Espace, distances et conjecture de Goldbach, juillet 2013.

Nombres premiers et brisure de symétrie, août 2013.

Parité, division euclidienne et conjecture de Goldbach, août 2013.

Division euclidienne et conjecture de Golbach, août 2013.

Partage de restes euclidiens et conjecture de Goldbach.

Pistes à creuser, septembre 2013.

transparents.

Décomposants de Goldbach dans le groupe des unités, octobre 2013.

Localisation en prose, octobre 2013.

Conjecture de Goldbach et corps de restes, octobre 2013.

transparents échanger.

Modélisation vectorielle de CG, novembre 2013.

Minimiser / Maximiser, novembre 2013.

Continuer de suivre Galois, décembre 2013.

Voir des analogies, décembre 2013.

références problème de Dirichlet de la corde vibrante, transparents de Bérard à Grenoble, janvier 2014.

Conjecture de Goldbach et anagrammes de mots de restes, janvier 2014.

Conjecture de Goldbach et disjonctions de mots cycliques, janvier 2014.

Une drôle de relation, janvier 2014.

Conjecture de Goldbach, mots booléens et loi de réciprocité quadratique, janvier 2014.

Leçons de solfège et de piano de Pascal Quignard, janvier 2014.

Conjecture de Goldbach, mots booléens et invariant, janvier 2014.

Conjecture de Goldbach, mots booléens, parité, imparité, invariant, février 2014.

Le maillage permet la visualisation des règles de réécriture, février 2014.

Conjecture de Goldbach, langage, réécriture, février 2014.

Annexe 2 : Application de la loi de composition de Ritz-Rydberg aux règles de réécriture.

extrait d'une conférence de Serge Haroche, février 2014.

Helsinki, janvier 2014.

Notes sur En cherchant Majorana d'Etienne Klein, décembre 2013.

extrait de l'Essai d'Albert Einstein Comment je vois le monde.

Extraits de Et si le temps n'existait pas ? de Carlo Rovelli, novembre 2013.

L'Homme magnétique. L'Homme non magnétique.

Conjecture de Goldbach : écrire, réécrire, compter, février 2014.

Petit baluchon, février 2014.

Liens physique quantique, mars 2014.

Conjecture de Goldbach : un monode, deux booléens, quatre lettres, seize règles, un invariant et des changements de parité, mars 2014.

Conjecture de Goldbach : 16 règles de réécriture si bizarres, mars 2014.

Conjecture de Goldbach et somme des diviseurs : utiliser une récurrence mystérieuse, mars 2014.

Conjecture de Goldbach et indicatrice d'Euler, mars 2014.

Conjecture de Goldbach et mouvement brownien.

Goldbach conjecture and Brownian motion.

Programme de la somme des diviseurs d'Euler.

Conjecture de Goldbach : mots bouclés.

Conjecture de Goldbach : revenir au maillage.

Extrait de la biographie Alan Turing ou l'énigme de l'intelligence d'Andrew Hodges.

Conjecture de Goldbach, réécriture, contradiction.

1 Espace, distances et conjecture de Goldbach

(Denise Chemla, 15 juillet 2013)

La lecture de ces textes de physique m'amène à choisir la représentation suivante, qui semble la plus pertinente pour trouver les décomposants de Goldbach d'un nombre pair $2n$ donné qui sont supérieurs à $\lfloor\sqrt{2n}\rfloor$.

On représente chaque nombre p de 1 à n par le n-uplet de ses restes $X_{p,m}$ dans des divisions euclidiennes par les nombres premiers m inférieurs ou égaux $\sqrt{2n}$.

On définit deux distances dont on fera le produit (voir tableau en fin de note) :

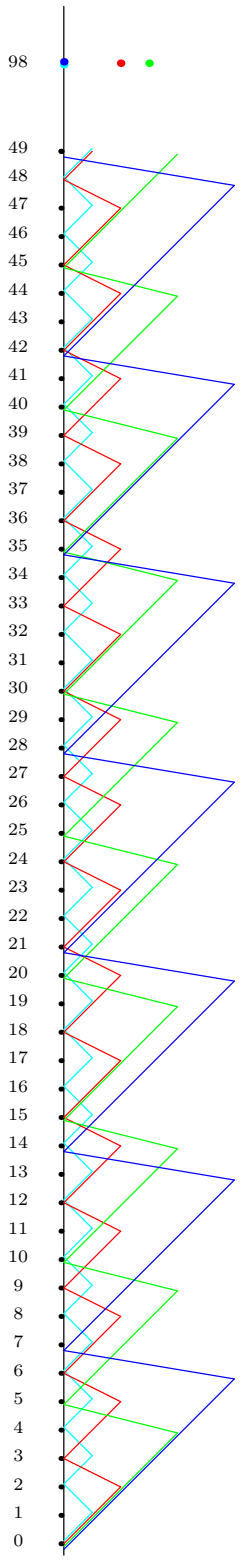
- une "distance à 0" : $d1(p,0) = \prod_{m=2}^{m=\lfloor\sqrt{2n}\rfloor} X_{p,m}$;
- une "distance à $2n$" : $d2(p,2n) = \prod_{m=2}^{m=\lfloor\sqrt{2n}\rfloor} (X_{2n,m} - X_{p,m})^{2*}$.

On cherche un nombre qui ne soit ni "synchrone à 0" (pour être premier), ni "synchrone à $2n$" (pour que son complémentaire à $2n$ soit premier aussi).

On peut voir, de très loin, une analogie entre la notion d'intrication quantique et le fait que le reste $X_{2n-p,m}$ est totalement lié au reste $X_{p,m}$.

On peut également voir une analogie entre cette manière de présenter le problème de Goldbach binaire et le paradoxe des jumeaux d'Einstein, chacun ayant sa propre horloge temporelle ; on peut considérer qu'on a de multiples horloges temporelles (les horloges modulaires de Gauss) de "durées" les différents nombres premiers inférieurs à $\sqrt{2n}$ que l'on pourrait représenter sur le dessin ci-dessous :

*On note $d2(p, 2n, m)$ la distance de p à $2n$ dans la division euclidienne par m qui vaut $(X_{2n,m} - X_{p,m})^2$.


98
49
48
47
46
45
44
43
42
41
40
39
38
37
36
35
34
33
32
31
30
29
28
27
26
25
24
23
22
21
20
19
18
17
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0

Les distances choisies, qui paraissent pertinentes pour déterminer les décomposants de Goldbach, nous placent dans une géométrie qui semble très simple ; cependant, ces distances ne sont pas euclidiennes.

p	$X_{p,2}$	$X_{p,3}$	$X_{p,5}$	$X_{p,7}$	$d1(p,0)$	$d2(p,98,2)$	$d2(p,98,3)$	$d2(p,98,5)$	$d2(p,98,7)$	$d2(p,98)$	DG
1	1	1	1	1	$\neq 0$	1	1	4	1	$\neq 0$	
2	0	2	2	2	0	0	0	1	4	0	
3	1	0	3	3	0	1	4	0	9	0	
4	0	1	4	4	0	0	1	1	16	0	
5	1	2	0	5	0	1	0	9	25	0	
6	0	0	1	6	0	0	4	4	36	0	
7	1	1	2	0	0	1	1	1	0	0	
8	0	2	3	1	0	0	0	0	1	0	
9	1	0	4	2	0	1	4	1	4	$\neq 0$	
10	0	1	0	3	0	0	1	9	9	0	
11	1	2	1	4	$\neq 0$	1	0	4	16	0	
12	0	0	2	5	0	0	4	1	25	0	
13	1	1	3	6	$\neq 0$	1	1	0	36	0	
14	0	2	4	0	0	0	0	1	0	0	
15	1	0	0	1	0	1	4	9	1	$\neq 0$	
16	0	1	1	2	0	0	1	4	4	0	
17	1	2	2	3	$\neq 0$	1	0	1	9	0	
18	0	0	3	4	0	0	4	0	16	0	
19	1	1	4	5	$\neq 0$	1	1	1	25	$\neq 0$	*
20	0	2	0	6	0	90	0	9	36	0	
21	1	0	1	0	0	1	4	4	0	0	
22	0	1	2	1	0	0	1	1	1	0	
23	1	2	3	2	$\neq 0$	1	0	0	4	0	
24	0	0	4	3	0	0	4	1	9	0	
25	1	1	0	4	0	1	1	9	16	$\neq 0$	
26	0	2	1	5	0	0	0	4	25	4	
27	1	0	2	6	0	1	4	1	36	$\neq 0$	
28	0	1	3	0	0	0	1	0	0	0	
29	1	2	4	1	$\neq 0$	1	0	1	1	0	
30	0	0	0	2	0	0	4	9	4	0	
31	1	1	1	3	$\neq 0$	1	1	4	9	$\neq 0$	*
32	0	2	2	4	0	0	0	1	16	0	
33	1	0	3	5	0	1	4	0	25	0	
34	0	1	4	6	0	0	1	1	36	0	
35	1	2	0	0	0	1	0	9	0	0	
36	0	0	1	1	0	0	4	4	1	0	
37	1	1	2	2	$\neq 0$	1	1	1	4	$\neq 0$	*
38	0	2	3	3	0	0	0	0	9	0	
39	1	0	4	4	0	1	4	1	16	$\neq 0$	
40	0	1	0	5	0	0	1	9	25	0	
41	1	2	1	6	$\neq 0$	1	0	4	36	0	
42	0	0	2	0	0	0	4	1	0	0	
43	1	1	3	1	$\neq 0$	1	1	0	1	0	
44	0	2	4	2	0	0	0	1	4	0	
45	1	0	0	3	0	1	4	9	9	$\neq 0$	
46	0	1	1	4	0	0	1	4	16	0	
47	1	2	2	5	$\neq 0$	1	0	1	25	0	
48	0	0	3	6	0	0	4	0	36	0	
49	1	1	4	0	0	1	1	1	0	0	
98	0	2	3	0						0	

1 Nombres premiers et brisure de symétrie

(Denise Chemla, 2 août 2013)

Chaque année (depuis 7 ans) se tient le colloque Science et humanisme près d'Ajaccio, au Lazaret ; l'intervention d'Etienne Klein, dans laquelle il évoque notamment la notion de brisure de symétrie, est visionnable à l'adresse *http://www.youtube.com/watch?v=bRqe7HZ-VLg*

On peut également trouver une présentation de la notion de brisure de symétrie ici, cette notion ayant valu le prix Nobel aux physiciens qui l'ont utilisée *http://lewebpedagogique.com/physique/quest-ce-que-la-brisure-de-symetrie/*

La symétrie, et sa perturbation, semble intervenir dans l'ensemble des nombres premiers (cf *http://denise.vella.chemla.free.fr/060201.pdf*).

On peut voir l'ensemble des nombres premiers comme une structure dont la symétrie serait de plus en plus perturbée.

Voici des calculs qui tendraient à montrer que cette notion de brisure de symétrie est tout à fait à l'oeuvre dans l'ensemble des nombres premiers. Prenons les nombres entiers de 1 à 30, on constate une symétrie entre les nombres premiers autour de la moitié de 30, 15, de la façon suivante :

$$\begin{array}{rlcrl} 13 & = 15-2 & \text{tandis que} & 17 & = 15+2 \\ 11 & = 15-4 & \text{tandis que} & 19 & = 15+4 \\ 7 & = 15-8 & \text{tandis que} & 23 & = 15+8. \end{array}$$

Pour l'ensemble fini de nombres compris entre 1 et $210 = 2.3.5.7$, de milieu 105, on trouve tous les nombres premiers symétriques suivants.

$$\begin{array}{rlcrl} 103 & = 105-2 & \text{tandis que} & 107 & = 105+2 \\ 101 & = 105-4 & \text{tandis que} & 109 & = 105+4 \\ 97 & = 105-8 & \text{tandis que} & 113 & = 105+8 \\ 83 & = 105-12 & \text{tandis que} & 127 & = 105+12 \\ 79 & = 105-26 & \text{tandis que} & 131 & = 105+26 \\ 73 & = 105-32 & \text{tandis que} & 137 & = 105+32 \\ 71 & = 105-34 & \text{tandis que} & 139 & = 105+34 \\ 61 & = 105-44 & \text{tandis que} & 149 & = 105+44 \\ 59 & = 105-46 & \text{tandis que} & 151 & = 105+46 \\ 53 & = 105-52 & \text{tandis que} & 157 & = 105+52 \\ 47 & = 105-58 & \text{tandis que} & 163 & = 105+58 \\ 43 & = 105-62 & \text{tandis que} & 167 & = 105+62 \\ 37 & = 105-68 & \text{tandis que} & 173 & = 105+68 \\ 31 & = 105-74 & \text{tandis que} & 179 & = 105+74 \\ 29 & = 105-76 & \text{tandis que} & 181 & = 105+76 \\ 19 & = 105-86 & \text{tandis que} & 191 & = 105+86 \\ 17 & = 105-88 & \text{tandis que} & 193 & = 105+88 \\ 13 & = 105-92 & \text{tandis que} & 197 & = 105+92 \\ 11 & = 105-94 & \text{tandis que} & 199 & = 105+94 \end{array}$$

Il y a bien évidemment des nombres premiers dont le "complémentaire" ne l'est pas, et cela ne va pas aller en s'améliorant, forcément. Cependant, cette façon de voir semble assez appropriée.

Problème : je ne sais pas comment ces "brisures de symétrie" s'écrivent, se formalisent, et donc j'en resterai à mes ressentis impressionnistes.

1 Parité, division euclidienne et conjecture de Goldbach

(Denise Chemla, 9 août 2013)

On n'expliquera pas ici l'argument *"évident pour tout arithméticien"* : étant donné $2n$ un nombre pair, un nombre premier impair p inférieur ou égal à n qui ne partage aucun de ses restes avec $2n$ dans les divisions euclidiennes de diviseurs q inférieur à $\sqrt{2n}$ est un décomposant de Goldbach de $2n$.

Exemple : on cherche un décomposant de Goldbach du nombre pair 98. 98 a pour reste 0 quand on le divise par 2, 2 quand on le divise par 3, 3 quand on le divise par 5 et 0 quand on le divise par 7.

19, qui est inférieur à $49 = \frac{98}{2}$, et qui a pour reste 1 dans une division euclidienne par 2, 1 quand on le divise par 3, 4 quand on le divise par 5 et 5 quand on le divise par 7, ne partage aucun de ses restes avec 98.

19 est donc un décomposant de Goldbach de 98. En effet, $98 = 19 + 79$ et 79 est premier, comme l'est 19.

Une manière de démontrer la conjecture de Goldbach consiste donc à comprendre pourquoi un tel nombre premier impair, inférieur ou égal à n, et qui ne partage aucun de ses restes (dans les divisions euclidiennes etc...) avec le nombre pair que l'on cherche à décomposer, existe toujours.

Pour démontrer cela, on cherche à démontrer qu'il n'est pas possible que TOUS les nombres premiers impairs inférieurs ou égaux à n, partagent chacun un reste (dans les divisions euclidiennes etc...) avec $2n$.

