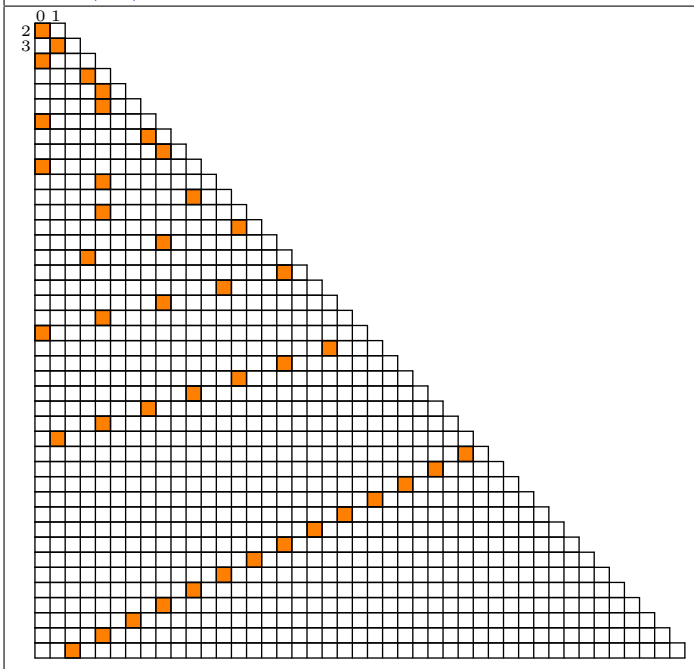
84 : 11, 13, 17, 23, 31, 37, 41



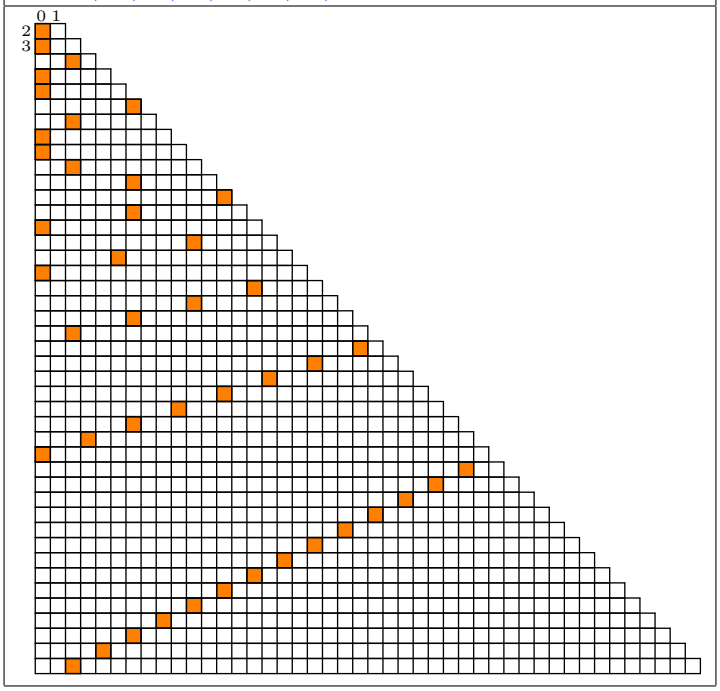
86 : 13, 19, 43



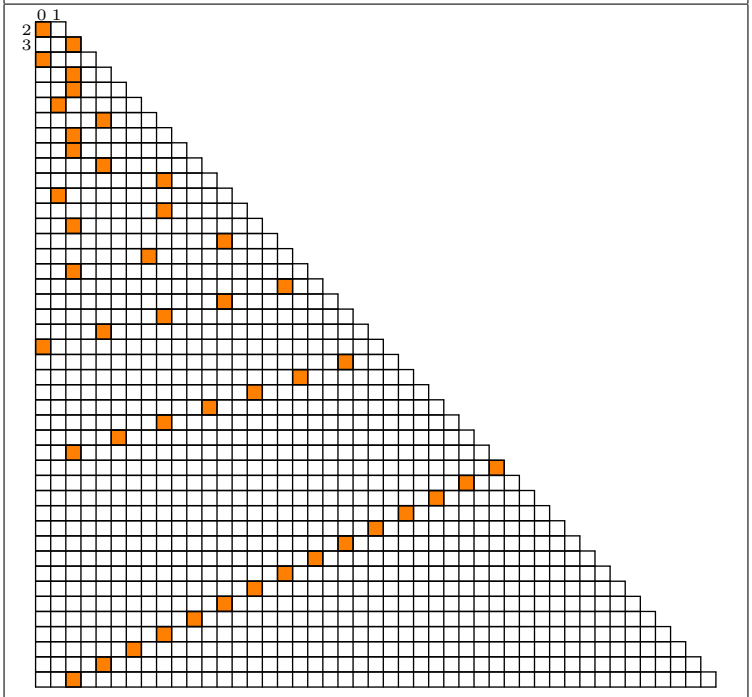
88 : 17, 29, 41



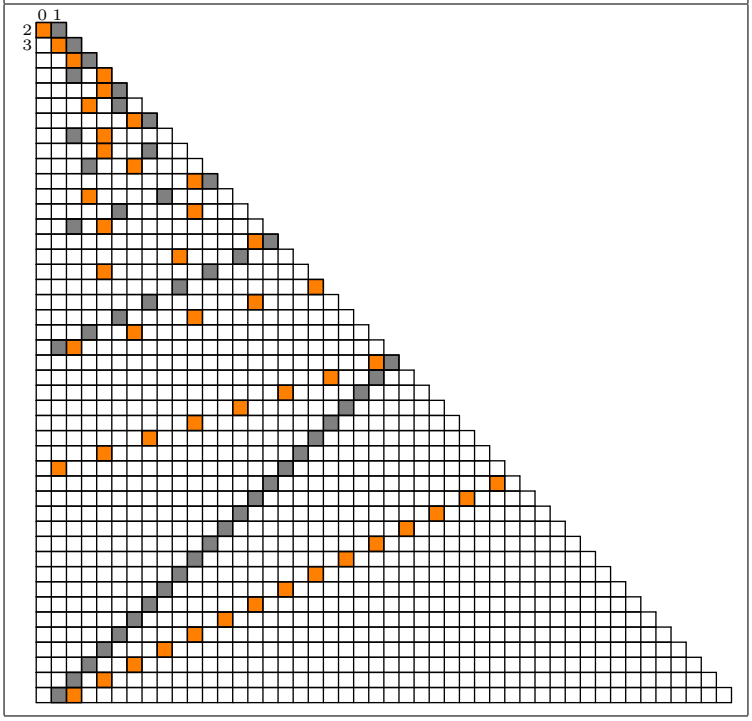
90 : 11, 17, 19, 23, 29, 31, 37, 43



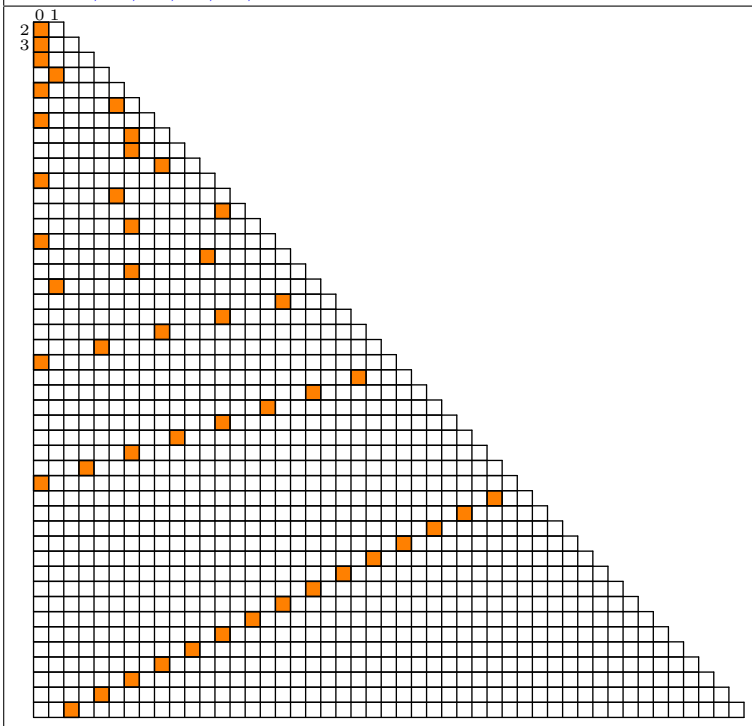
92 : 13, 19, 31



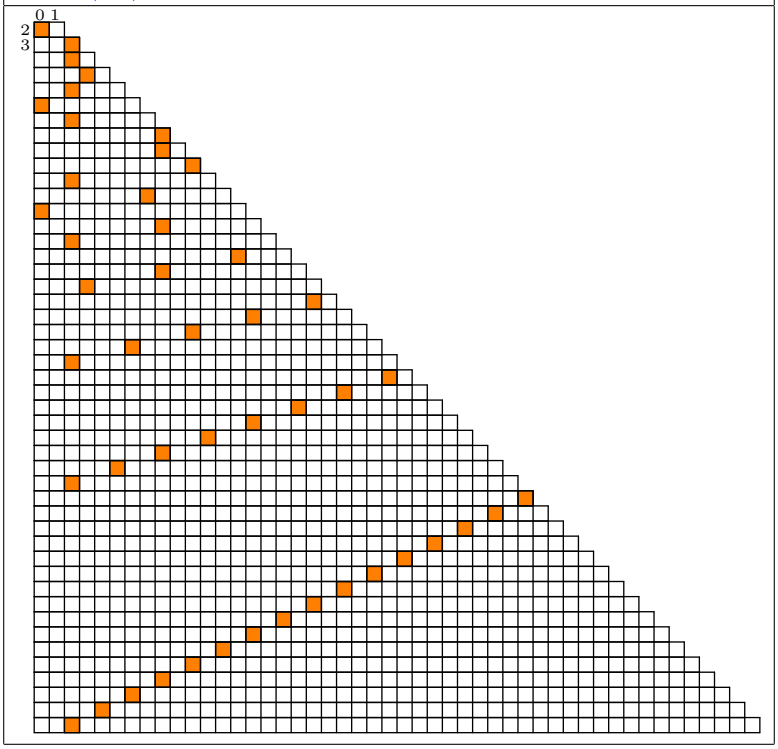
94 : 11, 23, 41, 47



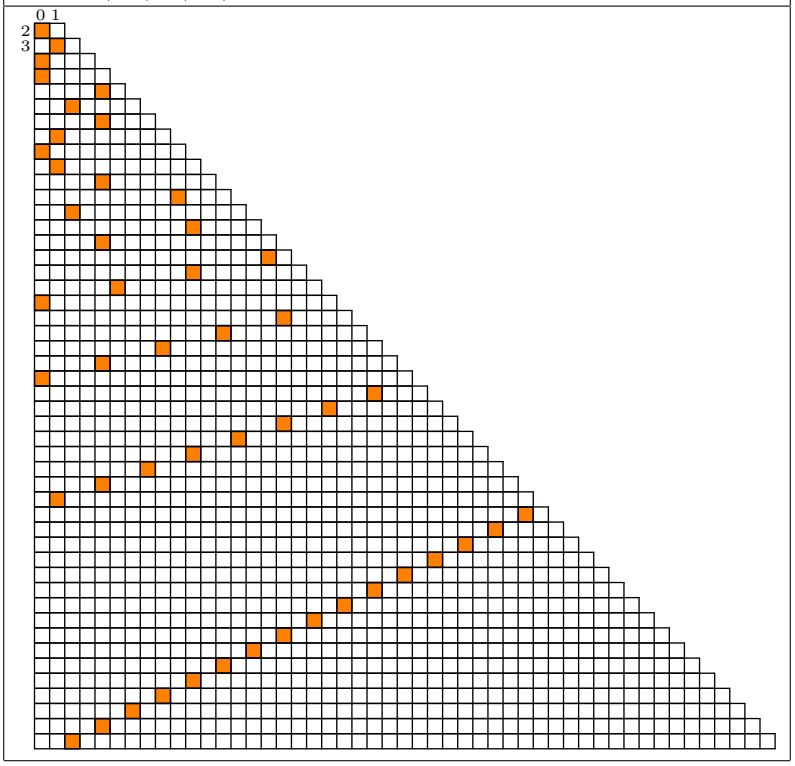
96 : 13, 17, 23, 29, 37, 43



98 : 19, 31, 37

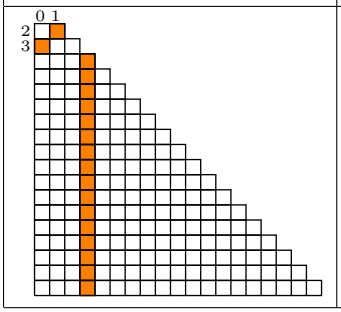


100 : 11, 17, 29, 41, 47

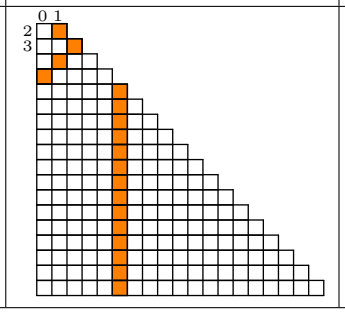


Ci-dessous, on peut observer les tores des nombres premiers 3, 5, 7, 11, 13, 17, 19 à la recherche des décomposants de Goldbach de 40.

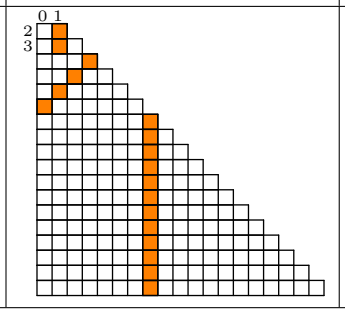
$n = 3$



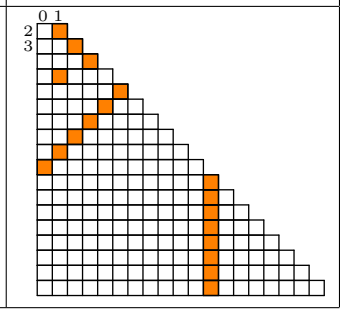
$n = 5$



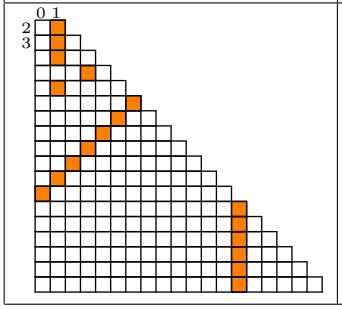
$n = 7$



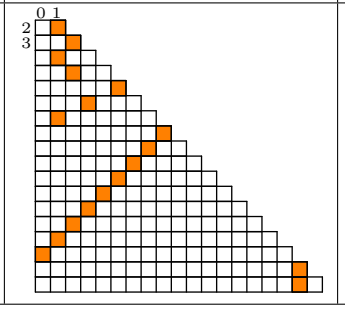
$n = 11$



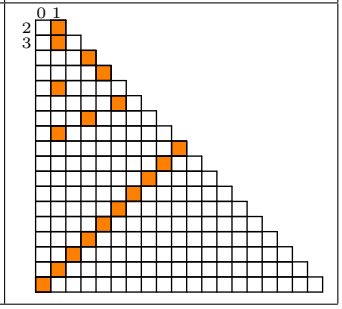
$n = 13$



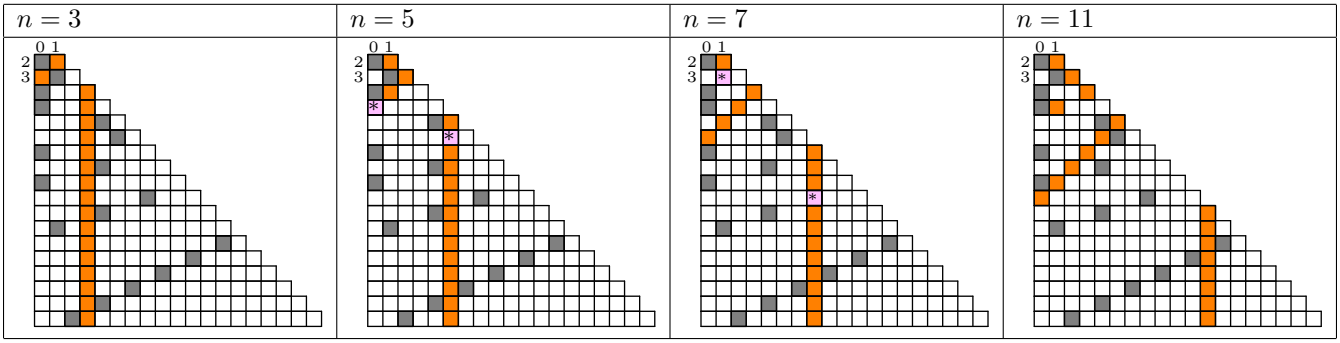
$n = 17$

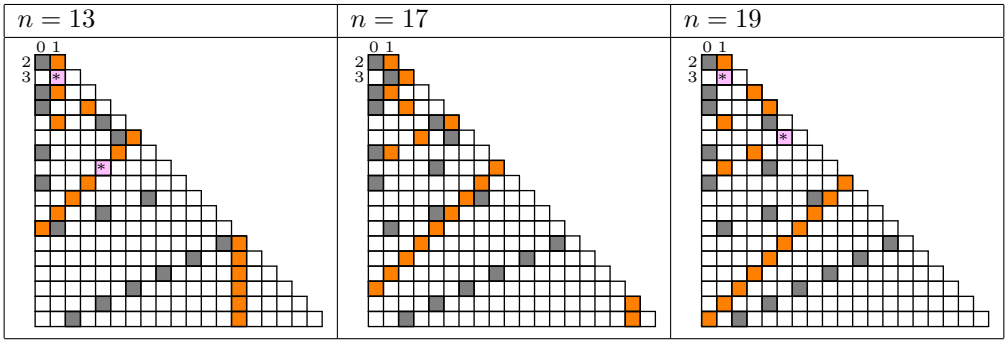


$n = 19$



Les mêmes tores des nombres premiers 3, 5, 7, 11, 13, 17, 19 avec en transparence (gris) le tore de 40 pour voir les conflits empêchant 5, 7, 13 et 19 d'être décomposants de Goldbach de 40.





Un nombre premier devant éviter les pixels colorés d'un nombre pair pour pouvoir le décomposer, on peut compter le nombre de pixels colorés à éviter : il y en a $\dfrac{n}{\dfrac{(n+1)(n+2)}{2} - 1} = \dfrac{2}{n+3}$.

Le nombre de pixels à éviter est ainsi de plus en plus petit au fur et à mesure de l'augmentation de n. Ceci est un argument supplémentaire en faveur du fait que la conjecture de Goldbach est en quelque sorte probabilistiquement de plus en plus vraie.

Cette connaissance un peu plus précise qu'on a du processus à l'œuvre, qui permet à un nombre d'être ou de ne pas être un décomposant de Goldbach d'un nombre pair, amène à des calculs différents de ceux qu'on a proposés dans http://denise.vella.chemla.free.fr/denitac.pdf.

Fournissons quelques exemples pour fixer les idées : plaçons nous dans la ligne de pixels d'un nombre premier p. On a vu que x a un reste valide pour être un décomposant de Goldbach de n si le pixel de x dans la ligne correspondant au nombre premier p est à la fois différent de 0 et différent du pixel de n.

Fixons $p = 5$. Il y a 5^2 possibilités de restes, i.e. de pixels possibles pour x et n qui sont

$$\begin{array}{c}(0,0),(0,1),(0,2),(0,3),(0,4),\\(1,0),(1,1),(1,2),(1,3),(1,4),\\(2,0),(2,1),(2,2),(2,3),(2,4),\\(3,0),(3,1),(3,2),(3,3),(3,4),\\(4,0),(4,1),(4,2),(4,3),(4,4).\end{array}$$

Là, on a le choix entre deux possibilités :

- soit on a la connaissance que x est un nombre premier, auquel cas son pixel est différent de 0 et il a 16 possibililités sur les 20 possibilités restantes d'avoir son pixel différent de celui de n, c'est-à-dire qu'il a $\dfrac{(p-1)^2}{p(p-1)} = \dfrac{p-1}{p}$ chances que ça soit le cas et il faut faire le produit de tous ces $\dfrac{p-1}{p}$ pour

avoir le nombre de chances total selon tous les nombres premiers ; on trouve une minoration du produit $\prod \frac{p-1}{p}$ dans [1]. Il faut multiplier cette minoration par la minoration de $\pi(\frac{n}{2})$, qui est $\frac{\frac{n}{2}}{ln\,\frac{n}{2}}$ (minoration fournie par la même référence).

- soit on n'a pas la connaissance que x est un nombre premier et x doit alors éviter deux pixels sur chaque ligne d'un nombre premier, et celui de n, et le pixel 0, de façon à assurer d'une part que x soit un nombre non divisible par tout nombre premier inférieur à $\sqrt{n}$, ce qui le rendra premier quant à lui ; d'autre part, pour ne pas avoir son pixel identique à celui de n, il y a toujours 16 possibilités qui conviennent pour x mais elles sont à ramener aux 25 possibilités totales, selon la formule $\frac{(p-1)^2}{p^2} = \left(\frac{p-1}{p}\right)^2$. Dans ce cas-là, on n'arrive pas à raisonner plus avant car les nombres étant inférieurs à 1, la minoration du produit des $\frac{p-1}{p}$ ne permet pas d'obtenir une minoration pour le produit de leur carré.

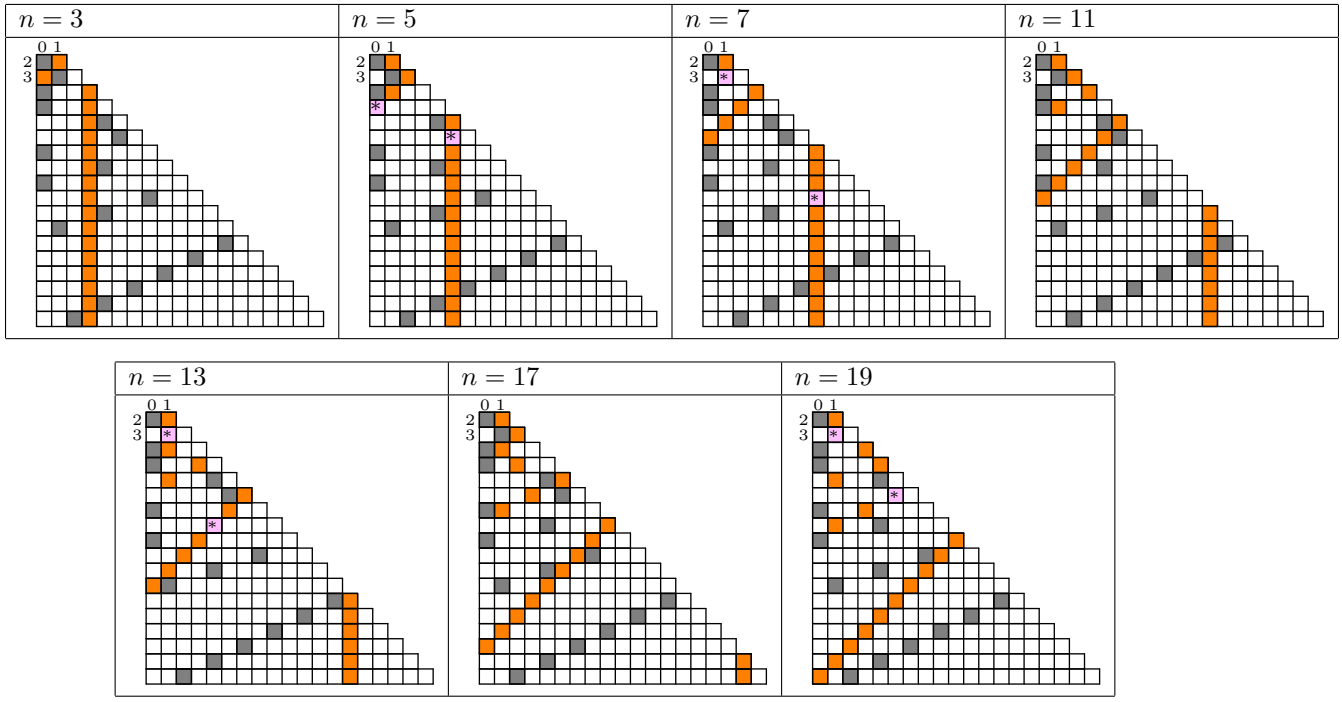
Référence

[1] J. B. Rosser et L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, dedicated to Hans Rademacher for his seventieth birthday, Illinois J. Math., Volume 6, Issue 1 (1962), 64-94.

```
import numpy as np
import math
from math import sqrt

pasdg = np.zeros((102), dtype='i')
tab=np.zeros((102,102,102),dtype='i')
for n in range(6,102,2):
    print('val de reference : '+str(n))
    for y in range(2,n/2+1):
        for z in range(0,y):
            if ((n % y) == z):
              tab[n][y][z] = 1
            print(str(tab[n][y][z])),
        print('')
    print('bzzzz')
    for x in range(3,n/2+1):
        pasdg[x] = 0
      for y in range(2,n/2):
          for z in range(0,y):
            tab[x][y][z] = 0
            if ((x % y) == z):
                tab[x][y][z] = 1
                if (tab[n][y][z] == 1):
                        pasdg[x] = 1 ;
          if (tab[x][y][0] == 1) and (x != y):
            pasdg[x] = 1
    for x in range(3,n/2+1):
        print(str(x))
        for y in range(2,n/2+1):
            for z in range(0,y):
                print(str(tab[x][y][z])),
            print('')
        print('')
    for x in range(3,n/2+1,2):
      if (pasdg[x] == 0):
        print(str(x)+" dg de "+str(n))
    print('')
```

Matrices de pixels (Denise Vella-Chemla, 13.6.2019)

On a présenté ici http://denise.vella.chemla.free.fr/pixels2.pdf une modélisation de la recherche de décomposants de Goldbach par ce qu'on a appelé les tores trapézoïdaux : il s'agit de lignes de pixels circulant (au sens donné à la notion de matrice circulante) et qui parfois, pour deux tores donnés, en l'occurrence celui d'un nombre pair et celui d'un décomposant potentiel de ce nombre pair, voient certains de leurs pixels coïncider ou pas.
Ci-dessous, on peut observer les tores des nombres premiers 3, 5, 7, 11, 13, 17, 19 à la recherche des décomposants de Goldbach de 40.
On a noté les restes de 40 en gris et les restes des nombres premiers en orange sauf lorsque les deux couleurs coïncidaient sur un même pixel qu'on a alors noté en rose pour bien voir les conflits ; de tels conflits empêchent 5, 7, 13 et 19 d'être décomposants de Goldbach de 40 et l'absence de conflits permet à 3, 11 et 17 d'être des décomposants de Goldbach de 40.



Voyons maintenant comment représenter les transformations opérées dans chaque ligne par des opérateurs matriciels :

- à la première ligne, qui correspond à la parité des nombres qui se succèdent selon le rythme pair, impair, pair, impair, etc..., on associe l'opérateur $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$;
  on a ainsi $\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{2k+1} = \begin{pmatrix} 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{2k} = \begin{pmatrix} 1 & 0 \end{pmatrix}$;
- à la seconde ligne, qui correspond à la divisibilité des nombres par 3 qui se succède au rythme oui, non, non, oui, non, non, etc..., on associe l'opérateur $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$;
  on a ainsi $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^{3k+1} = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^{3k+2} = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}^{3k} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$;

- à la ligne p, on associe l'opérateur matriciel à p lignes et p colonnes qui contient un 1 en bas à gauche et une diagonale de 1 à droite de la diagonale principale, tous ses autres éléments étant nuls ; il permet de faire "circuler" le bit 1 de place en place à droite vers le bout de la ligne et de le ramener au début de la ligne lorsque le bout de la ligne est atteint ;

Pour trouver les décomposants de Goldbach du si petit nombre 40, on est amené à fabriquer une matrice plutôt grosse (de taille 190×190 puisque $\frac{19\times 20}{2} = 190$) qu'on appellera G ; cette matrice contient les différents opérateurs $M1$, $M2$, etc., M_{19} bien alignés sur sa diagonale, on l'appelle matrice diagonale par blocs.

On voit alors que selon cette modélisation, 17 est un décomposant de Goldbach de 40 pour la raison très simple suivante : appelons L_1 la longue matrice à une seule ligne contenant les bits suivants :

10100100010000100000...1000000000000000000

Cette matrice modélise le nombre 1, elle contient des bits 1 entre lesquelles sont intercalés un bit 0, puis 2, puis 3, puis 4, etc. jusqu'à 18 bits 0 sur sa dernière ligne (c'est une matrice de $n/2-2$ lignes avec $n = 40$).

La matrice associée au nombre 17 s'obtient en multipliant la matrice A par la matrice G élevée à la puissance 17, la matrice associée au nombre 40 s'obtient en multipliant la matrice A par la matrice G élevée à la puissance 40. Pour que 17 soit un décomposant de Goldbach de 40, il faut que $A.G^{17}$ et $A.G^{40}$ ne contiennent aucun bit 1 à une position commune, ce qui peut s'exprimer par le fait que leur produit est nul. On peut aussi exprimer cette condition en utilisant la distance de Hamming, qui compte les bits différents de deux chaînes de caractères, et qui en l'occurrence doit être égale à $n - 6$ lorsqu'on cherche un décomposant de Goldbach de n.

On est ainsi ramené à la théorie des langages, à l'origine de l'informatique, dans la mesure où il s'agit, pour trouver un décomposant de Goldbach d'un nombre pair, de lire des chaînes de booléens et de repérer si elles contiennent des lettres 1 à des positions identiques.

Voici la forme générale de la matrice G.

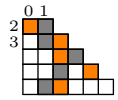
$$\begin{pmatrix}
0 & 1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
1 & 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
\dots & \dots & 0 & 1 & 0 & \dots & \dots & \dots & \dots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

Tous les ... sont des 0.

