Localisation en prose

Denise Chemla

25 octobre 2013

1 Introduction

Il s'agit ici de faire un point d'étape de mon travail[1] autour de la conjecture de Goldbach (CG).

On cherche à comprendre pourquoi tout nombre entier est la moyenne de deux nombres premiers, i.e. pourquoi tout nombre pair[2] est la somme de deux nombres premiers.

2 Points d'un espace

La modélisation de CG proposée représente les nombres par des n-uplets de restes modulaires[3].

On appelle par commodité pour la suite $Prem(n)$ l'ensemble des nombres premiers impairs inférieurs à $\sqrt{n}$. Donnons un exemple pour fixer les idées : dans notre représentation, $98 = (2, 3, 0)$ car 98 est $\equiv$ à $2\ (mod\ 3), 3\ (mod\ 5), 0\ (mod\ 7)$.

Un *dg* (pour décomposant de Goldbach) de n doit n'avoir aucune coordonnée nulle pour être premier (crible d'Eratosthène) et aucune coordonnée commune avec n (pour que son complémentaire à n soit premier).

Ce qui fait le "passage" entre les n-uplets de restes et les nombres entiers (ou plus exactement entre les n-uplets de restes et les ensembles d'entiers dans certaines progressions arithmétiques), c'est le théorème des restes chinois (*trc*).

On croit voir la théorie de Galois à l'œuvre dans le *trc* dans la mesure où les valeurs intervenant dans les différentes congruences à vérifier pour trouver la congruence globale résumant un système de plusieurs congruences pouvaient être permutées entre elles et où cela n'influerait pas sur le résultat ; Gauss présente le *trc* dans l'article 36 des RA tandis que l'article 34, noté 43 (sic !), explique comment traiter les modules composés, ce qui n'est jamais le cas des

[1] travail débuté il y a 8 ans, et effectué sur mon temps libre.

[2] supérieur ou égal à 4.

[3] On peut aussi représenter les nombres par des mots de restes, mais se placer dans la théorie des langages supposerait qu'on va faire des opérations sur les lettres d'un mot - en permuter par exemple, comme pour les anagrammes - ce qui n'est pas le cas.

systèmes que les dg doivent vérifier, où tous les modules à considérer sont premiers. Dans le cas de CG, on donne à trc un ensemble de restes (en fait, on lui donne une combinatoire d'ensemble de restes) selon les nombres premiers impairs[4] de $Prem(n)$, et trc renvoie une progression arithmétique de raison $\prod_{p \in Prem(n)} p$.

On voit bien tout ce que l'approche proposée a de géométrique : des points, des éliminations de points d'hyper-plans (ayant certaines coordonnées), c'est-à-dire des projections, dans un espace de dimension finie, cette dimension dépendant de n, mais avec tout de même des ensembles d'entiers à la recherche des dg desquels on peut se placer dans le même espace (si p_k et p_{k+1} sont deux nombres premiers successifs, par exemple 5 et 7, de $p_k^2 + 1$ à $p_{k+1}^2 - 1$, c'est-à-dire pour les nombres pairs de 50 à 120, $Prem(n) = \{3, 5, 7\}$ et on travaille dans le même espace). Les coordonnées appartiennent à des corps premiers dans lesquels on fait des trous, chaque coordonnée appartient à un ensemble fractal.

Cantor a travaillé sur Goldbach[5]. Ce qui semble poser souci ici, c'est cette sorte de "perte du bon ordre". Dans l'axiomatique de Peano,

$$succ(succ(succ(succ(succ(0))))) = 5$$

mais si on réordonne les entiers en mettant d'abord tous les pairs, puis tous les impairs, que vaut $prec(1)$? $\aleph_0$? On a aussi un gros souci pour CG du point de vue de l'ordre, même sans considérer des ensembles de cardinaux infinis : le trc permet de trouver les solutions susceptibles de convenir comme dg de n (nombres premiers et de complémentaire à n premier) mais comment être sûr que le plus petit des nombres en question est bien inférieur à $n/2$ dans la mesure où la progression arithmétique obtenue peut avoir pour minimum $\prod_{p \in Prem(n)} p - 1$ qui est la plupart du temps bien plus grand que $n/2$?

L'idée des bijections : choisissons un $2p$ (p premier) qui vérifie trivialement la conjecture ($2p = p+p$). Prenons $86 = 43+43$. Dans la base de premiers $(3, 5, 7)$, $86 = (2, 1, 2)$. Les dg de 86 sont les nombres inférieurs ou égaux à 43 que trouve trc quand on lui donne les n-uplets de $\mathbb{Z}/3\mathbb{Z}\backslash\{0, 2\} \times \mathbb{Z}/5\mathbb{Z}\backslash\{0, 1\} \times \mathbb{Z}/7\mathbb{Z}\backslash\{0, 2\}$. On va essayer de trouver une bijection qui "change les restes de 86 pour passer aux restes de 98 qui est quant à lui un double de nombre composé" (en considérant chaque ensemble du produit cartésien un par un) ; cette bijection "changera les restes du dg trivial de 86 qu'est 43 pour trouver les restes d'un dg potentiel de 98". Dans la mesure où les restes d'un dg de 86, notamment ceux de son décomposant trivial 43, sont un à un différents des restes de 86 et tous non-nuls, la bijection devra être choisie de manière à préserver l'inégalité des restes du dg de 98 aux restes de 98 ainsi que préserver leur non-nullité. Peut-être qu'il y aura tellement de possibilités combinatoires de trouver une telle bijection préservant simplement l'inégalité et la non-nullité que cela assurera l'existence d'un dg pour le double de composé également, dans l'intervalle $[3, n/2]$.