Intéressons-nous aux propriétés de parité/imparité des nombres entiers intervenant dans la célèbre formule $a = bq + r$ de vérification d'une division euclidienne.

Puisque d'une part, $pair + pair = impair + impair = pair$ et $impair + pair = pair + impair = impair$ et puisque d'autre part, $pair \times pair = impair \times pair = pair \times impair = pair$ et $impair \times impair = impair$, si a est pair dans la formule $a = bq + r$, il faut qu'un nombre pair (soit 0, soit 2) de nombres parmi b et r soient impairs tandis que si a est impair, il faut qu'un nombre impair de nombres (un des deux donc) parmi b et r soit impair.

Considérons l'exemple du nombre pair 40 pour étudier davantage cela en présentant les données dans un tableau dans lequel la case (a, q) contient le couple (b, r) tel que $a = bq + r$ est le résultat de la division euclidienne de a par q. Les nombres premiers ne partageant aucun de leurs restes avec 40 sont 3, 11 et 17. Effectivement, 40 se décompose en somme de deux nombres premiers en $3 + 37 = 11 + 29 = 17 + 23$.

	3	5	7
3	$(1,0)$	$(0,3)$	$(0,3)$
5	$(1,2)$	$(1,0)$	$(0,5)$
7	$(2,1)$	$(1,2)$	$(1,0)$
11	$(3,2)$	$(2,1)$	$(1,4)$
13	$(4,1)$	$(2,3)$	$(1,6)$
17	$(5,2)$	$(3,2)$	$(2,3)$
19	$(6,1)$	$(3,4)$	$(2,5)$
40	$(13,1)$	$(8,0)$	$(5,5)$

Comme attendu, dans l'égalité $11 = 3 \times 3 + 2$ de la forme $a = bq + r$, un nombre impair de nombres parmi $b = 3$ et $r = 2$ sont impairs (en l'occurrence, c'est l'unique nombre b qui vaut 3).

De manière plus générale, on considèrera le tableau suivant, avec

$$p_k \ = \ max\{p_u \ / \ p_u \ premier \ et \ 3 \leqslant p_u \leqslant \sqrt{2n}\}$$

et

$$p_i \ = \ max\{p_v \ / \ p_v \ premier \ et \ 3 \leqslant p_v \leqslant n\}$$

.

	p_1	p_2	p_3	$\dots$	p_k
p_1	$(1,0)$	$(0,p_1)$	$(0,p_1)$	$\dots$	$(0,p_1)$
p_2	$(q_{2,1},r_{2,1})$	$(1,0)$	$(0,p_2)$	$\dots$	$(0,p_2)$
p_3	$(q_{3,1},r_{3,1})$	$(q_{3,2},r_{3,2})$	$(1,0)$	$\dots$	$(0,p_3)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
p_k	$(q_{k,1},r_{k,1})$	$\dots$	$\dots$	$\dots$	$(1,0)$
p_{k+1}	$(q_{k+1,1},r_{k+1,1})$	$\dots$	$\dots$	$\dots$	$(q_{k+1,k},r_{k+1,k})$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
p_i	$(q_{i,1},r_{i,1})$	$\dots$	$\dots$	$\dots$	$(q_{i,k},r_{i,k})$
n	$(q_{n,1},r_{n,1})$	$\dots$	$\dots$	$\dots$	$(q_{n,k},r_{n,k})$

Problème : : je n'arrive pas à exprimer le fait que tout premier du tableau partagerait un reste au moins avec $2n$, de façon à aboutir à une contradiction, peut-être en comptant le nombre de pairs, ou le nombre d'égalités entre nombres du tableau*.

*A cause du postulat de Bertrand (ou théorème de Tchebychev), dans le tableau ci-dessus, $q_{k+1,k}$ vaut forcément 1

Division euclidienne et conjecture de Goldbach

Denise Chemla

10 août 2013

On n'expliquera pas ici l'argument *"évident pour tout arithméticien"* : étant donné $2n$ un nombre pair, un nombre premier impair p inférieur ou égal à n qui ne partage aucun de ses restes avec $2n$ dans les divisions euclidiennes de diviseurs q inférieurs à $\sqrt{2n}$ est un décomposant de Goldbach de $2n$.

Exemple : on cherche un décomposant de Goldbach du nombre pair 98. 98 a pour reste 0 quand on le divise par 2, 2 quand on le divise par 3, 3 quand on le divise par 5 et 0 quand on le divise par 7.

19, qui est inférieur à $49 = \frac{98}{2}$, et qui a pour reste 1 quand on le divise par 2, 1 quand on le divise par 3, 4 quand on le divise par 5 et 5 quand on le divise par 7, ne partage aucun de ses restes avec 98.

19 est donc un décomposant de Goldbach de 98. En effet, $98 = 19 + 79$ et 79 est un nombre premier, comme l'est 19.

Une manière de démontrer la conjecture de Goldbach consiste donc à comprendre pourquoi un tel nombre premier impair, inférieur ou égal à n, et qui ne partage aucun de ses restes (dans les divisions euclidiennes etc...) avec le nombre pair que l'on cherche à décomposer, existe toujours.

Pour démontrer cela, on cherche à démontrer qu'il n'est pas possible que *tous* les nombres premiers impairs inférieurs ou égaux à n, partagent chacun un reste (dans les divisions euclidiennes etc...) avec $2n$.

Considérons l'exemple du nombre pair 40 pour étudier davantage cela en présentant les données dans un tableau dans lequel la case (a, q) contient le couple (b, r) tel que $a = bq + r$ est le résultat de la division euclidienne de a par q. Les nombres premiers impairs ne partageant aucun de leurs restes avec 40 sont 3, 11 et 17. Effectivement, 40 se décompose en somme de deux nombres premiers impairs en $3 + 37 = 11 + 29 = 17 + 23$.

	3	5	7
3	$(1, 0)$	$(0, 3)$	$(0, 3)$
5	$(1, 2)$	$(1, 0)$	$(0, 5)$
7	$(2, 1)$	$(1, 2)$	$(1, 0)$
11	$(3, 2)$	$(2, 1)$	$(1, 4)$
13	$(4, 1)$	$(2, 3)$	$(1, 6)$
17	$(5, 2)$	$(3, 2)$	$(2, 3)$
19	$(6, 1)$	$(3, 4)$	$(2, 5)$
40	$(13, 1)$	$(8, 0)$	$(5, 5)$

Dans le tableau ci-dessus, on a coloré en bleu les restes que les nombres premiers impairs inférieurs à 20 partagent avec 40. Essayons de comprendre pourquoi il n'est pas possible qu'il y ait un reste coloré dans chaque ligne. Appelons $p_1 = 3, p_2 = 5$ et $p_3 = 7$ les nombres premiers qui interviennent dans ce cas particulier. Supposons par exemple par hypothèse que le reste selon le diviseur p_1 est commun à $2n$ et p_2, que le reste selon le diviseur p_2 est commun à $2n$ et p_3, et enfin que le reste selon le diviseur p_3 est commun à $2n$ et p_1.

Si $2n$ et p_2 ont même reste dans la division euclidienne par p_1, cela équivaut à $p_1 \mid (2n - p_2)$. On déduit des deux autres partages de restes que $p_2 \mid (2n - p_3)$ et que $p_3 \mid (2n - p_1)$.

On peut donc déduire du fait qu'un reste soit partagé par $2n$ et *tout* nombre premier impair inférieur ou égal à n le critère de divisibilité suivant :

$$p_1 p_2 p_3 \mid (2n - p_1)(2n - p_2)(2n - p_3)$$

Développons le produit à droite du signe “divise”.

$$\begin{aligned}(2n-p_1)(2n-p_2)(2n-p_3) &= (4n^2-2np_1-2np_2+p_1p_2)(2n-p_3)\\ &= 8n^3-4n^2p_1-4n^2p_2+2np_1p_2-4n^2p_3+2np_1p_3+2np_2p_3-p_1p_2p_3\\ &= 8n^3-4n^2(p_1+p_2+p_3)+2n(p_1p_2+p_1p_3+p_2p_3)-p_1p_2p_3\end{aligned}$$

Mais puisque $p_1p_2p_3$ se divise trivialement lui-même et puisqu'on peut mettre $2n$ en facteur dans le début de la somme obtenue $8n^3-4n^2(p_1+p_2+p_3)+2n(p_1p_2+p_1p_3+p_2p_3)$, alors il faudrait pour que $p_1p_2p_3 \mid (2n-p_1)(2n-p_2)(2n-p_3)$ que $p_1p_2p_3$ divise $2n$, ce qui est impossible (non, problème, pour conclure ça, il faudrait que $p_1p_2p_3$ soit premier avec $4n^2-2n(p_1+p_2+p_3)+(p_1p_2+p_1p_3+p_2p_3)$). On a ainsi abouti à une contradiction.

L'hypothèse qu'on a choisie au départ était très particulière, qui consistait à fixer que

$$p_1 \mid (2n-p_2) \quad \text{et} \quad p_2 \mid (2n-p_3) \quad \text{et} \quad p_3 \mid (2n-p_1)$$

On aboutirait à la même conclusion impossible en permutant de toutes les façons possibles la manière dont les p_i peuvent diviser les $2n-p_j$, si on prend comme hypothèse que *tous* les nombres premiers impairs inférieurs à n partagent un reste avec $2n$.

Appelons

$$p_k \;=\; max\{p_u \;/\; p_u \; premier \; et \; 3 \leqslant p_u \leqslant \sqrt{2n}\}$$

et

$$p_l \;=\; max\{p_v \;/\; p_v \; premier \; et \; 3 \leqslant p_v \leqslant n\}$$

Ce qui est nécessaire pour pouvoir mener un tel raisonnement, c'est de prendre un partage de reste au moins dans chaque colonne, de manière à obtenir le produit complet des nombres premiers impairs inférieurs à $\sqrt{2n}$, i.e. $\prod_{p_i=3}^{p_i=p_k} p_i$ comme diviseur du produit des $2n-p_j$, i.e. $\prod_{p_j=3}^{p_j=p_l}(2n-p_j)$

Puisqu'il n'est pas possible que tous les nombres premiers impairs inférieurs à n partagent un reste avec $2n$ dans les divisions euclidiennes par les nombres premiers impairs inférieurs à $\sqrt{2n}$, il existe pour tout nombre pair un nombre premier inférieur à sa racine qui ne partage aucun de ses restes avec $2n$. Ce nombre premier est un décomposant de Goldbach de $2n$.

Essayons une autre piste :
on peut penser que pour qu'il y ait un nombre coloré par ligne au moins, il faudrait que le produit $\prod_{p_i \leqslant n}(2n-p_i)$ soit divisible par un nombre de la forme $\prod_{p_i \leqslant \sqrt{2n}} p_i^{\alpha_i}$ avec $\sum \alpha_i \geqslant \pi(n)-1$. Mais un petit test montre que ce raisonnement ne convient pas non plus : à la recherche des décompositions de Goldbach de 80, écrivons les factorisations des nombres de la forme $2n-p_i$ pour p_i compris entre 3 et 37.

p_i	$2n-p_i$	$factorisation(2n-p_i)$
3	77	7.11
5	75	3.5^2
7	73	*premier*
11	69	3.23
13	67	*premier*
17	63	$3^2.7$
19	61	*premier*
23	57	3.19
29	51	3.17
31	49	7^2
37	43	*premier*

$3^6.5^2.7^4$ divise le produit des $(2n-p_i)$ avec $6+2+4$ supérieur au nombre de lignes et pourtant, il se trouve des premiers dans le produit, du fait de la grandeur des puissances dans les factorisations d'autres.

Le seul argument valable serait finalement de réussir à prouver que le $\prod_{p_i \leqslant n}(2n-p_i)$ contient au moins un diviseur premier plus grand que n.

Partage de restes euclidiens et conjecture de Goldbach

Denise Chemla

25 août 2013

1 Introduction

On n'expliquera pas ici l'argument *"évident pour tout arithméticien"* : étant donné $2n$ un nombre pair, un nombre premier impair p inférieur ou égal à n qui ne partage aucun de ses restes avec $2n$ dans les divisions euclidiennes de diviseurs q inférieurs à $\sqrt{2n}$ est un décomposant de Goldbach de $2n$.

Exemple : on cherche un décomposant de Goldbach du nombre pair 98. 98 a pour reste 0 quand on le divise par 2, 2 quand on le divise par 3, 3 quand on le divise par 5 et 0 quand on le divise par 7.

19, qui est inférieur à $49 = \dfrac{98}{2}$, et qui a pour reste 1 quand on le divise par 2, 1 quand on le divise par 3, 4 quand on le divise par 5 et 5 quand on le divise par 7, ne partage aucun de ses restes avec 98.

19 est donc un décomposant de Goldbach de 98. En effet, $98 = 19 + 79$ et 79 est un nombre premier, comme l'est 19.

Une manière de démontrer la conjecture de Goldbach consiste donc à comprendre pourquoi un tel nombre premier impair, inférieur ou égal à n, et qui ne partage aucun de ses restes (dans les divisions euclidiennes etc...) avec le nombre pair que l'on cherche à décomposer, existe toujours.

Pour cela, on cherche à démontrer qu'il n'est pas possible que tous les nombres premiers impairs inférieurs ou égaux à n, partagent chacun un reste (dans les divisions euclidiennes etc...) avec $2n$.

Considérons l'exemple du nombre pair 40 en présentant les données dans un tableau dans lequel la case (a, q) contient le couple (b, r) tel que $a = bq + r$ est le résultat de la division euclidienne de a par q. Les nombres premiers impairs ne partageant aucun de leurs restes avec 40 sont 3, 11 et 17. Effectivement, 40 se décompose en somme de deux nombres premiers impairs en $3 + 37 = 11 + 29 = 17 + 23$.

	3	5	7
3	$(1,0)$	$(0,3)$	$(0,3)$
5	$(1,2)$	$(1,0)$	$(0,5)$
7	$(2,1)$	$(1,2)$	$(1,0)$
11	$(3,2)$	$(2,1)$	$(1,4)$
13	$(4,1)$	$(2,3)$	$(1,6)$
17	$(5,2)$	$(3,2)$	$(2,3)$
19	$(6,1)$	$(3,4)$	$(2,5)$
40	$(13,1)$	$(8,0)$	$(5,5)$

On a coloré en bleu les restes que les nombres premiers impairs inférieurs à 20 partagent avec 40. Essayons de comprendre pourquoi il n'est pas possible qu'il y ait un reste partagé (coloré) dans chaque ligne.

Inventons un tableau factice qui contiendrait un partage de reste par ligne (on représente le partage de reste avec $2n$ par une croix et on omet la ligne de $2n$ qui était fournie pour l'exemple $2n = 40$ ci-dessus) et voyons si un tel tableau obligerait à aboutir à une contradiction.

	p_1	p_2	p_3
p_1	$\times$		
p_2		$\times$	
p_3		$\times$	
p_4	$\times$		
p_5			$\times$

A ce tableau pourraient être associées les équations de la forme $a = bq + r$ suivantes :

$$\begin{cases} p_1 = 2n - k_1 p_1 \\ p_2 = 2n - k_2 p_2 \\ p_3 = 2n - k_3 p_2 \\ p_4 = 2n - k_4 p_1 \\ p_5 = 2n - k_5 p_3 \end{cases}$$

Note : dans le cas présenté ici, p_1 et p_2 sont des diviseurs de $2n$.