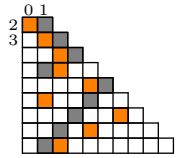
D'un Z qui veut dire... (Denise Vella-Chemla, 15.6.2019)

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

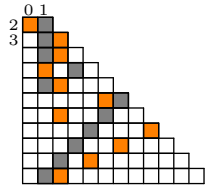
14



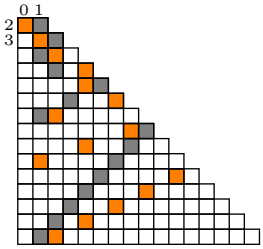
22



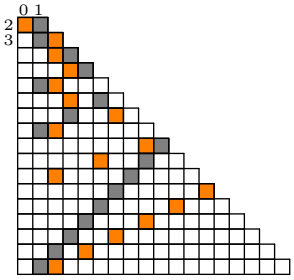
26



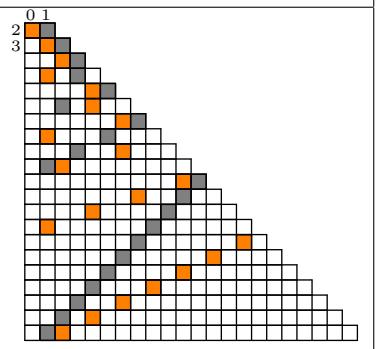
34



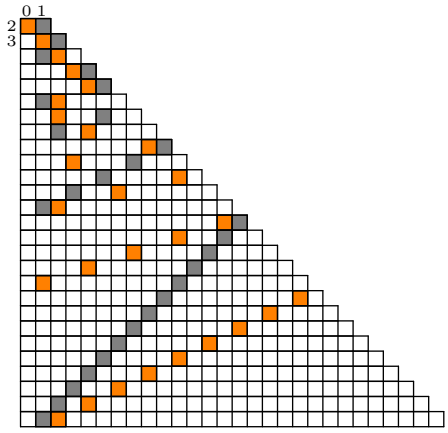
38



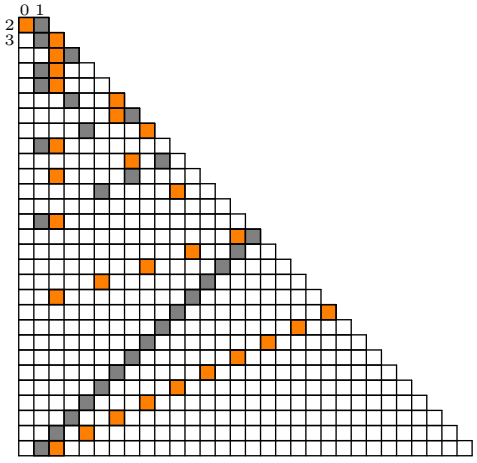
46



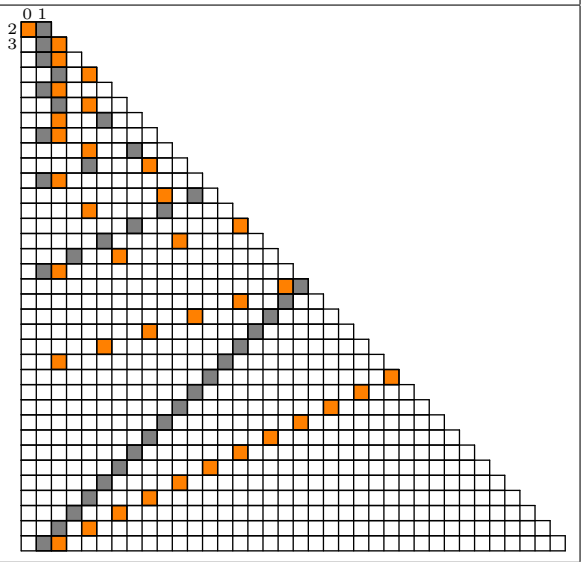
58



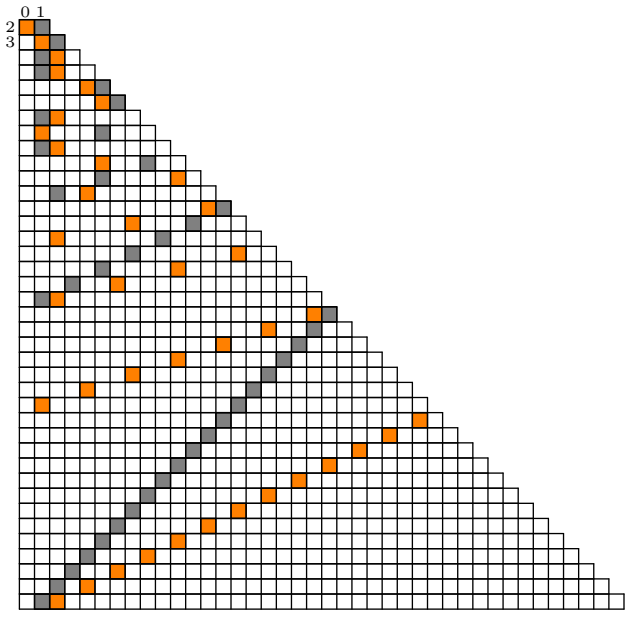
62



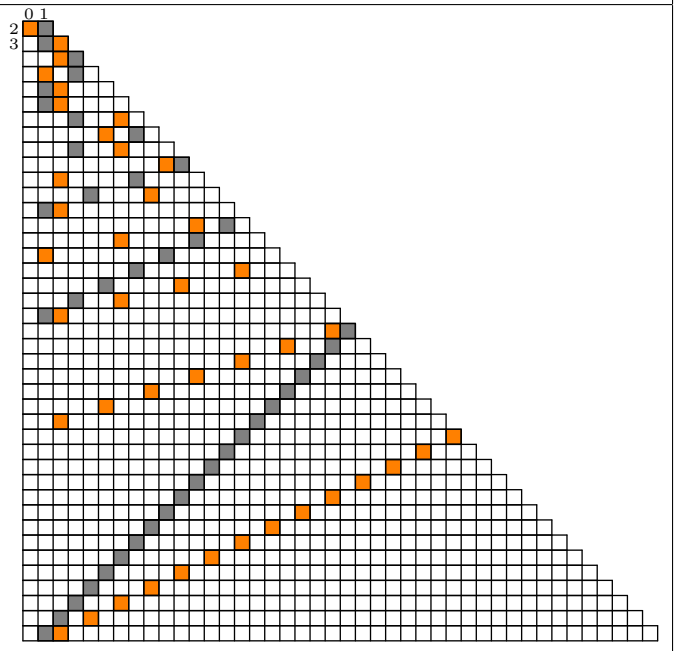
74



82



86



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.

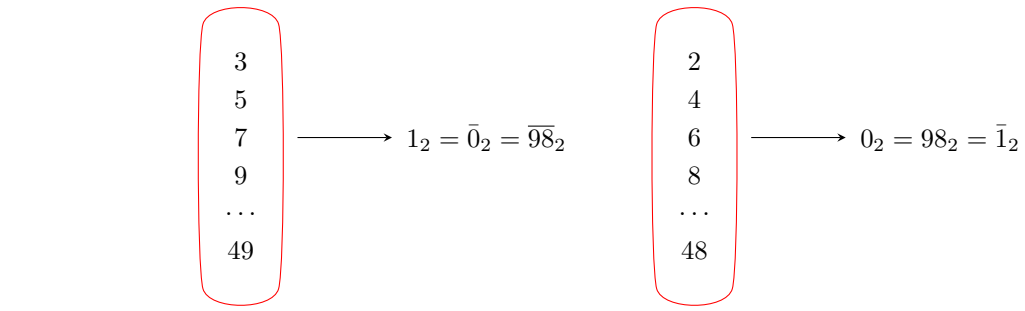
Une simple étude nous fait comprendre que la trace de la matrice atteinte par élévation à la puissance k de la matrice G permet de caractériser si k est premier ou non.

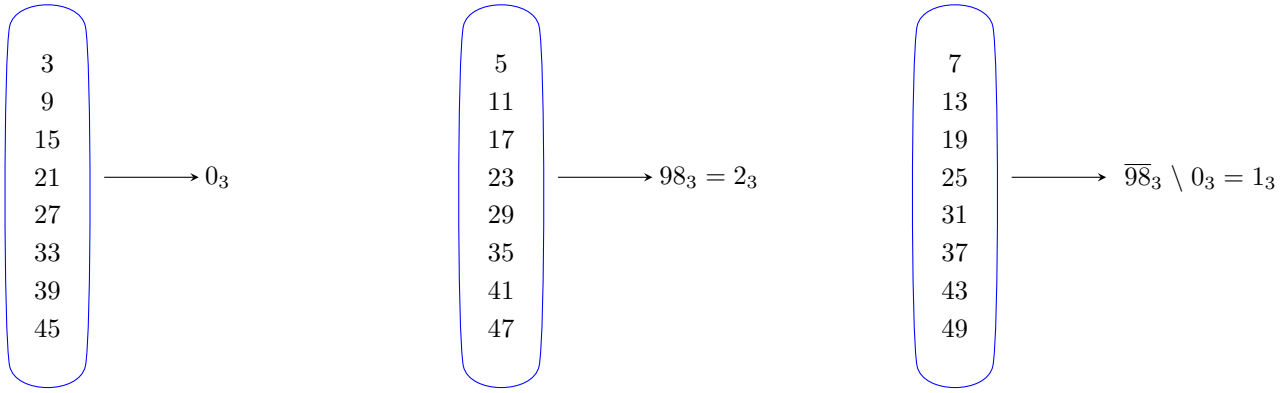
En effet, on a p est premier $\iff Trace(G^p) = p$.

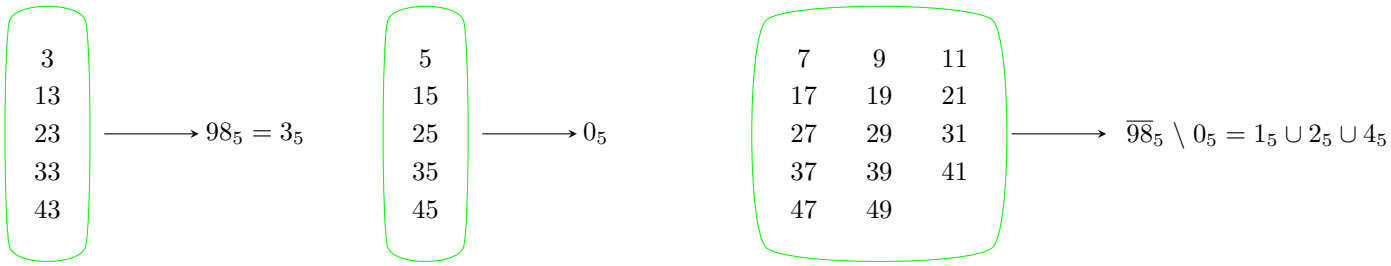
Quand on élève une matrice circulante de taille $k \times k$ à la puissance k, tous ses 1 s'alignent bien sur la diagonale pour obtenir la matrice Identité de taille k. Il en sera de même des 1 appartenant aux matrices circulantes de taille les diviseurs de k si k est composé.

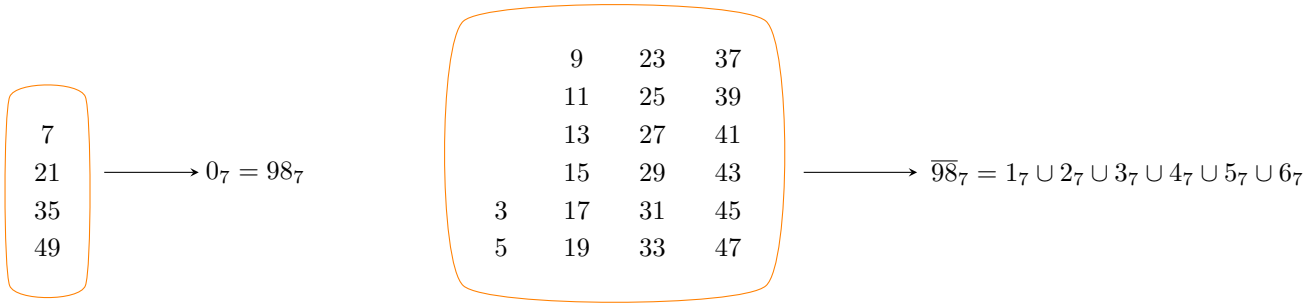
La complexité d'un tel algorithme pour caractériser la primalité d'un nombre étant de l'ordre de n^7 (en considérant la taille d'une matrice - en $\frac{n(n+1)}{2}$ -, le coût d'une multiplication matricielle en n^3, etc.), elle est complètement prohibitive. L'intérêt de cette idée est peut-être simplement 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.







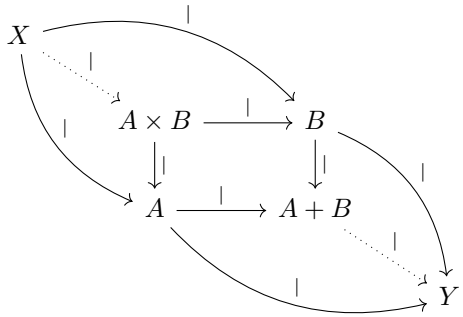


$$\overline{98}_2 \cap \overline{98}_3 \cap \overline{98}_5 \cap \overline{98}_7 = \{19, 31, 37\}$$

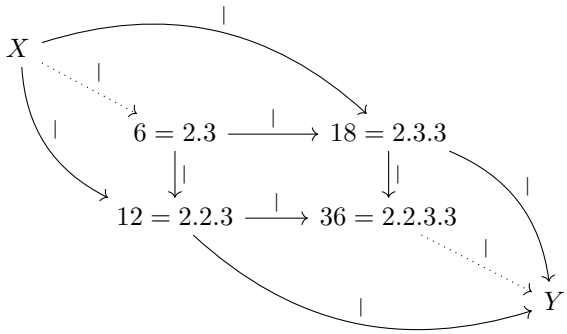
$$98 \;=\; 19{+}79 \;=\; 31{+}67 \;=\; 37{+}61$$

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

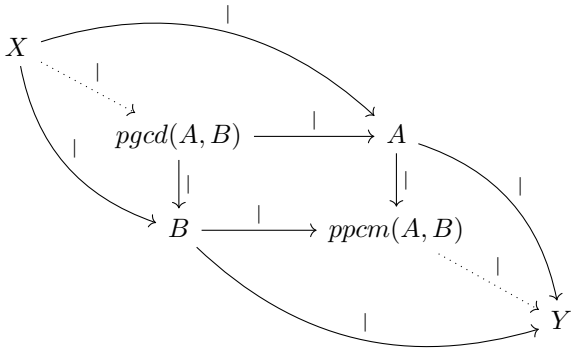
Le symbole | signifie *"divise"*.



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.

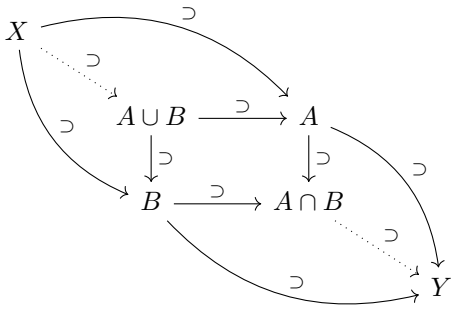


On voit ainsi le *pgcd* comme une intersection ensembliste (les ensembles pouvant contenir un facteur avec une certaine multiplicité, plusieurs fois : par exemple, deux occurrences de 2 et deux occurrences de 3 sont "contenues" dans 36).
Le *ppcm* est vu comme une union. C'est l'idée intuitive que l'on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

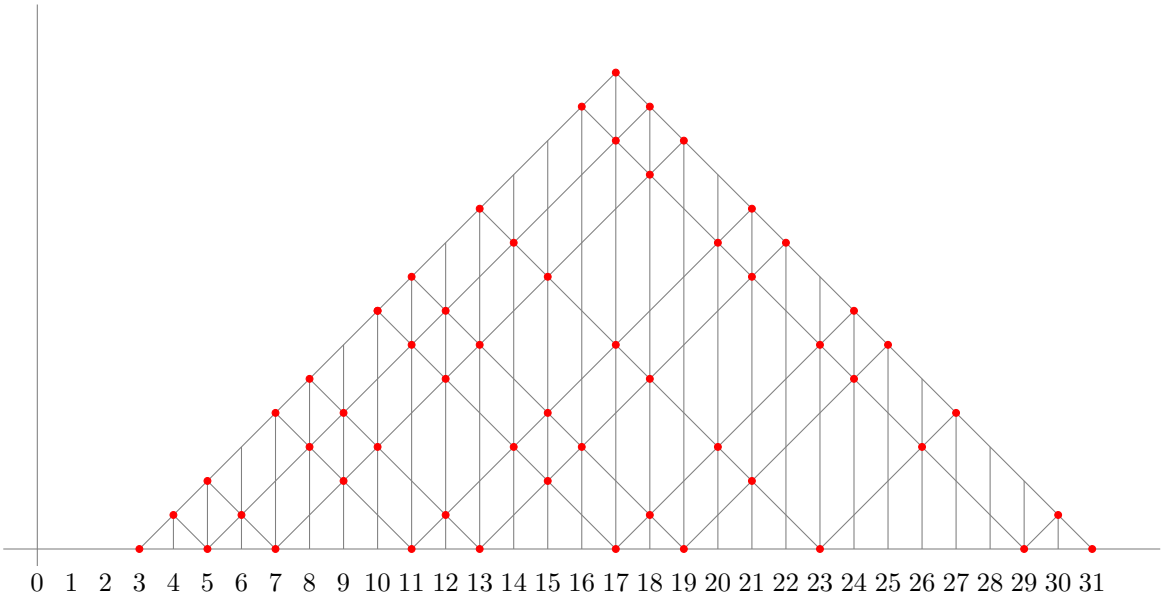


FIGURE 1 : Le treillis Goldbach

2. Les décompositions additives

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

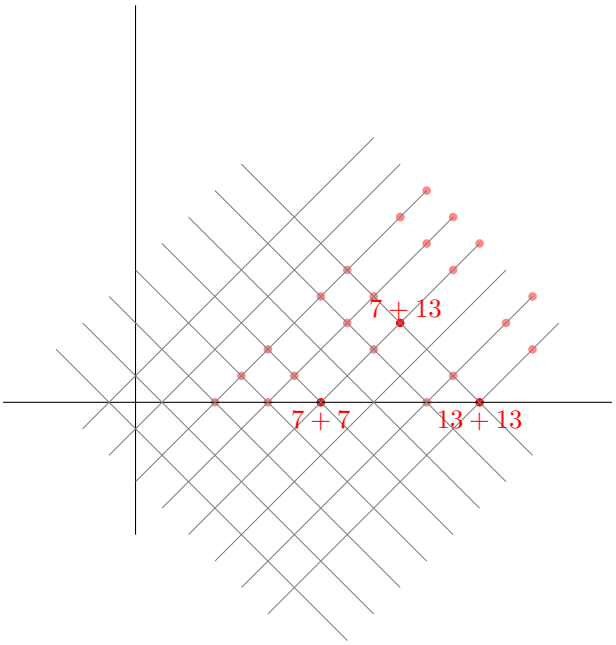


FIGURE 2 : Décompositions additives

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*.

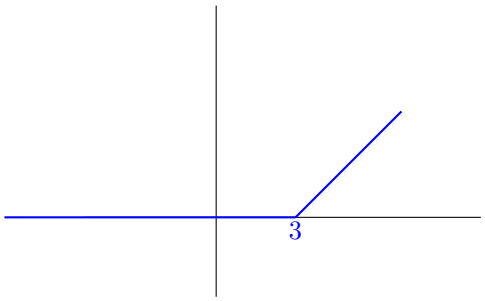


FIGURE 3 : Une droite tropicale d'équation $y = max(x - 3, 0)$

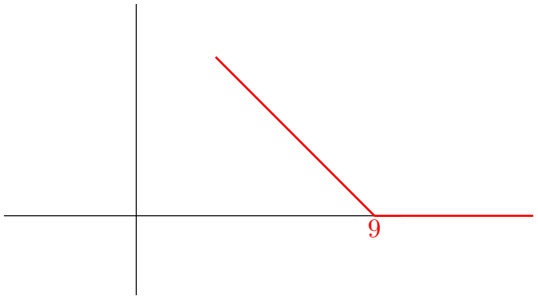


FIGURE 4 : Une autre droite tropicale d'équation $y = max(9 - x, 0)$

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. 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 $n/2$.

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

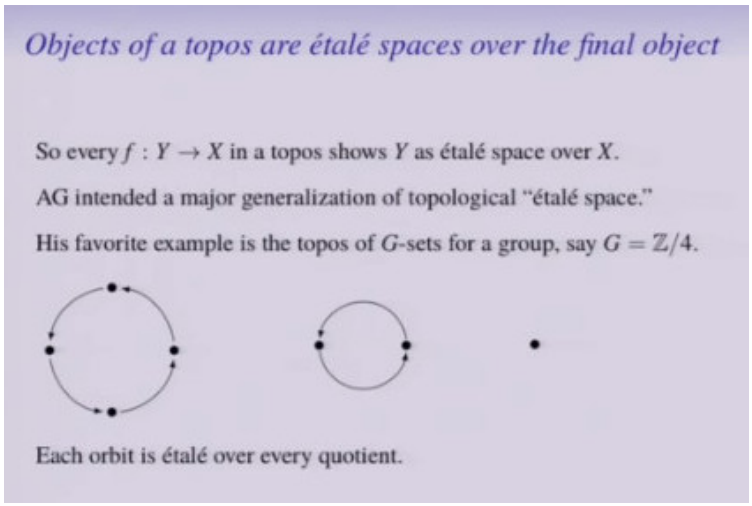
Mais on imagine bien qu'il existe au moins un nombre impair compris entre 3 et $n/2$ qui n'est pas congru à 0, tout en n'étant pas non plus congru à n selon un nombre premier p_k. Ce qui rend notre dernière assertion obligatoirement fausse, et la possibilité que l'intersection soit vide par là même.

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 $\mathscr{A}$ of sets, no two of which have any elements in common. That is, any two members of $\mathscr{A}$ 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 $\mathscr{A}$ is labelled in this way, so we write $\mathscr{A}$ as the collection of all these A_i's,

$$\mathscr{A} = \{A_i : i \in I\}.$$

The fact that the members of $\mathscr{A}$ 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:

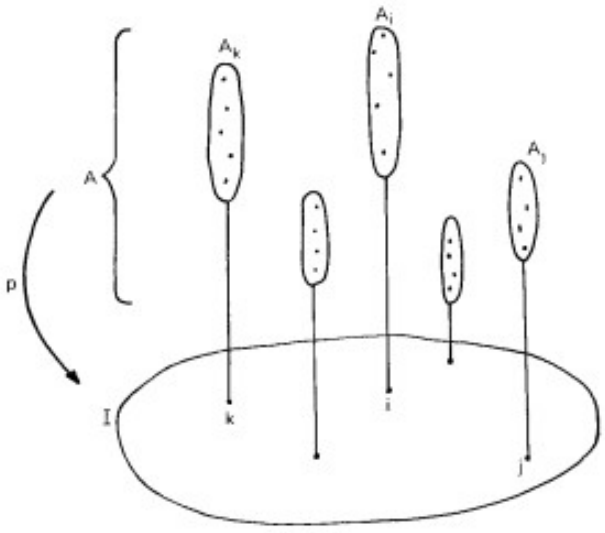


Fig. 4.4.

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.

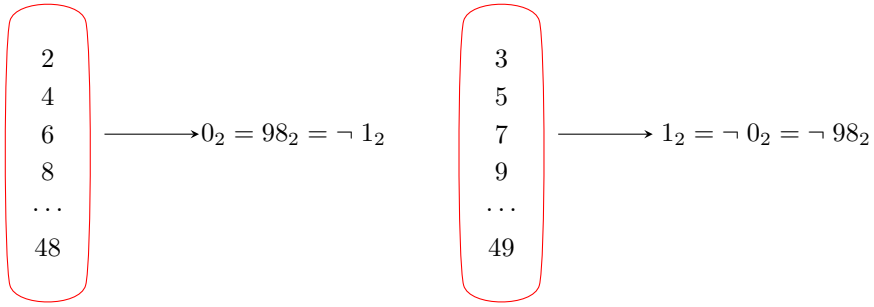
Annexe 5 : Somme des inverses des puissances de 2

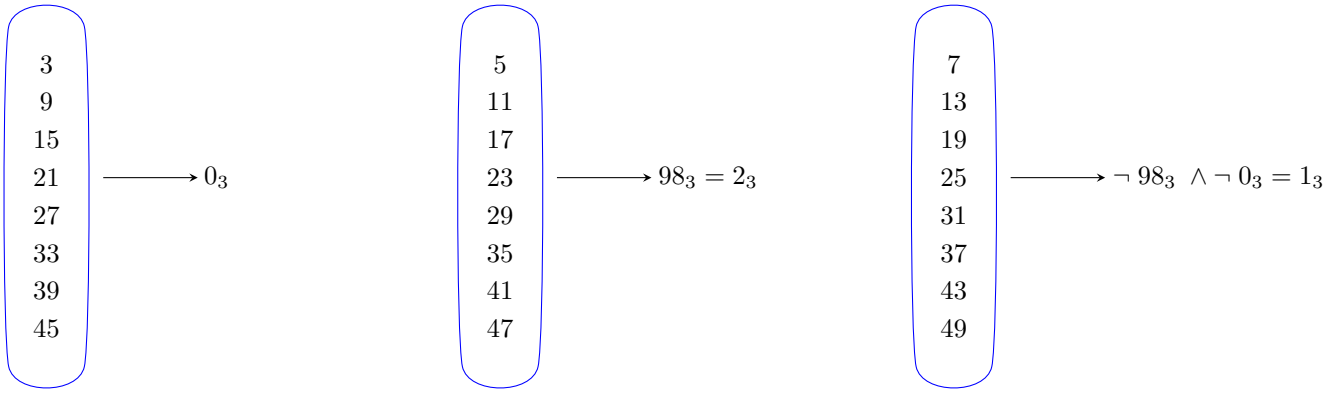
$$\sum_{i=1}^{n} \frac{1}{2^i} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^n}$$

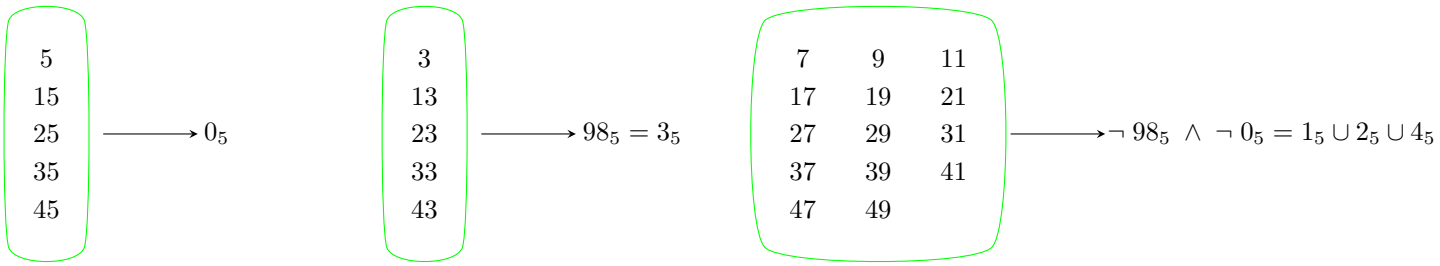
Il s'agit d'une suite géométrique de raison $\frac{1}{2}$ et de premier terme égal à $\frac{1}{2}$. La formule donne donc :

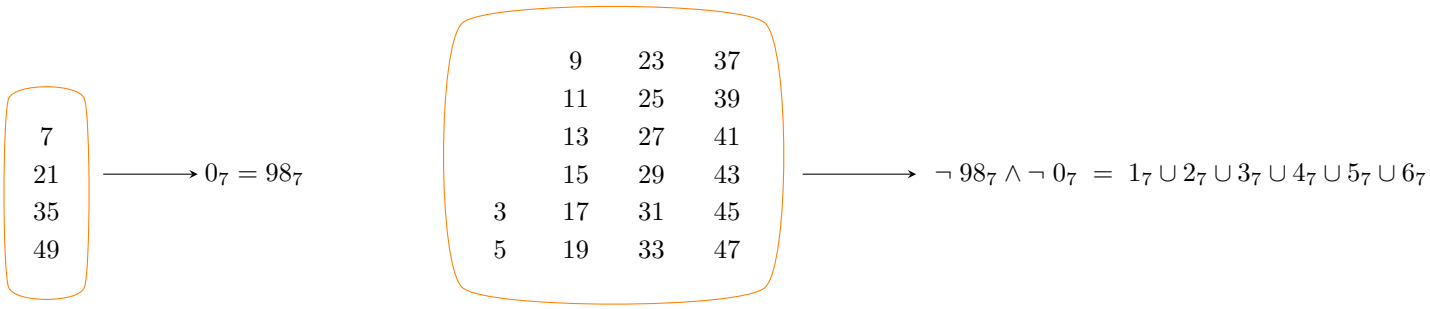
$$S_n = \frac{1}{2} \frac{1 - \frac{1}{2}^n}{1 - \frac{1}{2}} = \frac{1}{2} \frac{1 - \frac{1}{2^n}}{\frac{1}{2}} = 1 - \frac{1}{2^n}$$

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.

Expérience de pensée ensembliste (Denise Vella-Chemla, 10.11.2019)

On voudrait garder trace ici d'une petite expérience de pensée motivée par le souvenir d'une conférence de Gérard Berry dans laquelle il décrivait la « machine chimique ». L'extrait video est consultable ici, minute 47'31 : https://www.college-de-france.fr/site/gerard-berry/course-2008-01-25-10h30.htm.

On trouve dans le résumé du cours de l'année suivante ([1], p.21/30) l'extrait et l'image ci-dessous :

4.5. La machine chimique

La machine chimique ou CHAM a été introduite par moi-même et G. Boudol [Berry et Boudol, 1992]. Les processus y sont représentés par des molécules portant des valences d'interaction, nageant conceptuellement dans une solution, et pouvant librement se rencontrer à tout moment ; techniquement, cela s'exprime par de la réécriture de multi-ensembles. Une molécule peut hiérarchiquement contenir d'autres solutions contenues dans des membranes perméables aux valences. La machine la plus simple est le crible de Darwin de la figure 11 pour calculer les nombres premiers. Il utilise la règle chimique p, kp → p (tout nombre mange ses multiples). Un exemple plus complexe lié à CCS est présenté dans les transparents et vidéos.

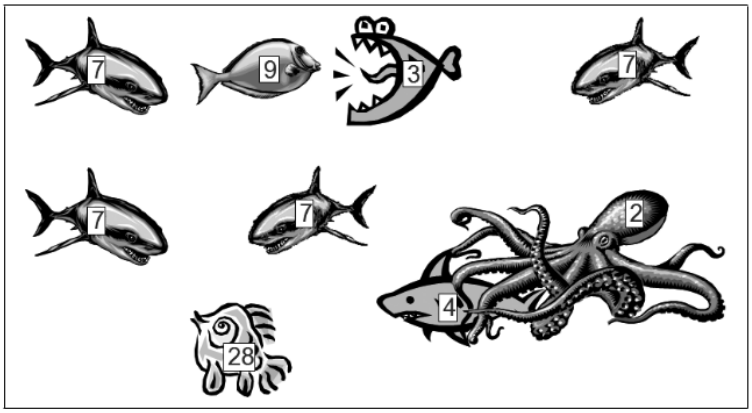


Figure 11 : **le crible chimique de Darwin**

Si l'on souhaite modéliser cela par des ensembles et une seule opération, on n'a qu'à considérer l'ensemble des multiples entiers de tout nombre entier supérieur ou égal à 2 et l'opération différence ensembliste, qu'on note habituellement \.

La différence ensembliste (comme la différence des nombres) est une opération non-commutative. Considérons l'ensemble des multiples de 2, qu'on note E_2 et l'ensemble des multiples de 4 qu'on note E_4 ; alors on a « $6 \in E_2 \backslash E_4$ » alors que « $E_4 \backslash E_2 = \varnothing$ » , ce qui s'exprime en français courant par « 6 est un multiple de 2 sans être un multiple de 4 » pour la première assertion et « tout multiple de 4 est un multiple de 2 » pour la seconde assertion.