[4] On pourrait enlever le mot *impairs* ici mais lorsque des exemples sont présentés, pour ne pas avoir des ensembles de nombres trop grands, on se focalise systématiquement sur les seuls nombres impairs.

[5] Les progressions arithmétiques du trc ont pu l'amener aux notions de sa théorie des ensembles infinis.

Il y a de très nombreuses possibilités qu'un nombre soit dg de n : tout nombre qui ne partage aucun de ses restes avec n et qui n'a aucun reste nul convient. Il ne s'agit pas de résoudre une équation polynomiale mais un système d'incongruences du premier degré dans chacun des corps premiers pour $p \in Prem(n)$: chercher un dg de n consiste à chercher un p tel que p premier et $\forall\, m \in Prem(n),\ p \not\equiv n\ (mod\ m)$. Pour une approche "à la Galois", voir la note marquée d'une astérisque intitulée *"CG et nullité du déterminant d'une matrice de Sylvester"*. A la recherche des dg de n, la seule permutation qui vient immédiatement à l'esprit et qui laisse invariant l'ensemble des racines semble être $x \mapsto n - x$.

Pour revenir à Cantor, ce qui est épatant dans le livre d'Anne-Marie Décaillot *Cantor et la France*, c'est qu'on voit que Cantor a bien vu que les $6k$ ont davantage de dg que les $6k + 2$ ou les $6k + 4$ alors qu'il ne semble pas en avoir l'explication. Les congruences permettent de comprendre pourquoi, même si on ne sait pas le démontrer[6] : à cause de leurs restes modulo 2 et 3, les $6k$ peuvent avoir des dg dans les deux progressions arithmétiques contenant des nombres premiers que sont les $6k + 1$ et les $6k - 1$ tandis que les $6k + 2$ ou les $6k + 4$ ne peuvent en avoir que dans l'une des deux progressions en question, à cause des partages de restes interdits.

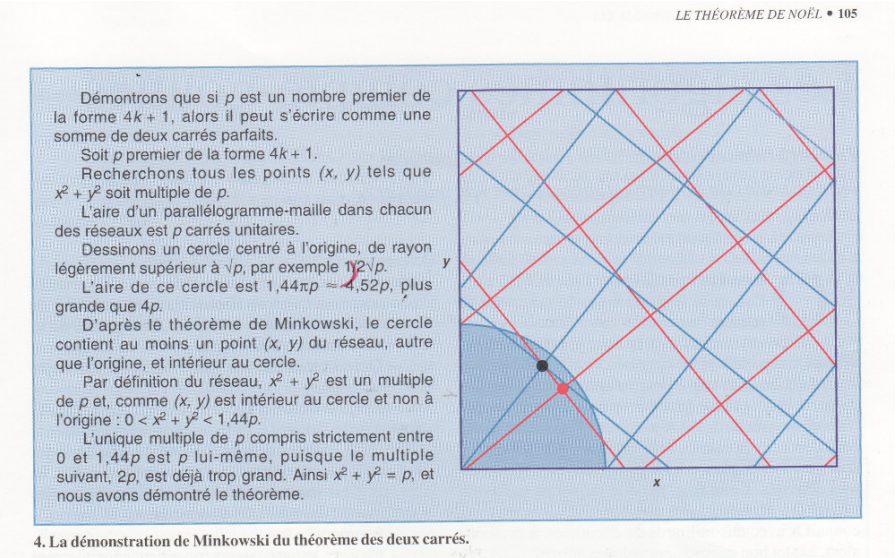
Par rapport à la théorie des groupes, Claude-Paul Bruter a toujours insisté pour que la recherche des dg s'effectue dans le groupe des unités car ce groupe est muni d'une structure connue. Mais cela n'amène à rien puisque le groupe des unités ne renseigne absolument pas sur les restes modulaires (i.e. on n'arrive pas à distinguer les unités selon ce critère-là, les unités u vérifient simplement pour n, l'équation $u^{\varphi(n)} \equiv 1\ (mod\ n)$). A noter, il est plus pratique de travailler dans le groupe des unités, "quotienté par $\{1, -1\}$" pour ne considérer que les seules unités inférieures à $n/2$.

Puisque p premier n'est pas une unité du groupe des unités de $2p$, on pourrait penser que la solution triviale est celle qu'il faut adjoindre pour faire ce que Galois appelle une "extension de corps" (quel corps ?) et ensuite établir une correspondance entre une solution pour un pair double d'un premier et une solution pour un pair double d'un composé : les solutions triviales $2p = p + p$ avec p premier sont les seules solutions de Goldbach dont l'existence est assurée (si on ne compte pas toutes celles qu'a calculées Oliveira e Silva au Portugal[7]), il serait donc judicieux de réussir à "amener" cette existence d'un dg trivial pour un double de premier sur l'existence d'un dg pour un double de composé.

Il y a enfin une démonstration qui m'a longtemps interpelée, parce qu'elle travaille aussi sur des réseaux de points dans des corps premiers (sans trous sûrement), mais qui pourrait peut-être servir aussi à un "technicien", c'est la démonstration par Minkowski du théorème de Fermat dit *de Noël*. Minkowski a aussi inventé la notion de *Géométrie des nombres* dans laquelle on a "atterri" en traçant des droites dans les tables de congruences.

[6] Tout est dit : le travail d'un mathématicien consiste à démontrer des théorèmes.

[7] C'est lui le plus avancé d'un point de vue informatique et il travaille au Cern à utiliser CG pour vérifier la Grid (cf *http* : *//sweet.ua.pt/tos/goldbach.html*).



LE THÉORÈME DE NOËL • 105

Démontrons que si p est un nombre premier de la forme $4k + 1$, alors il peut s'écrire comme une somme de deux carrés parfaits.