On transforme ce système en :

$$\begin{aligned} 2n &= p_1 + k_1 p_1 \\ &= p_2 + k_2 p_2 \\ &= p_3 + k_3 p_2 \\ &= p_4 + k_4 p_1 \\ &= p_5 + k_5 p_3 \end{aligned}$$

Mais puisque par ailleurs, on doit avoir :

$$\begin{cases} p_2 = k'_2 p_1 + r_2 \\ p_3 = k'_3 p_1 + r_3 \\ p_4 = k'_4 p_1 + r_4 \\ p_5 = k'_5 p_1 + r_5 \end{cases}$$

On en déduit que :

$$\begin{array}{lllll}
2n & = p_1 + k_1 p_1 & = (1 + k_1) & p_1 & \\
 & = (k'_2 p_1 + r_2) + k_2(k'_2 p_1 + r_2) & = (1 + k_2)k'_2 & p_1 & +r_2(1 + k_2) \\
 & = (k'_3 p_1 + r_3) + k_3(k'_2 p_1 + r_2) & = (k'_3 + k_3 k'_2) & p_1 & +(r_3 + k_3 r_2) \\
 & = (k'_4 p_1 + r_4) + k_4 p_1 & = (k'_4 + k_4) & p_1 & +r_4 \\
 & = (k'_5 p_1 + r_5) + k_5(k'_3 p_1 + r_3) & = (k'_5 + k_5 k'_3) & p_1 & +(r_5 + k_5 r_3)
\end{array}$$

Cela doit vraisemblablement engendrer une contradiction qu'il reste à déterminer.

J'envisagerais bien une contradiction comme celle intervenant dans la démonstration de l'infinité de l'ensemble des nombres premiers d'Euclide. Il dit : "admettons qu'on ait recensé tous les nombres premiers dans un ensemble fini. Fabriquons un nouveau nombre produit de tous les premiers recensés auquel on ajoute 1. Ce nombre a pour reste 1 dans une division par n'importe quel premier déjà recensé. S'il a un diviseur, ce diviseur est forcément un premier qui n'a pas été recensé. Contradiction. L'ensemble des premiers est donc infini."

Peut-être qu'ici la contradiction pourrait provenir du fait qu'on est censé avoir recensé[1] tous les premiers inférieurs à n dans le tableau et les calculs pourraient nous en faire découvrir un nouveau.

Il faudrait généraliser un tel raisonnement, en montrant que toutes les combinaisons possibles de partages de restes engendrent une contradiction. Il faudrait également envisager la façon dont la théorie de Galois, qui entraîne la résolubilité de certaines équations, selon certaines permutations des variables (en l'occurrence les différents nombres premiers inférieurs à n), intervient ici.

[1] Tous ces "censés", c'est insensé !

Pistes à creuser

Denise Chemla

vendredi 13 septembre 13

1 Problème à élucider n^o 1

1.1 Définition

Soit la fonction f définie par :

$$\begin{array}{l} f(4pk,p) = k \\ f(4pk+2p,p) = f(4pk,p)+1 \\ f(4pk+2a,p) = \left\{ \begin{array}{ll} 2.f(4pk,p) & si\ 1 \leqslant a < p \\ 2.f(4pk,p)+1 & si\ p < a < 2p \end{array} \right. \end{array}$$

On pourrait démontrer que f compte certains caractères de divisibilité de nombres impairs.

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

Fournissons ci-dessous les valeurs de $f(2x,p)$ pour $2x$ variant de 24 à 100 et p balayant l'ensemble des nombres premiers inférieurs à $\sqrt{2x}$. Dans la dernière colonne, la lettre P indique que $2x$ est le double d'un nombre premier impair et la lettre J indique que $2x$ est le double d'un nombre pair entre deux nombres premiers.

x	3	5	7	1^{er} *ou* J	x	3	5	7	1^{er} *ou* J
12	1				62	10	6	4	P
14	2				64	10	6	4	
16	2				66	6	6	4	
18	2				68	11	6	4	
20	3	1			70	11	4	3	
22	3	2			72	6	7	5	
24	2	2			74	12	7	5	P
26	4	2		P	76	12	7	5	
28	4	2	1		78	7	7	5	
30	3	2	2		80	13	4	5	
32	5	3	2		82	13	8	5	P
34	5	3	2	P	84	7	8	3	J
36	3	3	2	J	86	14	8	6	P
38	6	3	2	P	88	14	8	6	
40	6	2	2		90	8	5	6	
42	4	4	2		92	15	9	6	
44	7	4	3		94	15	9	6	P
46	7	4	3	P	96	8	9	6	
48	4	4	3		98	16	9	4	
50	8	3	3		100	16	5	5	
52	8	5	3						
54	5	5	3						
56	9	5	2						
58	9	5	4	P					
60	5	3	4						

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* $f(2p,q) = 2.f(2p-2,q)$.

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* $f(2j,q) = (f(2j-2,q)+1)/2$.

Cette fonction f serait-elle utilisable pour démontrer qu'il y a une infinité de nombres premiers jumeaux parce qu'on réussirait à établir une bijection entre l'ensemble des nombres premiers jumeaux et l'ensemble des nombres premiers (un peu comme Cantor a établi, ce qui reste troublant, une bijection entre l'ensemble des entiers et l'ensemble des carrés, par exemple) ?

1.2 La preuve de Don Zagier du théorème de Noël de Fermat

Il faudrait peut-être chercher une démonstration dans l'esprit de celle de Zagier en une phrase qui démontre qu'un nombre premier de la forme $4k+1$ se décompose de manière unique en somme de deux carrés.

Extrait de wikipedia ***Théorème des deux carrés de Fermat*** *(dit aussi Théorème de Fermat de Noël)*

L'article de Don Zagier *A One-Sentence Proof That Every Prime p=1 (mod 4) Is a Sum of Two Squares*, The American Mathematical Monthly, vol. 92, n^o 2, 1990, p. 144 est constitué d'une seule phrase :

≪ L'involution sur l'ensemble fini $S = \{(x,y,z) \in \mathbb{N}^3 / x^2 + 4yz = p\}$ définie par

$$(x,y,z) \mapsto \begin{cases} (x+2z, z, y-x-z) & \text{si} \quad x < y-z \\ (2y-x, y, x-y+z) & \text{si} \quad y-z < x < 2y \\ (x-2y, x-y+z, y) & \text{si} \quad x > 2y \end{cases}$$

a exactement un point fixe, donc $|S|$ est impair et l'involution définie par $(x,y,z) \mapsto (x,z,y)$ a aussi un point fixe. ≫

En effet, un calcul élémentaire permet de vérifier d'une part que ces deux applications sont bien des involutions de S (si bien que la parité du nombre de points fixes de chacune d'elles est la même que celle du nombre $|S|$ d'éléments de S) et d'autre part que la première a un unique point fixe (le triplet $(1,1,k)$, où k est l'entier tel que $p = 4k+1$). Ceci prouve que la seconde involution a un nombre impair de points fixes, donc au moins un, ce qui permet d'écrire p sous la forme $x^2 + (2y)^2$.

2 Problème à élucider n^o 2

Soit n un nombre pair supérieur à 4.

On a vu (évident pour tout arithméticien) qu'un nombre p inférieur à $n/2$ qui est d'une part premier

$$p \not\equiv 0 \ (mod\ q), \forall q\ premier \leqslant \sqrt{n}$$

et qui est d'autre part non congru à n selon tout module adéquat

$$p \not\equiv n \ (mod\ q), \forall q\ premier \leqslant \sqrt{n}$$

est un décomposant de Goldbach de n

Réécrivons les équations ; on cherche s'il existe p tel que :

$$\forall q\ premier\ impair \leqslant \sqrt{n}, \begin{cases} p \not\equiv 0 \ (mod\ q) \\ p \not\equiv n \ (mod\ q) \end{cases}$$

qui devient :

$$\forall q\ premier\ impair \leqslant \sqrt{n}, \begin{cases} p \not\equiv q \ (mod\ q) \\ p \not\equiv n+q \ (mod\ q) \end{cases}$$

qui, par soustraction de 1 et division par 2 des termes congrus, se transforme en :

$$\forall q\ premier\ impair \leqslant \sqrt{n}, \begin{cases} \frac{p-1}{2} \not\equiv \frac{q-1}{2} \ (mod\ q) \\ \frac{p-1}{2} \not\equiv \frac{n+q-1}{2} \ (mod\ q) \end{cases}$$

qui, par le changement de variable $y = \frac{p-1}{2}$ devient : existe-t-il $y \leqslant \frac{n}{2}$ tel que :

$$\forall q \; premier \; impair \leqslant \sqrt{n}, \begin{cases} y \not\equiv \frac{q-1}{2} \; (mod \; q) \\ y \not\equiv \frac{n}{2} + \frac{q-1}{2} \; (mod \; q) \end{cases}$$

N'y aurait-il pas moyen d'utiliser le fait que $\frac{q-1}{2}$ est précisément le nombre de résidus quadratiques de q pour exprimer que la recherche de décomposants de Goldbach d'un nombre pair est en fait la résolution d'une équation quadratique particulière, qui serait obligatoirement résoluble (soit directement grâce à des résultats de Gauss, ou bien à l'aide de la théorie de Galois) ?

3 Problème à élucider n^o 3

Les décomposants de Goldbach de n sont des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$, qui sont premiers à n ; les éléments inversibles sont en nombre $\varphi(n)$ et la moitié d'entre eux sont inférieurs ou égaux à $n/2$.

La structure du groupe des unités $(\mathbb{Z}/n\mathbb{Z})^\times$ est bien connue[1].

Notons $G_n = (\mathbb{Z}/n\mathbb{Z})^\times/\{1,-1\}$, le quotient de $(\mathbb{Z}/n\mathbb{Z})^\times$ par le sous-groupe $\{1,-1\}$.

La structure du groupe G_n dans lequel on se place pour trouver des décomposants de Goldbach de n se déduit aisément de la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$, comme présenté dans le tableau ci-après. G_n est de structure cyclique C_k si $(\mathbb{Z}/n\mathbb{Z})^\times$ est de structure cyclique C_{2k} ou bien de structure produit de groupes cycliques $\prod C_i$ si $(\mathbb{Z}/n\mathbb{Z})^\times$ est de structure $C_2.\prod C_i$.

n	$facto(n)$	$(\mathbb{Z}/n\mathbb{Z})^\times$	G_n	n	$facto(n)$	$(\mathbb{Z}/n\mathbb{Z})^\times$	G_n
8	2^3	Id	$C2$	60	$2^2.3.5$	$C4.C2.C2$	$C4.C2$
10	2.5	$C4$	$C2$	62	2.31	$C30$	$C15$
12	$2^2.3$	$C2.C4$	$C2$	64	2^6	$C16.C2$	$C16$
14	2.7	$C6$	$C3$	66	$2.3.11$	$C10.C2$	$C10$
16	2^4	$C4.C2$	$C4$	68	$2^2.17$	$C16.C2$	$C16$
18	2.3^2	$C6$	$C3$	70	$2.5.7$	$C12.C2$	$C12$
20	$2^2.5$	$C4.C2$	$C4$	72	$2^3.3^2$	$C6.C2.C2$	$C6.C2$
22	2.11	$C10$	$C5$	74	2.37	$C36$	$C18$
24	$2^3.3$	$C2.C2.C2$	$C2.C2$	76	$2^2.19$	$C18.C2$	$C18$
26	2.13	$C12$	$C6$	78	$2.3.13$	$C12.C2$	$C12$
28	$2^2.7$	$C6.C2$	$C6$	80	$2^4.5$	$C4.C4.C2$	$C4.C4$
30	$2.3.5$	$C4.C2$	$C4$	82	2.41	$C40$	$C20$
32	2^5	$C8.C2$	$C8$	84	$2^2.3.7$	$C6.C2.C2$	$C6.C2$
34	2.17	$C16$	$C8$	86	2.43	$C42$	$C21$
36	$2^2.3^2$	$C6.C2$	$C6$	88	$2^3.11$	$C10.C2.C2$	$C10.C2$
38	2.19	$C18$	$C9$	90	$2.3^2.5$	$C12.C2$	$C12$
40	$2^3.5$	$C4.C2.C2$	$C4.C2$	92	$2^2.23$	$C22.C2$	$C22$
42	$2.3.7$	$C6.C2$	$C6$	94	2.47	$C46$	$C23$
44	$2^2.11$	$C10.C2$	$C10$	96	$2^5.3$	$C8.C2.C2$	$C8.C2$
46	2.23	$C22$	$C11$	98	2.7^2	$C42$	$C21$
48	$2^4.3$	$C4.C2.C2$	$C4.C2$	100	$2^2.5^2$	$C20.C2$	$C20$
50	2.5^2	$C20$	$C10$				
52	$2^2.13$	$C12.C2$	$C12$				
54	2.3^3	$C18$	$C9$	242	2.11^2	$C55.C2$	$C55$
56	$2^3.7$	$C6.C2.C2$	$C6.C2$				
58	2.29	$C28$	$C14$				

Pour les nombres pairs de la forme $2p$, avec p premier impair, qui vérifient trivialement la conjecture (puisqu'alors $2p = p + p$), G_n est le groupe cyclique $C_{\frac{p-1}{2}}$.

Pour les nombres pairs de la forme $4p$ ou $6p$ avec p premier impair, G_n est le groupe cyclique C_{p-1}.

Pour les nombres pairs de la forme 2^k, G_n est le groupe cyclique $C_{2^{k-2}}$.

[1] On la trouve notamment dans le livre de Gilles Bailly-Maitre *Arithmétique et cryptologie* aux éditions Ellipses, 2012.

Pour les nombres pairs de la forme $2p^2$, G_n est le groupe cyclique $C_{p(\frac{p-1}{2})}$.

Ne serait-il pas possible de déduire l'existence de décomposants de Goldbach pour les nombres pairs doubles de nombres composés de l'existence triviale de décomposants de Goldbach pour les nombres pairs doubles de nombres premiers sous prétexte qu'il existe un isomorphisme entre leur groupe respectif ?

Par exemple, on voit que 98 a pour groupe $G_{98} = C_{21}$ car $7(\frac{7-1}{2}) = 21$. Mais $86 = 2.43$ a également pour groupe $G_{86} = C_{21}$. L'existence d'une solution pour l'équation polynomiale associée à 86 cumulée à l'équation correspondant au groupe cyclique C_{21} qui est $x^{21} = 1$ comme l'explique Galois n'entraîne-t-elle pas automatiquement l'existement d'une solution pour l'équation polynomiale associée à 98 ?

D'autre part, on constate que lorsqu'une unité p a l'une de ses puissances qui vaut -1 (sa k^{ieme} puissance par exemple) dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ considéré, sa puissance suivante (sa $k+1^{ieme}$ puissance) permet de trouver une décomposition de Goldbach : en effet, dans $(\mathbb{Z}/n\mathbb{Z})^\times$, $n-p$ est égal à $-p = (-1).p$.