Si notre objectif est de trouver un moyen qui permette de ne conserver que les nombres premiers et eux seuls, on peut considérer, et cela correspond au fonctionnement de la machine chimique de Berry & Boudol, que l'on travaille sur l'ensemble de tous les ensembles de multiples de tous les entiers supérieurs ou égaux à 2 et que chaque ensemble est mis en relation avec tous les autres ensembles par différence ensembliste. Par un tel processus, un ensemble des multiples d'un nombre composé quel qu'il soit sera vidé, tandis qu'un ensemble des multiples d'un nombre premier va se trouver vidé de tous les nombres qui ne sont pas le nombre premier en question et ainsi être transformé en le singleton contenant le nombre premier considéré et lui seul. Par la magie des seules différences ensemblistes, on trouve, en appliquant les différences simultanément à tous les ensembles de multiples pris 2 à 2, tous les singletons possibles contenant

un nombre premier chacun. C'est le crible d'Eratosthène regardé selon un point de vue ensembliste.

Remarque : la différence ensembliste n'est pas une opération associative : $\{1,2,3,4\}\backslash(\{3,4\}\backslash\{4\}) \neq (\{1,2,3,4\}\backslash\{3,4\})\backslash\{4\}$ puisque $\{1,2,3,4\}\backslash(\{3,4\}\backslash\{4\}) = \{1,2,3,4\}\backslash\{3\} = \{1,2,4\}$ tandis que $(\{1,2,3,4\}\backslash\{3,4\})\backslash\{4\} = \{1,2\}\backslash\{4\} = \{1,2\}$; je ne sais pas si, de ce fait, cette petite expérience de pensée présente un intérêt pour les mathématiciens.

Bibliographie

[1] Gérard Berry, résumé du cours au Collège de France 2009-2010, Penser, modéliser et maîtriser le calcul informatique (Chaire Informatique et sciences numériques) : https://www.college-de-france.fr/media/gerard-berry/UPL7123112924601846267$_R$0910$_B$*erry.pdf*

Crainte maladive de tout perdre (sic ;-)) (Denise Vella-Chemla, 10.11.2019)

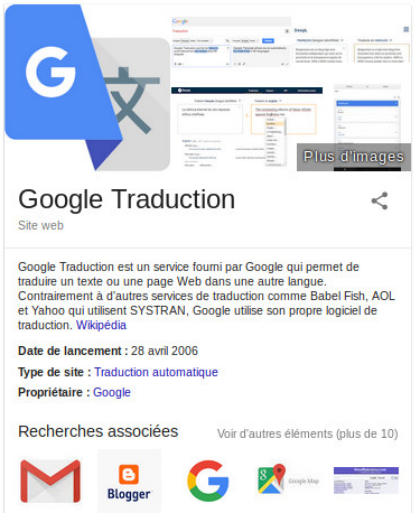
Les éléments ci-dessous sont une sauvegarde de ce que j'avais posté sur Google+, qui a été perdu, que j'ai reposté sur Blogger, je préfère le garder sous format pdf, c'est plus sûr !

1) Wiggles

Petit phare dans la nuit, petite magie du jour, qui m'amène le sourire : j'avais lu ça au sujet de la fonction $J(x)$ liée à la fonction ζ de Riemann :

$$\textit{Note that all the "wiggles" are in the term } \sum Li(x^{\rho}).$$

J'ai voulu m'assurer que comme je le pressentais wiggles voulait dire oscillations et j'ai trouvé ça, je trouve sympathique d'imaginer une courbe qui se trémousse * !



2) Soustraire les carrés des parties imaginaires des zéros de zêta du carré de la partie imaginaire du premier zéro de zêta puis diviser par $e^{2\pi}$

C'est marrant ce que l'on obtient lorsqu'on prend les carrés des parties réelles des zéros de zêta, qu'on leur soustrait le carré de la partie réelle du premier zéro de zêta et qu'on divise ces différences par $e^{2\pi}$.

$e^{2\pi} = 535.492$
$zeros[1] = 14.1347$ au carre 199.79 auquel on soustrait 199.79 et qu'on divise par $e^{2\pi} \rightarrow 0.373097$
zeros$[2] = 21.022 \rightarrow 441.926 \rightarrow 0.825272$
$zeros[3] = 25.0109 \rightarrow 625.543 \rightarrow 1.16817$
$zeros[4] = 30.4249 \rightarrow 925.673 \rightarrow 1.72864$
$zeros[5] = 32.9351 \rightarrow 1084.72 \rightarrow 2.02565$
$zeros[6] = 37.5862 \rightarrow 1412.72 \rightarrow 2.63818$
$zeros[7] = 40.9187 \rightarrow 1674.34 \rightarrow 3.12674$
$zeros[8] = 43.3271 \rightarrow 1877.24 \rightarrow 3.50563$
$zeros[9] = 48.0052 \rightarrow 2304.49 \rightarrow 4.30351$
$zeros[10] = 49.7738 \rightarrow 2477.43 \rightarrow 4.62647$
$zeros[11] = 52.9703 \rightarrow 2805.85 \rightarrow 5.23977$
$zeros[12] = 56.4462 \rightarrow 3186.18 \rightarrow 5.95001$

∗. J'avais posté ça sur Google+ le 1er novembre 2018, tout a été perdu en avril 2019 quand Google+ a fermé, je l'ai reposté sur Blogger, là, https://milliardsdautres.blogspot.com/2019/10/wiggles.html

$zeros[13] = 59.347 \to 3522.07 \to 6.57727$
$zeros[14] = 60.8318 \to 3700.51 \to 6.91048$
$zeros[15] = 65.1125 \to 4239.64 \to 7.91729$
$zeros[16] = 67.0798 \to 4499.7 \to 8.40293$
$zeros[17] = 69.5464 \to 4836.7 \to 9.03226$
$zeros[18] = 72.0672 \to 5193.68 \to 9.69889$
$zeros[19] = 75.7047 \to 5731.2 \to 10.7027$
$zeros[20] = 77.1448 \to 5951.33 \to 11.1138$
$zeros[21] = 79.3374 \to 6294.42 \to 11.7545$
$zeros[22] = 82.9104 \to 6874.13 \to 12.837$
$zeros[23] = 84.7355 \to 7180.1 \to 13.4084$
$zeros[24] = 87.4253 \to 7643.18 \to 14.2732$
$zeros[25] = 88.8091 \to 7887.06 \to 14.7286$

Et ça continue comme ça, au rythme d'environ un nombre de plus tous les 2 nombres environ, et ça, très loin (enfin, assez loin... Mais face à l'infini... enfin... cacahuètes, quoi) [†].

3) Que font là π et sa racine ? (enfin presque)

Tiens, c'est marrant ! [‡]

On prend le nombre premier 13, et on l'élève à la puissance du second zéro de zêta qui vaut

$$1/2 + 21.022039638771554992628479593896916 2i \ ,$$

on trouve :

$$-3.14073664252166 - 1.7708114925993i$$

Ces nombres réels (la partie réelle et la partie imaginaire du complexe obtenu) "ressemblent" à

$$\pi = 3.14159265359...$$

et à sa racine

$$\sqrt{\pi} = 1.77245385091...$$

On peut même dire que ce sont les mêmes nombres, jusqu'au 100ème !

Ca surprend...

4) Diviser les parties imaginaires des zéros par $\frac{\pi^2}{4}$

Un autre jeu expérimental sympathique, on obtient un peu pareil qu'en 1) , cette augmentation de 1 environ un coup sur deux, au niveau de la partie imaginaire [§].

Une nouvelle expérience marrante : prendre les parties imaginaires des zéros de zêta et les diviser par $\frac{\pi^2}{4}$. On choisit de diviser par $\frac{\pi^2}{4}$ parce que $\frac{\pi^2}{4}$ est le carré de $\frac{\pi}{2}$ et qu'on pense que cet angle de $\frac{\pi}{2}$ est important parce qu'il contient toutes les symétries entre les sinus et les cosinus qu'on a montrées sur une sorte de croix de Malte et comme on a trouvé une somme de somme de cosinus qui contient toute l'information nécessaire à la caractérisation des nombres premiers, on se dit que ce groupe de rotations et symétries à 4 ou 8 éléments est forcément important (groupe des symétries et rotations du carré).

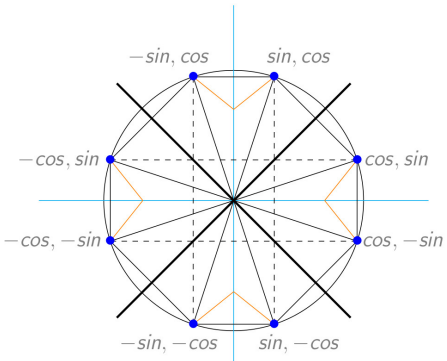
†. Posté initialement sur Google+ le 21.2.2018, sauvegardé sur Blogger ici https://milliardsdautres.blogspot.com/2019/10/jeu-avec-la-fonction-zeta.html

‡. Posté initialement sur Google+ le 22.9.2018, sauvegardé sur Blogger ici https://milliardsdautres.blogspot.com/2019/10/jeu-avec-la-fonction-zeta.html

§. posté initialement sur Google+ le 28.4.2018, sauvegardé sur Blogger ici https://milliardsdautres.blogspot.com/2019/10/jeu-avec-la-fonction-zeta.html

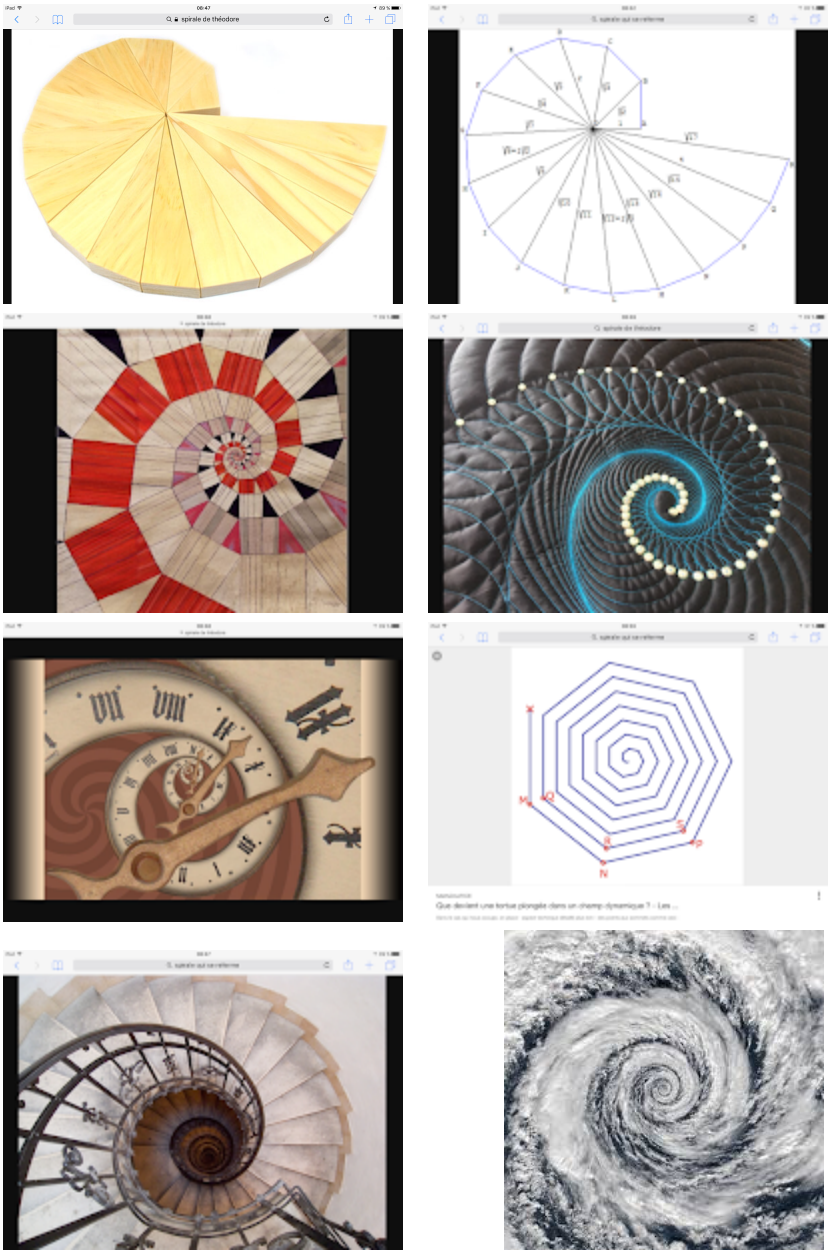
$1 \to (0.202642, 5.72859)$	$39 \to (0.202642, 49.1895)$	$77 \to (0.202642, 79.1381)$
$2 \to (0.202642, 8.51991)$	$40 \to (0.202642, 49.8285)$	$78 \to (0.202642, 79.791)$
$3 \to (0.202642, 10.1365)$	$41 \to (0.202642, 50.3594)$	$79 \to (0.202642, 80.2526$
$4 \to (0.202642, 12.3307)$	$42 \to (0.202642, 51.6806)$	$80 \to (0.202642, 81.5695)$
$5 \to (0.202642, 13.3481)$	$43 \to (0.202642, 52.5163)$	$81 \to (0.202642, 82.0676)$
$6 \to (0.202642, 15.2331)$	$44 \to (0.202642, 53.1278)$	$82 \to (0.202642, 82.755)$
$7 \to (0.202642, 16.5837)$	$45 \to (0.202642, 54.1046)$	$83 \to (0.202642, 83.2433$
$8 \to (0.202642, 17.5598)$	$46 \to (0.202642, 54.6148)$	$84 \to (0.202642, 84.2612)$
$9 \to (0.202642, 19.4558)$	$47 \to (0.202642, 55.9763)$	$85 \to (0.202642, 84.9382)$
$10 \to (0.202642, 20.1726$	$48 \to (0.202642, 56.633)$	$86 \to (0.202642, 85.7951)$
$11 \to (0.202642, 21.4681)$	$49 \to (0.202642, 57.1953$	$87 \to (0.202642, 86.4667)$
$12 \to (0.202642, 22.8768)$	$50 \to (0.202642, 58.001)$	$88 \to (0.202642, 86.9526)$
$13 \to (0.202642, 24.0525)$	$51 \to (0.202642, 59.172)$	$89 \to (0.202642, 87.6102)$
$14 \to (0.202642, 24.6542)$	$52 \to (0.202642, 59.7482$	$90 \to (0.202642, 88.7848)$
$15 \to (0.202642, 26.3891)$	$53 \to (0.202642, 60.8144)$	$91 \to (0.202642, 89.4524)$
$16 \to (0.202642, 27.1864)$	$54 \to (0.202642, 61.1677)$	$92 \to (0.202642, 89.7425)$
$17 \to (0.202642, 28.1861)$	$55 \to (0.202642, 62.0186)$	$93 \to (0.202642, 90.7866)$
$18 \to (0.202642, 29.2077)$	$56 \to (0.202642, 63.2702)$	$94 \to (0.202642, 91.1823)$
$19 \to (0.202642, 30.682)$	$57 \to (0.202642, 63.8719)$	$95 \to (0.202642, 92.1704)$
$20 \to (0.202642, 31.2656$	$58 \to (0.202642, 64.3795)$	$96 \to (0.202642, 92.947)$
$21 \to (0.202642, 32.1542)$	$59 \to (0.202642, 65.3274)$	$97 \to (0.202642, 93.7222$
$22 \to (0.202642, 33.6023)$	$60 \to (0.202642, 66.0739)$	$98 \to (0.202642, 94.0209)$
$23 \to (0.202642, 34.342)$	$61 \to (0.202642, 67.0896)$	$99 \to (0.202642, 94.7124)$
$24 \to (0.202642, 35.4321$	$62 \to (0.202642, 67.7573)$	$100 \to (0.202642, 95.8597$
$25 \to (0.202642, 35.993)$	$63 \to (0.202642, 68.5314)$	$101 \to (0.202642, 96.3645)$
$26 \to (0.202642, 37.4856$	$64 \to (0.202642, 68.8627)$	$102 \to (0.202642, 97.0882)$
$27 \to (0.202642, 38.3607)$	$65 \to (0.202642, 70.281)$	$103 \to (0.202642, 97.6935)$
$28 \to (0.202642, 38.8549)$	$66 \to (0.202642, 70.8252$	$104 \to (0.202642, 98.4126)$
$29 \to (0.202642, 40.0548)$	$67 \to (0.202642, 71.509)$	$105 \to (0.202642, 98.9182)$
$30 \to (0.202642, 41.0626)$	$68 \to (0.202642, 72.2936$	$106 \to (0.202642, 100.161)$
$31 \to (0.202642, 42.0384)$	$69 \to (0.202642, 72.9174)$	$107 \to (0.202642, 100.552)$
$32 \to (0.202642, 42.7359)$	$70 \to (0.202642, 73.8457)$	$108 \to (0.202642, 101.148)$
$33 \to (0.202642, 43.4338)$	$71 \to (0.202642, 74.9268)$	$109 \to (0.202642, 101.733)$
$34 \to (0.202642, 44.9986)$	$72 \to (0.202642, 75.2204)$	$110 \to (0.202642, 102.565)$
$35 \to (0.202642, 45.3411)$	$73 \to (0.202642, 75.881)$	$111 \to (0.202642, 103.472)$
$36 \to (0.202642, 46.3322)$	$74 \to (0.202642, 76.7675$	$112 \to (0.202642, 103.907)$
$37 \to (0.202642, 47.1049)$	$75 \to (0.202642, 77.8255)$	
$38 \to (0.202642, 48.1441)$	$76 \to (0.202642, 78.2523)$	

Malte



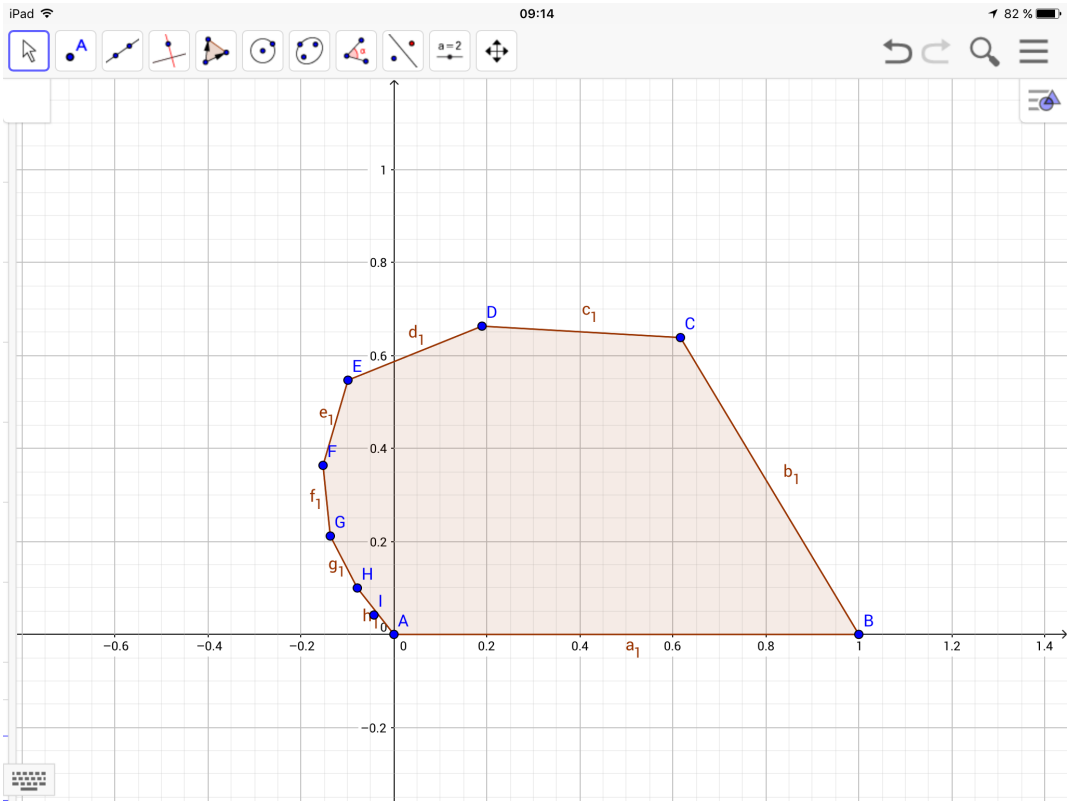
5) Spirales

Continuer à chercher... ¶
D'abord, regarder des spirales suite au visionnage d'une video sur zêta.
Parfois, l'angle entre deux côtés successifs est constant, parfois, c'est la longueur du côté qui l'est.



Bien-sûr que ça se pourrait que deux polygones ayant le même nombre de côtés, avec des côtés de longueurs proportionnelles 2 à 2, et d'angles égaux 2 à 2, ayant notamment comme plus grand côté un côté de longueur 1 (allant de l'origine au point d'abscisse 1 de l'axe réel) et des côtés de plus en plus petits de tailles les images des entiers successifs par une certaine fonction, se referment tous les 2 sur 0.

¶. Posté initialement sur Google+ le 30.7.2017, sauvegardé sur Blogger ici https://milliardsdautres.blogspot.com/2019/10/spirales-diverses-et-variees-fin.html



Ce qu'il faudrait comprendre, c'est pourquoi les côtés ont forcément pour longueurs les inverses des racines carrées simples des entiers successifs et pas les inverses des racines cubiques, ou les inverses des racines quartiques ou les inverses des racines quintiques, ou même les inverses des racines 3.14-tiques (!).

Ces polygones acceptables font un peu penser à des "duals" de la spirale de Théodore, dont tous les côtés valent 1 et dont les segments vers l'origine de la spirale sont de longueurs les racines carrées des entiers successifs. Là, ce sont les côtés des polygones qui doivent avoir pour longueurs les inverses des racines (carrées possiblement mais impossiblement cubiques, quartiques, etc) des entiers successifs.

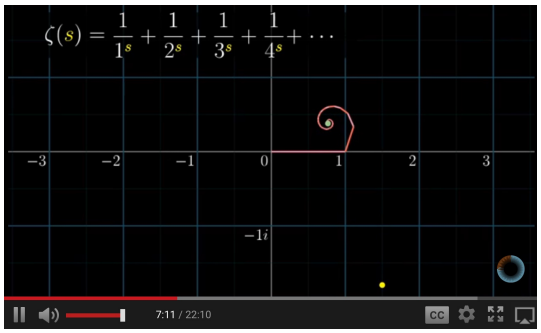
L'ange de la géométrie et le démon de l'algèbre, qu'ils disaient... Encore faudrait-il avoir une très bonne imagination visuelle.

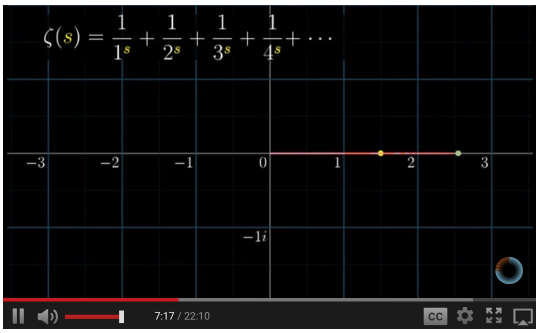
Se pourrait-il que le polygone à côtés de longueurs décroissantes associé à $Z'1$, dont les côtés seraient plus longs un à un de tous les côtés de $Z1$ mais dont les angles seraient identiques à ceux de $Z1$, aboutisse aussi, au terme du chemin, au point 0 ?

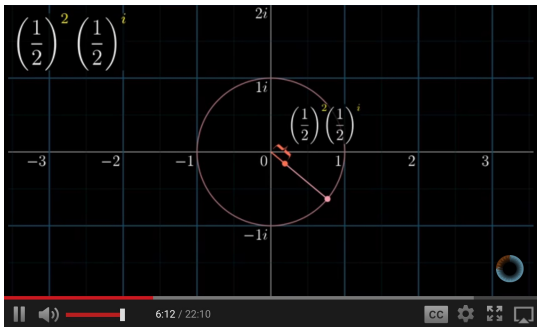
On pense à cela suite au visionnage de la video dont on a shooté des images en lien avec l'idée énoncée là.

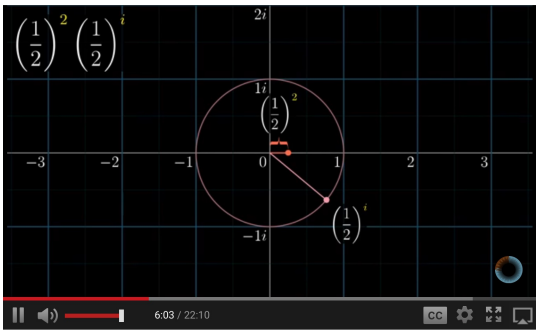
Si deux tels polygones ne pouvaient exister sous prétexte qu'ils ne pourraient tous deux "ramener à zéro" en ayant des côtés en rapport double l'un de l'autre (pour 2/3 / 1/3) ou bien en rapport quadruple l'un de l'autre par exemple (pour 4/5 / 1/5) ou en rapport $p-1$ l'un de l'autre (pour $p-1/p$ / $1/p$), alors peut-être que les seuls polygones acceptables seraient ceux pour lesquels le rapport des côtés est de 1 puisque $1/2 = 1 - 1/2$.

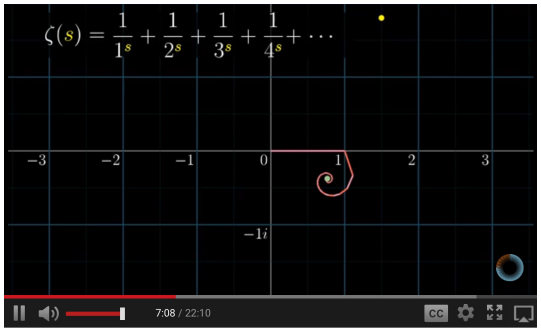
Sur les screenshots, s est le point jaune et $\zeta(s)$ est le point vert.


$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$
7:11 / 22:10

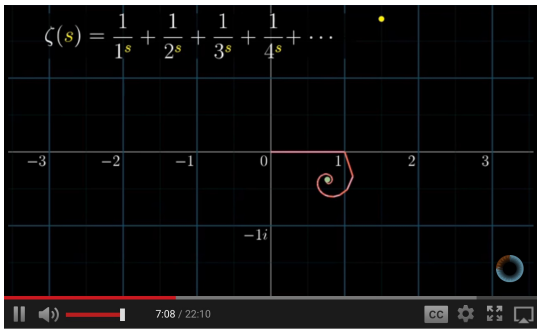

$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$
7:17 / 22:10


$\left(\frac{1}{2}\right)^2 \left(\frac{1}{2}\right)^i$
6:12 / 22:10

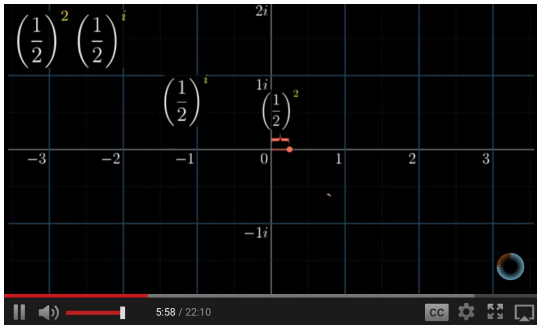

$\left(\frac{1}{2}\right)^2 \left(\frac{1}{2}\right)^i$
6:03 / 22:10

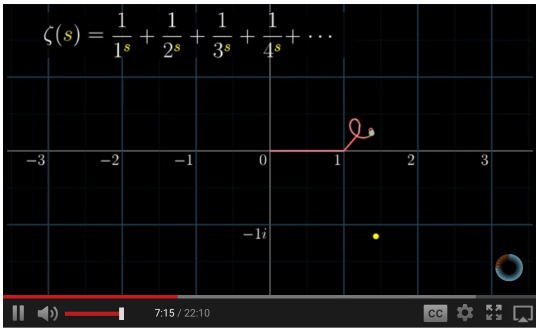

$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$
7:08 / 22:10

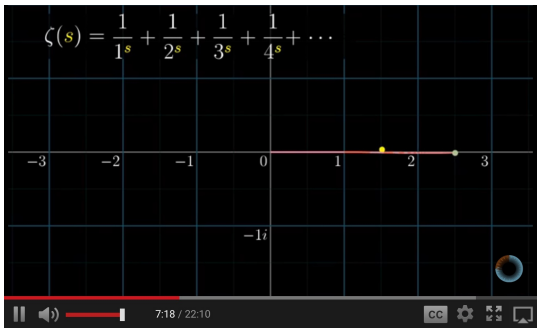

$\zeta(2+i) = \frac{1}{1^{2+i}} + \frac{1}{2^{2+i}} + \frac{1}{3^{2+i}} + \frac{1}{4^{2+i}} + \cdots = 1.15 - 0.44i$
$2+i$
6:40 / 22:10

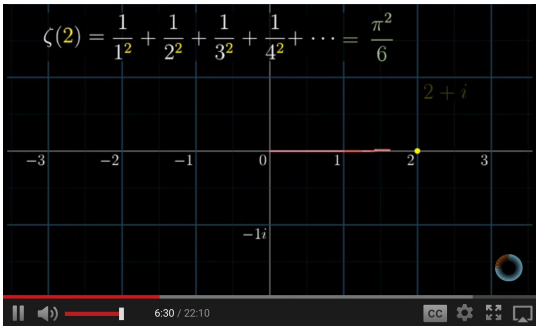

$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$
7:08 / 22:10

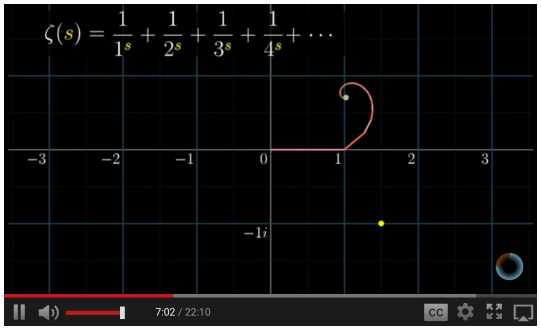

$\zeta(2+i) = \frac{1}{1^{2+i}} + \frac{1}{2^{2+i}} + \frac{1}{3^{2+i}} + \frac{1}{4^{2+i}} + \cdots = 1.15 - 0.44i$
$2+i$
6:40 / 22:10

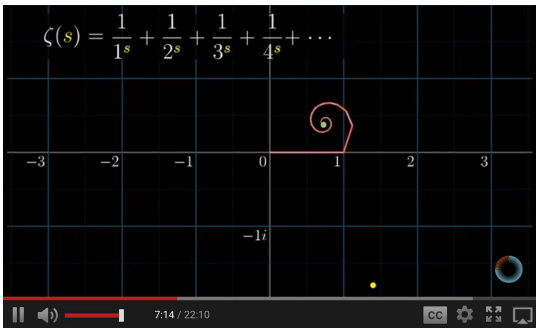

$\left(\frac{1}{2}\right)^2 \left(\frac{1}{2}\right)^i$
5:58 / 22:10

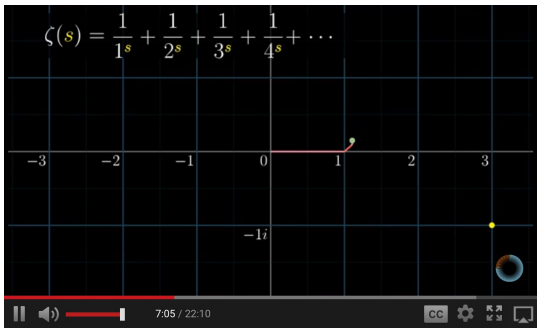

$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$
7:15 / 22:10









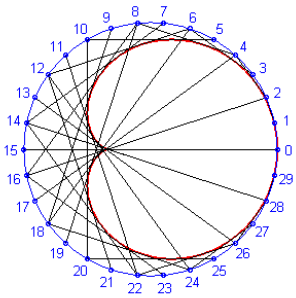


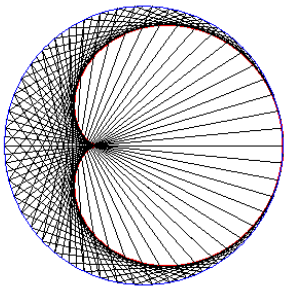
6) Une autre association d'idées ‖

Cette association d'idées relie deux images, l'une montrant la façon dont les parties imaginaires des zéros de ζ tournent autour de 0 lorsque leur partie réelle est $\frac{1}{2}$ (alors que cette même spirale se décale lorsque la partie réelle est différente de $\frac{1}{2}$), et une autre montrant la façon de construire une cardioïde comme tangente à des segments se promenant.