Soit p premier de la forme $4k + 1$.

Recherchons tous les points (x, y) tels que $x^2 + y^2$ soit multiple de p.

L'aire d'un parallélogramme-maille dans chacun des réseaux est p carrés unitaires.

Dessinons un cercle centré à l'origine, de rayon légèrement supérieur à $\sqrt{p}$, par exemple $1{,}2\sqrt{p}$.

L'aire de ce cercle est $1{,}44\pi p \approx 4{,}52p$, plus grande que $4p$.

D'après le théorème de Minkowski, le cercle contient au moins un point (x, y) du réseau, autre que l'origine, et intérieur au cercle.

Par définition du réseau, $x^2 + y^2$ est un multiple de p et, comme (x, y) est intérieur au cercle et non à l'origine : $0 < x^2 + y^2 < 1{,}44p$.

L'unique multiple de p compris strictement entre 0 et $1{,}44p$ est p lui-même, puisque le multiple suivant, $2p$, est déjà trop grand. Ainsi $x^2 + y^2 = p$, et nous avons démontré le théorème.

y

x

4. La démonstration de Minkowski du théorème des deux carrés.

Le théorème de Noël dans l'Univers des nombres de Ian Stewart

3 Permuter des solutions de congruences

Comme on le voit très bien sur les tableaux ci-dessous, si on trie les nombres premiers selon leur appartenance classique "à la Gauss ou à la Euler pour la LRQ (loi de réciprocité quadratique)", i.e. en $4k+1$ et $4k+3$, il y a comme une permutation des couples que l'on pourrait résumer par la phrase *"dans le tableau du haut, les A (en violet) sont appariés aux B (en vert) et les C (en orange) sont appariés aux D (en jaune) tandis que dans celui du bas, les A (en violet) sont appariés aux D (en jaune) tandis que les C (en orange) sont appariés aux B (en vert)"*. On a noté les congruences "éliminantes" de différentes couleurs pour bien avoir à l'œil leurs périodicités.

- $n = 144$

5 (p)	0 (mod 5)		139 (p)	
9	0 (mod 3)	0 (mod 3) et 0 (mod 5)	135	
13 (p)			131 (p)	13 + 131
17 (p)			127 (p)	17 + 127
21	0 (mod 3) et 0 (mod 7)	0 (mod 3)	123	
25	0 (mod 5)	0 (mod 7)	119	
29 (p)		0 (mod 5)	115	
33	0 (mod 3) et 0 (mod 11)	0 (mod 3)	111	
37 (p)			107 (p)	37 + 107
41 (p)			103 (p)	41 + 103
45	0 (mod 3) et 0 (mod 5)	0 (mod 3) et 0 (mod 11)	99	
49	0 (mod 7)	0 (mod 5)	95	
53 (p)		0 (mod 7)	91	
57	0 (mod 3)	0 (mod 3)	87	
61 (p)			83 (p)	61 + 83
65	0 (mod 5)		79 (p)	
7 (p)	0 (mod 7)		137 (p)	
11 (p)	0 (mod 11)	0 (mod 7)	133	
15	0 (mod 3) et 0 (mod 5)	0 (mod 3)	129	
19 (p)		0 (mod 5)	125	
23 (p)		0 (mod 11)	121	
27	0 (mod 3)	0 (mod 3)	117	
31 (p)			113 (p)	31 + 113
35	0 (mod 5) et 0 (mod 7)		109 (p)	
39	0 (mod 3)	0 (mod 3) et 0 (mod 5) et 0 (mod 7)	105	
43 (p)			101 (p)	43 + 101
47 (p)			97 (p)	47 + 97
51	0 (mod 3)	0 (mod 3)	93	
55	0 (mod 5) et 0 (mod 11)		89 (p)	
59 (p)		0 (mod 5)	85	
63	0 (mod 3) et 0 (mod 7)	0 (mod 3)	81	
67 (p)		0 (mod 7) et 0 (mod 11)	77	
71 (p)			73 (p)	71 + 73

- $n = 142$

5 (p)	0 (mod 5)		137 (p)	
9	0 (mod 3)	0 (mod 7)	133	
13 (p)		0 (mod 3)	129	
17 (p)		0 (mod 5)	125	
21	0 (mod 3) et 0 (mod 7)	0 (mod 11)	121	
25	0 (mod 5)	0 (mod 3)	117	
29 (p)			113 (p)	29 + 113
33	0 (mod 3) et 0 (mod 11)		109 (p)	
37 (p)		0 (mod 3) et 0 (mod 5) et 0 (mod 7)	105	
41 (p)			101 (p)	41 + 101
45	0 (mod 3) et 0 (mod 5)		97 (p)	
49	0 (mod 7)	0 (mod 3)	93	
53 (p)			89 (p)	53 + 89
57	0 (mod 3)	0 (mod 5)	85	
61 (p)		0 (mod 3)	81	
65	0 (mod 5)	0 (mod 7) et 0 (mod 11)	77	
11 (p)	0 (mod 11)		131 (p)	
15 (p)	0 (mod 3) et 0 (mod 5)		127 (p)	
19 (p)		0 (mod 3)	123	
23 (p)		0 (mod 7)	119	
27	0 (mod 3)	0 (mod 5)	115	
31 (p)		0 (mod 3)	111	
35	0 (mod 5) et 0 (mod 7)		107 (p)	
39	0 (mod 3)		103 (p)	
43		0 (mod 3) et 0 (mod 11)	99	
47 (p)		0 (mod 5)	95	
51	0 (mod 3)	0 (mod 7)	91	
55	0 (mod 5) et 0 (mod 11)	0 (mod 3)	87	
59 (p)			83 (p)	59 + 83
63	0 (mod 3) et 0 (mod 7)		79 (p)	
67 (p)		0 (mod 3) et 0 (mod 5)	75	
71 (p)			71 (p)	71 + 71

Décomposants de Goldbach des nombres 144 et 142

Cette manière de voir est grossière, puisqu'on aura bien compris que selon tous les autres modules qui viennent ensuite (5, 7, 11, etc), l'égalité de restes ne va pas toujours conserver / éliminer les mêmes nombres dans les deux cas. Mais peut-être que les progressions arithmétiques $6k+1$ et $6k-1$ contenant beaucoup de nombres par rapport aux progressions arithmétiques de plus grandes raisons (les $10k+1$, $10k+3$, $10k-3$, $10k-1$, par exemple, pour parler des progressions arithmétiques selon le module 5), cette approche permettrait cependant de mener un raisonnement.