Il faudrait être capable de déterminer à quelle condition existe une telle racine k^{ieme} de -1.

4 Problème à élucider n^o 4

On calcule par programme[2] le nombre de décomposants de Goldbach (noté $r(n)$) des nombres pairs de la forme $2^k p$

C.P.Bruter me fait remarquer que, pour les nombres de la forme $2^k.p$, $r(n)$ est souvent la somme de plusieurs nombres $r(a_i)$ de la même forme avec $a_i < n$. Effectivement, dans le tableau des $2^k.13$, on relève les partitions suivantes :

$$\begin{aligned}
r(2^5.13) &= 10 \\
&= 7+3 \\
&= r(2^4.13) + r(2^2.13)
\end{aligned}$$

$$\begin{aligned}
r(2^6.13) &= 22 \\
&= 10+7+5 \\
&= r(2^5.13) + r(2^4.13) + r(2^3.13)
\end{aligned}$$

$$\begin{aligned}
r(2^7.13) &= 28 \\
&= 10+7+5+3+3 \\
&= r(2^5.13) + r(2^4.13) + r(2^3.13) + r(2^2.13) + r(2^1.13)
\end{aligned}$$

$$\begin{aligned}
r(2^8.13) &= 46 \\
&= 28+10+5+3 \\
&= r(2^7.13) + r(2^5.13) + r(2^3.13) + r(2^2.13)
\end{aligned}$$

$$\begin{aligned}
r(2^9.13) &= 80 \\
&= 46+28+3+3 \\
&= r(2^8.13) + r(2^7.13) + r(2^2.13) + r(2^1.13)
\end{aligned}$$

$$\begin{aligned}
r(2^{10}.13) &= 139 \\
&= 80+46+10+3 \\
&= r(2^9.13) + r(2^8.13) + r(2^5.13) + r(2^2.13)
\end{aligned}$$

$$\begin{aligned}
r(2^{11}.13) &= 230 \\
&= 139+46+28+10+7 \\
&= r(2^{10}.13) + r(2^8.13) + r(2^7.13) + r(2^5.13) + r(2^4.13)
\end{aligned}$$

$$\begin{aligned}
r(2^{12}.13) &= 404 \\
&= 230+139+28+7 \\
&= r(2^{11}.13) + r(2^{10}.13) + r(2^7.13) + r(2^4.13)
\end{aligned}$$

[2]Je remercie Daniel Diaz qui a écrit une bibliothèque de programmes dédiés à la conjecture de Goldbach.

$$
\begin{aligned}
r(2^{13}.13) &= 688 \\
&= 404 + 230 + 46 + 5 + 3 \\
&= r(2^{12}.13) + r(2^{11}.13) + r(2^{8}.13) + r(2^{3}.13) + r(2^{2}.13)
\end{aligned}
$$

$$
\begin{aligned}
r(2^{14}.13) &= 1222 \\
&= 688 + 404 + 80 + 28 + 22 \\
&= r(2^{13}.13) + r(2^{12}.13) + r(2^{9}.13) + r(2^{7}.13) + r(2^{6}.13)
\end{aligned}
$$

$$
\begin{aligned}
r(2^{15}.13) &= 2146 \\
&= 1222 + 688 + 230 + 3 + 3 \\
&= r(2^{14}.13) + r(2^{13}.13) + r(2^{11}.13) + r(2^{2}.13) + r(2^{1}.13)
\end{aligned}
$$

$$
\begin{aligned}
r(2^{16}.13) &= 3874 \\
&= 2146 + 1222 + 404 + 80 + 22 \\
&= r(2^{15}.13) + r(2^{14}.13) + r(2^{12}.13) + r(2^{9}.13) + r(2^{6}.13)
\end{aligned}
$$

$$
\begin{aligned}
r(2^{17}.13) &= 6972 \\
&= 3874 + 2146 + 688 + 230 + 28 + 3 + 3 \\
&= r(2^{16}.13) + r(2^{15}.13) + r(2^{13}.13) + r(2^{11}.13) + r(2^{7}.13) + r(2^{2}.13) + r(2^{1}.13)
\end{aligned}
$$

$$
\begin{aligned}
r(2^{18}.13) &= 12558 \\
&= 6972 + 3874 + 1222 + 404 + 80 + 3 + 3 \\
&= r(2^{17}.13) + r(2^{16}.13) + r(2^{14}.13) + r(2^{12}.13) + r(2^{9}.13) + r(2^{2}.13) + r(2^{1}.13)
\end{aligned}
$$

$$
\begin{aligned}
r(2^{19}.13) &= 22769 \\
&= 12558 + 6972 + 2146 + 688 + 230 + 139 + 28 + 5 + 3 \\
&= r(2^{18}.13) + r(2^{17}.13) + r(2^{15}.13) + r(2^{13}.13) + r(2^{11}.13) + r(2^{10}.13) \\
&\quad + r(2^{7}.13) + r(2^{3}.13) + r(2^{2}.13)
\end{aligned}
$$

Pour les $2^k.5$, on peut trouver une partition du nombre de décompositions :

$$
\begin{aligned}
r(2^{20}.5) &= r(5242880) \\
&= 22134 \\
&= 12226 + 6762 + 2133 + 671 + 234 + 76 + 18 + 8 + 4 + 2 \\
&= r(2^{19}.5) + r(2^{18}.5) + r(2^{16}.5) + r(2^{14}.5) + r(2^{12}.5) + r(2^{10}.5) \\
&\quad + r(2^{7}.5) + r(2^{5}.5) + r(2^{4}.5) + r(2^{2}.5)
\end{aligned}
$$

Il semblerait que l'on puisse toujours, pour les nombres de décompositions des nombres pairs de la forme $2^k.p$ avec p premier impair, obtenir le nombre de décompositions d'un certain d'entre eux par addition de certains nombres de décompositions de nombres pairs de la même forme et plus petits.

Il faut tout de même avoir à l'esprit la chose suivante : on pourrait croire que ces partitions ne sont possibles que parce que les ensembles de nombres premiers dont on additionne les cardinaux sont disjoints deux à deux, ce qui n'est pas le cas : 71 et 91 par exemple sont tous deux décomposants des nombres 13312 et 3328 et appartiennent à des ensembles dont on va ajouter les cardinaux pour obtenir le cardinal de l'ensemble de décompositions de 26624. C'est donc bien la relation qu'entretiennent les décomposants de Goldbach avec le pair qu'ils décomposent et non leurs qualités intrinsèques qui intervient vraisemblablement ici, ce qui nous conforte dans l'idée qu'il faut utiliser la théorie des groupes.

5 Petite remarque à propos des décomposants de Goldbach négatifs

$109 = (1, 1, 4, 4)$ ne partage aucun de ses restes avec $98 = (0, 2, 3, 0)$ et fournit une décomposition de Goldbach de 98 qui est $109 + (-11)$.

Conjecture de Goldbach (1742)

- On cherche les DG (décomposants de Goldbach) de $n = 98$.
- Un DG de n est forcément premier à n, puisqu'il est premier et qu'il ne peut diviser n (s'il divise n, son complémentaire à n est composé). Il vérifie donc la congruence $p^{\varphi(n)} \equiv 1 \pmod{n}$ en vertu du théorème d'Euler.
- Or, $\begin{cases} 98 & \equiv 0\ (2) \\ & \equiv 2\ (3) \\ & \equiv 3\ (5) \\ & \equiv 0\ (7) \end{cases}$
- Donc p, un DG de n, est également solution du système de congruences $\begin{cases} p & \equiv 1\ (2) \\ & \equiv 1\ (3) \\ & \equiv 1, 2, 4\ (5) \\ & \equiv 1, 2, 3, 4, 5, 6\ (7) \end{cases}$

Solutions potentielles

- Par le théorème des restes chinois, chaque sous-système de congruences du système disjonctif ci-dessus est équivalent à une seule congruence du premier degré dans $\mathbb{Z}/(\prod_{p_i \text{ premier} \leq \sqrt{n}} p_i)\mathbb{Z}$.
- On dispose donc de :

$$\prod_{p \nmid n} (p-2) \prod_{p \mid n} (p-1)$$

équations du premier degré de la forme

$$x \equiv a \ (mod \ \prod_{p_i \text{ premier} \leq \sqrt{n}} p_i)$$

à résoudre, chacune d'entre elles fournissant un nombre $< \prod_{p_i \text{ premier} \leq \sqrt{n}} p_i$ dont on sait qu'il est premier et jamais congru à n.

Solutions effectives

- Pourquoi l'un de ces nombres est-il forcé d'appartenir au groupe des unités ?
- Le fait que $\frac{\prod_{p_i \text{ premier} \leq \sqrt{n}} p_i}{\varphi(n)} \geqslant 1$ le garantirait-il ?

Décomposants de Goldbach dans le groupe des unités

Denise Chemla

13 octobre 2013

1 Groupes $C3$ et $C4$

Pour $n = 14$, le groupe des unités quotienté par $\{-1, 1\}$ est le groupe cyclique $C3$. On représente ci-dessous sa table de Cayley pour la multiplication et les décomposants de Goldbach sont colorés en rouge dans les entêtes de colonnes. On met une colonne fictive pour 7 bien que 7 ne soit pas une unité (pas premier à 14 puisque diviseur de 14) (en fait, on se dit que c'est peut-être une racine qu'il faudrait adjoindre parce qu'il est un décomposant trivial de 14).

$n = 14$	1	3	5	7
1	1	3	5	–
3	3	5	1	–
5	5	1	3	–
7	–	–	–	–

Pour les nombres $n = 16$, $n = 20$ ou $n = 30$, le groupe des unités quotienté est le groupe cyclique $C4$. On modifie l'ordre croissant habituel sur les entiers de manière à bien faire apparaître la cyclicité du groupe dans les lignes des tables de Cayley.

$n = 16$	1	3	7	5
1	1	3	7	5
3	3	7	5	1
7	7	5	1	3
5	5	1	3	7

$n = 20$	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

$n = 30$	1	7	11	13
1	1	7	11	13
7	7	11	13	1
11	11	13	1	7
13	13	1	7	11

Passons à $n = 60$ parce qu'alors le groupe des unités quotienté est $C4 \times C2$.

$n = 60$	1	7	11	17	13	19	23	29
1	1	7	11	17	13	19	23	29
7	7	11	17	1	29	13	19	23
11	11	17	1	7	23	29	13	19
17	17	1	7	11	19	23	29	13
13	13	29	23	19	11	7	1	17
19	19	13	29	23	7	1	17	11
23	11	13	1	7	1	7	11	13
29	29	23	19	13	17	11	7	1

Voyons pour $n = 80$ dans la mesure où le groupe des unités quotienté est $C4 \times C4$.

$n = 80$	1	3	9	27	7	21	17	29	11	33	19	23	13	39	37	31
1	1	3	9	27	7	21	17	29	11	33	19	23	13	39	37	31
3	3	9	27	1	21	17	29	7	33	19	23	11	39	37	31	13
9	9	27	1	3	17	29	7	21	19	23	11	33	37	31	13	39
27	27	1	3	9	29	7	21	17	23	11	33	19	31	13	39	37
7	7	21	17	29	31	13	39	37	3	9	27	1	11	33	19	23
21	21	17	29	7	13	39	37	31	9	27	1	3	33	19	23	11
17	17	29	7	21	39	37	31	13	27	1	3	9	19	23	11	33
29	29	7	21	17	37	31	13	39	1	3	9	27	23	11	33	19
11	11	33	19	23	3	9	27	1	39	37	31	13	17	29	7	21
33	33	19	23	11	9	27	1	3	37	31	13	39	29	7	21	17
19	19	23	11	33	27	1	3	9	31	13	39	37	7	21	17	29
23	23	11	33	19	1	3	9	27	13	39	37	31	21	17	29	7
13	13	39	37	31	11	33	19	23	17	29	7	21	9	27	1	3
39	39	37	31	13	33	19	23	11	29	7	21	17	27	1	3	9
37	37	31	13	39	19	23	11	33	7	21	17	29	1	3	9	27
31	31	13	39	37	23	11	33	19	21	17	29	7	3	9	27	1

2 Groupes $C5$ et $C6$

Pour $n = 22$, le groupe des unités quotienté par $\{-1, 1\}$ est le groupe cyclique $C5$. On met une colonne fictive pour 11 décomposant de Goldbach trivial de 22.

$n = 22$	1	3	9	5	7	11
1	1	3	9	5	7	–
3	3	9	5	7	1	–
9	9	5	7	1	3	–
5	5	7	1	3	9	–
7	7	1	3	9	5	–
11	–	–	–	–	–	–

Pour les nombres $n = 26$ et $n = 28$, le groupe des unités quotienté est le groupe cyclique $C6$. Pour rappel, pour $n = 26$ existe également le décomposant de Goldbach trivial 13 premier.

$n = 26$	1	7	3	5	9	11
1	1	7	3	5	9	11
7	7	3	5	9	11	1
3	3	5	9	11	1	7
5	5	9	11	1	7	3
9	9	11	1	7	3	5
11	11	1	7	3	5	9

$n = 28$	1	5	3	13	9	11
1	1	5	3	13	9	11
5	5	3	13	9	11	1
3	3	13	9	11	1	5
13	13	9	11	1	5	3
9	9	11	1	5	3	13
11	11	1	5	3	13	9

3 Groupe $C9$

Le groupe cyclique $C9$ est celui trouvé pour $n = 38$ et $n = 54$.
On ne fournit plus la table de Cayley : pour $n = 38$, les puissances de 3 sont dans l'ordre $\{1, 3, 9, 11, 5, 15, 7, 17, 13\}$.
Pour $n = 54$, les puissances de 5 sont dans l'ordre $\{1, 5, 25, 17, 23, 7, 19, 13, 11\}$.

4 Groupe $C10$

Le groupe cyclique $C10$ est celui trouvé pour $n = 44$, $n = 50$ et $n = 66$.
Pour $n = 44$, les puissances de 3 sont dans l'ordre $\{1, 3, 9, 17, 7, 21, 19, 13, 5, 15\}$.
Pour $n = 50$, les puissances de 3 sont dans l'ordre $\{1, 3, 9, 23, 19, 7, 21, 13, 11, 17\}$.
Pour $n = 66$, les puissances de 5 sont dans l'ordre $\{1, 5, 25, 7, 31, 23, 17, 19, 29, 13\}$.

5 Note

Ci-dessous, pour $n = 36$, est présenté le procédé de quotient par $\{1, -1\}$. D'abord, la table de Cayley avec les unités dans l'ordre croissant traditionnel sur les entiers, puis la même table mais dont on a interverti certaines colonnes de manière à bien voir apparaître les sous-groupes cycliques et enfin, le quotient pour ne garder que les unités inférieures à $n/2$ dont on rappelle qu'il s'agit de ne conserver que celles qui d'une part sont des nombres premiers et d'autre part ne sont jamais congrus à n selon un module premier inférieur à $\sqrt{n}$.