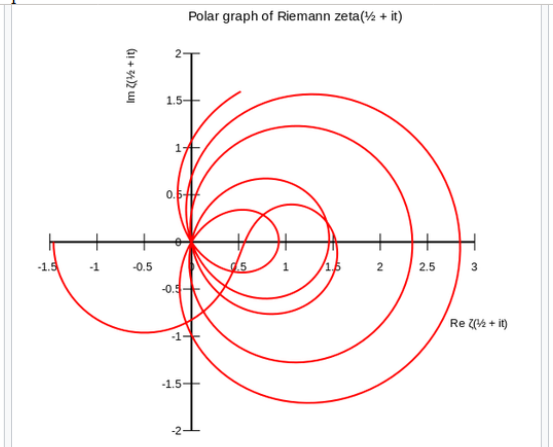
‖. jamais postée sur la toile

e) l'enveloppe d'une corde (PQ) du cercle de centre W et de rayon $\frac{3a}{2}$ (cercle circonscrit à la cardioïde), P et Q parcourant ce cercle dans le même sens, l'un ayant une vitesse double de l'autre (génération dite "de Cremona").





Ci-dessus, le point n est relié au point $2n$ modulo 30.

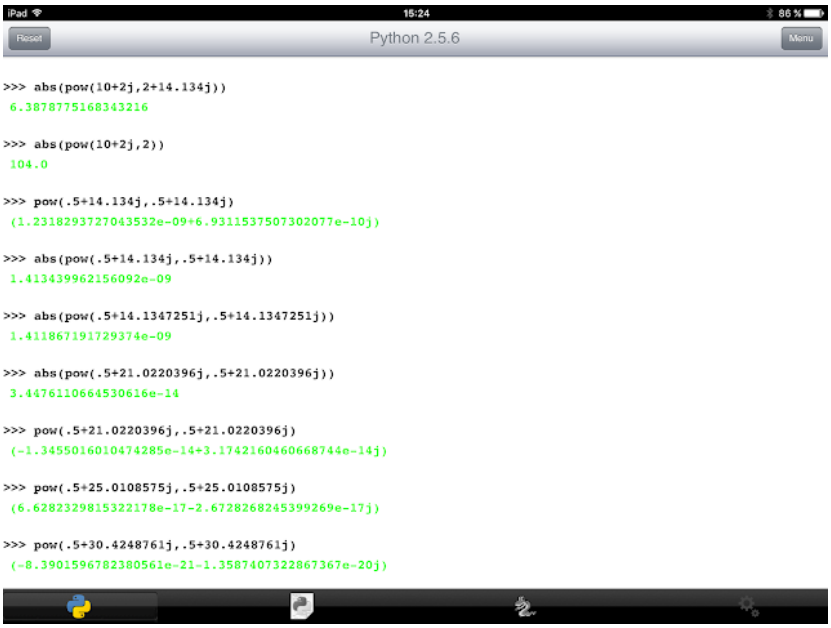


This image shows a plot of the Riemann zeta function along the critical line for real values of t running from 0 to 34. The first five zeros in the critical strip are clearly visible as the place where the spirals pass through the origin.

7) On travaille sur des nombres minis minis quand il s'agit de sommer des inverses de puissances d'entiers, forcément

Un zéro de zêta puissance lui-même, c'est vraiment mini-mini ** ! Et ça aussi, c'est minus !

**. Posté initialement sur Google+ le 27.7.2017, sauvegardé sur Blogger ici https://milliardsdautres.blogspot.com/2019/10/trucs-minuscules-vraiment.html



8) Indiscernabilité des zéros de zêta

La fonction qui rend les zéros de zêta indiscernables [††] au sens de Galois peut être décrite ainsi : quel que soit l'entier que l'on considère, lorsqu'on l'élève à la puissance d'un zéro de zêta, la norme du complexe obtenu est toujours égale à la racine de l'entier considéré.

Voyons un exemple pour fixer un peu les idées : prenons l'entier 13 dont la racine carrée vaut à peu près 3.605. Considérons les parties imaginaires des 5 premiers zéros de zêta qui valent à peu près $b1 = 14.134, b2 = 21.022, b3 = 25.010, b4 = 30.424$ et $b5 = 32.935$.

Elevons 13 aux puissances $0.5 + k_i * \sqrt{-1}$ à l'aide de python téléchargeable sur tablette en partance.
On obtient $pow(13, 0.5 + 14.134i) = 0.448 - 3.577i$
(noter au passage que python appelle i "j", pourquoi ? On le note i comme d'habitude car on n'est pas sur tablette en voyage.)
ou encore $pow(13, 0.5 + 21.022i) = -3.14 - 1.77i$
ou encore $pow(13, 0.5 + 25.01i) = 0.903 + 3.49i$
ou pour le quatrième zéro $pow(13, 0.5 + 30.424i) = -3.157 + 1.74i$
ou enfin $pow(13, 0.5 + 32.935i) = -3.391 + 1.224i$.

On vérifie alors que $\sqrt{0.448^2 + 3.577^2} = 3.605 = \sqrt{13}$ et de même pour le second zéro que $\sqrt{3.14^+1.77^2} = \sqrt{13}$.

Au sujet de l'indiscernabilité des zéros de zêta d'hier, ça ne va pas : quel que soit le complexe a+bi, quand on élève un entier à la puissance de ce complexe, seul a et l'entier considéré interviennent dans le calcul de la norme. Ce n'est pas le cas lorsqu'on élève un complexe à une puissance complexe.

$$|x^{a+bi}| = |x^a|$$

pour x entier mais pas pour x complexe.

††. Posté initialement sur Google+ le 26.7.2017 et le 27.7.2017, sauvegardé sur Blogger ici https://milliardsdautres.blogspot.com/2019/10/trucs-minuscules-vraiment.html

A défaut de deviner, Denise devise (Denise Vella-Chemla, 16.11.2019)

On avait eu l'idée en juillet 2014 de considérer la somme de sommes de cosinus que les nombres premiers annulent. On a présenté à plusieurs reprises cette idée ou des variations autour de cette idée (cf. [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14]). Victor Varin nous a fourni une démonstration de l'annulation de la somme de cosinus considérée pour les nombres premiers et pour eux seulement. On voudrait ici étudier une analogie entre le fait d'alterner les signes + et - devant les termes de la somme de sommes de cosinus, ce qui permet d'associer une image 0 ou une image 1 aux nombres premiers selon qu'ils sont de la forme $4k+1$ ou $4k+3$, et le fait d'utiliser des sommes alternant beaucoup plus simplement seulement des $+1$ et des -1.

Pourquoi le fait d'alterner les signes de la somme de sommes de cosinus permet-il d'obtenir une image 0 ou 1 pour les nombres premiers ? On peut imaginer que pour les nombres premiers, et seulement pour eux, les cosinus s'éliminent 2 à 2, par exemple parce qu'on pourrait parfois avoir $\cos\frac{2\pi no}{b} = \cos\frac{2\pi n(b-o)}{b}$.

Il est possible que la somme de cosinus alternée soit toujours telle que, dans le cas des nombres premiers, si elle contient l'ajout d'une certaine valeur $+x$ correspondant à un cosinus particulier, elle contient également le retrait de la valeur en question $-x$ correspondant au cosinus d'un autre angle, (que ce soit $\pi+\theta$ ou $\pi-\theta$), l'objet de cette note est de deviser, de faire saisir notre idée, puis de vérifier la validité de cette idée par programme ultérieurement.

Et puis après tout, quelle différence, entre le fait de faire $+x \ldots - x$ et le fait de faire $+1 \ldots - 1$?

On trouve alors sur la toile plusieurs éléments concernant cette série de $(-1)^n$, par exemple ici :

http://serge.mehl.free.fr/chrono/Grandi.htmlserie

ou bien ici

https://ljk.imag.fr/membres/Bernard.Ycart/mel/sn/sn.pdf §3.4 pages 50 à 54.

On peut mettre en bijection nos sommes alternées de cosinus avec des séries alternées à nombres finis de termes, ces séries ne contenant que des nombres de valeur absolue 1 et contenant autant de $+1$ que de -1. La limite asymptotique de la série $\sum(-1)^n$ est $\frac{1}{2}$ selon Grandi ou Leibniz. On rêve d'un lien entre cette limite asymptotique et un autre $\frac{1}{2}$ bien connu.

Il faudrait d'une part comprendre pourquoi dans le cas des nombres composés, il n'y a pas équilibre entre les $+1$ et les -1 ; en fait, comme on l'a expliqué, il faudrait étudier le déséquilibre entre les $+x$ et les $-x$, les $+x$ correspondant à certains cos et les $-x$ correspondant à d'autres cos qui leur sont liés par les relations trigonométriques bien connues.

Il faudrait d'autre part être capable de relier nos sommes de cosinus à la fonction Γ d'Euler, qui est la généralisation de la factorielle aux nombres complexes, peut-être en utilisant la définition du cosinus basée sur la série entière qui converge pour tout réel x :

$$\cos x = \sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n)!} x^{2n}$$

Un petit élément qui conforte ce début de réflexion est que quand on compare le nombre de $+1$ au nombre de -1, c'est un peu comme si on étudiait une dérivée (dans le sens d'une différence d'images rapportée à une différence d'antécédents) et qu'on a l'impression que ce qui donne son aspect à ζ, c'est la dérivée de Γ plutôt que Γ elle-même (cf. des images colorées du plan complexe de ζ, Γ et Γ', par exemple, cf. [15]).

On s'est, une fois de plus, octroyé le droit de deviser.

Notes précédentes

On a concaténé tous les fichiers ici
http://denisevellachemla.eu/devise.pdf

[1] 10.7.2014 : Primalité et zéros de sommes de cosinus,
http://denisevellachemla.eu/primesommecos-avec-lien-sur-forum.pdf

[2] 16.7.2015 : Discret / continu,
http://denisevellachemla.eu/matcos.pdf

[3] 18.7.2015 : Discret / continu (suite),
http://denisevellachemla.eu/matrices-polynomes-de-Tchebychev.pdf

[4] 21.5.2016 : Programme préféré : les nombres premiers annulent une somme de cosinus,
http://denisevellachemla.eu/pgm-prefere.pdf

[5] 12.7.2017 : programme et plot de la somme de cosinus en python,
http://denisevellachemla.eu/Capture-du-2017-07-12-11-21-09.png

[6] 13.7.2017 : preuve de Victor Varin que les nombres premiers annulent ma somme de sommes de cosinus et qu'ils sont les seuls nombres à le faire,
http://denisevellachemla.eu/VictorVarinKeldyshSumsumcos.pdf

[7] 31.5.2018 : chercher des idées,
http://denisevellachemla.eu/sommecosTJ.pdf

[8] 28.10.2018 : Alterner les termes de la somme de cosinus qui s'annule pour les nombres premiers,
http://denisevellachemla.eu/alternesommecos.pdf

[9] 28.10.2018 : Programme en C++ pour les sommes alternées de cosinus (les $4k+3$ ont pour image 0 et les $4k+1$ ont pour image 1),
http://denisevellachemla.eu/gardeprogcpp.pdf

[10] 4.11.2018 : Interrupteurs ou bien une somme alternée de cosinus assez surprenante,
http://denisevellachemla.eu/premiers-image-un-demi.pdf

[11] 9.12.2018 : programme en python de la somme de cosinus initiale,
http://denisevellachemla.eu/sumsumcos.pdf

[12] 9.12.2018 : résultat du programme [11],
http://denisevellachemla.eu/ressumsumcos.pdf

[13] 4.3.2019 : Spectres de la somme de somme de cosinus (spectres divers obtenus par programmes utilisant des transformées de Fourier disponibles dans des librairies python),
http://denisevellachemla.eu/concatspectres.pdf

[14] 2.5.2019 : joli spectre couleurs de feu,
http://denisevellachemla.eu/variation1.jpg

[15] 11.7.2017 : petit memo,
http://denisevellachemla.eu/memo.pdf

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))
```

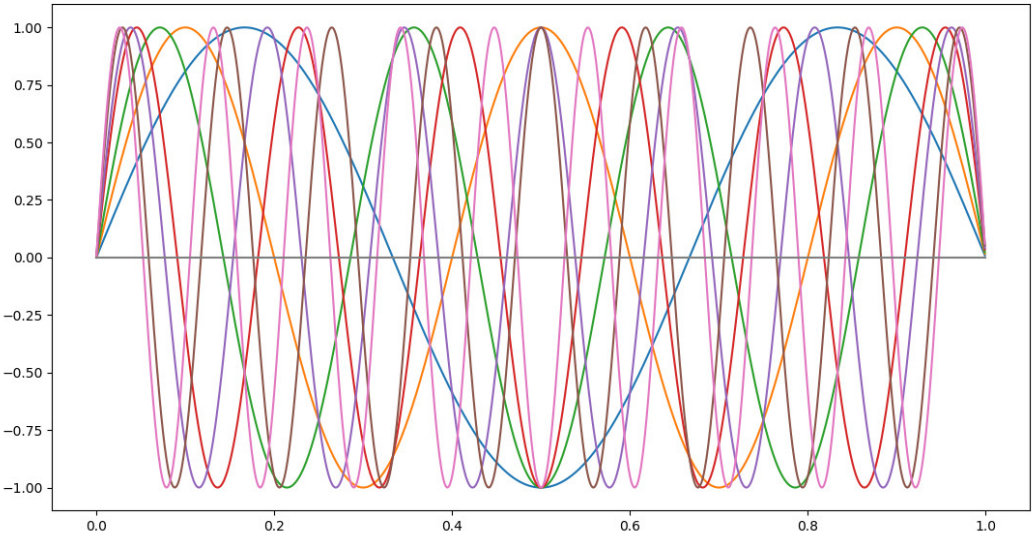
Voici les images des nombres de 1 à 100 fournies par la fonction :

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

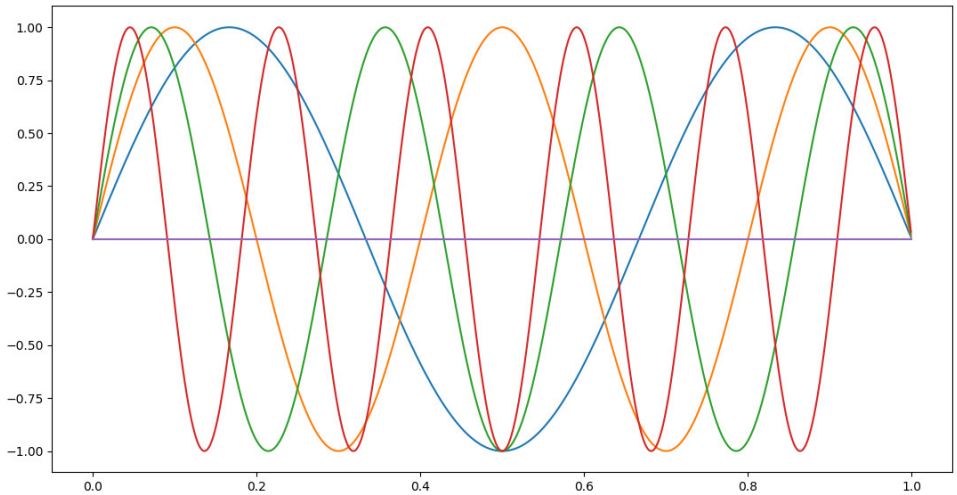
On est étonné de voir que la fonction associe l'opposé $-p$ d'un nombre premier p à son double $2p$ lorsque c'est un nombre premier de la forme $4k+1$ (voir les images $sac(10) = -5, sac(26) = -13, sac(34), sac(58), sac(74), sac(82), \ldots$).

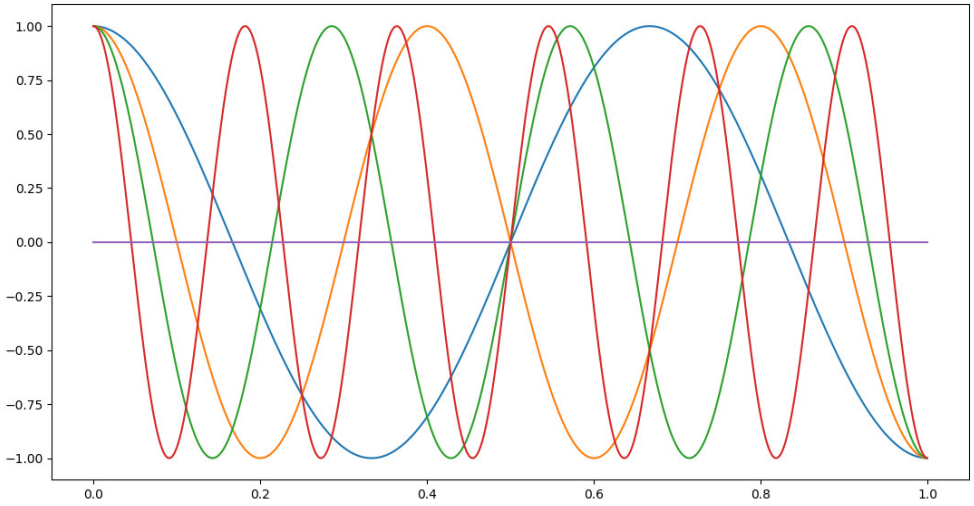
Aux doubles de nombres premiers $2p$ avec p de la forme $4k+3$, la fonction associe $-p-2$ (voir les images $sac(6) = -5, sac(14) = -9, sac(22) = -13, sac(38), sac(46), sac(62), sac(86), sac(94), \ldots$).

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.





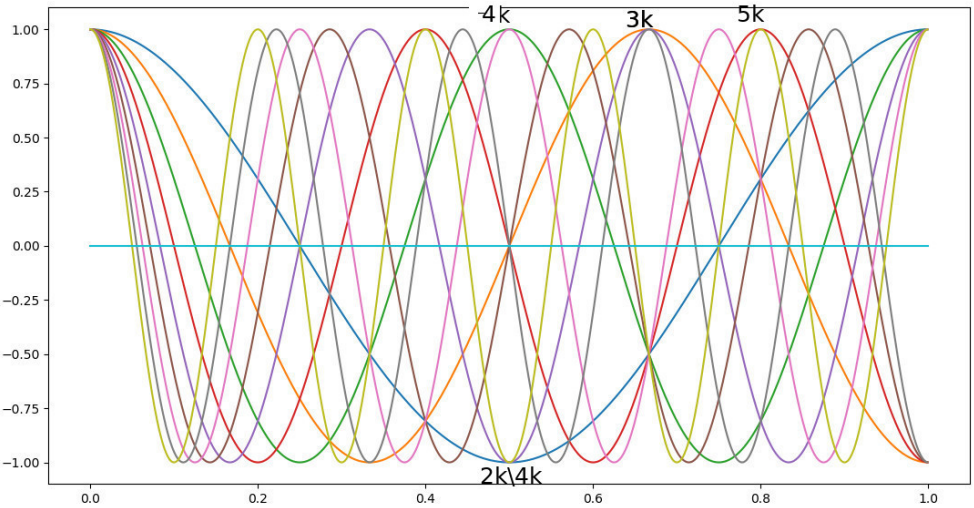
Toutes les cosinusoïdes de fonctions de la forme $\cos(k\pi x)$ avec k impair se croisent en $1/2$.

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 ?

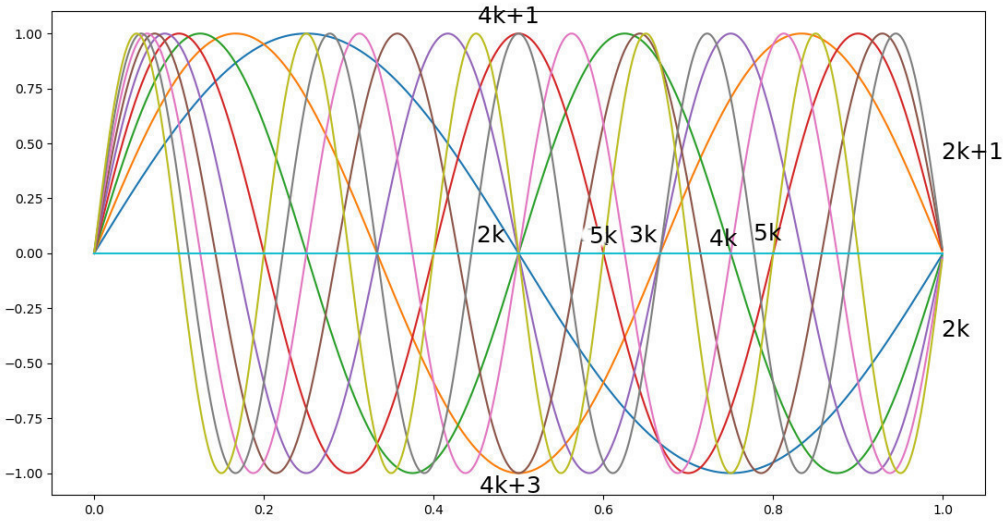


En abscisse 1/2, les courbes des entiers pairs se croisent en haut (ordonnée = +1) ou en bas (ordonnée = -1), les courbes des entiers impairs se croisent sur l'axe des ordonnées (ordonnée = 0). Le point commun à plusieurs courbes en haut au centre voit se croiser les courbes des entiers $4k$ (là, 4 et 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.

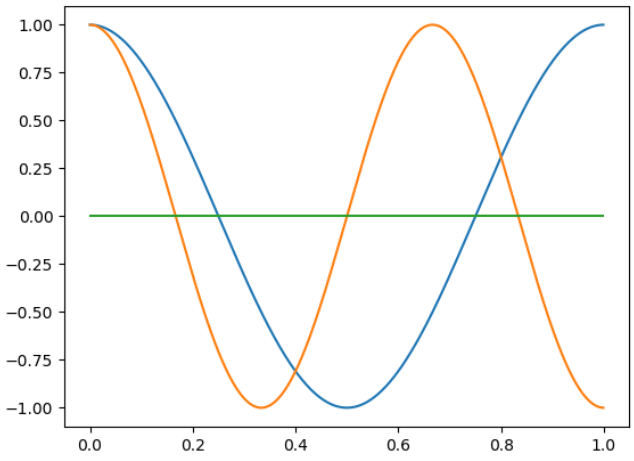
Sur une visualisation utilisant plutôt des courbes de sinus, les points multiples sont amenés sur l'axe des ordonnées.

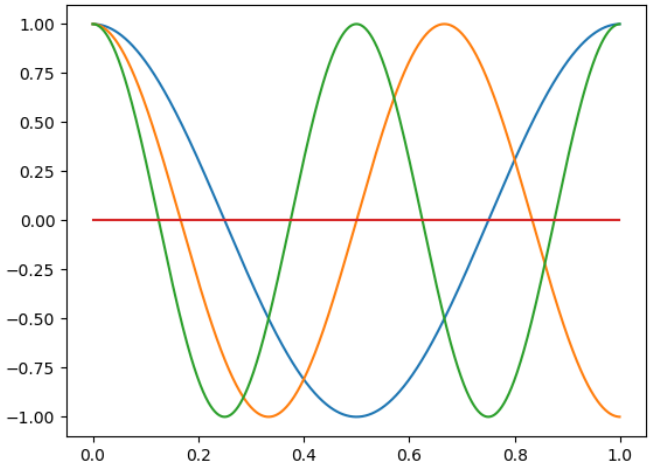


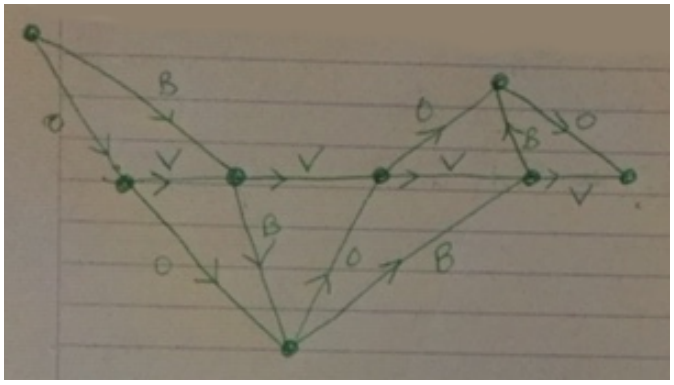
Comment ils passent peut-être des courbes à leurs triangles fléchés (Denise Vella-Chemla, 20.11.2019)

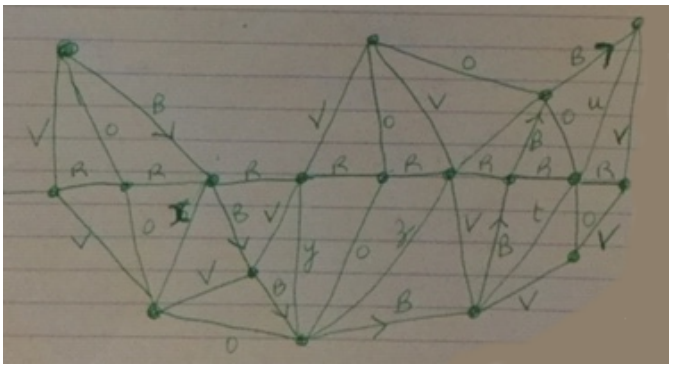
On présente, sur 4 graphiques qui se passent de commentaire, comment on imagine qu'il faut envisager le passage des courbes à des graphes orientés ne contenant que des triangles et dont les arcs sont étiquetés par des +1 et des -1.

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, 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 $n/2$.

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

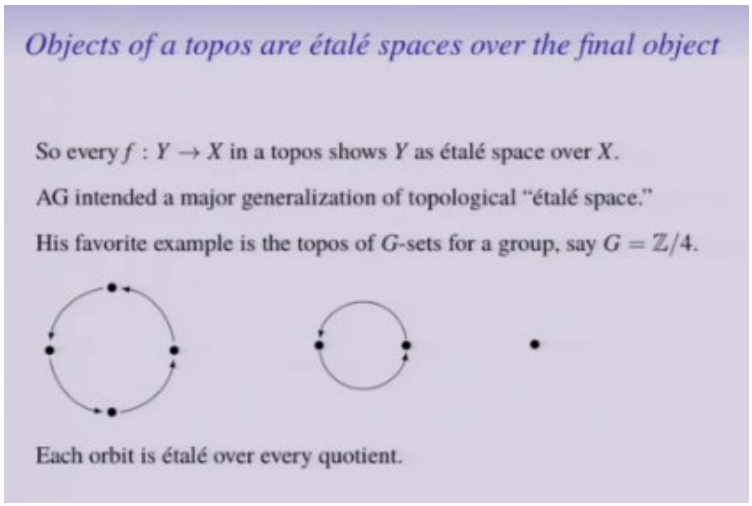
Mais on imagine bien qu'il existe au moins un nombre impair compris entre 3 et $n/2$ qui n'est pas congru à 0, tout en n'étant pas non plus congru à n selon un nombre premier p_k. Ce qui rend notre dernière assertion obligatoirement fausse, et la possibilité que l'intersection soit vide par là même.

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:

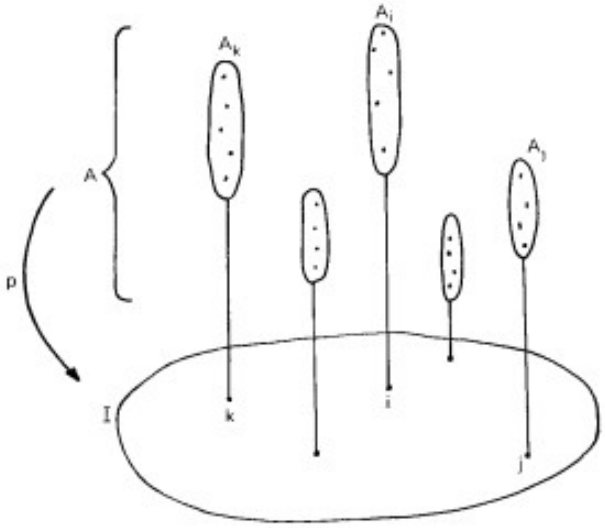


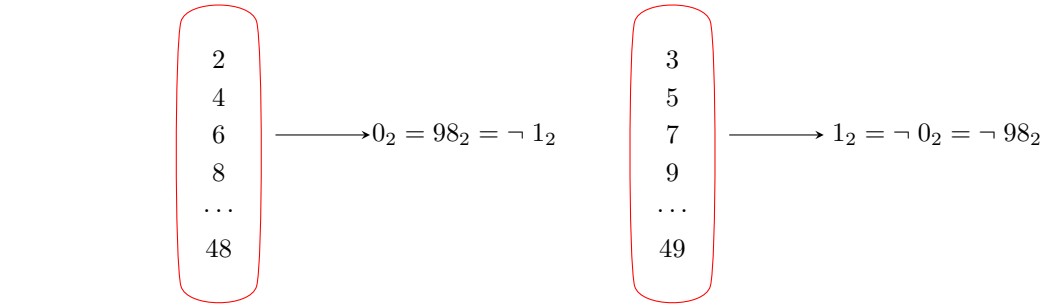
Fig. 4.4.

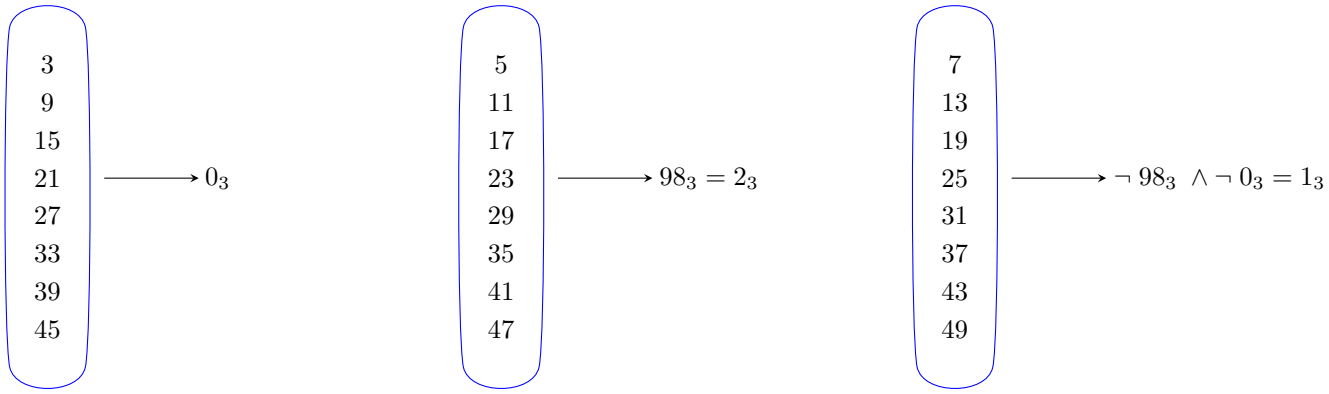
If we let A be the union of all the A_i's, i.e.

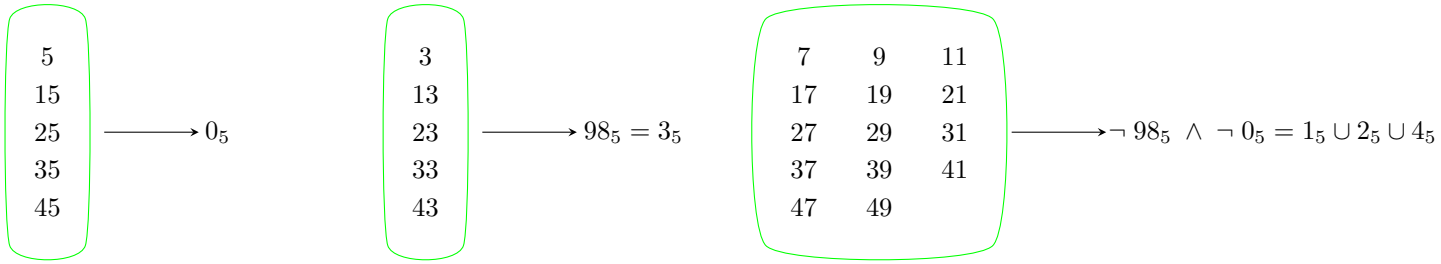
$$A = \{x : \text{for some } i,\ x \in A_i\}$$

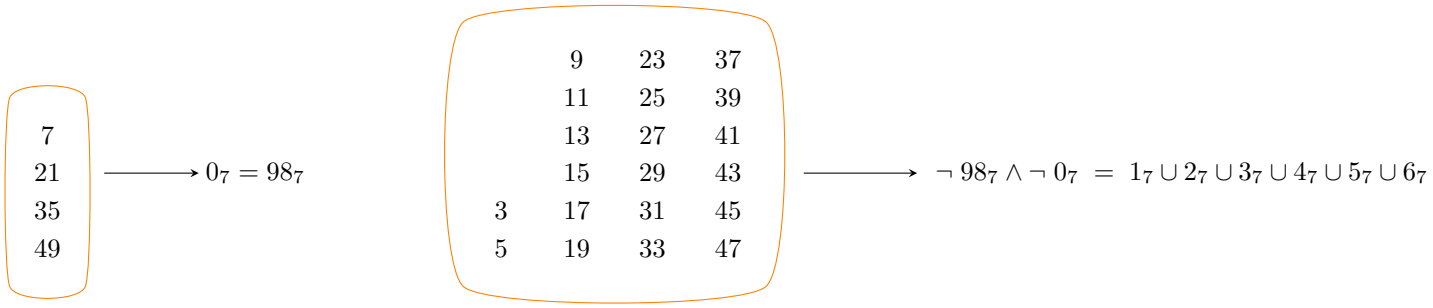
then there is an obvious map $p : A \to I$. If $x \in A$ then there is exactly one A_i such that $x \in A_i$, by the disjointness condition. We put $p(x) = i$. Thus

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).

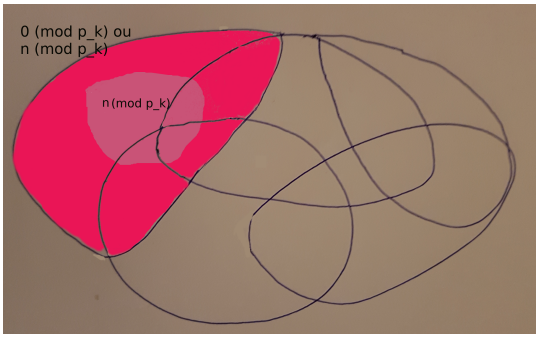
On pose maintenant $D(n) = \cap F(p_k, n)$, c'est l'intersection des ensembles $F(p_k, n)$ pour tous les premiers p_k compris entre 3 et $\sqrt{n}$.

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.*

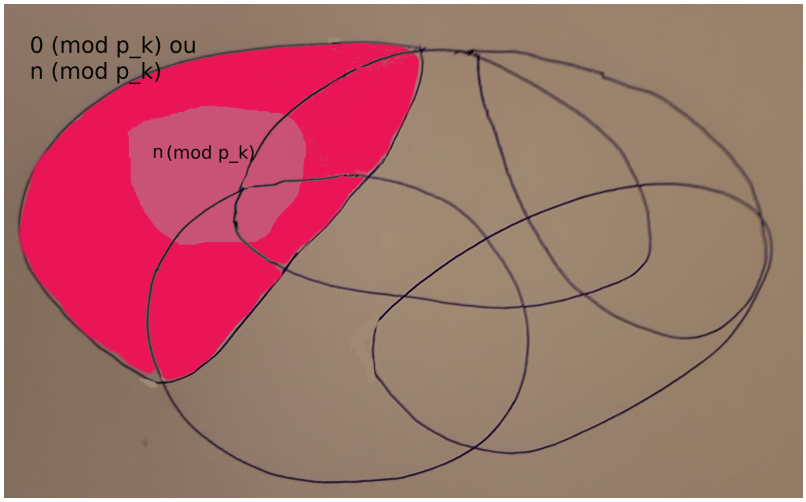
2. Existence d'un décomposant de Goldbach pour tout nombre pair

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.

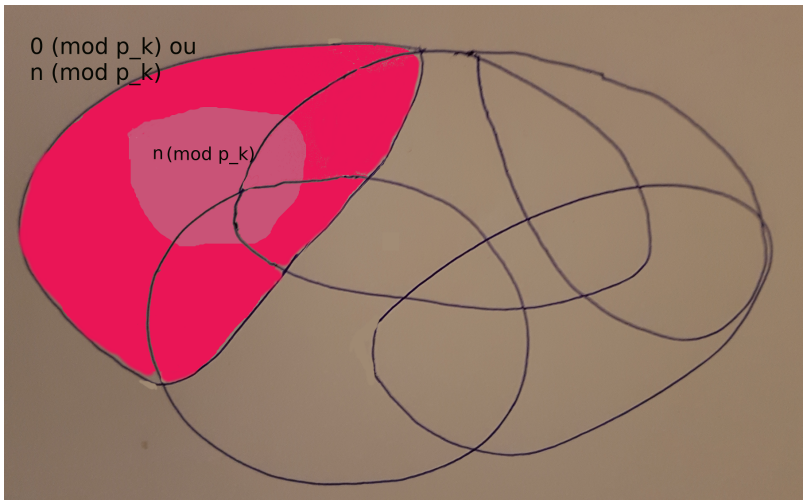
Essayons de comprendre pourquoi $D(n) = \cap F(p_k, n)$ ne peut être vide. On reprend l'écriture initiale qu'on avait choisie, sous forme logique : dire que l'intersection des ensembles de la forme $\{\neg 0_{p_k} \wedge \neg n_{p_k}\}$

∗. 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]

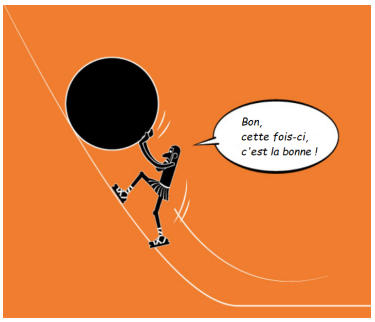
Soit $n \in 2\mathbb{N}+6$ un entier pair supérieur à 6. Pour tout $p \in \mathbb{P}^*$ premier impair inférieur à $\sqrt{n}$ (*i.e.* $3 \leq p \leq \sqrt{n}$), on définit l'ensemble :

$$F_n(p) = \{m \in 2\mathbb{N}+1 : 3 \leq m \leq n/2,\ m \not\equiv 0\ [p],\ m \not\equiv n\ [p]\}$$

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.

1. Leila Schneps d'abord, Jacques Chemla ensuite, ont réécrit cette partie.

Lemme 4 : Soit $n \in 2\mathbb{N}+6$. Si $D_n \neq \varnothing$, alors n vérifie la conjecture de Goldbach.

Démonstration : Si $D_n \neq \varnothing$, il contient un entier p nécessairement premier (d'après le lemme 1), tel que $q = n - p$ est également premier (d'après le lemme 2), et donc $n = p + q$ vérifie la conjecture de Goldbach.

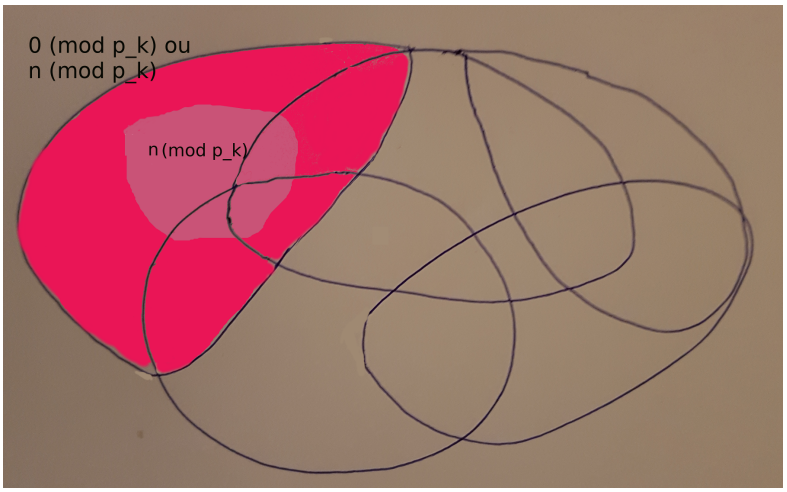
2. Existence d'un décomposant de Goldbach pour tout nombre pair

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.

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*".

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 [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

$$\begin{aligned}
100 &= \ldots && + 11\\
100 &= 29 \times 3 && + 13\\
100 &= \ldots && + 17\\
100 &= 27 \times 3 && + 19\\
100 &= 11 \times 7 && + 23\\
100 &= \ldots && + 29\\
100 &= 23 \times 3 && + 31\\
100 &= 21 \times 3 && + 37\\
100 &= \ldots && + 41\\
100 &= 19 \times 3 && + 43\\
100 &= \ldots && + 47
\end{aligned}$$

3. puisqu'on est 100 (sans) démonstration !

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.

$$\begin{cases} n = a_1 \times q_1 & + p_1 \\ n = a_2 \times q_2 & + p_2 \\ \dots & \\ n = a_k \times q_k & + p_k \end{cases}$$

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.

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.

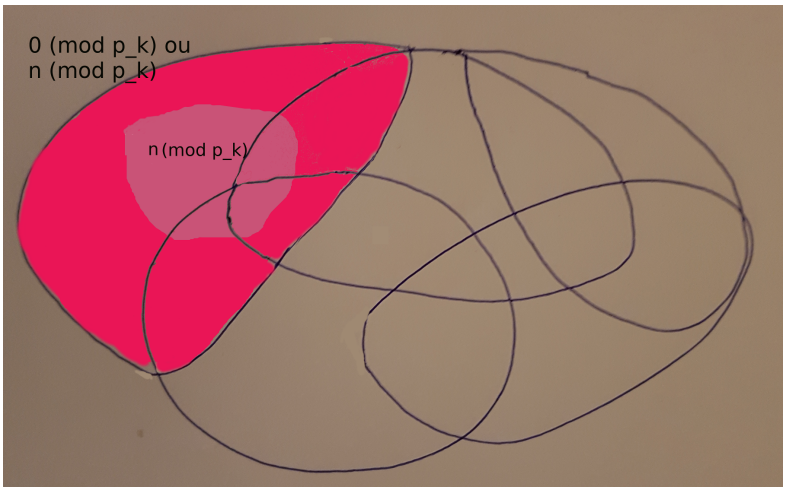
2. Existence d'un décomposant de Goldbach pour tout nombre pair

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.

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 $n/2$.

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

int tabfacteurs[10000], tabpuiss[10000], tabexpo[10000], tab0[10000],
tab1[10000], tab2[10000] ;

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, k, p, nbdiv, tempo, expo, nbdivt1, nbdivt2, nbprime ;

  nbprime = 0 ;
  for (n = 1 ; n <= 1157 ; n=n+2)
    {
      std::cout << "\n" << n << " -> " ;
      tabfacteurs[n] = 1 ;
      tab0[n] = 1 ;
      tab1[n] = 1 ;
      tab2[n] = 1 ;
      tabpuiss[n] = 1 ;
      tabexpo[n] = 1 ;
      tempo = n ; p = n/2 ;
      nbdiv = 1 ;
      nbdivt1 = 0 ;
      nbdivt2 = 0 ;
      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(n))) nbdiv=nbdiv-1 ;
      if ((nbdiv == 1) && (prime(n)))
      {
        tabpuiss[1] = n ;
        tabexpo[1] = 1 ;
        if ((n % 4) == 1) nbdivt1 = nbdivt1+1 ;
        else if ((n % 4) == 3) nbdivt2 = nbdivt2+1 ;
      }
      else if ((nbdiv == 1) && (not(prime(n))))
      {
        tempo = tabfacteurs[1] ;
        tabpuiss[1] = n ;
        expo = 1 ;
        while (tempo < n)
          {
            tempo=tempo*tabfacteurs[1] ;
            expo = expo+1 ;
          }
        tabexpo[1] = expo ;
        if ((tabfacteurs[1] % 4) == 1) nbdivt1 = nbdivt1+expo ;
        else if ((tabfacteurs[1] % 4) == 3) nbdivt2 = nbdivt2+expo ;
      }
      else if (nbdiv > 1)
      {
        for (k = 1 ; k <= nbdiv ; ++k)
          {
            tempo = tabfacteurs[k] ;
            expo = 1 ;
            while (((n % tempo) == 0) && (tempo < n))
            {
              tempo=tempo*tabfacteurs[k] ;
              expo = expo+1 ;
            }
```

```
            tabpuiss[k] = tempo/tabfacteurs[k] ;
            tabexpo[k] = expo-1 ;
            if ((tabfacteurs[k] % 4) == 1) nbdivt1 = nbdivt1+expo-1 ;
            else if ((tabfacteurs[k] % 4) == 3) nbdivt2 = nbdivt2+expo-1 ;
          }
      }
      for (k = 1 ; k <= nbdiv ; ++k)
      {
          std::cout << tabfacteurs[k] << "^" ;
        std::cout << tabexpo[k] << "." ;
      }
      tab0[n] = nbdiv ;
      tab1[n] = nbdivt1 ;
      tab2[n] = nbdivt2 ;
    }
  std::cout << "\n\n" ;
  std::cout << "Nombres de diviseurs 4k+1 \n" ;
  for (n = 1 ; n <= 1157 ; n=n+2)
    std::cout << tab1[n] << "    " ;
  std::cout << "\n\n" ;
  std::cout << "Nombres de diviseurs 4k+3 \n" ;
  for (n = 1 ; n <= 1157 ; n=n+2)
    std::cout << tab2[n] << "    " ;
  std::cout << "\n\n" ;
  std::cout << "Nombres total de facteurs premiers différents\n" ;
  for (n = 1 ; n <= 1157 ; n=n+2)
    std::cout << tab0[n] << "    " ;
}
```