4 Preuve par l'absurde

Une fois que j'avais mis au jour cette notion de partage de restes, j'ai longtemps essayé de trouver une démonstration par descente infinie de Fermat : si tous les premiers inférieurs à $n/2$ partageait chacun au moins un de leurs restes avec n, il y aurait un nombre plus petit que n à qui incomberait forcément le même sort (si par exemple, on diminuait le cardinal de l'ensemble des restes partagés, par inclusion), d'où contradiction par descente infinie de Fermat, il n'y a pas de suite infinie strictement décroissante d'entiers. Voilà la raison de toutes ces tentatives pour essayer de trouver la solution minimale vérifiant un ensemble donné de congruences, pour ainsi descendre de pair non-Goldbach en pair non-Goldbach, comme on m'avait appris à le faire en cours de Recherche opérationnelle en fac, à la recherche du point d'un simplexe minimisant une fonction donnée et vérifiant un ensemble d'inéquations (mais tout ceci se passait dans $\mathbb{R}$).

Utilitaire : solutions minimales de systèmes de congruences

$$\mathcal{S}\begin{cases} x \equiv 0\ (mod\ 2) \\ x \equiv 1\ (mod\ 3) \\ x \equiv 4\ (mod\ 5) \\ x \equiv 5\ (mod\ 7) \\ x \equiv 6\ (mod\ 11) \\ x \equiv 3\ (mod\ 13) \end{cases}$$

sol.min.	2	3	5	7	11	13
21544	0	1	4	5	6	3
754	0	1	4	5	6	×
2434	0	1	4	5	×	3
124	0	1	4	5	×	×
94	0	1	4	×	6	3
94	0	1	4	×	6	×
94	0	1	4	×	×	3
4	0	1	4	×	×	×
3526	0	1	×	5	6	3
292	0	1	×	5	6	×
250	0	1	×	5	×	3
40	0	1	×	5	×	×
94	0	1	×	×	6	3
28	0	1	×	×	6	×
16	0	1	×	×	×	3
4	0	1	×	×	×	×

sol.min.	2	3	5	7	11	13
1524	0	×	4	5	6	3
754	0	×	4	5	6	×
614	0	×	4	5	×	3
54	0	×	4	5	×	×
94	0	×	4	×	6	3
94	0	×	4	×	6	×
94	0	×	4	×	×	3
4	0	×	4	×	×	×
1524	0	×	×	5	6	3
138	0	×	×	5	6	×
68	0	×	×	5	×	3
12	0	×	×	5	×	×
94	0	×	×	×	6	3
6	0	×	×	×	6	×
16	0	×	×	×	×	3
×	0	×	×	×	×	×

5 Nombres pairs dans les écrits de Galois

En deux endroits dans ses textes, Galois utilise une notation désignant un nombre pair, aux pages 414 et 444.

Dans le premier extrait, il écrit "L'équation qui donne la division des périodes en p parties égales est du degré $p^{2n} - 1$. Son groupe a en tout

$$(p^{2n} - 1)(p^{2n} - p) \dots (p^{2n} - p^{2n-1})$$

permutations.
Dans le deuxième extrait, on tombe en plein milieu de la page 444 sur un *savoir* :

$$(m - n)^2 = 2N$$

absolument ininterprétable.

On peut rêver et penser que l'un de ces deux seuls passages écrits par Galois suffirait à démontrer la conjecture de Goldbach.

On peut aussi rêver à Gauss, en se disant que lorsqu'il écrit *Vicimus GEGAN*, le 21 octobre 1796 à Brunswick, les deux premières lettres de GEGAN sont les initiales de Goldbach et Euler et qu'il vient de prouver la conjecture à laquelle il s'est attaqué, selon son journal en latin, le 14 avril 1796, en écrivant : *Numeri cuiusvis divisibilitas varia in binos primos.*.

6 Minimiser la somme des sommes des diviseurs d'Euler des deux décomposants

Quand j'ai trouvé l'article d'Euler *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs* sur Gallica, j'ai été subjuguée. C'était quasiment le seul texte en français d'Euler. Mais surtout s'en dégageait tout son émerveillement pour les nombres premiers. La manière dont il amène sa récurrence est superbe. Même le fait de la programmer ne m'a pas permis d'en pénétrer le sens : elle reste hermétique. Ce qui est génial également dans le texte, c'est la manière dont Euler obtient les nombres pentagonaux en faisant des différences entre la suite des entiers et la suite des impairs (p.245). On peut penser que puisqu'on peut calculer les sommes de diviseurs par une récurrence, il doit être possible de calculer la somme des décomposants de Goldbach par une récurrence également, ou bien leur nombre, qui sait ? (toutes ces fonctions sont des fonctions arithmétiques (cf mon travail sur les comètes à Noël 2010).