Table de Cayley initiale pour la multiplication dans $\mathbb{Z}/36\mathbb{Z}$ *:*

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

Interversion de certaines colonnes pour bien "voir" $C6 \times C2$ *:*

	1	11	13	35	25	23	5	19	29	31	17	7	
1	1	11	13	35	25	23	5	19	29	31	17	7	$a^0 = Id$
11	11	13	35	25	23	1	19	29	31	17	7	5	a^1
13	13	35	25	23	1	11	29	31	17	7	5	19	a^2
35	35	25	23	1	11	13	31	17	7	5	19	29	a^3
25	25	23	1	11	13	35	17	7	5	19	29	31	a^4
23	23	1	11	13	35	25	7	5	19	29	31	17	a^5
5	5	19	29	31	17	7	25	23	1	11	13	35	b
19	19	29	31	17	7	5	23	1	11	13	35	25	$a.b$
29	29	31	17	7	5	19	1	11	13	35	25	23	$a^2.b$
31	31	17	7	5	19	29	11	13	35	25	23	1	$a^3.b$
17	17	7	5	19	29	31	13	35	25	23	1	11	$a^4.b$
7	7	5	19	29	31	17	35	25	23	1	11	13	$a^5.b$

Quotient par $\{1, -1\}$ *pour se focaliser les unités inférieures à* $n/2$ *:*

$n = 36$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	11	1	17	7	13
7	7	1	13	5	17	11
11	11	17	5	13	1	7
13	13	7	17	1	11	5
17	17	13	11	7	5	1

Interversion des colonnes pour bien reconnaître $C6$ *:*

$n = 36$	1	5	11	17	13	7
1	1	5	11	17	13	7
5	5	11	17	13	7	1
11	11	17	13	7	1	5
17	17	13	7	1	5	11
13	13	7	1	5	11	17
7	7	1	5	11	17	13

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.

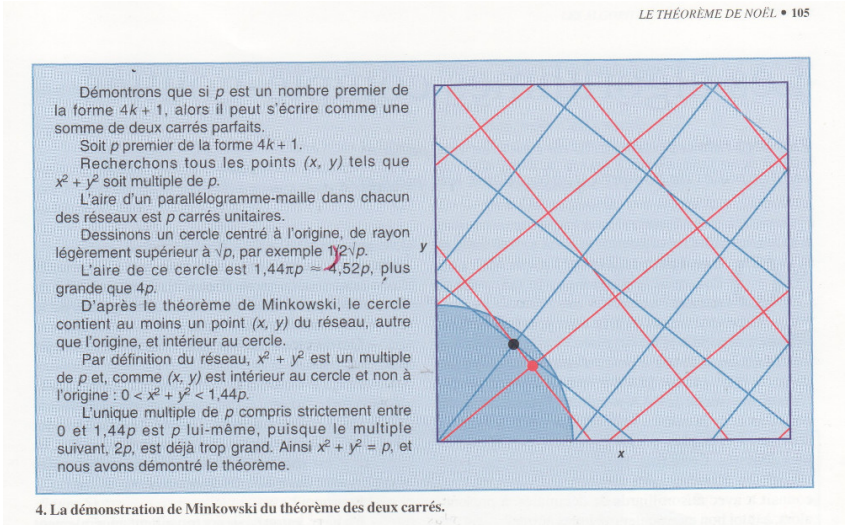
Par rapport à la théorie des groupes, Claude-Paul Bruter a toujours insisté pour que la recherche des dg s'effectue dans le groupe des unités car ce groupe est muni d'une structure connue. Mais cela n'amène à rien puisque le groupe des unités ne renseigne absolument pas sur les restes modulaires (i.e. 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* :

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

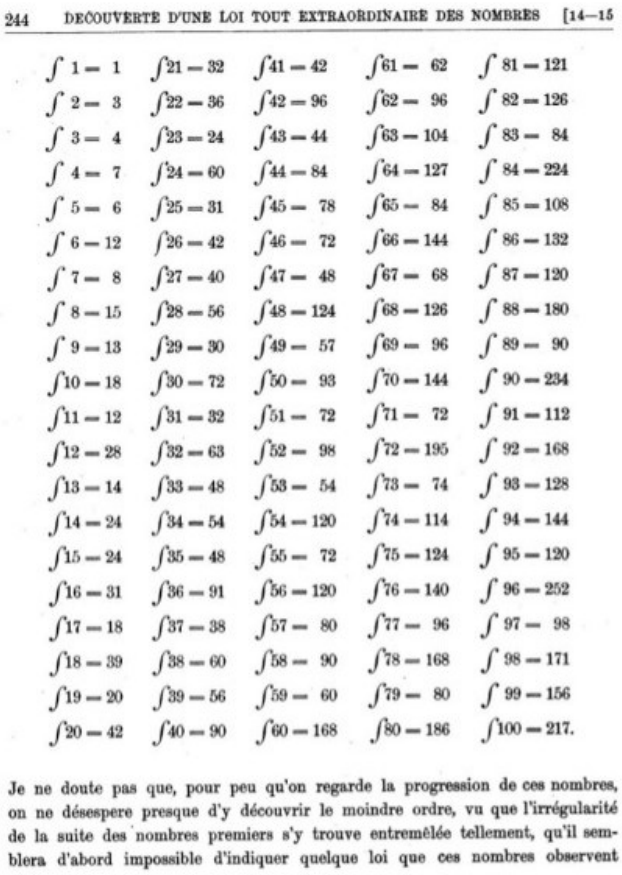
absolument ininterprétable.

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).



244 DÉCOUVERTE D'UNE LOI TOUT EXTRAORDINAIRE DES NOMBRES [14—15

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

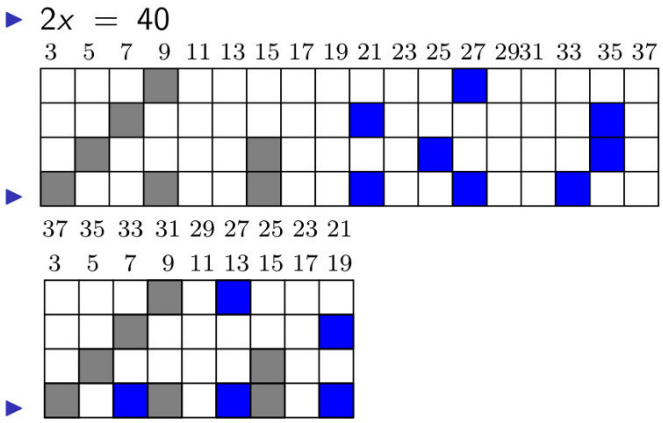
7 Diagonale de Cantor et "passage" CG-CJ

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 :

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

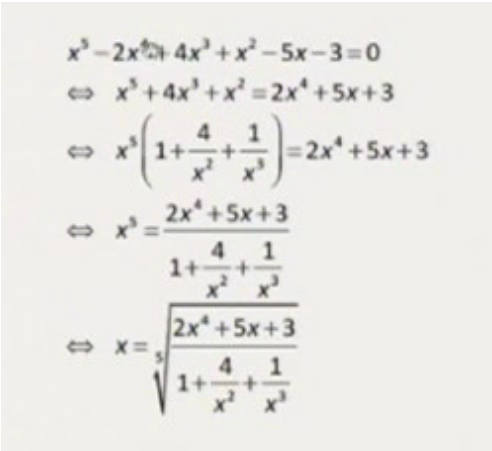
Il est sûrement démontrable que f compte certains caractères de divisibilité de nombres impairs.

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

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.

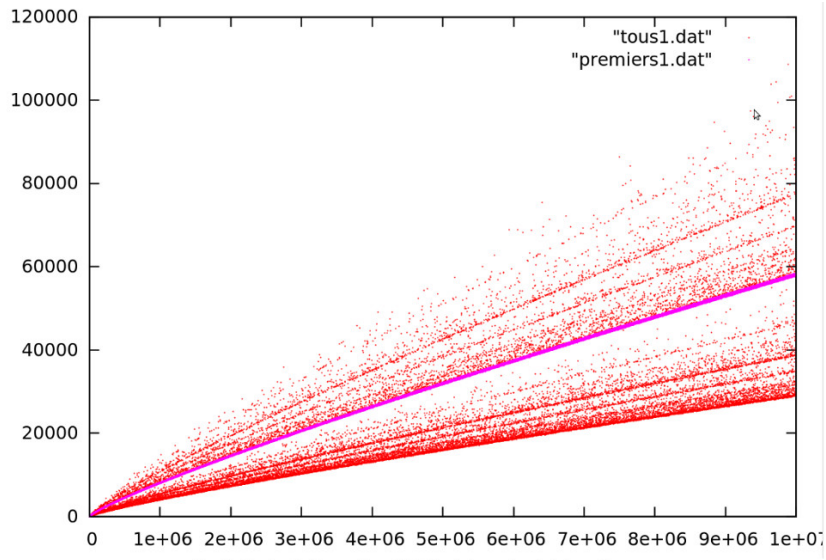


Fig. 10 : Nombre de décompositions de Goldbach des nombres de la forme $6p$

Tige des $6p$

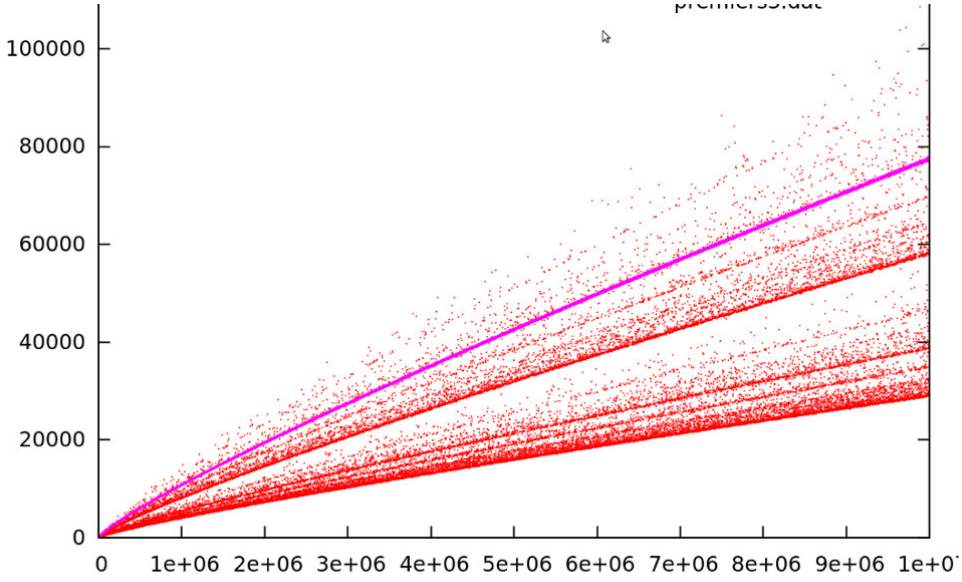


Fig. 11 : Nombre de décompositions de Goldbach des nombres de la forme $30p$

Tige des $30p$

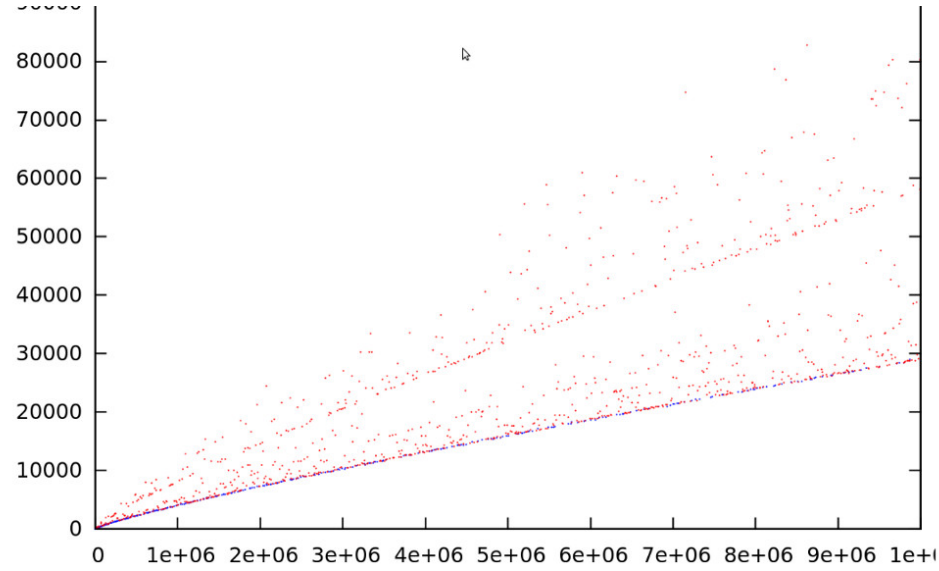
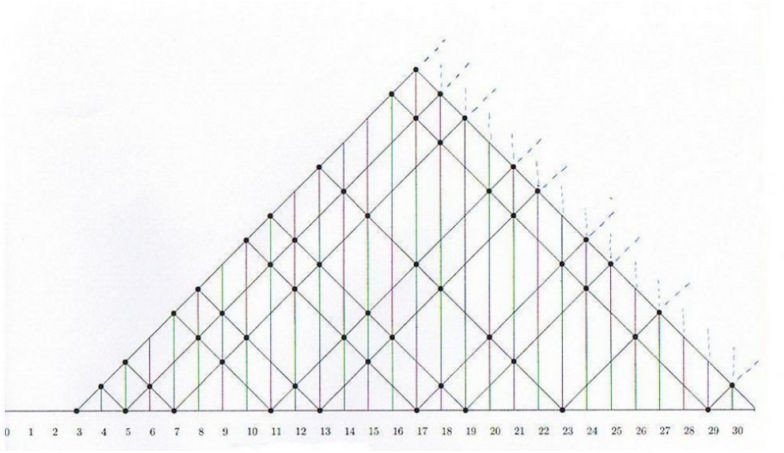


Fig. 12 : Les nombres de décompositions de Goldbach des doubles de carrés de premiers sont sur la première tige de concentration de points.

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.

Conjecture de Goldbach et corps de restes

Denise Chemla

Octobre 2013

1 Présentation en prose

Voici une dernière idée liée à la conjecture de Goldbach[1]: choisissons un $2p$ (p premier) qui vérifie trivialement la conjecture ($2p = p+p$). Prenons $94 = 47+47$. Dans la base de premiers $(3, 5, 7)$, $94 = (1, 4, 3)$. Les dg de 94 sont les nombres inférieurs ou égaux à 47 que trouve trc quand on lui donne les n-uplets de $\mathbb{Z}/3\mathbb{Z}\backslash\{0, 1\} \times \mathbb{Z}/5\mathbb{Z}\backslash\{0, 4\} \times \mathbb{Z}/7\mathbb{Z}\backslash\{0, 3\}$. On va essayer de trouver une bijection qui "change les restes de 94 pour passer aux restes de 88 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 94 qu'est 47 pour trouver les restes d'un dg potentiel de 88". Dans la mesure où les restes d'un dg de 94, notamment ceux de son décomposant trivial 47, 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 88 aux restes de 88 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 $[3, n/2]$.