1 ->
3 -> 3^1.
5 -> 5^1.
7 -> 7^1.
9 -> 3^2.
11 -> 11^1.
13 -> 13^1.
15 -> 5^1.3^1.
17 -> 17^1.
19 -> 19^1.
21 -> 7^1.3^1.
23 -> 23^1.
25 -> 5^2.
27 -> 3^3.
29 -> 29^1.
31 -> 31^1.
33 -> 11^1.3^1.
35 -> 7^1.5^1.
37 -> 37^1.
39 -> 13^1.3^1.
41 -> 41^1.
43 -> 43^1.
45 -> 5^1.3^2.
47 -> 47^1.
49 -> 7^2.
51 -> 17^1.3^1.
53 -> 53^1.
55 -> 11^1.5^1.
57 -> 19^1.3^1.
59 -> 59^1.
61 -> 61^1.
63 -> 7^1.3^2.
65 -> 13^1.5^1.
67 -> 67^1.
69 -> 23^1.3^1.
71 -> 71^1.
73 -> 73^1.
75 -> 5^2.3^1.
77 -> 11^1.7^1.
79 -> 79^1.
81 -> 3^4.
83 -> 83^1.
85 -> 17^1.5^1.
87 -> 29^1.3^1.
89 -> 89^1.
91 -> 13^1.7^1.
93 -> 31^1.3^1.
95 -> 19^1.5^1.
97 -> 97^1.
99 -> 11^1.3^2.
101 -> 101^1.
103 -> 103^1.
105 -> 7^1.5^1.3^1.
107 -> 107^1.
109 -> 109^1.
111 -> 37^1.3^1.
113 -> 113^1.
115 -> 23^1.5^1.
117 -> 13^1.3^2.
119 -> 17^1.7^1.
121 -> 11^2.
123 -> 41^1.3^1.
125 -> 5^3.
127 -> 127^1.
129 -> 43^1.3^1.
131 -> 131^1.
133 -> 19^1.7^1.
135 -> 5^1.3^3.
137 -> 137^1.
139 -> 139^1.
141 -> 47^1.3^1.
143 -> 13^1.11^1.
145 -> 29^1.5^1.
147 -> 7^2.3^1.
149 -> 149^1.
151 -> 151^1.
153 -> 17^1.3^2.
155 -> 31^1.5^1.
157 -> 157^1.
159 -> 53^1.3^1.
161 -> 23^1.7^1.
163 -> 163^1.
165 -> 11^1.5^1.3^1.
167 -> 167^1.
169 -> 13^2.
171 -> 19^1.3^2.
173 -> 173^1.
175 -> 7^1.5^2.
177 -> 59^1.3^1.
179 -> 179^1.

181 -> 181^1.
183 -> 61^1.3^1.
185 -> 37^1.5^1.
187 -> 17^1.11^1.
189 -> 7^1.3^3.
191 -> 191^1.
193 -> 193^1.
195 -> 13^1.5^1.3^1.
197 -> 197^1.
199 -> 199^1.
201 -> 67^1.3^1.
203 -> 29^1.7^1.
205 -> 41^1.5^1.
207 -> 23^1.3^2.
209 -> 19^1.11^1.
211 -> 211^1.
213 -> 71^1.3^1.
215 -> 43^1.5^1.
217 -> 31^1.7^1.
219 -> 73^1.3^1.
221 -> 17^1.13^1.
223 -> 223^1.
225 -> 5^2.3^2.
227 -> 227^1.
229 -> 229^1.
231 -> 11^1.7^1.3^1.
233 -> 233^1.
235 -> 47^1.5^1.
237 -> 79^1.3^1.
239 -> 239^1.
241 -> 241^1.
243 -> 3^5.
245 -> 7^2.5^1.
247 -> 19^1.13^1.
249 -> 83^1.3^1.
251 -> 251^1.
253 -> 23^1.11^1.
255 -> 17^1.5^1.3^1.
257 -> 257^1.
259 -> 37^1.7^1.
261 -> 29^1.3^2.
263 -> 263^1.
265 -> 53^1.5^1.
267 -> 89^1.3^1.
269 -> 269^1.
271 -> 271^1.
273 -> 13^1.7^1.3^1.
275 -> 11^1.5^2.
277 -> 277^1.
279 -> 31^1.3^2.
281 -> 281^1.
283 -> 283^1.
285 -> 19^1.5^1.3^1.
287 -> 41^1.7^1.
289 -> 17^2.
291 -> 97^1.3^1.
293 -> 293^1.
295 -> 59^1.5^1.
297 -> 11^1.3^3.
299 -> 23^1.13^1.
301 -> 43^1.7^1.
303 -> 101^1.3^1.
305 -> 61^1.5^1.
307 -> 307^1.
309 -> 103^1.3^1.
311 -> 311^1.
313 -> 313^1.
315 -> 7^1.5^1.3^2.
317 -> 317^1.
319 -> 29^1.11^1.
321 -> 107^1.3^1.
323 -> 19^1.17^1.
325 -> 13^1.5^2.
327 -> 109^1.3^1.
329 -> 47^1.7^1.
331 -> 331^1.
333 -> 37^1.3^2.
335 -> 67^1.5^1.
337 -> 337^1.
339 -> 113^1.3^1.
341 -> 31^1.11^1.
343 -> 7^3.
345 -> 23^1.5^1.3^1.
347 -> 347^1.
349 -> 349^1.
351 -> 13^1.3^3.
353 -> 353^1.
355 -> 71^1.5^1.
357 -> 17^1.7^1.3^1.
359 -> 359^1.
361 -> 19^2.

363 -> 11^2.3^1.
365 -> 73^1.5^1.
367 -> 367^1.
369 -> 41^1.3^2.
371 -> 53^1.7^1.
373 -> 373^1.
375 -> 5^3.3^1.
377 -> 29^1.13^1.
379 -> 379^1.
381 -> 127^1.3^1.
383 -> 383^1.
385 -> 11^1.7^1.5^1.
387 -> 43^1.3^2.
389 -> 389^1.
391 -> 23^1.17^1.
393 -> 131^1.3^1.
395 -> 79^1.5^1.
397 -> 397^1.
399 -> 19^1.7^1.3^1.
401 -> 401^1.
403 -> 31^1.13^1.
405 -> 5^1.3^4.
407 -> 37^1.11^1.
409 -> 409^1.
411 -> 137^1.3^1.
413 -> 59^1.7^1.
415 -> 83^1.5^1.
417 -> 139^1.3^1.
419 -> 419^1.
421 -> 421^1.
423 -> 47^1.3^2.
425 -> 17^1.5^2.
427 -> 61^1.7^1.
429 -> 13^1.11^1.3^1.
431 -> 431^1.
433 -> 433^1.
435 -> 29^1.5^1.3^1.
437 -> 23^1.19^1.
439 -> 439^1.
441 -> 7^2.3^2.
443 -> 443^1.
445 -> 89^1.5^1.
447 -> 149^1.3^1.
449 -> 449^1.
451 -> 41^1.11^1.
453 -> 151^1.3^1.
455 -> 13^1.7^1.5^1.
457 -> 457^1.
459 -> 17^1.3^3.
461 -> 461^1.
463 -> 463^1.
465 -> 31^1.5^1.3^1.
467 -> 467^1.
469 -> 67^1.7^1.
471 -> 157^1.3^1.
473 -> 43^1.11^1.
475 -> 19^1.5^2.
477 -> 53^1.3^2.
479 -> 479^1.
481 -> 37^1.13^1.
483 -> 23^1.7^1.3^1.
485 -> 97^1.5^1.
487 -> 487^1.
489 -> 163^1.3^1.
491 -> 491^1.
493 -> 29^1.17^1.
495 -> 11^1.5^1.3^2.
497 -> 71^1.7^1.
499 -> 499^1.
501 -> 167^1.3^1.
503 -> 503^1.
505 -> 101^1.5^1.
507 -> 13^2.3^1.
509 -> 509^1.
511 -> 73^1.7^1.
513 -> 19^1.3^3.
515 -> 103^1.5^1.
517 -> 47^1.11^1.
519 -> 173^1.3^1.
521 -> 521^1.
523 -> 523^1.
525 -> 7^1.5^2.3^1.
527 -> 31^1.17^1.
529 -> 23^2.
531 -> 59^1.3^2.
533 -> 41^1.13^1.
535 -> 107^1.5^1.
537 -> 179^1.3^1.
539 -> 11^1.7^2.
541 -> 541^1.
543 -> 181^1.3^1.

545 -> 109^1.5^1.
547 -> 547^1.
549 -> 61^1.3^2.
551 -> 29^1.19^1.
553 -> 79^1.7^1.
555 -> 37^1.5^1.3^1.
557 -> 557^1.
559 -> 43^1.13^1.
561 -> 17^1.11^1.3^1.
563 -> 563^1.
565 -> 113^1.5^1.
567 -> 7^1.3^4.
569 -> 569^1.
571 -> 571^1.
573 -> 191^1.3^1.
575 -> 23^1.5^2.
577 -> 577^1.
579 -> 193^1.3^1.
581 -> 83^1.7^1.
583 -> 53^1.11^1.
585 -> 13^1.5^1.3^2.
587 -> 587^1.
589 -> 31^1.19^1.
591 -> 197^1.3^1.
593 -> 593^1.
595 -> 17^1.7^1.5^1.
597 -> 199^1.3^1.
599 -> 599^1.
601 -> 601^1.
603 -> 67^1.3^2.
605 -> 11^2.5^1.
607 -> 607^1.
609 -> 29^1.7^1.3^1.
611 -> 47^1.13^1.
613 -> 613^1.
615 -> 41^1.5^1.3^1.
617 -> 617^1.
619 -> 619^1.
621 -> 23^1.3^3.
623 -> 89^1.7^1.
625 -> 5^4.
627 -> 19^1.11^1.3^1.
629 -> 37^1.17^1.
631 -> 631^1.
633 -> 211^1.3^1.
635 -> 127^1.5^1.
637 -> 13^1.7^2.
639 -> 71^1.3^2.
641 -> 641^1.
643 -> 643^1.
645 -> 43^1.5^1.3^1.
647 -> 647^1.
649 -> 59^1.11^1.
651 -> 31^1.7^1.3^1.
653 -> 653^1.
655 -> 131^1.5^1.
657 -> 73^1.3^2.
659 -> 659^1.
661 -> 661^1.
663 -> 17^1.13^1.3^1.
665 -> 19^1.7^1.5^1.
667 -> 29^1.23^1.
669 -> 223^1.3^1.
671 -> 61^1.11^1.
673 -> 673^1.
675 -> 5^2.3^3.
677 -> 677^1.
679 -> 97^1.7^1.
681 -> 227^1.3^1.
683 -> 683^1.
685 -> 137^1.5^1.
687 -> 229^1.3^1.
689 -> 53^1.13^1.
691 -> 691^1.
693 -> 11^1.7^1.3^2.
695 -> 139^1.5^1.
697 -> 41^1.17^1.
699 -> 233^1.3^1.
701 -> 701^1.
703 -> 37^1.19^1.
705 -> 47^1.5^1.3^1.
707 -> 101^1.7^1.
709 -> 709^1.
711 -> 79^1.3^2.
713 -> 31^1.23^1.
715 -> 13^1.11^1.5^1.
717 -> 239^1.3^1.
719 -> 719^1.
721 -> 103^1.7^1.
723 -> 241^1.3^1.
725 -> 29^1.5^2.

727 -> 727^1.
729 -> 3^6.
731 -> 43^1.17^1.
733 -> 733^1.
735 -> 7^2.5^1.3^1.
737 -> 67^1.11^1.
739 -> 739^1.
741 -> 19^1.13^1.3^1.
743 -> 743^1.
745 -> 149^1.5^1.
747 -> 83^1.3^2.
749 -> 107^1.7^1.
751 -> 751^1.
753 -> 251^1.3^1.
755 -> 151^1.5^1.
757 -> 757^1.
759 -> 23^1.11^1.3^1.
761 -> 761^1.
763 -> 109^1.7^1.
765 -> 17^1.5^1.3^2.
767 -> 59^1.13^1.
769 -> 769^1.
771 -> 257^1.3^1.
773 -> 773^1.
775 -> 31^1.5^2.
777 -> 37^1.7^1.3^1.
779 -> 41^1.19^1.
781 -> 71^1.11^1.
783 -> 29^1.3^3.
785 -> 157^1.5^1.
787 -> 787^1.
789 -> 263^1.3^1.
791 -> 113^1.7^1.
793 -> 61^1.13^1.
795 -> 53^1.5^1.3^1.
797 -> 797^1.
799 -> 47^1.17^1.
801 -> 89^1.3^2.
803 -> 73^1.11^1.
805 -> 23^1.7^1.5^1.
807 -> 269^1.3^1.
809 -> 809^1.
811 -> 811^1.
813 -> 271^1.3^1.
815 -> 163^1.5^1.
817 -> 43^1.19^1.
819 -> 13^1.7^1.3^2.
821 -> 821^1.
823 -> 823^1.
825 -> 11^1.5^2.3^1.
827 -> 827^1.
829 -> 829^1.
831 -> 277^1.3^1.
833 -> 17^1.7^2.
835 -> 167^1.5^1.
837 -> 31^1.3^3.
839 -> 839^1.
841 -> 29^2.
843 -> 281^1.3^1.
845 -> 13^2.5^1.
847 -> 11^2.7^1.
849 -> 283^1.3^1.
851 -> 37^1.23^1.
853 -> 853^1.
855 -> 19^1.5^1.3^2.
857 -> 857^1.
859 -> 859^1.
861 -> 41^1.7^1.3^1.
863 -> 863^1.
865 -> 173^1.5^1.
867 -> 17^2.3^1.
869 -> 79^1.11^1.
871 -> 67^1.13^1.
873 -> 97^1.3^2.
875 -> 7^1.5^3.
877 -> 877^1.
879 -> 293^1.3^1.
881 -> 881^1.
883 -> 883^1.
885 -> 59^1.5^1.3^1.
887 -> 887^1.
889 -> 127^1.7^1.
891 -> 11^1.3^4.
893 -> 47^1.19^1.
895 -> 179^1.5^1.
897 -> 23^1.13^1.3^1.
899 -> 31^1.29^1.
901 -> 53^1.17^1.
903 -> 43^1.7^1.3^1.
905 -> 181^1.5^1.
907 -> 907^1.