$\int 1 = 1$	$\int 21 = 32$	$\int 41 = 42$	$\int 61 = 62$	$\int 81 = 121$
$\int 2 = 3$	$\int 22 = 36$	$\int 42 = 96$	$\int 62 = 96$	$\int 82 = 126$
$\int 3 = 4$	$\int 23 = 24$	$\int 43 = 44$	$\int 63 = 104$	$\int 83 = 84$
$\int 4 = 7$	$\int 24 = 60$	$\int 44 = 84$	$\int 64 = 127$	$\int 84 = 224$
$\int 5 = 6$	$\int 25 = 31$	$\int 45 = 78$	$\int 65 = 84$	$\int 85 = 108$
$\int 6 = 12$	$\int 26 = 42$	$\int 46 = 72$	$\int 66 = 144$	$\int 86 = 132$
$\int 7 = 8$	$\int 27 = 40$	$\int 47 = 48$	$\int 67 = 68$	$\int 87 = 120$
$\int 8 = 15$	$\int 28 = 56$	$\int 48 = 124$	$\int 68 = 126$	$\int 88 = 180$
$\int 9 = 13$	$\int 29 = 30$	$\int 49 = 57$	$\int 69 = 96$	$\int 89 = 90$
$\int 10 = 18$	$\int 30 = 72$	$\int 50 = 93$	$\int 70 = 144$	$\int 90 = 234$
$\int 11 = 12$	$\int 31 = 32$	$\int 51 = 72$	$\int 71 = 72$	$\int 91 = 112$
$\int 12 = 28$	$\int 32 = 63$	$\int 52 = 98$	$\int 72 = 195$	$\int 92 = 168$
$\int 13 = 14$	$\int 33 = 48$	$\int 53 = 54$	$\int 73 = 74$	$\int 93 = 128$
$\int 14 = 24$	$\int 34 = 54$	$\int 54 = 120$	$\int 74 = 114$	$\int 94 = 144$
$\int 15 = 24$	$\int 35 = 48$	$\int 55 = 72$	$\int 75 = 124$	$\int 95 = 120$
$\int 16 = 31$	$\int 36 = 91$	$\int 56 = 120$	$\int 76 = 140$	$\int 96 = 252$
$\int 17 = 18$	$\int 37 = 38$	$\int 57 = 80$	$\int 77 = 96$	$\int 97 = 98$
$\int 18 = 39$	$\int 38 = 60$	$\int 58 = 90$	$\int 78 = 168$	$\int 98 = 171$
$\int 19 = 20$	$\int 39 = 56$	$\int 59 = 60$	$\int 79 = 80$	$\int 99 = 156$
$\int 20 = 42$	$\int 40 = 90$	$\int 60 = 168$	$\int 80 = 186$	$\int 100 = 217.$

Je ne doute pas que, pour peu qu'on regarde la progression de ces nombres, on ne désespere presque d'y découvrir le moindre ordre, vu que l'irrégularité de la suite des nombres premiers s'y trouve entremêlée tellement, qu'il semblera d'abord impossible d'indiquer quelque loi que ces nombres observent

Page de l'article d'Euler *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*

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

Formule récursive fournie par Giard dans la séquence de l'OEIS *A*000203

On peut voir les nombres premiers comme des minima locaux de la fonction somme des diviseurs, notée $\sigma(x)$ ci-dessus, mais notée avec le signe de l'intégrale dans l'article d'Euler. $\sigma(p) = p+1$ pour p premier et $\sigma(c) > c+1$ si c est composé. On voit alors les décomposants de Goldbach comme minimisant $\sigma(p) + \sigma(n-p)$ pour n pair fixé, en rendant d'ailleurs $\sigma(p) + \sigma(n-p)$ égal à $n+2$.

On peut trouver sur la toile la formule récursive fournie par M. Giard. Elle provient de la théorie des fonctions modulaires[8]. On pourrait trouver exactement d'où elle provient mais là n'est pas le but.

[8] et de l'équation de Chazy ; ce domaine est hors d'atteinte des novices.

Le souhait était alors d'utiliser cette formule pour trouver par calcul un décomposant de Goldbach de n en disant que c'est une solution p de l'équation

$$\sigma(p) + \sigma(n-p) - n - 2 = 0.$$

On a essayé sans succès mettre la formule sous une autre forme ("dérécursiver la formule" en jargon informatique), de manière à trouver plus directement une solution. On aimerait savoir si une telle formule plus simple peut ou ne peut pas être trouvée.

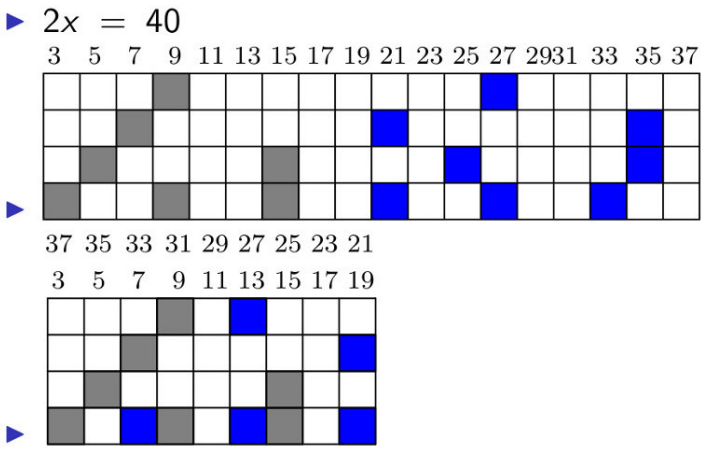
7 Diagonale de Cantor et "passage" CG-CJ

CJ signifie conjecture de l'infinitude de l'ensemble des nombres premiers jumeaux.