On comprend que si p_k et p_{k+1} sont deux nombres premiers successifs (par exemple 5 et 7), et qu'on recherche les dg des nombres pairs compris entre $p_k^2 + 1$ à $p_{k+1}^2 - 1$ (en l'occurrence entre 50 et 120), on a seulement à considérer les restes modulaires des nombres selon les nombres premiers appartenant à $Prem(n) = \{3, 5, 7\}$ (on peut appeler cet ensemble la base du codage).

2 Outils

Le nombre de bijections d'un ensemble de cardinal n dans lui-même est $n!$.

Dans un premier temps, nous souhaitions établir le "passage de la décomposition triviale d'un double de premier à une décomposition de Goldbach d'un double de composé" concerné par une même base, i.e. qui est compris entre deux carrés de premiers consécutifs. Malheureusement, rien n'assure encore l'existence d'un double de premier entre deux tels carrés.

On s'est donc rabattu (et cela nécessitera peut-être simplement de mener un raisonnement par récurrence) sur l'idée qui consiste à établir le "passage de la

[1] Tout nombre pair supérieur ou égal à 4 est la somme de deux nombres premiers.

décomposition triviale d'un double de premier $2p_k$ vers une décomposition de Goldbach d'un pair double de composé" pour tout double de composé inférieur à $2p_k$ et supérieur à $2p_{k-1}$ (en fait, c'est ici que j'ai un gros problème : si je garde la base, les nombres obtenus par *trc* peuvent être trop grands, ils peuvent aller jusqu'au produit des modules (auquel on soustrait 1). Si du coup, je décide d'effectuer le passage seulement vers des pairs "assez petits pour être tranquille", par exemple les pairs compris entre $p_i^2 + 1$ et $p_{i+1}^2 - 1$ avec $p_{i+1}^2 - 1 < 2p_k$, je crains qu'ils soient alors si petits qu'à nouveau, la solution minimale du *trc* qui peut aller jusqu'au produit des modules ne dépasse leur moitié.).

3 Inventer une bijection

On aimerait établir les correspondances suivantes, où p_1 et p_2 sont des nombres premiers tandis que c est un nombre composé (g est la fonction qui associe à un nombre l'un de ses dg, on note g_t la fonction qui associe au pair double d'un nombre premier son dg trivial) :

$$\begin{array}{ccc} 2p_1 & \xrightarrow{f} & 2c \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ p_1 & \xrightarrow{f} & p_2 \end{array}$$

Par exemple, pour $94 = 2.47$ et $88 = 2.44$, on aurait :

$$\begin{array}{ccc} 94 = (1,4,3) & \xrightarrow{f} & 88 = (1,3,4) \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ 47 = (2,2,5) & \xrightarrow{f} & 29 = (2,4,1) \end{array}$$

Les bijections à l'œuvre dans l'exemple ci-dessus seraient :

$$\begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ \mathbb{Z}/3\mathbb{Z}\backslash\{0,1\} \times \mathbb{Z}/5\mathbb{Z}\backslash\{0,4\} \times \mathbb{Z}/7\mathbb{Z}\backslash\{0,3\} & \xrightarrow{f} & \mathbb{Z}/3\mathbb{Z}\backslash\{0,1\} \times \mathbb{Z}/5\mathbb{Z}\backslash\{0,3\} \times \mathbb{Z}/7\mathbb{Z}\backslash\{0,4\} \end{array}$$

Pour f, on peut prendre la fonction $f_1 \times f_2 \times f_3$ avec f_1, la permutation de $\mathbb{Z}/3\mathbb{Z}$ dans $\mathbb{Z}/3\mathbb{Z}$ Id, f_2, la permutation de $\mathbb{Z}/5\mathbb{Z}$ dans $\mathbb{Z}/5\mathbb{Z}$ $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 2 & 3 \end{pmatrix}$ et f_3, la permutation de $\mathbb{Z}/7\mathbb{Z}$ dans $\mathbb{Z}/7\mathbb{Z}$ $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$.

Conjecture de Goldbach (5 juin 1742)

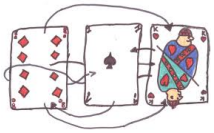
- 271 ans
- **Énoncé** : Tout entier pair (n) supérieur à 2 est la somme de deux nombres premiers.
- $\Longleftrightarrow$ Tout entier supérieur à 1 est la moyenne de deux nombres premiers ($\frac{1}{2}p_1 + \frac{1}{2}p_2$).
- Échanger, permuter
- notations : CG, dg

Représenter les nombres par des mots de restes

- *Base modulaire* : (3,5,7)
- $98 = (2,3,0)$
- $dg \rightarrow 19 = (1,4,5)$
- $86 = (2,1,2)$
- dg trivial $\rightarrow 43 = (1,3,1)$

Échanger, permuter

- Jeu du bonneteau



- Jeu du taquin ou pousse-pousse (cf Bicentenaire)

- Pouss-Pouss (La tige en plastique finit par prendre la place de la glace à l'intérieur du cylindre.)

Permuter deux variables en informatique

- $X \leftrightarrow Y$
- *méthode 1* :

  $X \leftarrow 1$
  $Y \leftarrow 0$

  $X \leftarrow Y$
  $Y \leftarrow X$

  X ? Y ?

  X=0, Y=0

Permuter deux variables en informatique

- *méthode 2* :

  X $\leftarrow$ 1
  Y $\leftarrow$ 0

  Z $\leftarrow$ X
  X $\leftarrow$ Y
  Y $\leftarrow$ Z

  X ? Y ?

  X=0, Y=1

Permuter les lettres de mots dans les anagrammes

- Galilée envoie un cryptogramme à Kepler :

  smaismrmilmepoetaleumibunenugttauiras

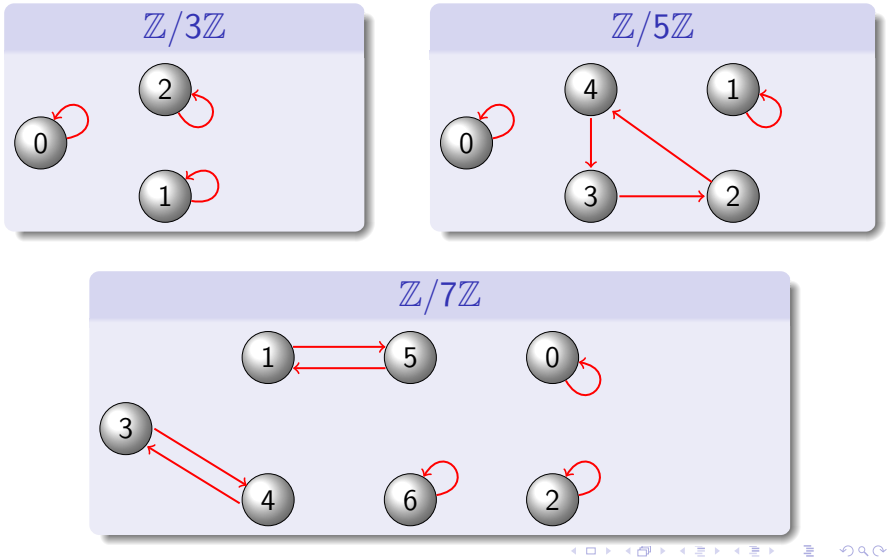
  → Salve umbistineum geminatum Martia proles. (Kepler)

  (Salut, double protection du bouclier, enfants de Mars.)

  → Altissimum planetam tergeminum observavi. (Galilée)

  (J'ai observé que la planète la plus lointaine est en forme de trois.)

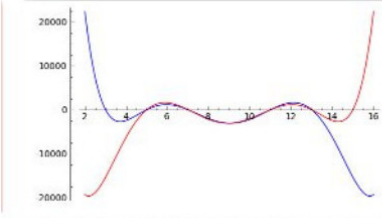
Echanger les racines dans la théorie de Galois



Les *dg* sont solutions d'une équation polynomiale

- On le postule.
- Galois cite Libri.
- On peut fabriquer cette équation en "remontant" des solutions :
  - une première éq. poly. de racines les nombres premiers ($\leqslant n$),
  - une deuxième obtenue en remplaçant x par $n - x$ dans la première ($x \mapsto n - x$),
  - solutions communes aux deux équations.
- Nullité du déterminant d'une matrice de Sylvester

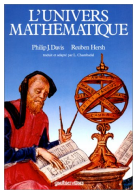
```
x=var('decomp18')
f=plot(x^6-56*x^5+1237*x^4-13712*x^3+79891*x^2-230456*x+255255,(x,2,16),rgbcolor=(0,0,1))
g=plot(x^6-52*x^5+1057*x^4-10552*x^3+52891*x^2-118420*x+75075,(x,2,16),rgbcolor=(1,0,0))
```




```
h=plot(2*x^6-108*x^5+2294*x^4-24264*x^3+132782*x^2-348876*x+330330,(x,2,16),rgbcolor=(0,1,0))
show(h)
```

Le partage de *dg*

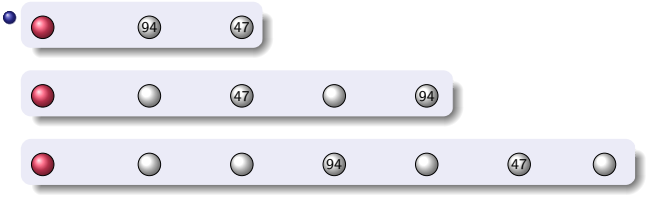
- $20902 = 3 + 20899$ $20962 = 3 + 20959$
  $20904 = 5 + 20899$ $20964 = 5 + 20959$
  $20906 = 3 + 20903$ $20966 = 3 + 20963$
  $20908 = 5 + 20903$ $20968 = 5 + 20963$
  $20910 = 7 + 20903$ $20970 = 7 + 20963$
  $20912 = 13 + 20899$ $20972 = 13 + 20959$
  $20914 = 11 + 20903$ $20974 = 11 + 20963$
  $20916 = 13 + 20903$ $20976 = 13 + 20963$
  $20918 = 19 + 20899$ $20978 = 19 + 20959$
  $20920 = 17 + 20903$ $20980 = 17 + 20963$
  $20922 = 19 + 20903$ $20982 = 19 + 20963$
  $20924 = 3 + 20921$ $20984 = 3 + 20981$

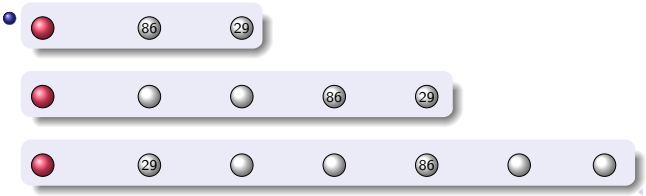


- Des causes différentes produisent les mêmes effets (écart de 60, congrus mod 3 et 5).

Utiliser une solution triviale

- faire découler l'existence d'un *dg* pour un pair double de composé de l'existence obligatoire d'un *dg* trivial pour un double de premier en permutant les classes.





Permutations des racines

- $$\begin{array}{ccc} 2p_i & \xrightarrow{f} & 2c \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ p_i & \xrightarrow{f} & p_j \end{array}$$

- $$\begin{array}{ccc} 94 = (1,4,3) & \xrightarrow{f} & 88 = (1,3,4) \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ 47 = (2,2,5) & \xrightarrow{f} & 29 = (2,4,1) \end{array}$$

$$\begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ \frac{\mathbb{Z}/3\mathbb{Z}}{\setminus\{0,1\}} \times \frac{\mathbb{Z}/5\mathbb{Z}}{\setminus\{0,4\}} \times \frac{\mathbb{Z}/7\mathbb{Z}}{\setminus\{0,3\}} & \xrightarrow{f} & \frac{\mathbb{Z}/3\mathbb{Z}}{\setminus\{0,1\}} \times \frac{\mathbb{Z}/5\mathbb{Z}}{\setminus\{0,3\}} \times \frac{\mathbb{Z}/7\mathbb{Z}}{\setminus\{0,4\}} \end{array}$$

Permutations des racines

- $$\begin{array}{ccc} 94 = (1,4,3) & \xrightarrow{f} & 88 = (1,3,4) \\ \downarrow g_t & & \downarrow g \\ 47 = (2,2,5) & \xrightarrow{f} & 29 = (2,4,1) \end{array}$$

- $\mathbb{Z}/3\mathbb{Z} \to Id$,
  $\mathbb{Z}/5\mathbb{Z} \to \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 2 & 3 \end{pmatrix}$,
  $\mathbb{Z}/7\mathbb{Z} \to \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$

Outils

- Théorie des groupes (moins fois moins égal plus, impair plus impair égal pair).
- Le nombre de bijections d'un ensemble de cardinal n dans lui-même est $n!$
- **Première idée** : on veut passer d'une décomposition triviale $2p_k = p_k + p_k$ aux décompositions pour tous les pairs qui "sont touchés" par la même base, i.e. entre deux carrés de premiers consécutifs.

Outils

- **Question :** Pourquoi trouve-t-on toujours un double de premier entre 2 carrés de premiers ? (celui qui va servir de "modèle")

$$p_k^2 + 1 \quad \leqslant 2p \quad < p_{k+1}^2 + 1 \quad ?$$

- **Théorème de Tchebychev** : on trouve toujours un premier entre un nombre et son double.

$$\forall x \in \mathbb{N}^*,\ \exists p \text{ premier},\ x \leqslant p \leqslant 2x$$

Corollaire :

$$\frac{2}{5}\, n \ln n < p_n < 3\, n \ln n$$

- **Conjecture de Legendre** : on trouve toujours un premier entre deux carrés d'entiers consécutifs.

$$\forall x \in \mathbb{N}^*,\ \exists p \text{ premier},\ x^2 \leqslant p \leqslant (x+1)^2$$

- **Problème** : la **question** est toujours ouverte, il faut une autre idée.

Récurrence

- On va faire passer une solution triviale $2p_k = p_k + p_k$ à tous les pairs inférieurs à $2p_k$ et supérieurs à $2p_{k-1}$
- Soit on travaillera dans le même produit cartésien de corps premiers qui a servi de base modulaire, soit on travaillera dans un sous-produit cartésien de la base.
- Remarque : les restes non-nuls et non égaux à ceux du pair double de premier doivent sûrement pouvoir être permutés avec d'autres (il y a de la marge) de manière à ce que les contraintes assez "légères" que sont la non-nullité et la non-égalité aux restes du double de composé puissent être vérifiées.

Congruences

- Les $6k$ ont des *dg* dans les deux ensembles de nombres premiers en progression arithmétique, soit de la forme $6k+1$, soit de la forme $6k-1$.
- Les $6k+2$ ont des *dg* uniquement dans l'ensemble des premiers de la forme $6k+1$ (car les $6k+2$ et les $6k-1$ sont congrus à 2 (*mod* 3)).
- Les $6k+4$ ont des *dg* uniquement dans l'ensemble des premiers de la forme $6k-1$ (car les $6k+4$ et les $6k+1$ sont congrus à 1 (*mod* 3)).
- On sépare ces trois cas de manière à ne s'occuper que des congruences selon les modules supérieurs ou égaux à 5. Cela permet d'obtenir un traitement homogène selon tous les modules.
- Je crois que le nombre de bijections est à calculer sur des ensembles dans lesquels on élimine 3 congruences (pour que les permutations respectent et la non-nullité des restes du *dg* et leur non-égalité aux restes de n).
- De l'existence d'un *dg trivial* pour un seul pair, je crois qu'on peut déduire l'existence d'un *dg* pour $\prod_p (p-3)!$ nombres, ce qui est beaucoup...