909 -> 101^1.3^2.
911 -> 911^1.
913 -> 83^1.11^1.
915 -> 61^1.5^1.3^1.
917 -> 131^1.7^1.
919 -> 919^1.
921 -> 307^1.3^1.
923 -> 71^1.13^1.
925 -> 37^1.5^2.
927 -> 103^1.3^2.
929 -> 929^1.
931 -> 19^1.7^2.
933 -> 311^1.3^1.
935 -> 17^1.11^1.5^1.
937 -> 937^1.
939 -> 313^1.3^1.
941 -> 941^1.
943 -> 41^1.23^1.
945 -> 7^1.5^1.3^3.
947 -> 947^1.
949 -> 73^1.13^1.
951 -> 317^1.3^1.
953 -> 953^1.
955 -> 191^1.5^1.
957 -> 29^1.11^1.3^1.
959 -> 137^1.7^1.
961 -> 31^2.
963 -> 107^1.3^2.
965 -> 193^1.5^1.
967 -> 967^1.
969 -> 19^1.17^1.3^1.
971 -> 971^1.
973 -> 139^1.7^1.
975 -> 13^1.5^2.3^1.
977 -> 977^1.
979 -> 89^1.11^1.
981 -> 109^1.3^2.
983 -> 983^1.
985 -> 197^1.5^1.
987 -> 47^1.7^1.3^1.
989 -> 43^1.23^1.
991 -> 991^1.
993 -> 331^1.3^1.
995 -> 199^1.5^1.
997 -> 997^1.
999 -> 37^1.3^3.
1001 -> 13^1.11^1.7^1.
1003 -> 59^1.17^1.
1005 -> 67^1.5^1.3^1.
1007 -> 53^1.19^1.
1009 -> 1009^1.
1011 -> 337^1.3^1.
1013 -> 1013^1.
1015 -> 29^1.7^1.5^1.
1017 -> 113^1.3^2.
1019 -> 1019^1.
1021 -> 1021^1.
1023 -> 31^1.11^1.3^1.
1025 -> 41^1.5^2.
1027 -> 79^1.13^1.
1029 -> 7^3.3^1.
1031 -> 1031^1.
1033 -> 1033^1.
1035 -> 23^1.5^1.3^2.
1037 -> 61^1.17^1.
1039 -> 1039^1.
1041 -> 347^1.3^1.
1043 -> 149^1.7^1.
1045 -> 19^1.11^1.5^1.
1047 -> 349^1.3^1.
1049 -> 1049^1.
1051 -> 1051^1.
1053 -> 13^1.3^4.
1055 -> 211^1.5^1.
1057 -> 151^1.7^1.
1059 -> 353^1.3^1.
1061 -> 1061^1.
1063 -> 1063^1.
1065 -> 71^1.5^1.3^1.
1067 -> 97^1.11^1.
1069 -> 1069^1.
1071 -> 17^1.7^1.3^2.
1073 -> 37^1.29^1.
1075 -> 43^1.5^2.
1077 -> 359^1.3^1.
1079 -> 83^1.13^1.
1081 -> 47^1.23^1.
1083 -> 19^2.3^1.
1085 -> 31^1.7^1.5^1.
1087 -> 1087^1.
1089 -> 11^2.3^2.

```
1091 -> 1091^1.
1093 -> 1093^1.
1095 -> 73^1.5^1.3^1.
1097 -> 1097^1.
1099 -> 157^1.7^1.
1101 -> 367^1.3^1.
1103 -> 1103^1.
1105 -> 17^1.13^1.5^1.
1107 -> 41^1.3^3.
1109 -> 1109^1.
1111 -> 101^1.11^1.
1113 -> 53^1.7^1.3^1.
1115 -> 223^1.5^1.
1117 -> 1117^1.
1119 -> 373^1.3^1.
1121 -> 59^1.19^1.
1123 -> 1123^1.
1125 -> 5^3.3^2.
1127 -> 23^1.7^2.
1129 -> 1129^1.
1131 -> 29^1.13^1.3^1.
1133 -> 103^1.11^1.
1135 -> 227^1.5^1.
1137 -> 379^1.3^1.
1139 -> 67^1.17^1.
1141 -> 163^1.7^1.
1143 -> 127^1.3^2.
1145 -> 229^1.5^1.
1147 -> 37^1.31^1.
1149 -> 383^1.3^1.
1151 -> 1151^1.
1153 -> 1153^1.
1155 -> 11^1.7^1.5^1.3^1.
1157 -> 89^1.13^1.
```

Nombres de diviseurs 4k+1

```
0   0   1   0   0   0   1   1   1   0   0   0   2   0   1   0   0   1   1   1
1   0   1   0   0   1   1   1   0   0   1   0   2   0   0   0   1   2   0   1
0   0   2   1   1   1   0   1   1   0   0   1   0   1   0   1   1   1   1   1
0   1   3   0   0   0   0   1   1   0   0   1   2   0   1   0   1   1   1   1
0   0   1   0   2   0   1   2   0   0   1   1   2   1   0   0   1   2   1   0
0   1   2   0   0   0   0   1   0   1   2   0   2   0   1   0   1   1   0   0
1   0   1   1   0   0   0   2   1   1   1   0   2   1   1   0   1   2   1   0
1   0   1   1   2   1   1   1   0   1   0   1   2   0   0   0   1   1   1   1
0   1   3   1   0   0   1   1   1   1   0   0   1   0   1   1   1   1   1   0
0   0   2   0   1   1   1   3   2   0   0   0   1   0   1   1   0   1   1   0
1   1   1   1   1   1   0   1   0   0   1   0   3   1   1   0   1   2   0   0
0   0   2   1   1   1   0   2   1   1   1   0   1   0   0   1   0   2   1   0
2   0   2   0   0   0   2   1   0   0   0   0   2   2   1   1   0   1   0   1
1   0   2   1   0   0   2   1   0   0   1   1   2   0   1   1   0   2   1   1
1   0   2   0   1   0   0   2   1   1   0   1   2   0   0   1   1   2   0   0
1   0   1   0   1   1   1   2   1   0   0   1   4   0   2   0   0   1   1   0
1   0   1   0   0   0   1   1   1   0   1   2   1   1   0   1   1   2   1   1
0   0   2   1   2   0   0   1   2   1   1   1   1   1   1   0   0   2   0   0
0   1   3   0   0   1   1   1   0   0   1   0   2   0   0   0   0   1   1   0
1   1   2   1   1   1   1   2   1   1   0   1   2   0   0   1   2   2   1   1
1   1   1   1   1   0   0   1   0   1   1   0   2   0   1   1   1   1   0   1
2   1   3   0   0   1   1   1   1   0   1   0   2   2   0   1   1   3   1   1
1   0   1   0   0   0   0   1   1   1   2   0   2   0   1   0   0   2   0   0
0   1   3   0   1   0   0   2   1   1   1   1   1   0   2   1   1   1   1   1
0   0   2   0   1   0   0   3   1   1   1   0   2   0   0   0   0   1   1   1
1   1   1   1   1   1   1   2   1   0   1   0   3   1   0   0   1   1   2   0
0   1   1   1   1   0   1   1   0   1   1   0   1   1   1   1   2   2   0   1
0   0   1   0   0   0   1   2   1   1   0   0   3   1   1   1   1   1   1   1
0   0   3   0   1   2   0   1   0   1   0   0   2   1   0   0   1   1   2
```

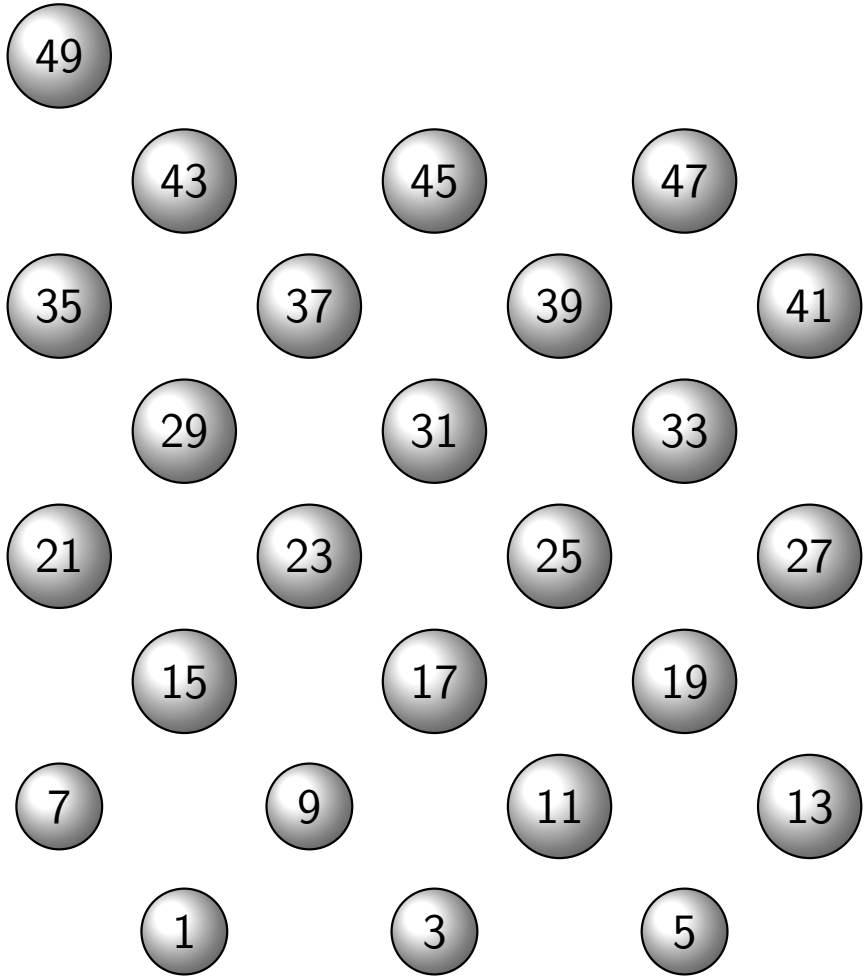
Nombres de diviseurs 4k+3

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

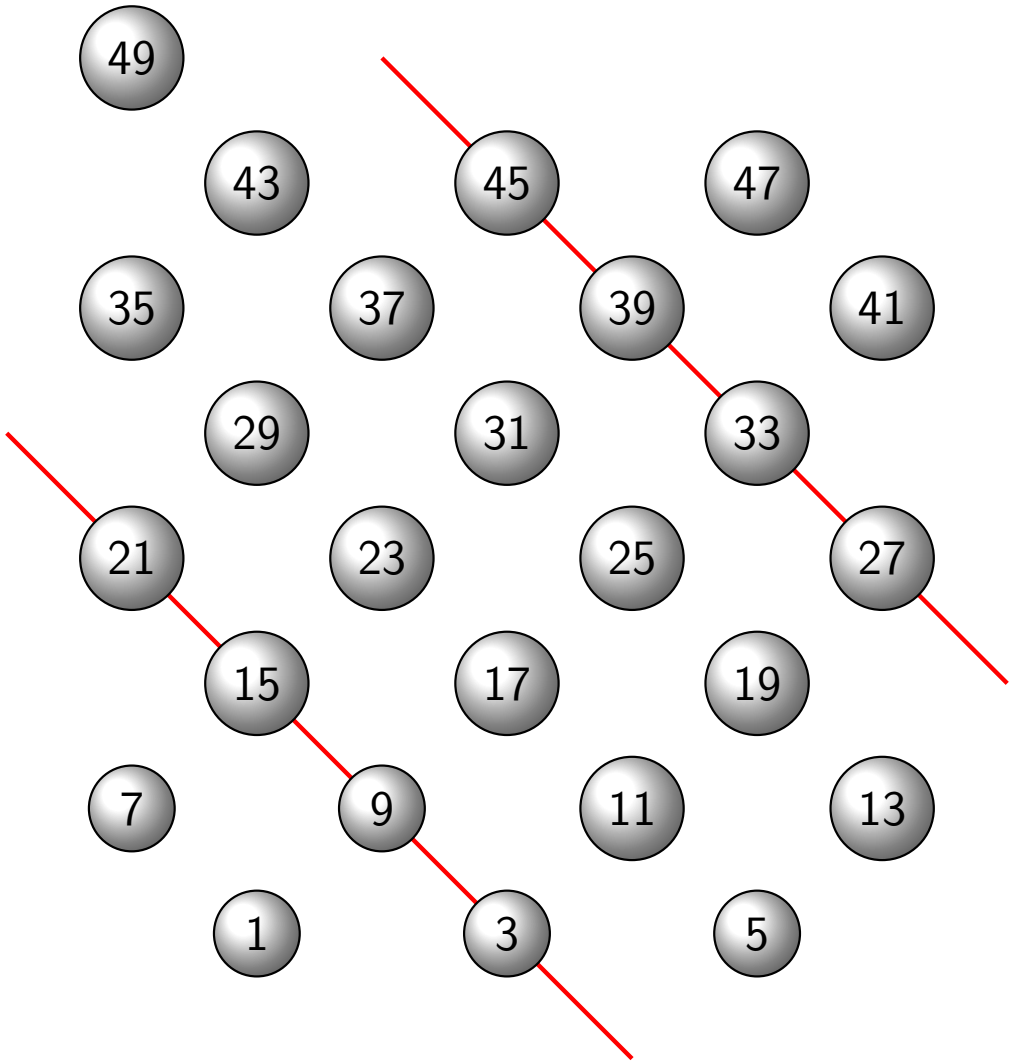
```
2   3   0   1   2   1   2   1   0   1   2   1   0   3   2   1   2   1   0   3
2   1   2   1   0   1   0   1   2   1   0   3   0   1   4   1   0   3   0   1
2   1   2   1   0   1   4   1   2   1   0   1   2   1   0   3   0   1   2   1
2   3   2   1   4   1   0   1   0   1   2   1   0   3   0   1   2   1   0   1
2   1   2   3   0   1   2   1   2   1   2   3   0   1   2   1   0   3   0
```

Nombres total de facteurs premiers différents

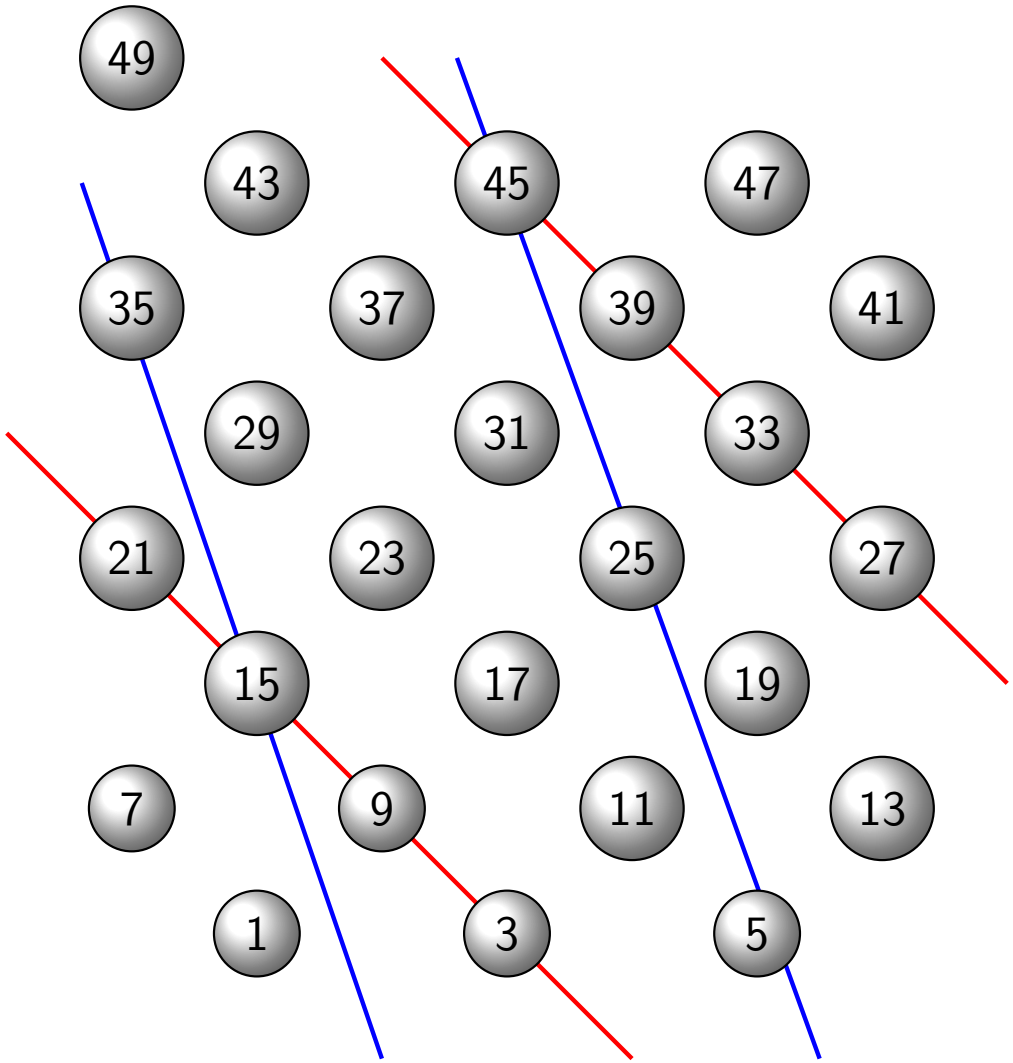
```
0   1   1   1   1   1   1   2   1   1   2   1   1   1   1   1   2   2   1   2
1   1   2   1   1   2   1   2   2   1   1   2   2   1   2   1   1   2   2   1
1   1   2   2   1   2   2   2   1   2   1   1   3   1   1   2   1   2   2   2
1   2   1   1   2   1   2   2   1   1   2   2   2   2   1   1   2   2   1   2
2   1   3   1   1   2   1   2   2   1   1   2   2   2   2   1   1   3   1   1
2   2   2   2   2   1   2   2   2   2   2   1   2   1   1   3   1   2   2   1
1   1   2   2   2   1   2   3   1   2   2   1   2   2   1   1   3   2   1   2
1   1   3   2   1   2   1   2   2   2   2   2   2   1   2   1   1   3   1   2
2   2   2   2   2   1   2   2   1   2   2   1   3   1   1   2   1   2   3   1
1   2   2   1   2   2   1   2   2   1   2   1   3   2   1   2   2   2   1   3
1   2   2   2   1   2   2   2   2   1   1   2   2   2   3   1   1   3   2   1
2   1   2   2   1   2   2   3   1   2   1   1   3   1   2   2   2   2   2   1
2   3   2   1   2   1   2   3   2   1   2   1   2   2   1   2   2   2   2   2
1   1   3   2   1   2   2   2   2   2   1   2   2   1   2   2   2   3   1   2
3   1   2   2   1   1   2   2   1   2   2   2   3   1   2   2   1   3   2   1
1   2   2   1   3   2   1   3   1   1   2   2   1   3   2   1   2   2   2   2
1   1   3   1   2   3   1   2   2   1   1   3   3   2   2   2   1   2   1   2
2   1   2   2   2   1   3   2   2   2   1   2   3   2   1   2   2   3   2   1
2   2   2   1   1   2   1   3   2   1   3   1   2   2   2   1   2   2   1   3
1   2   3   2   1   2   1   2   3   2   2   2   2   1   2   2   2   3   1   2
2   2   3   2   1   1   2   2   2   3   1   1   3   1   1   2   2   2   2   1
1   2   2   2   2   2   1   3   1   1   3   1   2   2   2   2   2   2   1   2
1   1   3   1   2   2   2   2   3   2   2   3   2   1   2   1   2   3   2   1
2   2   2   2   1   2   2   3   1   2   1   2   3   1   2   2   1   2   3   2
1   2   2   1   3   1   2   3   1   2   2   1   2   3   1   2   1   2   2   2
3   2   3   2   1   2   1   3   2   1   1   3   2   2   2   1   1   3   2   1
2   2   3   2   1   1   2   2   2   2   1   1   3   2   1   3   2   2   2   2
2   2   3   1   2   1   1   3   1   2   2   1   3   2   1   2   3   2   1   2
2   1   2   2   1   3   2   2   2   2   2   2   2   2   2   1   1   4   2
```



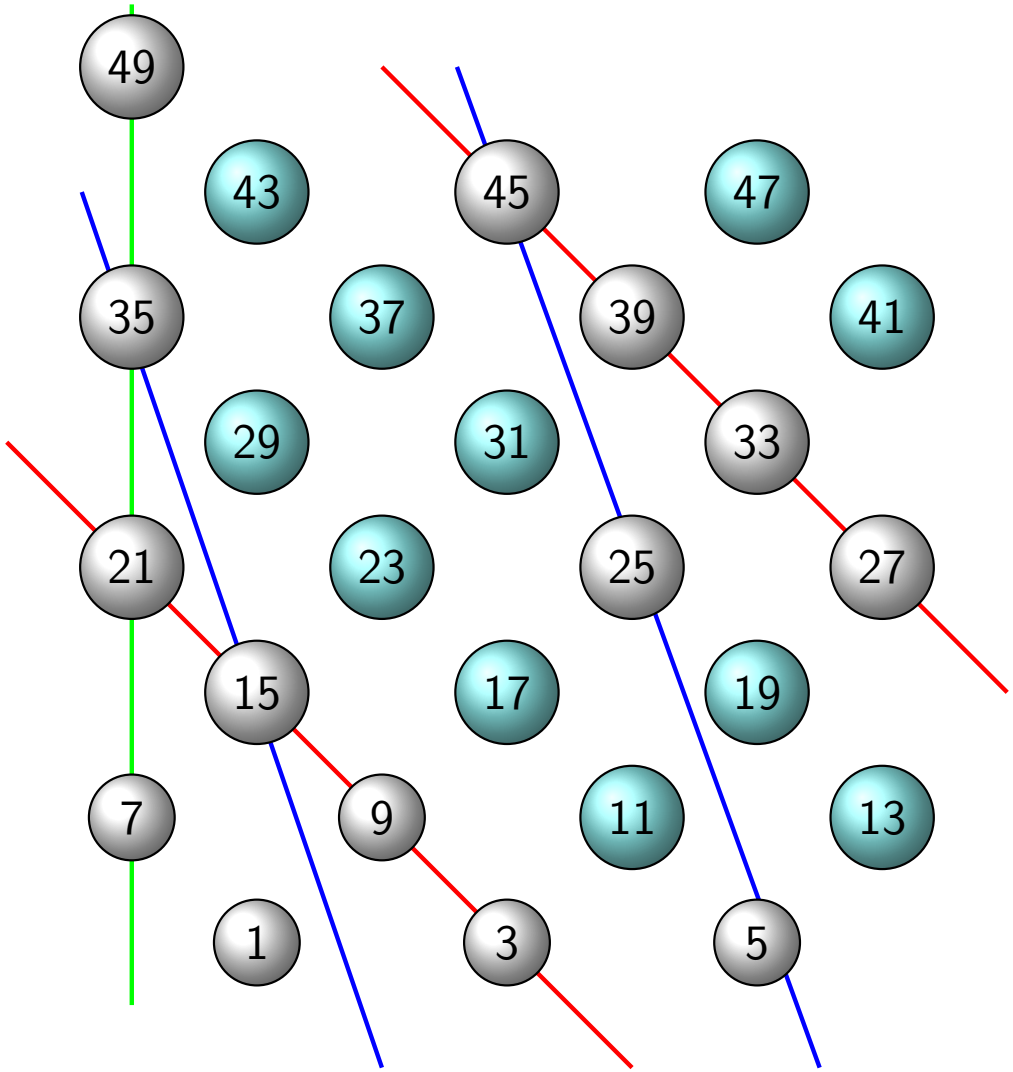
- on cherche les décomposants de Goldbach de 98 ;
- on écrit les nombres impairs de 1 à 49.



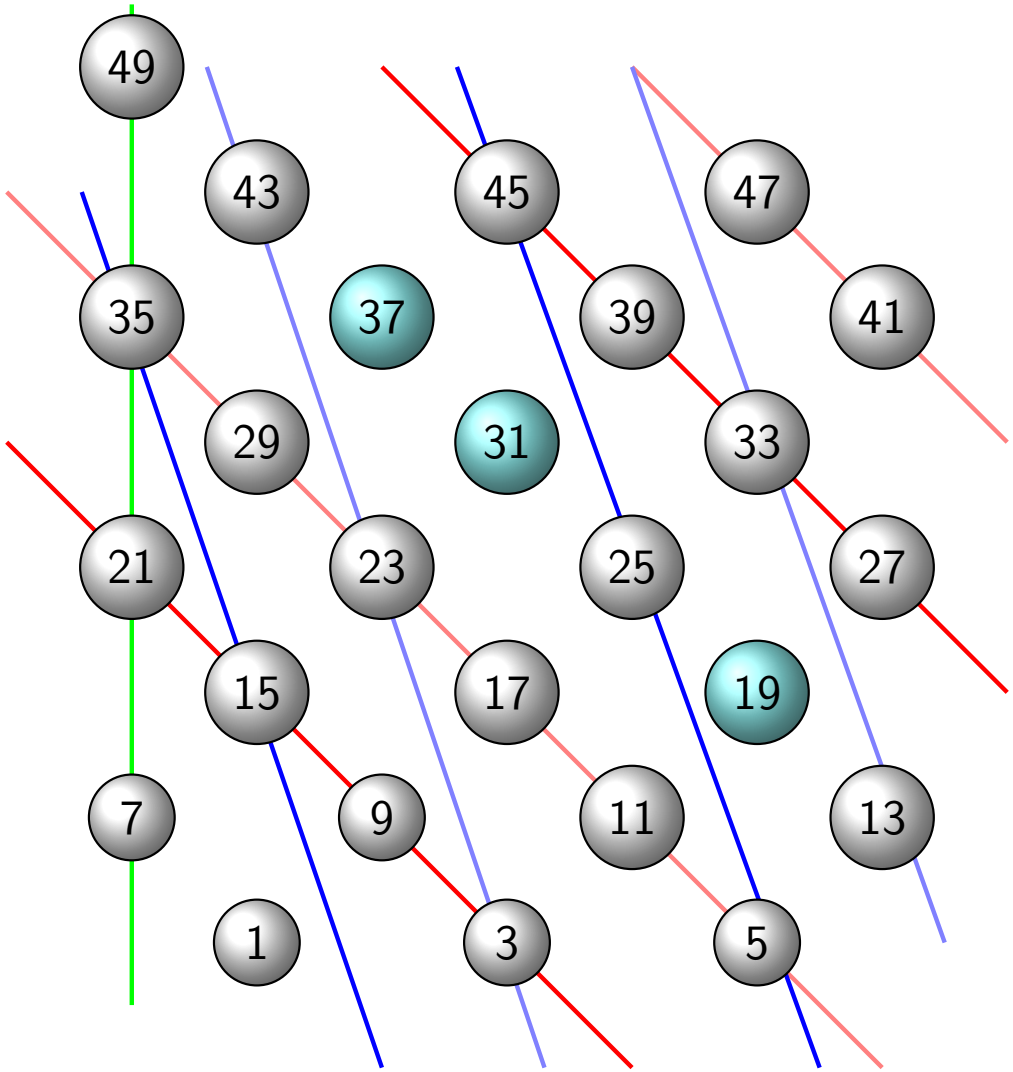
- on crible les multiples de 3 ;



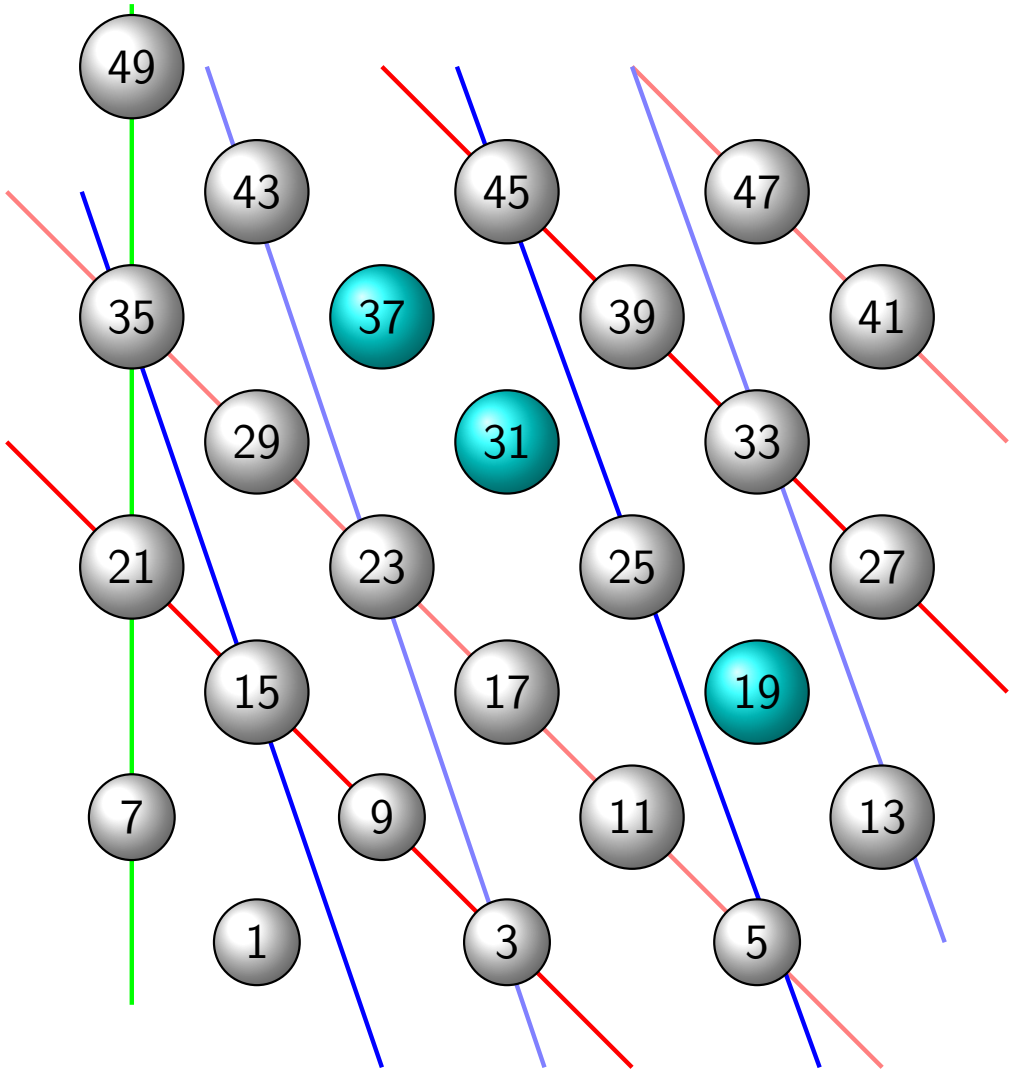
- on crible les multiples de 5 ;



- on crible les multiples de 7 ;
- ne restent (n'appartiennent à aucune droite colorée) que des nombres premiers $> \sqrt{98}$ (et le nombre 1) puisqu'on a criblé tous les multiples de nombres premiers inférieurs à $\sqrt{98}$.

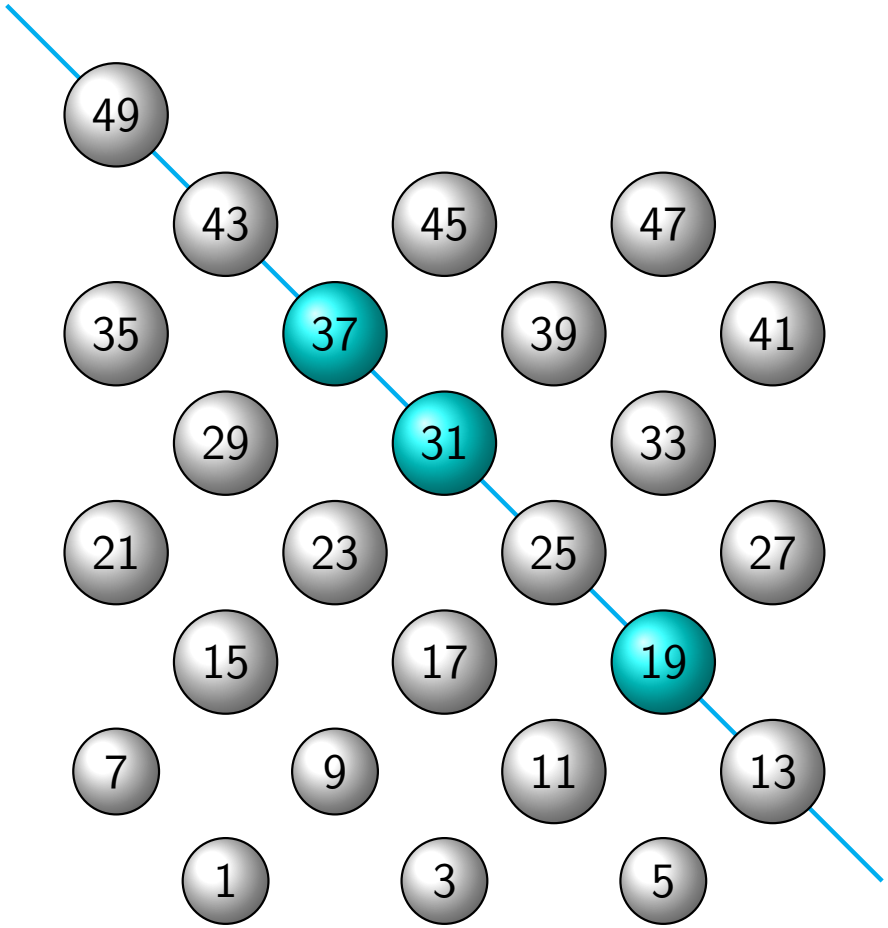


- on crible aussi les $3x + 2$ et les $5x + 3$ car $n = 98$ en est un, pour obtenir un nombre premier dont le complémentaire à n est premier.