En fait, on peut considérer que chercher les *dg* d'un nombre pair et chercher les nombres pairs coincés entre deux nombres premiers jumeaux (comme 18 entre 17 et 19, par exemple, que Claude-Paul Bruter m'a suggéré d'appeler les "pères" de jumeaux) sont des problèmes très similaires : dans le cas de Goldbach, on n'a pas le droit aux restes nuls et aux restes égaux à ceux de n, tandis que dans le cas des pères de jumeaux, on n'a pas le droit aux restes égaux à 1 ou à $p-1$ $(mod\ p)$ pour que le *prec* et le *succ* au sens de Peano soit bien premiers l'un et l'autre. Du coup, ça semble une bonne idée de voir le problème de Goldbach comme un problème *"relatif"* (sous-entendu relatif aux restes modulaires de n) tandis que le problème des jumeaux serait le problème *"absolu"* correspondant (dans le sens où dans chaque corps premier $\mathbb{Z}/p\mathbb{Z}$, on élimine "la même chose", les restes 1 et $p-1$).

J'ai essayé sans succès de "passer au continu" ; il s'agissait d'associer à chaque entier un réel compris entre 0 et 1 dans la partie décimale duquel était codé son mot de restes (en informatique, on appelle ça sa représentation *RNS*, pour *Residue Numeration System*) et d'utiliser un argument proche de celui de la diagonale de Cantor pour conclure que l'ensemble des pères de jumeaux ne peut pas être fini (on perturbe la diagonale pour découvrir un nouveau nombre non déjà recensé) : tentative avortée.

8 Grilles, fonctions récursives et points fixes



Grille de divisibilité pour $n = 40$

Les "grilles de divisibilité", comme celle de $n = 40$ ci-dessus, permettent de bien appréhender la conjecture de Goldbach. On peut les lier à l'arithmétique des tissus de Lucas, à la thèse sur Lucas de Mme Anne-Marie Décaillot, à Jacquart, et donc aux cartes perforées d'ordinateurs. Le "pliage" selon la ligne médiane permet de bien comprendre les éliminations de nombres ($2/p$ pour p ne divisant pas n, dans le cas où les cases bleues et grises ne coïncident pas, et $1/p$ pour p divisant n, lorsque les cases des deux couleurs coïncident par pliage).

J'ai mis du temps à me convaincre qu'il ne fallait pas se préoccuper des caractères de divisibilité par les nombres composés (le but était de travailler sur l'ensemble complet des impairs, dans la mesure où c'est ce que fait Euler avec sa formule récurrente, et puisqu'on ne sait pas où sont les nombres premiers).

J'ai trouvé la fonction qui compte le nombre de cases colorées par ligne. Deux petits détails sont à noter :
1) lorsqu'on "plie le tissu", des cases colorées en bleu peuvent se retrouver à gauche de la diagonale ascendante grise à l'extrême gauche des grilles, f ne les compte pas) ;
2) par cette méthode d'élimination, on ne trouve pas les décompositions de Goldbach faisant intervenir comme plus petit sommant un nombre premier inférieur à $\sqrt{n}$ (l'application du crible d'Eratosthène dit *"entourer le premier nombre non barré p, puis barrer ses multiples"*, tandis qu'ici *"on barre un nombre tous les p nombres, y compris le plus petit d'entre eux"*).

La fonction f est définie par :

$$\begin{cases} f(4pk,p) & = k \\ f(4pk+2p,p) & = f(4pk,p)+1 \\ f(4pk+2a,p) & = 2.f(4pk,p) & \text{si } 1 \leqslant a < p \\ f(4pk+2a,p) & = 2.f(4pk,p)+1 & \text{si } p < a < 2p \end{cases}$$

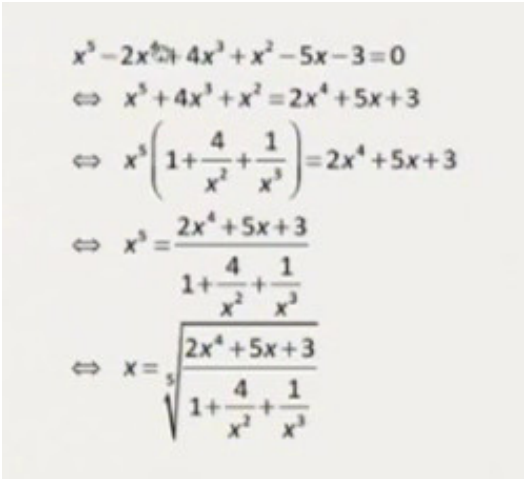
Il est sûrement démontrable que f compte certains caractères de divisibilité de nombres impairs.

$$f(2n,p) = \sum_{i\ impair,\ 3\leqslant i\leqslant n} (p|i) \vee (p|2n-i)$$

On remarque que, si p est un nombre premier impair, alors pour tout q premier impair inférieur à $\sqrt{2p}$, $f(2p,q) = f(2p-2,q)$ *ou* $f(2p,q) = 2.f(2p-2,q)$ (cela peut également avoir lieu pour d'autres nombres, mais qui sont tous des doubles de pairs).

On remarque que, si j est un nombre pair entre deux nombres premiers impairs (appelés nombres premiers jumeaux), alors pour tout q premier impair inférieur à $\sqrt{2j}$, $f(2j,q) = f(2j-2,q)$ *ou* $f(2j,q) = (f(2j-2,q)+1)/2$.