Conjecture

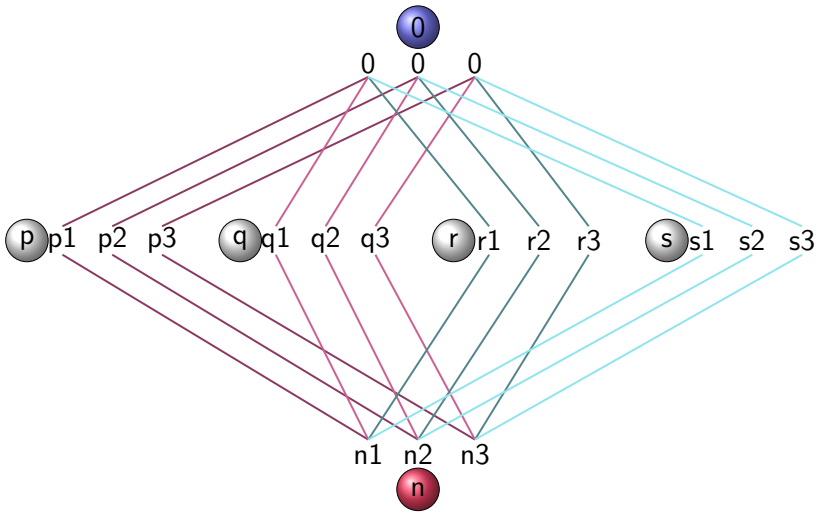
- Tout nombre pair n supérieur à 12 partage l'un de ses dg avec $n - 6$.

- vérifiée par ordinateur jusqu'à 4.10^6.

Passer entre les gouttes : les $6k + 2$

- 26 $(2,1) \to 7 \quad (1,2)$ *ou* 13 $(1,3)$ (t)
  32 $(2,2) \to 13 \quad (1,3)$
  38 $(2,3) \to 19 \quad (1,4)$ (t)
  44 $(2,4) \to 7 \quad (1,2)$ *ou* 13 $(1,3)$
- 50 $(2,0,1) \to 13 \quad (1,3,6)$ *ou* 7 $(1,2,0)$
  56 $(2,1,0) \to 19 \quad (1,4,5)$ *ou* 13 $(1,3,6)$
  62 $(2,2,6) \to 7 \quad (1,2,0)$ *ou* 19 $(1,4,5)$
  68 $(2,3,5) \to 31 \quad (1,1,3)$ *ou* 7 $(1,2,0)$
  74 $(2,4,4) \to 7 \quad (1,2,0)$ *ou* 37 $(1,2,2)$ (t)
- Galois $\to$ Sagiol : au bout de combien d'applications revient-on à Galois ? (merci Norbert Verdier).
- Jeu plus petit / plus grand dans les réels en élémentaire.

Congruences



Notion d'invariant en informatique

- *trouver le double d'un nombre n* :

```
X ← 0 ;
Y ← n ;
while (y > 0) {
  Y ← Y-1 ;
  X ← X+2 ;
}
```

Invariant de boucle : $(Y=0) \vee (X=2(n-Y))$.

Conclusion

- **Hilbert** :

  Wir mussen wissen, wir werden wissen (pas d'ignorabimus en mathématiques.)

- **Poincaré** :

  Le terrain le plus naturel et le plus favorable pour cette étude est l'arithmétique élémentaire, c'est à dire les opérations mettant en jeu des nombres entiers. Quand nous analysons des opérations telles que l'addition et la multiplication, nous nous rendons compte qu'un type de raisonnement se "retrouve à chaque pas", c'est la démonstration "par récurrence" : "on établit d'abord un théorème pour n égal à 1 ; on montre ensuite que, s'il est vrai de $n-1$, il est vrai de n, et on en conclut qu'il est vrai pour tous les nombres entiers." C'est là le "raisonnement mathématique par excellence". Sa particularité est "qu'il contient, sous une forme condensée, une infinité de syllogismes", et qu'il permet de passer du particulier au général, du fini à l'infini, concept qui apparaît dès les premiers pas de l'arithmétique élémentaire et sans lequel "il n'y aurait pas de science parce qu'il n'y aurait rien de général", mais uniquement des énoncés particuliers.

Conclusion

- **Poincaré** :

  D'où nous vient ce "raisonnement pas récurrence" ?

  Certainement pas de l'expérience. Celle-ci peut nous suggérer que la règle est vraie pour les dix ou les cent premiers nombres, mais elle est désarmée face à l'infinité de tous les nombres naturels. Le principe de contradiction (on dirait aujourd'hui le raisonnement par l'absurde) est aussi impuissant : il nous permet d'obtenir certaines vérités, mais non d'en enfermer une infinité en une seule formule. "Cette règle (le raisonnement par récurrence), inaccessible à la démonstration analytique et à l'expérience, est le véritable type du jugement synthétique a priori. L"'irrésistible évidence" avec laquelle ce "principe" s'impose n'est autre que "l'affirmation de la puissance de l'esprit qui se sait capable de concevoir la répétition indéfinie d'un même acte dès que cet acte est une fois possible"... *(extrait de la biographie "Poincaré : mathématicien et philosophe" d'Umberto Bottazzini, éd. Belin Pour la Science)*

Conclusion

- On a utilisé un SNURPF : un Système de NUmération par les Restes dans les Parties Finies de $\mathbb{N}$.
- On se situe dans une théorie lexicale des nombres, selon laquelle les nombres sont des mots.

Modélisation vectorielle de CG (D.Chemla, 6/11/2013)

L'espace $G7$ (G pour Goldbach, on imagine aisément la généralisation G_{p_k}) est un espace vectoriel de dimension finie sur $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ muni du produit scalaire dg défini ainsi :

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} dg \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \iff min(|x2 - x1|, |y2 - y1|, |z2 - z1|) > 0.$$

L'espace vectoriel G_7 contient 210 points ($210 = 2.3.5.7$). Les nombres premiers supérieurs à 7 sont représentés dans cet espace par des points qui n'appartiennent pas aux quatre plans passant par l'origine (le plan $x = 0$ contient les points associés aux nombres pairs, le plan $y = 0$ contient les points associés aux multiples de 3, etc). Chaque nombre de 0 à 210 est représenté par un point qui est l'intersection de 4 plans. Les vecteurs des décomposants de Goldbach d'un nombre pair sont "orthogonaux" au vecteur de ce nombre, i.e. ils ne partagent aucune de leurs coordonnées avec lui.

Si on considère de tels espaces vectoriels (qui "gonflent vers la droite" à chaque ajout d'un nouveau nombre premier), est-on sûr qu'il y ait dans chacun d'eux un point représentant un double de nombre premier ? Est-on assuré qu'il y a un double de premier entre deux primorielles successives ?

L'idée serait de trouver une bijection qui "passerait" du décomposant trivial d'un nombre pair double d'un nombre premier à un décomposant non trivial pour tous les pairs du même espace, une telle bijection devant mettre les points éliminés en bijection avec les points éliminés et les points conservés en bijection avec les points conservés (on pourrait sûrement trouver une telle bijection - dans le cas où on serait assuré d'avoir un point représentant un double de premier dans chacun des espaces vectoriels emboîtés - parce qu'il y a davantage de nombres orthogonaux à un double de premier qu'à un double de composé : 6 plans d'élimination (i.e. $2k$ plans dans le cas de l'espace vectoriel G_{p_k}) puisque le vecteur d'un nombre double de nombre premier n'a aucune coordonnée nulle alors que pour les doubles de composés, l'un des plans d'élimination s'avère confondu avec le plan passant par l'origine correspondant.

On peut aussi définir la notion de *"ligne"* passant par différents points.
La ligne associée aux nombres $\{0, 1, 2, 3, 4, 5\}$ est toute bizarre (brisée et se poursuivant dans un peu toutes les directions) : elle passe par les points $\{(0, 0, 0, 0), (1, 1, 1, 1), (0, 2, 2, 2), (1, 0, 3, 3), (0, 1, 4, 4), (1, 2, 0, 5)\}$.
On se focalisera sur les lignes qui relient les points correspondant à des nombres impairs.
Quand l'espace vectoriel courant (de dimension i) est "emboîté" dans un espace vectoriel plus grand (de dimension $i + 1$, à l'ajout d'un nouveau nombre premier, lorsqu'on étudie l'existence de décomposants de Goldbach pour des nombres supérieurs à p_{i+1}^2), toutes les lignes sont "prolongées", on ajoute un point à leur extrémité. De l'existence d'un dg dans la ligne courte l associée à un certain nombre pair doit découler l'existence de dg pour les nombres pairs dont les lignes prolongent l.

C'est le théorème des restes chinois (trc) qui permet de passer d'un n-uplet au nombre correspondant.
C'est le produit vectoriel qui permet de trouver des décomposants de Goldbach d'un nombre donné.
Par exemple, à la recherche des dg de 98, on cherche tous les vecteurs de la forme $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$ qui, multipliés par le vecteur $\begin{pmatrix} 105 \\ 70 \\ 126 \\ 120 \end{pmatrix}$, permettent d'obtenir un scalaire ($105x_1 + 70x_2 + 126x_3 + 120x_4$) dont le reste dans une division par 210 est un impair compris entre 3 et 49.
C'est ainsi qu'on trouve $19 = \begin{pmatrix} 1 \\ 1 \\ 4 \\ 5 \end{pmatrix}$ ou bien $31 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 3 \end{pmatrix}$ ou encore $37 = \begin{pmatrix} 1 \\ 1 \\ 2 \\ 2 \end{pmatrix}$.
En effet,

$$105 \times 1 + 70 \times 1 + 126 \times 4 + 120 \times 5 = 1279 \,\%\, 210 = 19$$
$$105 \times 1 + 70 \times 1 + 126 \times 1 + 120 \times 3 = 661 \,\%\, 210 = 31$$
$$105 \times 1 + 70 \times 1 + 126 \times 2 + 120 \times 2 = 667 \,\%\, 210 = 37.$$

Démontrer la conjecture de Goldbach consiste à vérifier que l'intersection de l'ensemble de points obtenus par résolution de multiples systèmes de congruences (élimination des points appartenant à différents hyperplans) grâce à l'application du trc et de l'ensemble des points de la ligne des impairs compris entre 3 et $n/2$ (à la recherche des décomposants de Goldbach de n) n'est jamais vide.

Minimiser / Maximiser

Denise Chemla

10 novembre 2013

1 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[1]. On pourrait trouver exactement d'où elle provient mais là n'est pas le but.

[1] 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.

2 Dualité

A travailler hier sur la manière dont les restes "tournent", on trouve l'idée suivante : partons du nombre 15 qui a pour reste $(0, 0)$ modulo 3 et 5 et considérons les nombres de 15 à 45. Considérons également les nombres premiers à 15 qui sont $\{1, 2, 4, 7, 8, 11, 13, 14\}$. En ajoutant ces nombres à 15, après les avoir multipliés par 2 pour ne trouver que des impairs, on ne doit effectivement trouver que des nombres premiers puisqu'on obtient des nombres qui n'ont forcément aucun reste nul, modulo 3 et 5.

On vérifie effectivement que :

$$\begin{aligned}
15 + 2 \times 1 &= 17 \\
15 + 2 \times 2 &= 19 \\
15 + 2 \times 4 &= 23 \\
15 + 2 \times 7 &= 29 \\
15 + 2 \times 8 &= 31 \\
15 + 2 \times 11 &= 37 \\
15 + 2 \times 13 &= 41 \\
15 + 2 \times 14 &= 43
\end{aligned}$$

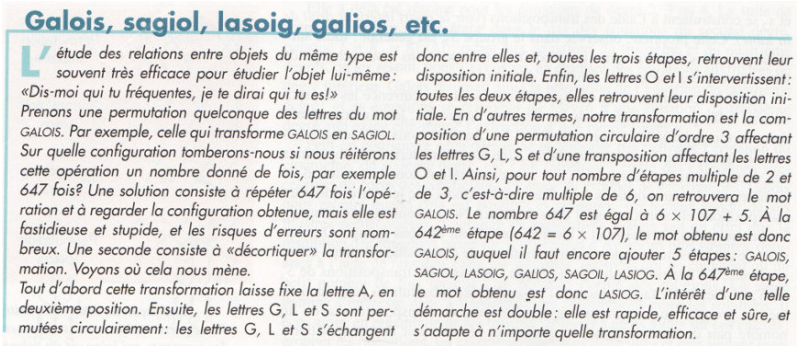
Du coup, on a l'idée suivante, duale de celle présentée au premier paragraphe, qui consistait à trouver les décomposants de Goldbach en minimisant la somme des sommes des diviseurs des deux décomposants.

L'idée duale est que trouver les décomposants de Goldbach doit également correspondre au fait de maximiser le produit des indicateurs d'Euler des deux décomposants.

Il semblerait que p un décomposant de Goldbach de n maximise le produit des indicateurs d'Euler des deux décomposants de la somme (il se produit seulement une exception pour le nombre pair 44 jusqu'à 10^6 : pour $n = 44$, et la décomposition $13+31$ et la décomposition $19+25$ maximise le produit qui prend la valeur 360, i.e. le maximum n'est alors pas un maximum "absolu" mais un maximum "ex-aequo").

$$p \textit{ est un dg de } n \iff p = arg\_max_{p_i \leqslant n/2}[\varphi(p_i)\varphi(n-p_i)]$$

Dominique Ceugniet a vérifié cette idée par programme jusqu'à 7.10^6.



Galois, sagiol, lasoig, galios, etc.

L'étude des relations entre objets du même type est souvent très efficace pour étudier l'objet lui-même : «Dis-moi qui tu fréquentes, je te dirai qui tu es!»
Prenons une permutation quelconque des lettres du mot GALOIS. Par exemple, celle qui transforme GALOIS en SAGIOL. Sur quelle configuration tomberons-nous si nous réitérons cette opération un nombre donné de fois, par exemple 647 fois? Une solution consiste à répéter 647 fois l'opération et à regarder la configuration obtenue, mais elle est fastidieuse et stupide, et les risques d'erreurs sont nombreux. Une seconde consiste à «décortiquer» la transformation. Voyons où cela nous mène.
Tout d'abord cette transformation laisse fixe la lettre A, en deuxième position. Ensuite, les lettres G, L et S sont permutées circulairement : les lettres G, L et S s'échangent donc entre elles et, toutes les trois étapes, retrouvent leur disposition initiale. Enfin, les lettres O et I s'intervertissent : toutes les deux étapes, elles retrouvent leur disposition initiale. En d'autres termes, notre transformation est la composition d'une permutation circulaire d'ordre 3 affectant les lettres G, L, S et d'une transposition affectant les lettres O et I. Ainsi, pour tout nombre d'étapes multiple de 2 et de 3, c'est-à-dire multiple de 6, on retrouvera le mot GALOIS. Le nombre 647 est égal à $6 \times 107 + 5$. À la $642^{\text{ème}}$ étape ($642 = 6 \times 107$), le mot obtenu est donc GALOIS, auquel il faut encore ajouter 5 étapes : GALOIS, SAGIOL, LASOIG, GALIOS, SAGOIL, LASIOG. À la $647^{\text{ème}}$ étape, le mot obtenu est donc LASIOG. L'intérêt d'une telle démarche est double : elle est rapide, efficace et sûre, et s'adapte à n'importe quelle transformation.