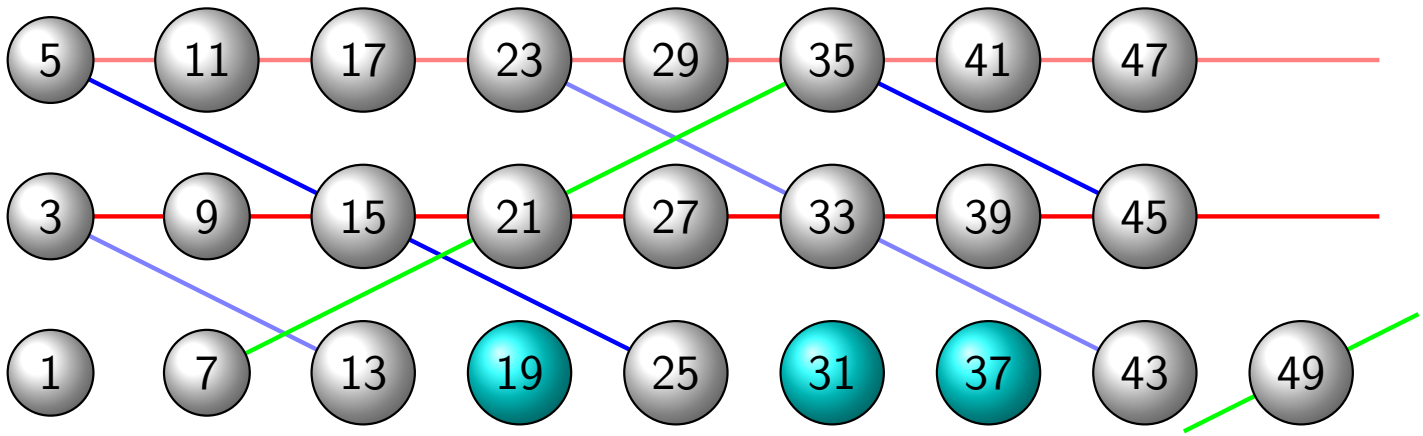


- seuls restent, qui sont passés au travers des mailles du crible, les décomp. de Goldbach de 98 ;

- on crible selon $\pi(\sqrt{n})$ directions ; le nombre de droites parallèles dans une direction donnée est fonction du choix de la base qui affecte les positions des nombres dans le plan cartésien.



- les décomposants de Goldbach de 98 sont tous de la forme $6k+1$ car 98 est un $6k+2$;
- les nombres pairs de la forme $6k$ ont environ deux fois plus de décomposants de Goldbach que les $6k+2$ ou les $6k+4$ car les $6k+2$ n'ont que des décomposants de forme $6k+1$ tandis que les $6k+4$ n'ont que des décomposants de la forme $6k+5$.



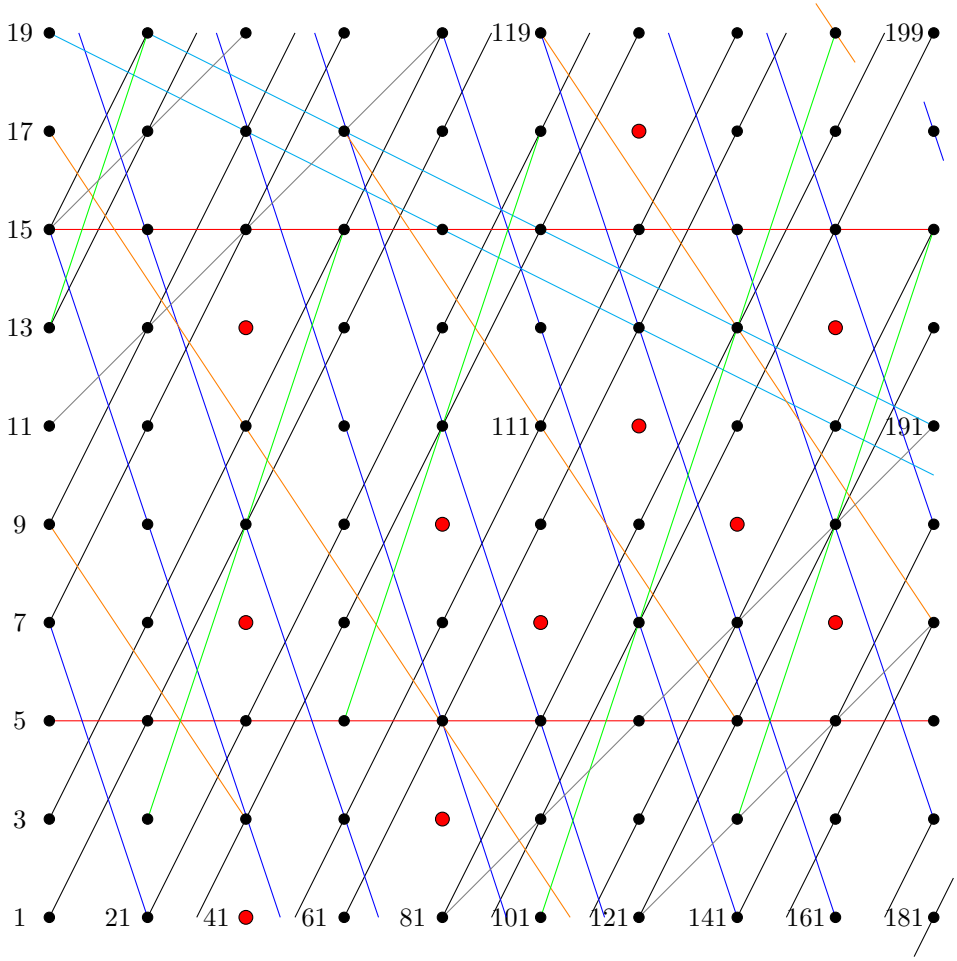
- cylindre (infini) plus simple à lire car il contient moins de lignes ;
- principe identique : à la recherche des décomposants de Goldbach de n, selon chaque direction correspondant à un nombre premier p_k inférieur à $\sqrt{n}$, on crible selon 2 restes ($mod\ p_k$) ou bien selon un seul reste si p_k divise n. Les décomposants de Goldbach sont alignés sur l'une et / ou l'autre des deux droites des $6k+1$ et des $6k-1$ selon que le reste de x par 6 est 0, 2 ou 4 ;
- ce que je trouve très chouette : les droites $5x+k$ et les droites $7x+k'$ se trouvent avoir des orientations "symétriques" dans ce cylindre, ainsi par exemple que les droites $11x+k$ et les droites $13x+k'$ ou plus généralement les droites $(6k-1)x+k'$ et $(6k+1)x+k''$;
- pour faciliter la lecture du graphique, on a placé le nombre x à la position $(\lfloor x/6 \rfloor, x\ mod\ 6)$ (la position de x sur le cylindre dépend de son quotient et de son reste par 6).

Cristal pour trouver les décomposants de Goldbach de 400 (Denise Vella-Chemla, 7.2.2020)

On trace les droites affines des nombres à cribler pour trouver les décomposants de Goldbach de 400 sur un carré de côté $20 = \sqrt{400}$.

On crible les $3a$, les $5b$, les $7c$, les $11d$, les $13e$, les $17f$ et les $19g$. Les nombres qui passent au travers des mailles du filet sont les nombres premiers supérieurs à 20.

400 appartenant à toutes les suites arithmétiques ci-après, pour que le complémentaire du nombre premier trouvé par le crible ci-dessus soit lui-aussi un nombre premier, on crible également les $3a+1$, les $5b$ (déjà criblés), les $7c+1$, les $11d+4$, les $13e+10$, les $17f+9$ et les $19g+1$.

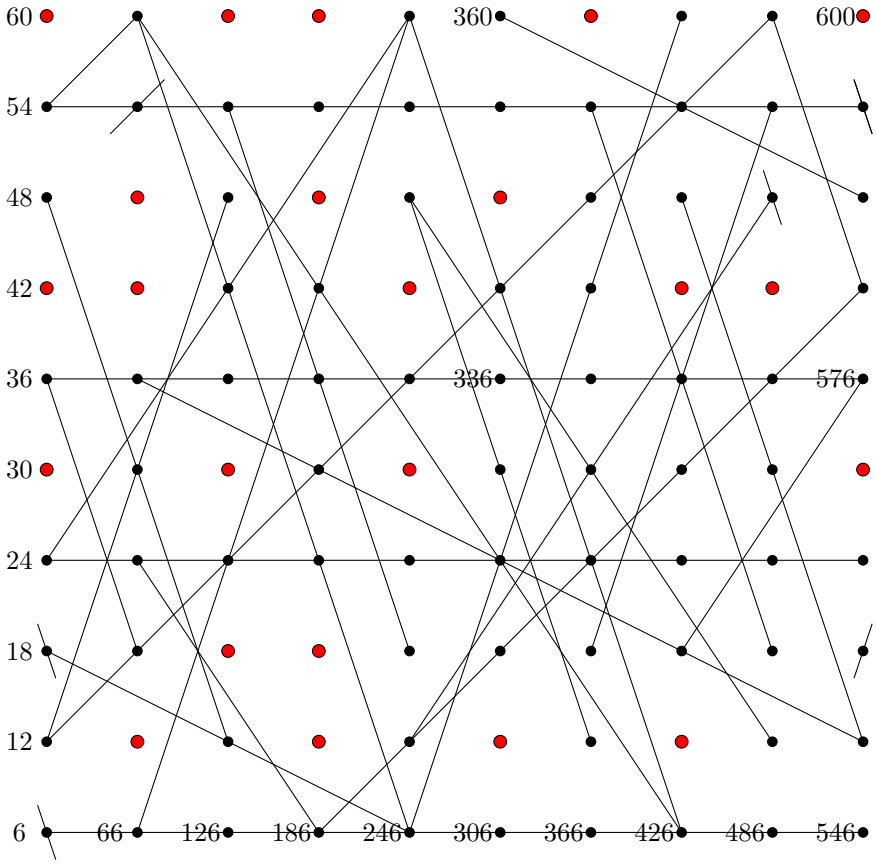


Les décomposants de Goldbach de 400 (supérieurs à $20 = \sqrt{400}$) sont marqués en rouge (on fournit entre parenthèses leurs coordonnées) : 41 (3,1), 47 (3,4), 53 (3,7), 83 (5,2), 89 (5,5), 107 (6,4), 131 (7,6), 137 (7,9), 149 (8,5), 167 (9,4) et 173 (9,7).

```
vella-chemla@vellachemla-X510UA:~/Desktop/2019/gb-tools-0.7.0$ ./gb-decomp -d 40
0
***** End sieve in 0..400 there are 78 primes (biggest is 397)
              3 +       397 = 400
             11 +       389 = 400
             17 +       383 = 400
             41 +       359 = 400
             47 +       353 = 400
             53 +       347 = 400
             83 +       317 = 400
             89 +       311 = 400
            107 +       293 = 400
            131 +       269 = 400
            137 +       263 = 400
            149 +       251 = 400
            167 +       233 = 400
            173 +       227 = 400
     400 has       14 decomp
```

Cristal pour trouver les couples de nombres premiers de différence 2 jusqu'à 600 (Denise Vella-Chemla, 13.2.2020)

Un nombre x divisible par 6 (ici x inférieur à $n = 600$) a son prédécesseur et son successeur qui sont des nombres premiers s'il vérifie $x^2 \not\equiv 1$ $(mod\ p_k)$ pour tout p_k un nombre premier inférieur à $\sqrt{n}$[1].



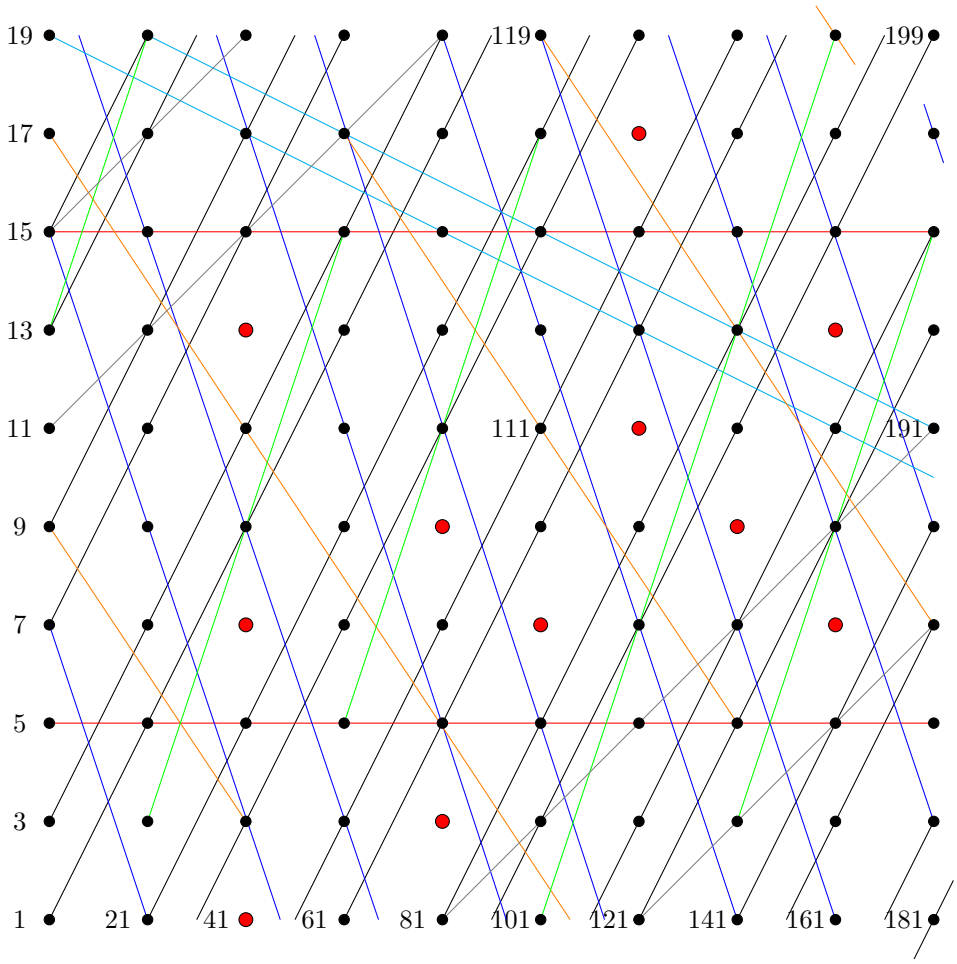
On a noté les nombres divisibles par 6 inférieurs à 600 sur une sorte de tore. On barre les nombres alignés qui sont de la forme $5m-1$, $5m+1$, $7m-1$, $7m+1$, etc. jusqu'à $23m-1$, $23m+1$, i.e. de la forme $p_k \times m \pm 1$ pour p_k un nombre premier impair inférieur à 23 (le plus grand nombre premier inférieur à $\sqrt{600}$).

Les nombres pairs entre deux nombres premiers jumeaux, qui n'appartiennent à aucune suite arithmétique de la forme $p_k \times m \pm 1$, sont les nombres 30, 42, 60, 72, 102, 108, 138, 150, 180, 192, 198, 228, 240, 270, 282, 312, 348, 420, 432, 462, 522, 570 et 600.

[1] cf. http://denisevellachemla.eu/invariante.pdf.

Comprendre comment on pourrait peut-être compter les décomposants de Goldbach sur le cristal de 400 (Denise Vella-Chemla, 4.3.2020)

On rappelle le schéma qui fournit les décomposants de Goldbach de 400.



On cherche à compter les décomposants de Goldbach de 400 supérieurs à $\sqrt{400}$.

Il y a 100 nombres candidats ($100 = 400/4$ soit $n/4$).

Parmi eux, 33 sont divisibles par 3 et 34 sont congrus à 1 modulo 3, ce qui fait 67 nombres à éliminer initialement. On a aussi 20 nombres divisibles par 5 et pas de nombres de la forme $5a + b$ à éliminer modulo 5 (puisque 5 divise 400). On doit également éliminer 14+15 nombres modulo 7, 9+9 nombres modulo 11, 8+7 nombres modulo 13, 6+6 nombres modulo 17 et 5+6 nombres modulo 19.

Note : ces nombres de nombres à éliminer sont calculables, il s'agit de diviser n par tout $2p$ avec p premier inférieur à $\sqrt{n}$ pour obtenir chaque sous-total, sauf pour les diviseurs de n pour lesquels il faut diviser n par $4p$ (en l'occurrence, modulo 5).

Ce qui fait un total de 172 nombres à éliminer, qui dépasse amplement le nombre 100 de nombres disponibles.

400 a pourtant des décomposants de Goldbach : on a oublié de rajouter (en fait de soustraire au nombre de nombres à éliminer) les nombres qui sont intersections de plusieurs droites, combinatoirement (par exemple qui sont à la fois des $3a + 1$ et des $5a'$, etc.).

Comptons simplement ces nombres sur le schéma : on en trouve 52 qui sont intersections de 2 droites ou plus, 23 qui sont intersections de 3 droites ou plus, 5 qui sont intersections de 4 droites ou plus, ce qui fait un total de 80 nombres intersections de deux droites au moins sur le schéma.

On soustrait ce nombre 80 (qui correspond aux double-comptages effectués à tort) du nombre 172 (car ce nombre correspondait au fait d'éliminer un nombre dès qu'il est composé, en le comptant autant de fois qu'il a de diviseurs premiers différents ou bien qu'il est congru à n selon un nombre premier inférieur à $\sqrt{n}$, on appelle ça des multiplicités), on obtient 92 et c'est ce nombre 92 qu'on doit soustraire à 100, le nombre de nombres potentiellement décomposants de Goldbach (nombre de nombres du schéma).

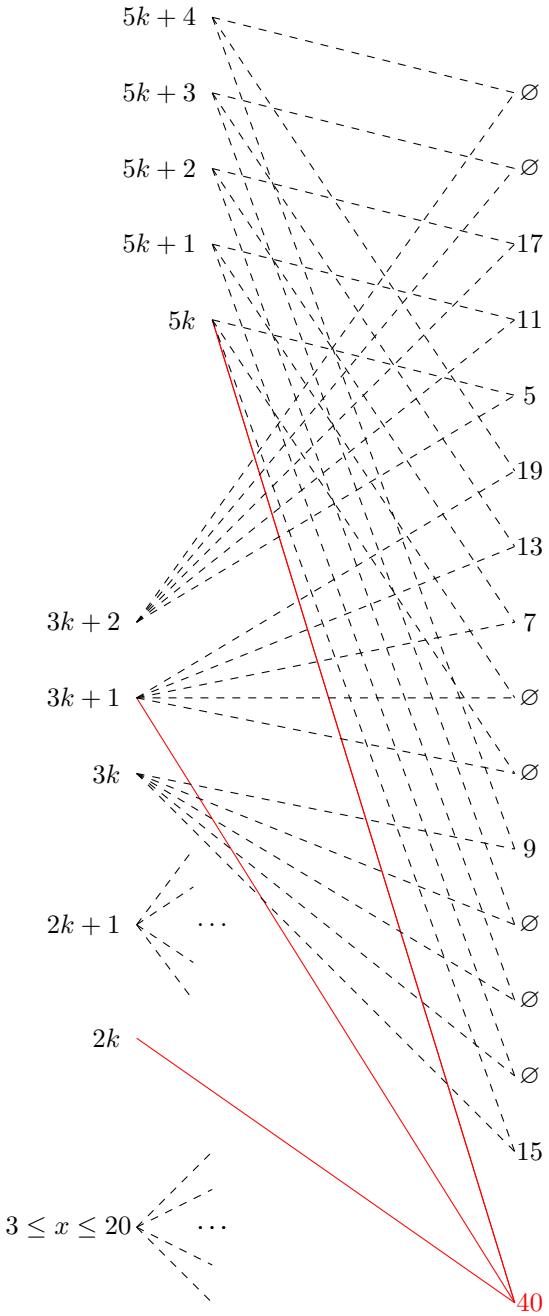
100-92=8, alors que 400 a effectivement 11 décomposants de Goldbach supérieurs à sa racine.

Problème : on ne sait de toute façon absolument pas compter les multiplicités mais si l'on veut établir un lien avec des propriétés géométriques, il faudrait être capable de compter les nombres appartenant à au moins deux droites (i.e. ayant au moins deux propriétés, soit de divisibilité par un premier, soit de congruence à n selon un nombre premier inférieur à $\sqrt{n}$), ceux appartenant à au moins 3 droites, etc. On ne sait pas faire cela. Une minuscule indication est que les droites correspondant aux nombres de la forme $3a$ ou $3a + b$ (ou plus généralement aux nombres de la forme $pa + b$ avec b potentiellement nul et p premier inférieur à $\sqrt{n}$) n'ont jamais d'intersections entre elles.

Puisqu'il s'agit dans tous les cas de n'éliminer que 2 classes de congruences au plus selon chaque module premier inférieur à la racine carrée de n, on préfère conserver la façon de considérer le problème consistant à utiliser le produit :

$$\prod_{p\ premier,\ p\leqslant\sqrt{n}} \left(1 - \frac{2}{p}\right)$$

Treillis distributif pour décomposants de Goldbach de 40 (Denise Vella-Chemla, 13.6.2020)



Note : Pour ne pas surcharger le dessin, on n'a pas noté les liens de relation d'intersections entre les $\{2k+1\}$ et tous les nœuds à droite (on se concentre à la recherche de décomposants de Goldbach d'un nombre pair sur les nombres impairs). C'est la borne (la restriction à l'intervalle $[3, n/2]$, symbolisée sur le schéma par le nœud $3 \leq x \leq 20$) qui pose peut-être problème pour prouver l'existence. On trouvera ici, là, là, ou encore là des éléments de référence concernant les treillis distributifs, les espaces de Stone, les espaces booléens. Un décomposant de Goldbach de n appartient au complémentaire ou ensemble orthogonal du singleton $\{n\}$. On peut se reporter également aux articles de wikipedia suivants : Filtre topologique, Espace de Stone, Treillis, Algèbre de Boole.

Pour bien décrire l'espace dans lequel on se place, on recopie texto un extrait de l'article de wikipedia Théorème de représentation de Stone pour les algèbres de Boole :
https://fr.wikipedia.org/wiki/Th%C3%A9or%C3%A8me_de_repr%C3%A9sentation_de_Stone_pour_les_alg%C3%A8bres_de_Boole :
Exemple : L'algèbre des parties finies ou cofinies
Soit E un ensemble infini. Posons $FC(E)$ l'ensemble des parties finies ou cofinies de E. $FC(E)$ forme

une algèbre de Boole avec les opérations ensemblistes usuelles (union, intersection, complémentaire). Les ultrafiltres de $FC(E)$ sont :

- *Les ultrafiltres principaux U_x , dont les éléments sont les parties finies ou cofinies de E contenant un élément x donné de E,*
- *L'ultrafiltre U_∞, dont les éléments sont les parties cofinies de E.*

Par conséquent, l'espace de Stone $S(FC(E))$, ensemble des ultrafiltres précédents, peut être assimilé à l'ensemble E auquel on a ajouté un élément ∞. Topologiquement, il s'agit du compactifié d'Alexandrov de E, lorsque ce dernier est muni de la topologie discrète. Les parties ouvertes-fermées de $S(FC(E))$ sont d'une part les parties finies incluses dans E, d'autre part les parties cofinies contenant ∞. L'ensemble de ces parties ouvertes-fermées, avec les opérations ensemblistes usuelles, redonnent une algèbre de Boole isomorphe à $FC(E)$ [1].

Transposons au problème qui nous intéresse :
Soit $\mathbb{N}$ l'ensemble infini des entiers naturels. Posons $FC(\mathbb{N})$ l'ensemble des parties finies ou cofinies de $\mathbb{N}$. $FC(\mathbb{N})$ forme une algèbre de Boole avec les opérations ensemblistes usuelles (union, intersection, complémentaire). Les ultrafiltres de $FC(\mathbb{N})$ sont :

- Les ultrafiltres principaux U_x, dont les éléments sont les parties finies ou cofinies [2] de $\mathbb{N}$ contenant un élément x donné de $\mathbb{N}$,
- L'ultrafiltre U_∞, dont les éléments sont les parties cofinies de $\mathbb{N}$.

Par conséquent, l'espace de Stone $S(FC(\mathbb{N}))$, ensemble des ultrafiltres précédents, peut être assimilé à l'ensemble $\mathbb{N}$ auquel on a ajouté un élément ∞. Topologiquement, il s'agit du compactifié d'Alexandrov de $\mathbb{N}$, lorsque ce dernier est muni de la topologie discrète. Les parties ouvertes-fermées de $S(FC(\mathbb{N}))$ sont d'une part les parties finies incluses dans $\mathbb{N}$, d'autre part les parties cofinies contenant ∞. L'ensemble de ces parties ouvertes-fermées, avec les opérations ensemblistes usuelles, redonnent une algèbre de Boole isomorphe à $FC(\mathbb{N})$ [3].

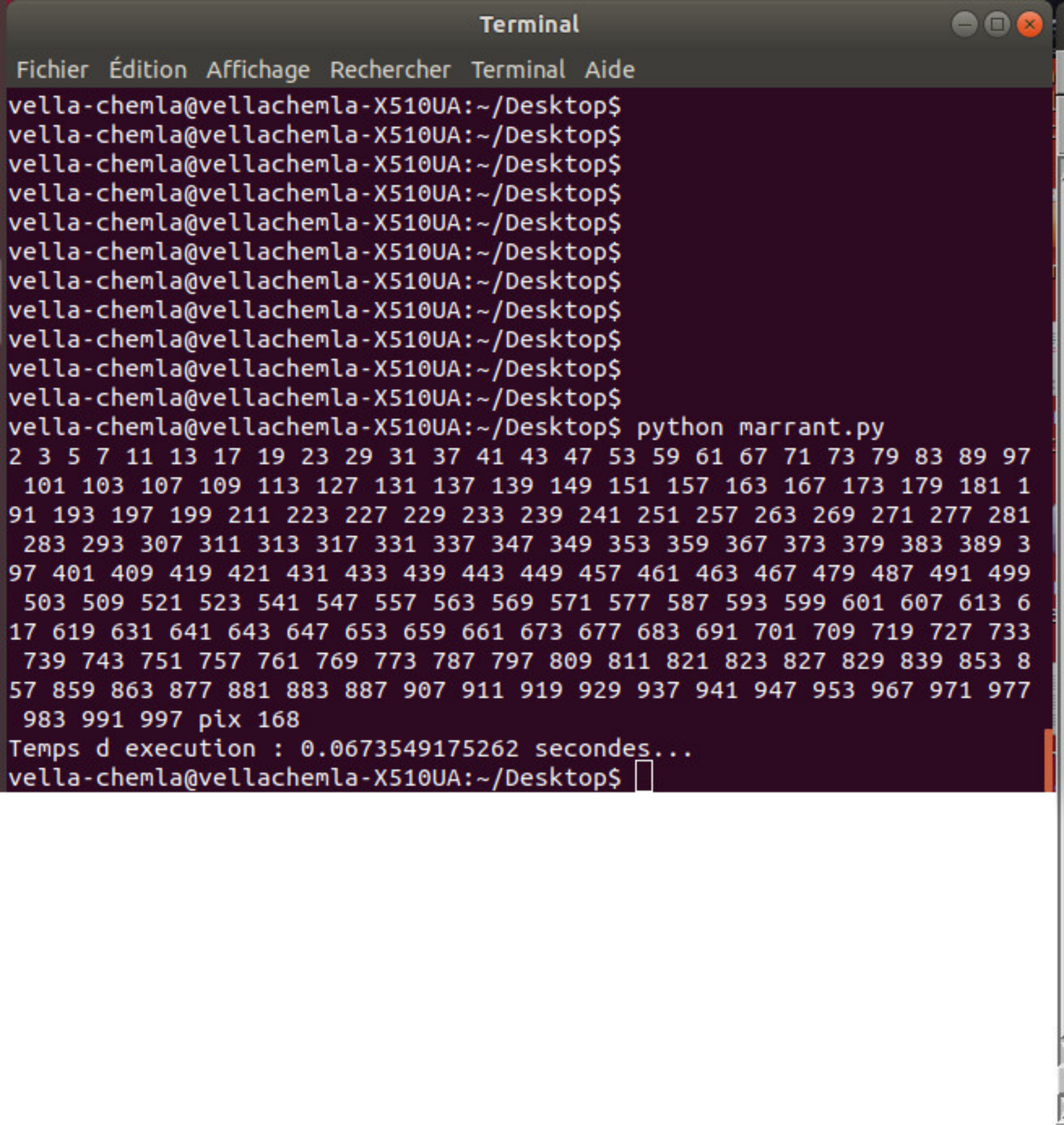
1. Il suffit d'"oublier" l'élément ∞ pour retrouver $FC(\mathbb{E})$.
2. cofini = dont le complémentaire est fini. Par exemple, $[20, \infty]$ est une partie cofinie de $\mathbb{N}$. C'est cette notion qui nous permet de calculer les intersections avec les intervalles de la forme $[0, n/2]$ pour trouver les décomposants de Goldbach ; on ne sait pas si le fait d'avoir mieux "délimité" l'espace sur lequel il convient de se placer permet de prouver l'existence d'un décomposant de Goldbach pour tout entier pair supérieur ou égal à 4 ou pas.
3. Il suffit d'"oublier" l'élément ∞ pour retrouver $FC(\mathbb{N})$.