Cela fait un certain temps que cette fonction me tarabuste : on peut se dire que c'est complètement crétin de calculer autant de résultats, pour connaître la primalité de n alors qu'il suffit de faire seulement $\pi(\sqrt{n})$ divisions pour savoir ce qu'il en est, mais ce qui est troublant, c'est le fait qu'avec cette fonction, il y a comme une "similitude" entre les nombres premiers et les nombres pairs coincés entre deux premiers : les uns sont impairs tandis que les autres sont pairs mais ce sont en tout cas les seuls nombres dont les grilles ont la dernière colonne à l'extrême-droite qui est vide de toute case colorée (pour les doubles de premiers, cette colonne représente les caractères de divisibilité de la somme $p+p$ tandis que pour les pairs entre deux jumeaux, elle représente les caractères de divisibilité de $(p-1)+(p+1)$. Pour prouver en une phrase le théorème de Fermat de Noël, Don Zagier utilise des fonctions à points fixes, et cette dernière colonne qui "ne bouge pas" fait automatiquement penser à la notion de "point fixe", d'"invariance". Dominique Tournès dans sa conférence lors du bicentenaire de l'IHES présente très bien les fonctions invariantes que Galois utilise, notées $\varphi x = x$ dans le transparent ci-dessous :



Transparent de la conférence de Dominique Tournès pour les 50 ans de l'IHES

Cette “similitude” ne permettrait-elle pas d'établir une bijection entre l'ensemble des nombres premiers et l'ensemble des nombres pères de jumeaux, qui amènerait l'infinitude de ce dernier ensemble ?

La conjecture de Goldbach, comme la conjecture de l'infinitude de l'ensemble des nombres premiers jumeaux, sont des sous-cas du huitième problème de Hilbert, qui concerne la preuve de l'hypothèse de Riemann.

9 A quels nombres correspondent les points de la comète

En décembre 2010, j'ai mené toute une série d'expérimentations, en utilisant les outils dédiés à CG programmés par Daniel Diaz, qui m'a ainsi rendu un immense service, et qui montrent, comme on s'en doutait, que les points de la comète correspondent à des nombres de factorisation précise, ainsi que les points des comètes d'autres fonctions arithmétiques, comme l'indicateur d'Euler par exemple, ou la somme des diviseurs évoquée plus haut.