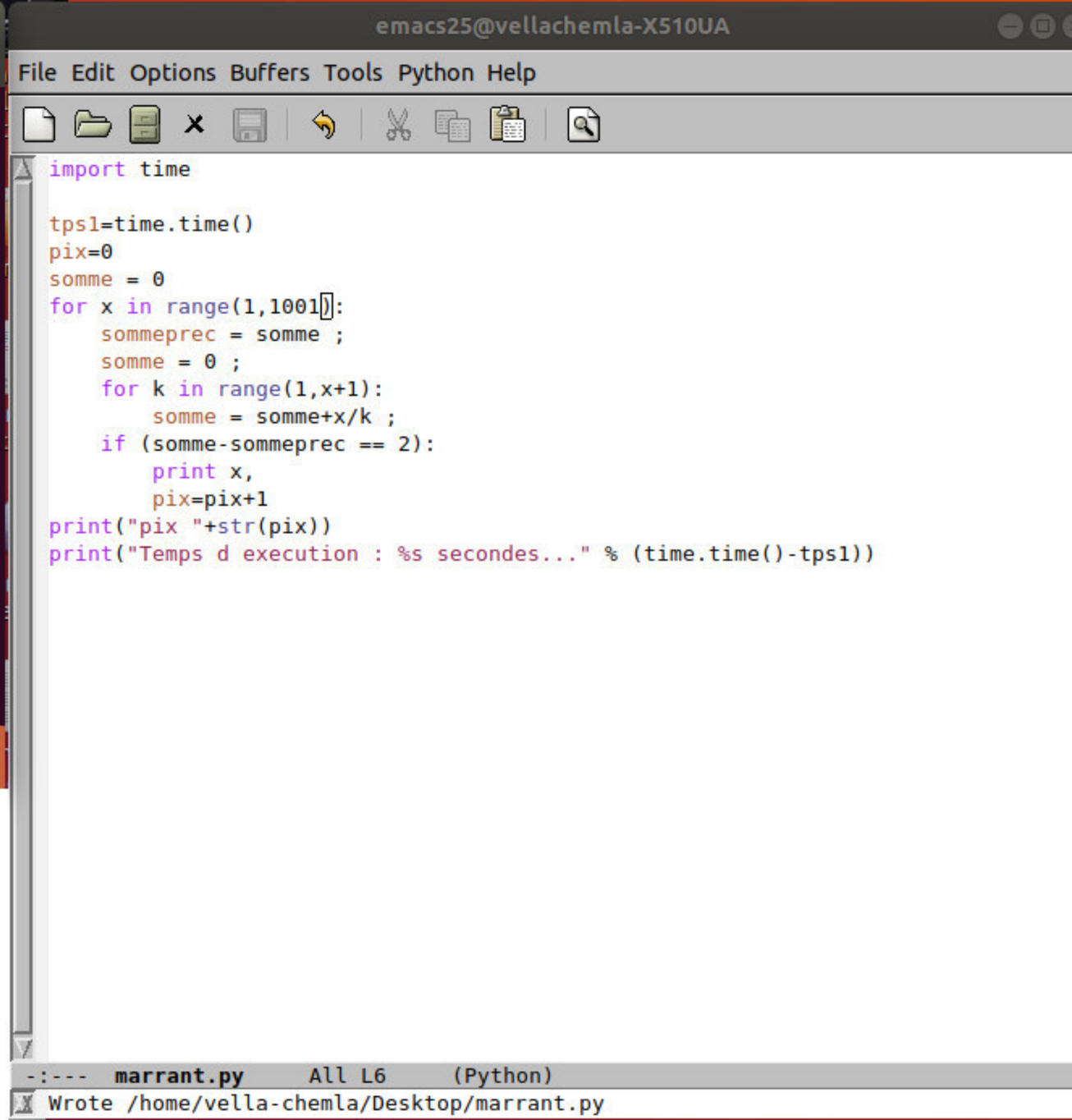
Orthogonalité

- On note $\mathcal{F}(x) = \{y \in \mathbb{N}^\times \mid 3 \leq y \leq x\}$
- On note $98^\perp$ l'ensemble des décomposants de Goldbach de 98.
- $98 \in (2\mathbb{N}) \cap (3\mathbb{N}+2) \cap (5\mathbb{N}+3) \cap (7\mathbb{N})$.
- $98^\perp \in \mathcal{F}(49) \cap [(2\mathbb{N}+1) \cap (3\mathbb{N}+1) \cap [(5\mathbb{N}+1) \cup (5\mathbb{N}+2) \cup (5\mathbb{N}+4)] \cap [(7\mathbb{N}+1) \cup \ldots \cup (7\mathbb{N}+6)]]$.

  Attention : Bien avoir à l'esprit que les règles de développement de la multiplication $\cap$ sur l'addition $\cup$ se font comme habituellement en algèbre, i.e. l'union $(7\mathbb{N}+1) \cup \ldots \cup (7\mathbb{N}+6)$ ne représente pas tous les entiers sauf les multiples de 7 par exemple. On développe par distributivité d'une opération sur l'autre.

- Plus généralement, si on note $\mathcal{P}$ l'ensemble des nombres premiers.
- $n \in \bigcap_{a \in \mathcal{F}(\sqrt{n}) \cap \mathcal{P}^\times, b \in \{0,\ldots,a-1\}} \{ax+b\}$ et
- $n^\perp \in \mathcal{F}(n/2) \cap \bigcap_{a \in \mathcal{F}(\sqrt{n}) \cap \mathcal{P}^\times, b' \in \{1,\ldots,a-1\}} \{ax+b', \text{ avec } b' \neq b, \forall a\}$.


Terminal
Fichier Édition Affichage Rechercher Terminal Aide
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$
vella-chemla@vellachemla-X510UA:~/Desktop$ python marrant.py
2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97
101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 1
91 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281
283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 3
97 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499
503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 6
17 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727 733
739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 8
57 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977
983 991 997 pix 168
Temps d execution : 0.0673549175262 secondes...
vella-chemla@vellachemla-X510UA:~/Desktop$


emacs25@vellachemla-X510UA
File Edit Options Buffers Tools Python Help
import time
tps1=time.time()
pix=0
somme = 0
for x in range(1,1001):
sommeprec = somme ;
somme = 0 ;
for k in range(1,x+1):
somme = somme+x/k ;
if (somme-sommeprec == 2):
print x,
pix=pix+1
print("pix "+str(pix))
print("Temps d execution : %s secondes..." % (time.time()-tps1))
-:--- marrant.py All L6 (Python)
Wrote /home/vella-chemla/Desktop/marrant.py

emacs25@vellachemla-X510UA

File Edit Options Buffers Tools C++ Help

```
#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

```
#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:~/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$
```

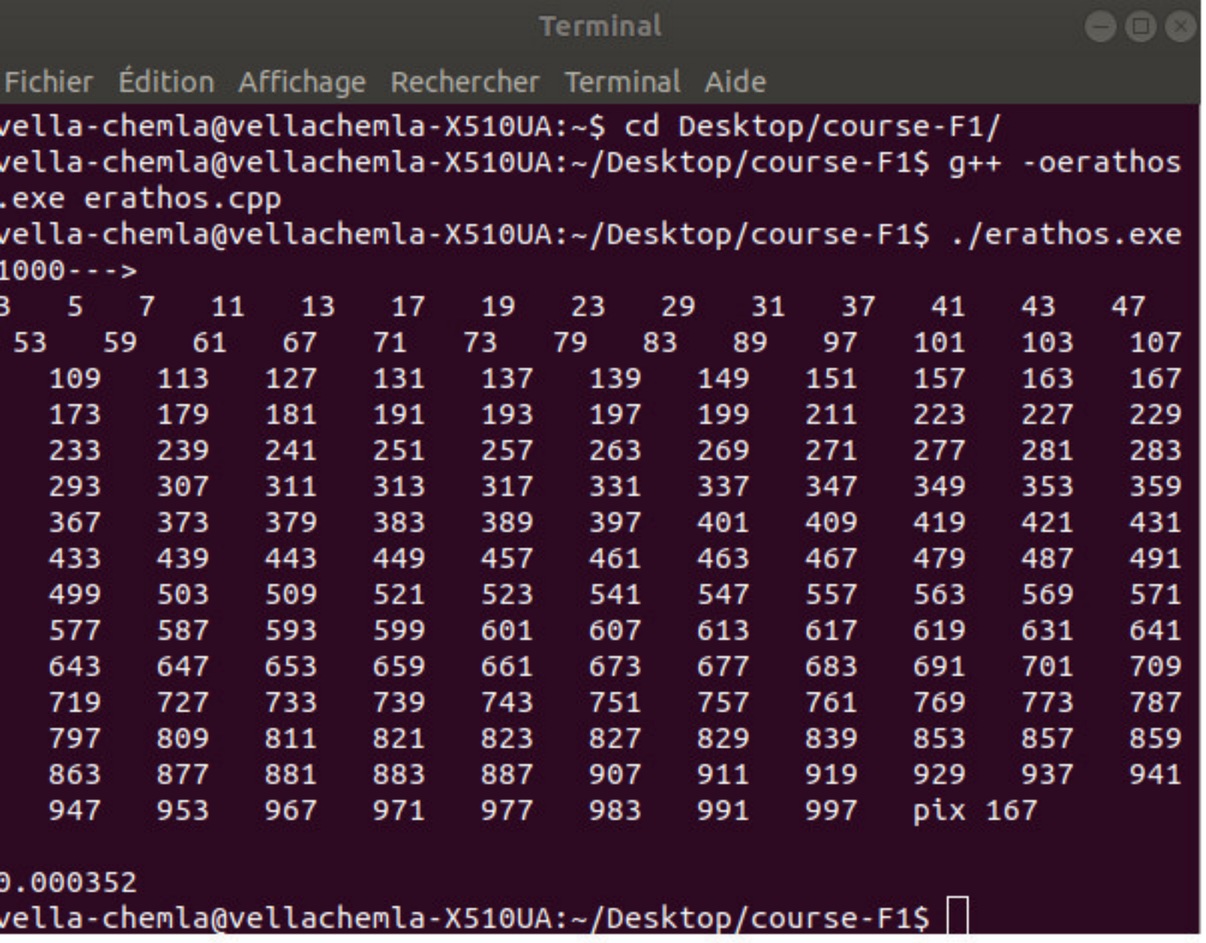
emacs25@vellachemla-X510UA

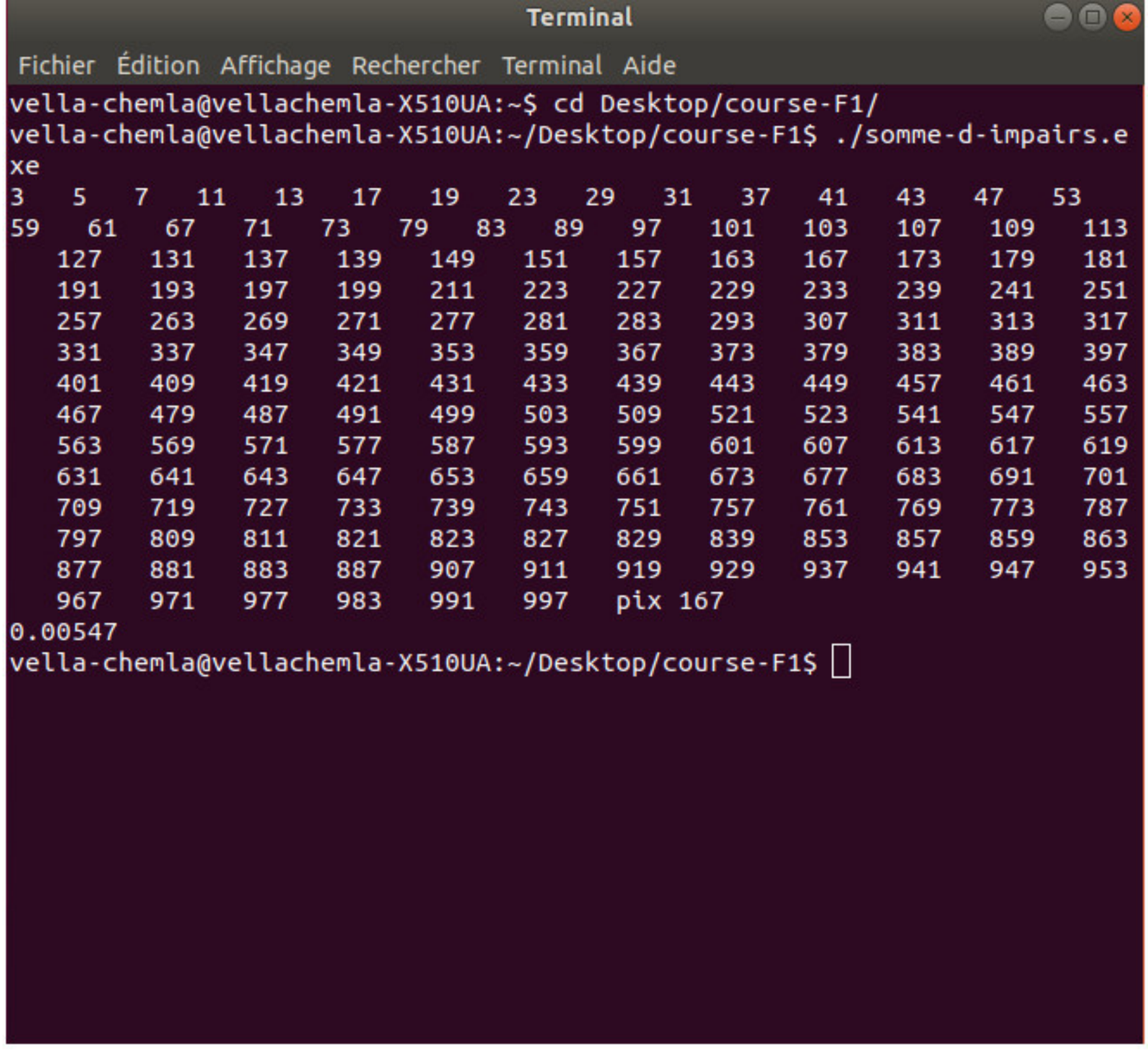
File Edit Options Buffers Tools Python Help

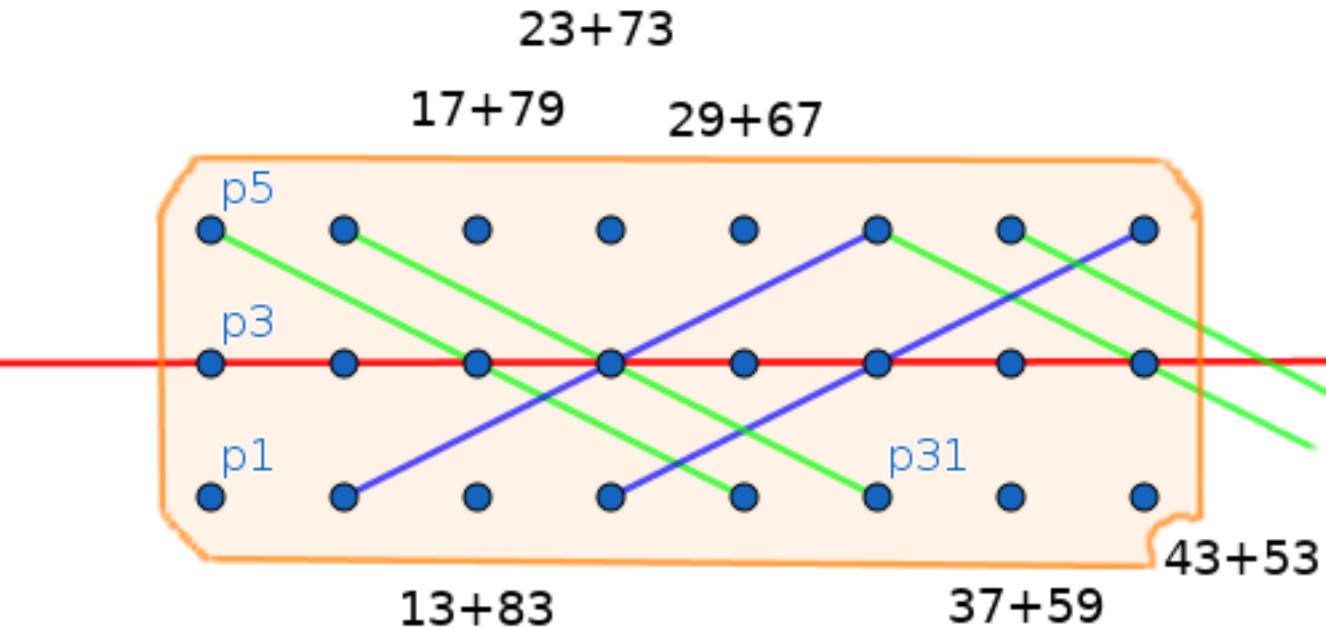
```
import numpy as np
from numpy import *
import time

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))
```

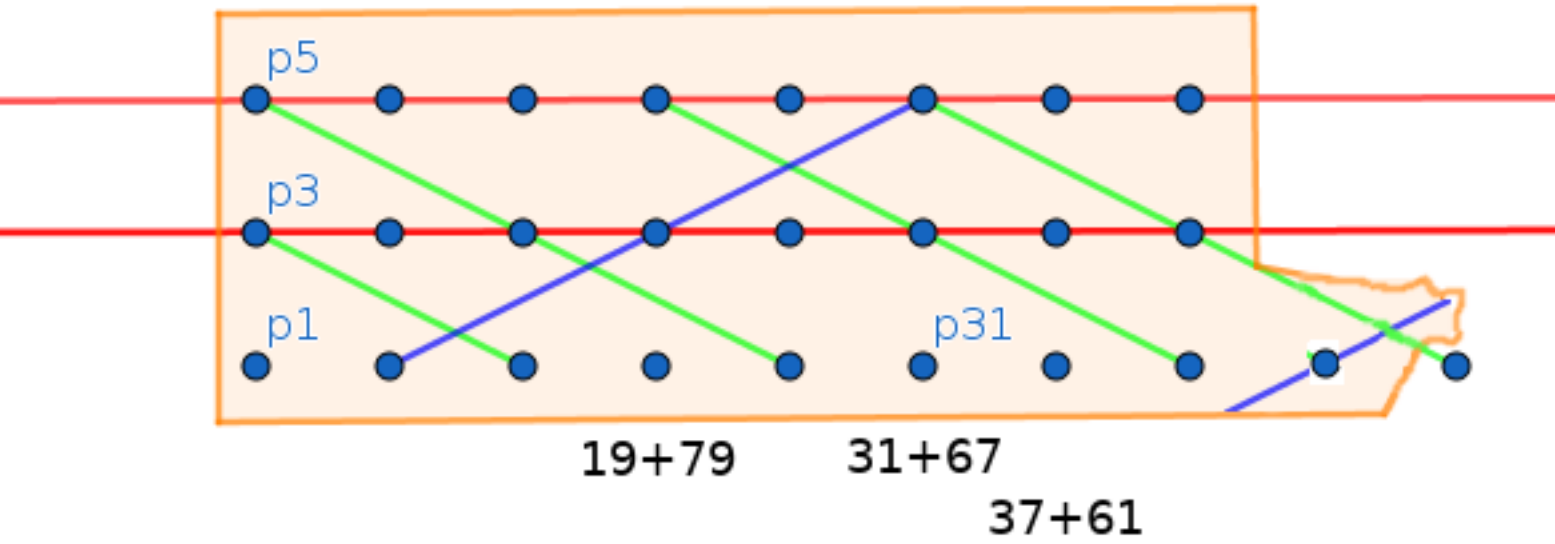
-:--- chazy.py All L1 (Python)

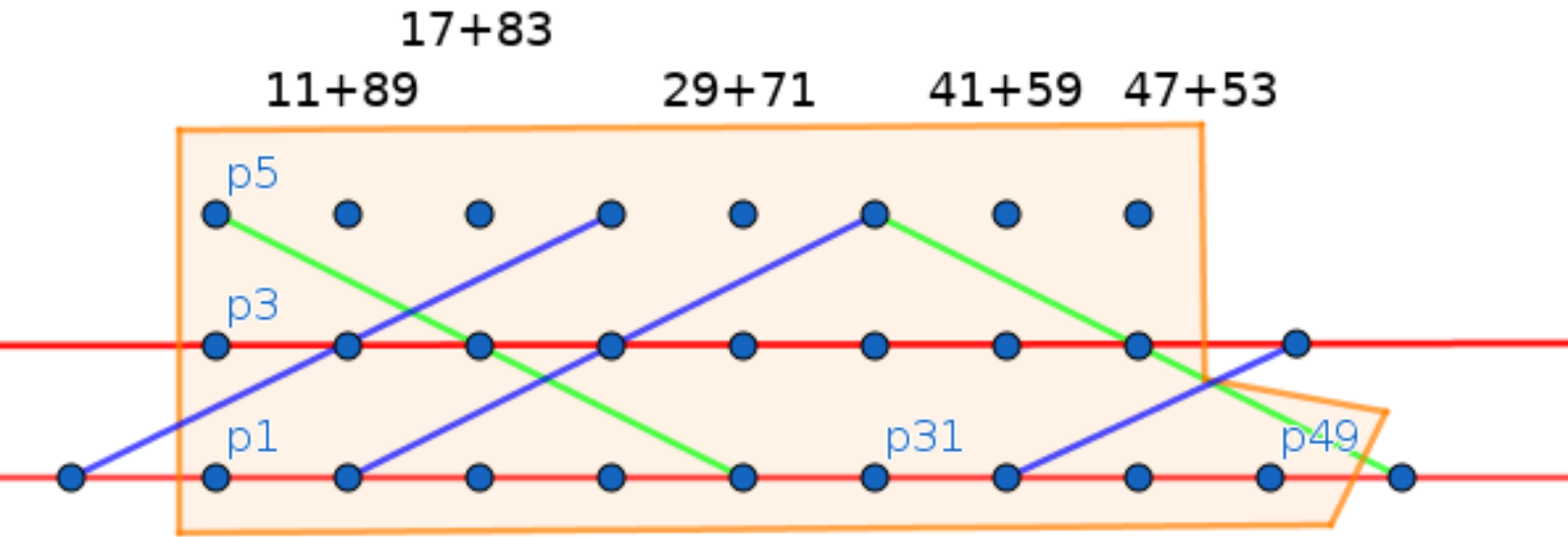
5 1


Terminal
Fichier Édition Affichage Rechercher Terminal Aide
vella-chemla@vellachemla-X510UA:~$ 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$


23+73
17+79
29+67
p5
p3
p1
p31
43+53
13+83
37+59


p5
p3
p1
p31
19+79
31+67
37+61


17+83
11+89
29+71
41+59
47+53
p5
p3
p1
p31
p49

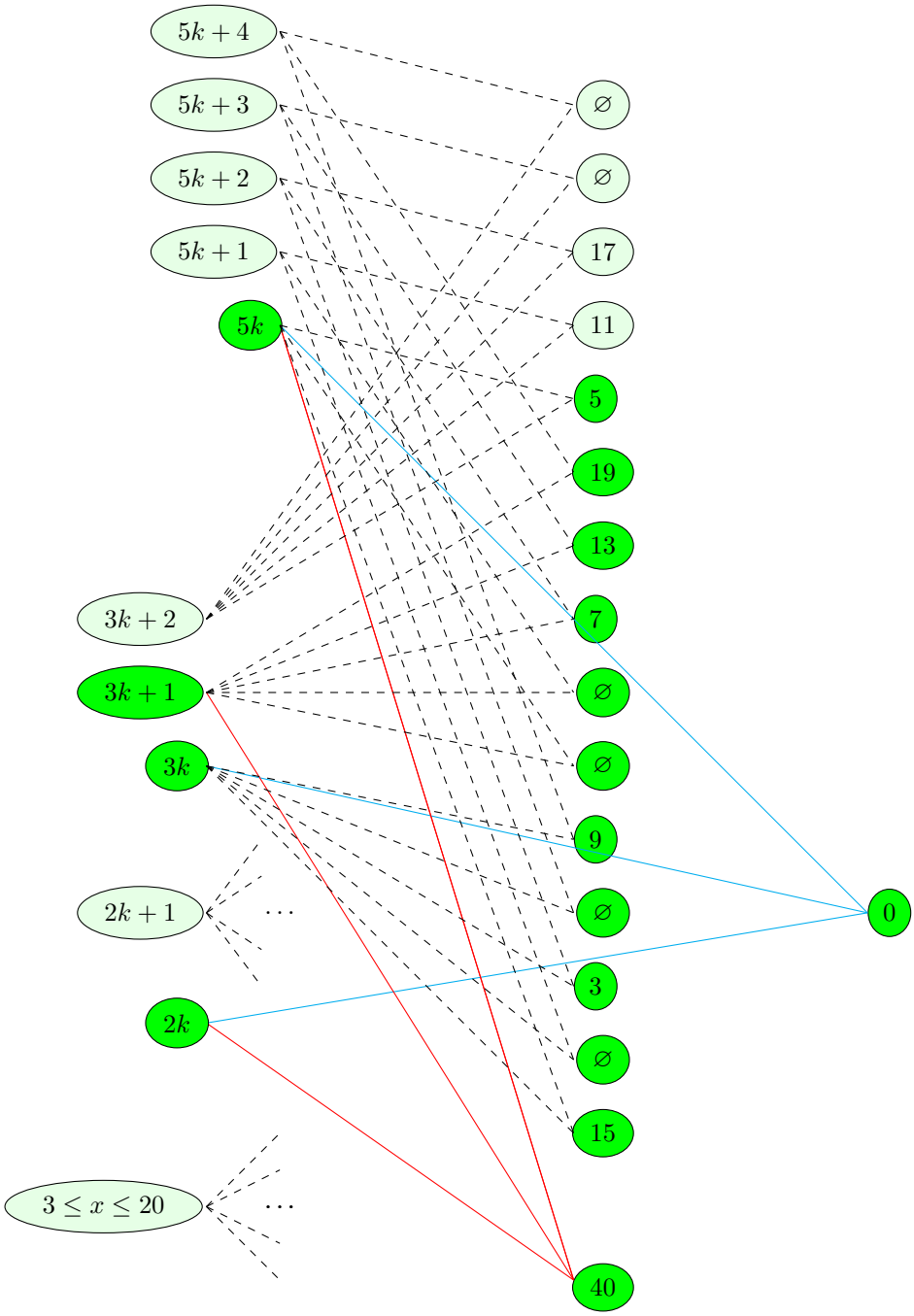
Orthogonalité

- On note $\mathcal{F}(x) = \{y \in \mathbb{N}^\times \mid 3 \leq y \leq x\}$
- On note $98^\perp$ l'ensemble des décomposants de Goldbach de 98.
- $98 \in (2\mathbb{N}) \cap (3\mathbb{N}+2) \cap (5\mathbb{N}+3) \cap (7\mathbb{N})$.
- $98^\perp \in \mathcal{F}(49) \cap [(2\mathbb{N}+1) \cap (3\mathbb{N}+1) \cap [(5\mathbb{N}+1) \cup (5\mathbb{N}+2) \cup (5\mathbb{N}+4)] \cap [(7\mathbb{N}+1) \cup \ldots \cup (7\mathbb{N}+6)]]$.

  Attention : Bien avoir à l'esprit que les règles de développement de la multiplication $\cap$ sur l'addition $\cup$ se font comme habituellement en algèbre, i.e. l'union $(7\mathbb{N}+1) \cup \ldots \cup (7\mathbb{N}+6)$ ne représente pas tous les entiers sauf les multiples de 7 par exemple. On développe par distributivité d'une opération sur l'autre.

- Plus généralement, si on note $\mathcal{P}$ l'ensemble des nombres premiers.
- $n \in \bigcap_{a \in \mathcal{F}(\sqrt{n}) \cap \mathcal{P}^\times, b \in \{0,\ldots,a-1\}} \{ax+b\}$ et
- $n^\perp \in \mathcal{F}(n/2) \cap \bigcap_{a \in \mathcal{F}(\sqrt{n}) \cap \mathcal{P}^\times, b' \in \{1,\ldots,a-1\}} \{ax+b', \text{ avec } b' \neq b, \forall a\}$.

Treillis distributif pour décomposants de Goldbach de 40 (Denise Vella-Chemla, 13.6.2020)



Sont notées en vert clair (resp. en vert vif) les solutions potentielles (resp. tout ce que le filtre élimine). On notera que le filtre élimine 3 alors que 3 est un décomposant de Goldbach de 40 car on fait le choix de ne conserver que les nombres premiers décomposants de Goldbach supérieurs à la racine carrée du nombre pair considéré.

Note : Pour ne pas surcharger le dessin, on n'a pas noté les liens de relation d'intersections entre les $\{2k+1\}$ et tous les nœuds à droite (on se concentre à la recherche de décomposants de Goldbach d'un nombre pair sur les nombres impairs, qui sont tous potentiellements solutions (i.e. notés en vert clair)). C'est la borne (la restriction à l'intervalle $[3, n/2]$, symbolisée sur le schéma par le nœud $3 \leq x \leq 20$) (vert clair) qui pose peut-être problème pour prouver l'existence d'un décomposant de Goldbach pour tout nombre pair.

On trouvera ici, là, là, ou encore là des éléments de référence concernant les treillis distributifs, les espaces de Stone, les espaces booléens. Un décomposant de Goldbach de n appartient au complémentaire

ou ensemble orthogonal de l'ensemble $\{n\} \cup \{0\}$. On peut se reporter également aux articles de wikipedia suivants : Filtre topologique, Espace de Stone, Treillis, Algèbre de Boole.

Pour bien décrire l'espace dans lequel on se place, on recopie texto un extrait de l'article de wikipedia *Théorème de représentation de Stone pour les algèbres de Boole* :
https://fr.wikipedia.org/wiki/Th%C3%A9or%C3%A8me_de_repr%C3%A9sentation_de_Stone_pour_les_alg%C3%A8bres_de_Boole :
Exemple : L'algèbre des parties finies ou cofinies
Soit E un ensemble infini. Posons $FC(E)$ l'ensemble des parties finies ou cofinies[1] *$FC(E)$ forme une algèbre de Boole avec les opérations ensemblistes usuelles (union, intersection, complémentaire). Les ultrafiltres de $FC(E)$ sont :*

- *Les ultrafiltres principaux U_x , dont les éléments sont les parties finies ou cofinies de E contenant un élément x donné de E,*
- *L'ultrafiltre U_∞, dont les éléments sont les parties cofinies de E.*

Par conséquent, l'espace de Stone $S(FC(E))$, ensemble des ultrafiltres précédents, peut être assimilé à l'ensemble E auquel on a ajouté un élément ∞. Topologiquement, il s'agit du compactifié d'Alexandrov de E, lorsque ce dernier est muni de la topologie discrète. Les parties ouvertes-fermées de $S(FC(E))$ sont d'une part les parties finies incluses dans E, d'autre part les parties cofinies contenant ∞. L'ensemble de ces parties ouvertes-fermées, avec les opérations ensemblistes usuelles, redonnent une algèbre de Boole isomorphe à $FC(E)$[2]*.*

Transposons au problème qui nous intéresse :
Soit $\mathbb{N}$ l'ensemble infini des entiers naturels. Posons $FC(\mathbb{N})$ l'ensemble des parties finies ou cofinies de $\mathbb{N}$. $FC(\mathbb{N})$ forme une algèbre de Boole avec les opérations ensemblistes usuelles (union, intersection, complémentaire). Les ultrafiltres de $FC(\mathbb{N})$ sont :

- Les ultrafiltres principaux U_x, dont les éléments sont les parties finies ou cofinies. de $\mathbb{N}$ contenant un élément x donné de $\mathbb{N}$,
- L'ultrafiltre U_∞, dont les éléments sont les parties cofinies de $\mathbb{N}$.

Par conséquent, l'espace de Stone $S(FC(\mathbb{N}))$, ensemble des ultrafiltres précédents, peut être assimilé à l'ensemble $\mathbb{N}$ auquel on a ajouté un élément ∞. Topologiquement, il s'agit du compactifié d'Alexandrov de $\mathbb{N}$, lorsque ce dernier est muni de la topologie discrète. Les parties ouvertes-fermées de $S(FC(\mathbb{N}))$ sont d'une part les parties finies incluses dans $\mathbb{N}$, d'autre part les parties cofinies contenant ∞. L'ensemble de ces parties ouvertes-fermées, avec les opérations ensemblistes usuelles, redonnent une algèbre de Boole isomorphe à $FC(\mathbb{N})$.

La notion d'ultrafiltre principal permet de calculer les intersections du complémentaire de $\{n\} \cup \{0\}$ avec les intervalles de la forme $[0, n/2]$ pour trouver les décomposants de Goldbach ; on ne sait pas si le fait d'avoir mieux "délimité" l'espace sur lequel il convient de se placer permet de prouver l'existence d'un décomposant de Goldbach pour tout entier pair supérieur ou égal à 4 ou pas.

1. cofini = dont le complémentaire est fini. Par exemple, $[20, \infty]$ est une partie cofinie de $\mathbb{N}$ de E.
2. Il suffit d'"oublier" l'élément ∞ pour retrouver $FC(\mathbb{E})$.