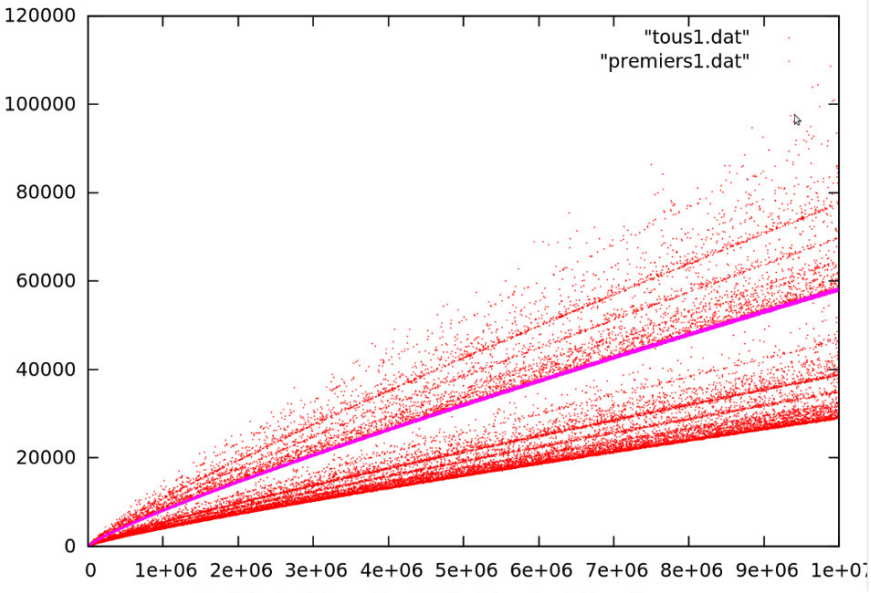


Fig. 10 : Nombre de décompositions de Goldbach des nombres de la forme $6p$

Tige des $6p$

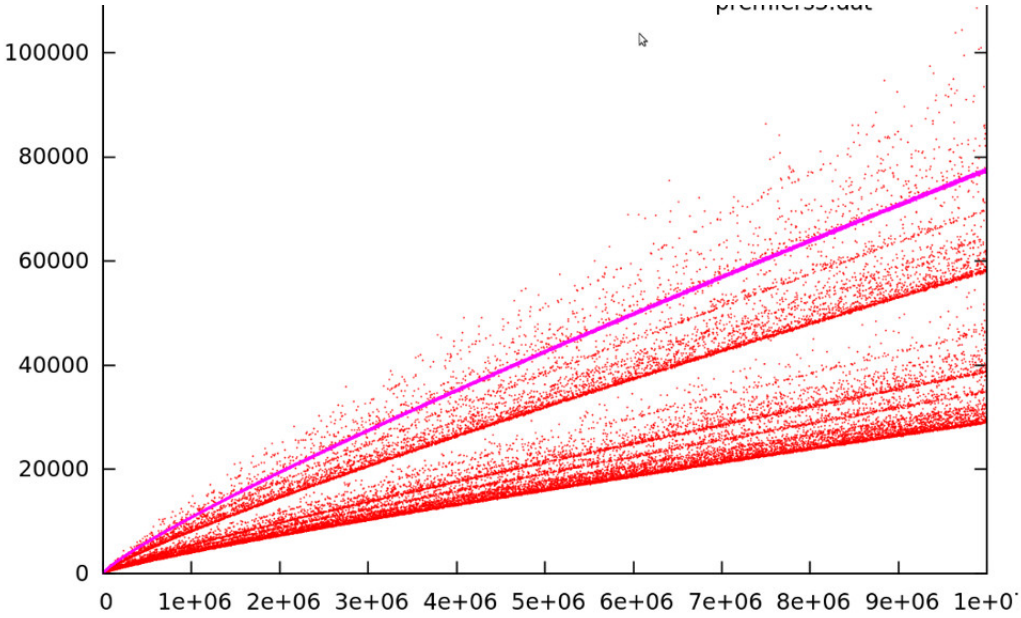


Fig. 11 : Nombre de décompositions de Goldbach des nombres de la forme $30p$

Tige des $30p$

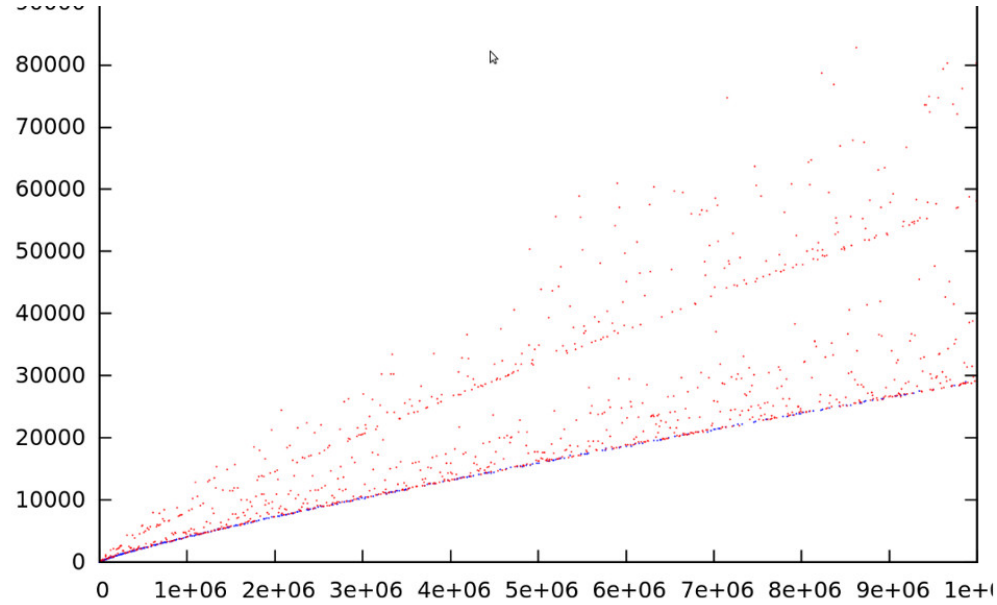
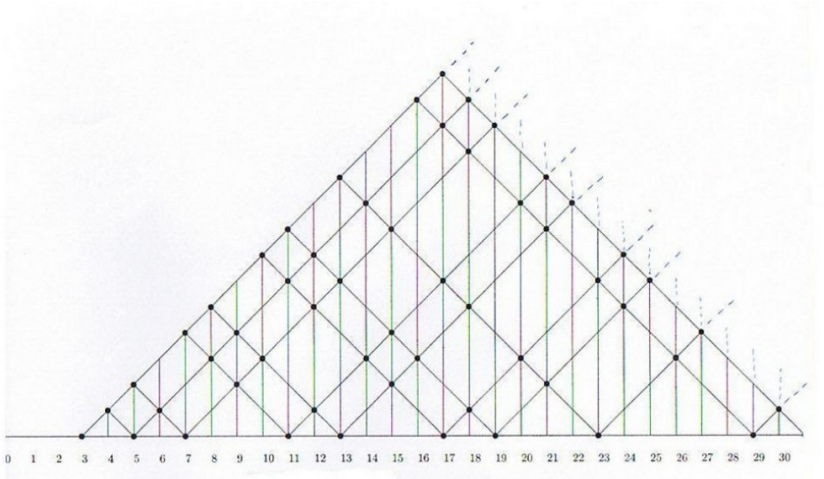


Fig. 12 : Les nombres de décompositions de Goldbach des doubles de carrés de premiers sont sur la première tige de concentration de points.

Tige des $2p^2$

10 Le détour par la physique : maillage et photons



Décompositions de Goldbach

Quand on observe ce que j'appelle à tort mon *treillis*, et pour lequel le mot *maillage* serait plus approprié, on voit qu'en général, on arrive à "couvrir" les entiers jusqu'au 3/4 de l'hypothénuse des triangles environ (l'hypothénuse des 1/2 carrés successifs concorde avec l'axe des abscisses sur lequel on lit le point $n/2$) ; les points marqués à la verticale de $n/2$ fournissent les dg de n comme somme de deux nombres premiers qu'on trouve "au bout" des deux côtés du 1/2 carré ; l'ajout d'un nombre premier supplémentaire sur l'axe des abscisses permet alors de "couvrir" les nombres pairs suivants. Il faut s'assurer qu'on ne laisse pas de "trous" parmi les entiers successifs. On voit bien qu'on génère, par les sommes $3+x$, $5+x$, $7+x$, ..., des infinités d'entiers. Par rapport à cette notion de "couverture environ aux 3/4 des triangles", on obtient par programme que la fraction 22/29 semble être la limite supérieure jamais atteinte ensuite (ce qui serait bien sûr à prouver). Cette fraction *numérateur/dénominateur* représente le plus petit nombre pair (au numérateur, en l'occurrence 22) non-couvert, c'est à dire non moyenne de deux nombres premiers, par un ensemble de nombres premiers allant jusqu'au nombre premier représenté par le dénominateur (en l'occurrence 29) et on avait trouvé sur la toile que cette fraction (22/29) est l'inverse de la densité du photon par nanomètre cube. Bis repetita placent : la fraction 22/29 correspond au fait que si l'on s'autorise à sommer deux nombres premiers appartenant à l'ensemble des nombres premier impairs inférieurs ou égaux à 29, 44 est le plus petit nombre pair que l'on ne peut pas obtenir. Cette fraction 22/29 semble ne jamais être surpassée jusqu'à 10^6.