Un exemple extrêmement pédagogique de "racines qui tournent", fourni par Norbert Verdier, dans le magazine Pour la Science Les génies de la Science consacré à Galois

Continuer de suivre Galois (Denise Chemla - 21/12/2013)

On cherche une équation polynomiale qui aurait ses racines qui se verraient permutées par une certaine fonction et dont les solutions seraient les décomposants de Goldbach de n, un nombre pair, i.e. les nombres premiers dont les complémentaires à n seraient premiers également.

On "sent bien" que le générateur doit sûrement être la fonction $f : x \mapsto n - x$ car cette fonction envoie chaque nombre entier sur son complémentaire à n, la somme de ces deux nombres permettant d'obtenir n.

On trouve donc l'inéquation polynomiale $x^2 - nx \neq 0$ qui est invariante par la fonction f. En effet, $(n-x)^2 - n(n-x) = x^2 + n^2 - 2nx - n^2 + nx = x^2 - nx$. On est conforté dans cette idée par le fait que le polynôme proposé est égal à $x(n-x)$:

- d'une part, ce polynôme s'annule lorsque x est nul et la congruence $x \not\equiv 0 \ (mod\ p_i)$ dans tous les corps premiers $\mathbb{Z}/p_i\mathbb{Z}$ pour p_i un nombre premier quelconque inférieur à $\sqrt{n}$ correspond au fait que x est un nombre premier supérieur à $\sqrt{n}$;

- d'autre part, ce polynôme s'annule lorsque $x = n$ et la congruence $x \not\equiv n \ (mod\ p_i)$ dans tous les corps premiers $\mathbb{Z}/p_i\mathbb{Z}$ pour p_i un nombre premier quelconque inférieur à $\sqrt{n}$ correspond au fait que le complémentaire de x à n est premier.

Il faudrait pour prouver la conjecture de Goldbach être assuré que cette inéquation polynomiale $x^2 - nx \neq 0$ a une solution commune inférieure à $n/2$ dans tous les corps premiers $\mathbb{Z}/p_i\mathbb{Z}$ avec p_i un nombre premier quelconque inférieur à $\sqrt{n}$.

Traitons l'exemple de la recherche des décompositions de Goldbach de 98.
Le polynôme $x^2 - 98x$ est égal à $x^2 - 2x$ dans $\mathbb{Z}/3\mathbb{Z}$ tandis qu'il est égal à $x^2 - 3x$ dans $\mathbb{Z}/5\mathbb{Z}$, ou encore égal à x^2 tout simplement dans $\mathbb{Z}/7\mathbb{Z}$ puisque 7 divise 98.

Notons dans un tableau pour les nombres premiers supérieurs à $\sqrt{98}$ et inférieurs à 49 la moitié de 98 les valeurs des polynômes en question et voyons ceux qui sont éliminés dans chacun des corps premiers.

	11	13	17	19	23	29	31	37	41	43	47
x^2 (dont on teste la nullité dans $\mathbb{Z}/7\mathbb{Z}$)	121	169	289	361	529	841	961	1369	1681	1849	2209
$x^2 - 2x$ (dont on teste la nullité dans $\mathbb{Z}/3\mathbb{Z}$)	~~99~~	143	~~255~~	323	~~483~~	~~783~~	899	1295	~~1599~~	1763	~~2115~~
$x^2 - 3x$ (dont on teste la nullité dans $\mathbb{Z}/5\mathbb{Z}$)	88	~~130~~	238	304	~~460~~	754	868	1258	1558	~~1720~~	2068

On voit que ne sont conservés que les nombres 19, 31 et 37 qui sont comme attendu les décomposants de Goldbach de 98.

Voir des analogies
(Denise Chemla - 23/12/2013)

Je ne fais pas des mathématiques au sens usuel du terme, au sens où l'entendent les vrais mathématiciens, puisque je ne suis pas capable de démontrer quoi que ce soit. En même temps, on ne peut pas tout à fait dire que ce que je poste soit de la broderie, ou du roman (encore que...), c'est de la prose tout du moins.

Je voudrais ici seulement fournir la manière dont je lie HR et CG.

Ce lien vient d'une formule lue dans le texte de la conférence MaMuX de M. Le Méhauté du 6 décembre 2013 à l'IRCAM :

$$\pi^{-s/2}\Gamma\Big(\frac{s}{2}\Big)\zeta(s) = \pi^{-(1-s)/2}\Gamma\Big(\frac{1-s}{2}\Big)\zeta(1-s)$$

On peut avoir la curiosité d'identifier s et $1-s$ car les termes à gauche et à droite du signe égal se ressemblent étrangement, à cette identification près.

En écrivant $s = 1-s$, on obtient $2s = 1$, et on peut penser que cela "correspond au fait" que les nombres premiers sont tous sur la droite de partie réelle $1/2$. L'hypothèse de Riemann établit un lien entre les zéros non-triviaux de la fonction ζ et les nombres premiers. On a entendu lors d'une conférence que si des nombres premiers (des zéros non triviaux en fait) s'avéraient ne pas être sur la droite en question, ils iraient par 2 et seraient symétriques l'un de l'autre par rapport à la droite $1/2$. En fait, pour CG, la ligne médiane de grilles, qu'on dénomme ligne de pliage du tissu, joue un peu ce rôle d'axe de symétrie. Les décomposants de Goldbach d'un nombre pair n sont symétriques l'un de l'autre par rapport au milieu $n/2$. Pour retrouver la formule correspondant à celle ci-dessus dans le cas de la conjecture de Goldbach, il faudrait remplacer le $(1-s)$, du côté droit du signe $=$ par $(n-s)$ de manière à obtenir par identification de s et $n-s$ comme on l'a fait plus haut $s = n-s \iff 2s = n$ qui est exactement la formulation de la conjecture de Goldbach lorsque n est le double d'un nombre premier.

Si on écoute sur la toile Grothendieck au Cern en 1972 ou bien Valette en 2010, on est encouragé à chercher de telles analogies mais franchement, sans le bagage technique qui permet de les interpréter, elles ne servent strictement à rien.

En mai 2009, j'avais proposé une méthode permettant de trouver les décomposants de Goldbach d'un nombre pair en calculant des produits de sinusoïdes. J'ai à nouveau présenté cette méthode sur un forum l'hiver dernier mais sans résultat.

J'ai enfin trouvé des références à propos de ces produits de sinus mais ils ne me permettent pas davantage d'avancer sur ce chemin-là :

- dans le fichier Berard-texte.pdf, à la page 3 sont présentés des exemples en dimension 1 : le problème de Dirichlet (sur la corde-segment) et le problème fermé (sur le cercle) ;

- dans le fichier Berard-transp.pdf, on voit apparaître le produit de sinus dans la page 8 concernant l'équation des ondes ; pages 13 et 14 sont présentés le problème de Dirichlet et le problème fermé ;

(DV, 3/1/14)

Conjecture de Goldbach et anagrammes de mots de restes

Denise Vella-Chemla

4/1/14

1 Introduction

On souhaite trouver une démonstration de la conjecture de Goldbach, qui stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers [1].

On propose dans ce but une modélisation qui associe à chaque nombre pair une matrice dont les éléments sont les lettres de "mots de restes".

Pour trouver les mots du nombre pair $n+2$ à partir de ceux du nombre pair n, on utilisera des règles de réécriture.

Il faudra alors caractériser l'existence d'un décomposant de Goldbach d'un nombre pair n par certaines conditions que vérifieront les mots de n.

Il faudra aussi fournir un certain "invariant" du processus de passage d'un pair au suivant, qui assurera que l'existence d'un décomposant de Goldbach pour n reste garantie pour $n+2$.

On essaiera enfin de caractériser les mots de nombres pairs particuliers :

- les doubles $2p$ de premiers p, qui vérifient trivialement la conjecture (puisque $2p = p + p$) ;
- les doubles $2.père$ de nombres pairs qui sont tels que $père - 1$ et $père + 1$ sont premiers tous les deux (les "pères de jumeaux").

2 Modélisation

A chaque nombre pair est associé une matrice dont les éléments ligne par ligne sont les lettres de mots.

Appelons K le nombre de nombres premiers impairs compris entre 3 et $n/2$. Appelons *milieu* le plus grand impair inférieur ou égal à $n/2$.

1. Dans l'égalité $n = p + q$ avec n pair supérieur à 2, p et q premiers, on appellera p et q décomposants de Goldbach de n ou sommants.

On peut oublier dans un premier temps l'idée de matrice pour ne garder à l'esprit que le fait qu'à chaque nombre pair n est associé un ensemble de $2K$ mots, qu'on appellera ses mots gris et ses mots bleus.

Sont ainsi associés à n :

- K mots gris, correspondant aux restes des divisions euclidiennes des nombres impairs compris entre 3 et *milieu* inclus par les nombres premiers impairs compris entre 3 et $\sqrt{n}$;
- K mots bleus, correspondant aux restes des divisions euclidiennes des nombres impairs compris entre *milieu* et $n-3$ inclus par les nombres premiers impairs compris entre 3 et $\sqrt{n}$.

Tous les mots associés au nombre pair n sont de longueur $\left\lfloor \frac{n/2-1}{2} \right\rfloor$.

Les mots de $n+2$:

- ont le même nombre de lettres que les mots de n si n est un double d'impair ;
- ont une lettre de plus que les mots de n si n est un double de pair.

Pour faciliter la lecture, on pourra intercaler des parenthèses autour d'ensemble de lettres mais ces parenthèses ne doivent pas être considérées comme des lettres.

Fournissons l'exemple des nombres pairs 40 et 42. La notation $f(n,p,G)$ dénote les lettres du mot gris associé à n : les divisions euclidiennes ont pour diviseur p. La notation $f(n,p,B)$ dénote les lettres du mot bleu associé à n : les divisions euclidiennes ont pour diviseur p. On a noté en première et dernière lignes en cyan les nombres auxquels correspondent les restes, pour se repérer un peu.

Mots de 40

	37	35	33	31	29	27	25	23	21
$f(40,5,B)$	2	0	3	1	4	2	0	3	1
$f(40,3,B)$	1	2	0	1	2	0	1	2	0
$f(40,5,G)$	3	0	2	4	1	3	0	2	4
$f(40,3,G)$	0	2	1	0	2	1	0	2	1
	3	5	7	9	11	13	15	17	19

Mots de 42

	39	37	35	33	31	29	27	25	23	21
$f(42,5,B)$	4	2	0	3	1	4	2	0	3	1
$f(42,3,B)$	0	1	2	0	1	2	0	1	2	0
$f(42,5,G)$	3	0	2	4	1	3	0	2	4	1
$f(42,3,G)$	0	2	1	0	2	1	0	2	1	0
	3	5	7	9	11	13	15	17	19	21

On reconnaît les séquences périodiques de restes modulaires chères à Gauss.

Comme il est trop fastidieux d'écrire des suites périodiques de lettres, on utilisera une notation indicée pour exprimer qu'un mot est une suite réitérée d'une même séquence de lettres et contenant un certain nombre de lettres.

Par exemple, $(120)_7$ sera le mot 1201201 qui s'obtient par répétition de la séquence des lettres 1, 2 et 0 et qui contient 7 lettres.

3 Réécriture, anagrammes

Pour passer d'un mot de n (par exemple, $f(n,p,G)$ (resp. $f(n,p,B)$) au mot de $n+2$ correspondant (i.e. $f(n+2,p,G)$ (resp. $f(n+2,p,B)$), on utilise deux règles de réécriture :

- permuter cycliquement les lettres d'un mot,
- concaténer une lettre à un mot.

Exprimons récursivement comment s'obtiennent les mots de $n+2$ à partir des mots de n.

En annexe sont fournis les mots des nombres pairs de 24 à 100.

4 Invariant

Il faut exprimer par un invariant cette perception que l'on a eue en regardant les grilles de divisibilité de "formes" qui restent fixes (en l'occurence les formes grises) ou sont translatées à droite (dans le cas des formes bleues) d'un nombre pair au suivant. Cette "invariance de forme" devrait assurer l'existence d'un "mot-colonne" sans lettre nulle dans chaque matrice de lettres.

5 Nombres premiers, nombres pères de jumeaux

Mots de 26 (double de 13 premier)

	23	21	19	17	15	13
$f(26,5,B)$	3	1	4	2	0	3
$f(26,3,B)$	2	0	1	2	0	1
$f(26,5,G)$	3	0	2	4	1	3
$f(26,3,G)$	0	2	1	0	2	1
	3	5	7	9	11	13

Mots de 34 (double de 17 premier)

	31	29	27	25	23	21	19	17
$f(34,5,B)$	1	4	2	0	3	1	4	2
$f(34,3,B)$	1	2	0	1	2	0	1	2
$f(34,5,G)$	3	0	2	4	1	3	0	2
$f(34,3,G)$	0	2	1	0	2	1	0	2
	3	5	7	9	11	13	15	17

On voit que les mots gris et bleus doivent bien sûr se terminer par la même lettre (puisqu'ils concernent les restes du même nombre p).

On constate également que le mot bleu s'obtient en effectuant une symétrie-miroir du mot gris, puis un certain nombre de shifts. Shift correspond à l'élévation à la puissance. Il faut trouver quelle est la condition sur les puissances qui a pour conséquence que les dernières lettres des mots sont identiques.

Annexe : mots des pairs de 24 à 100

On ne fournira les mots détaillés que pour les pairs jusqu'à 34.

Deux mots pour 24 (selon le seul module 3)

$f(24,3,G) = (021)_5 = 02102$
$f(24,3,B) = (012)_5 = 01201$

Quatre mots pour les pairs de 26 à 48 (selon les modules 3 et 5)

Précisons toutes les lettres des mots pour les pairs de 26 à 34 puis généralisons.

$$\begin{array}{lll} f(26,3,G) & = (021)_6 & = 021021 \\ f(26,5,G) & = (30241)_6 & = 302413 \\ f(26,3,B) & = (201)_6 & = 201201 \\ f(26,5,B) & = (31420)_6 & = 314203 \end{array}$$

$$\begin{array}{lll} f(28,3,G) & = (021)_6 & = 021021 \\ f(28,5,G) & = (30241)_6 & = 302413 \\ f(28,3,B) & = (120)_6 & = 12012 \\ f(28,5,B) & = (03142)_6 & = 031420 \end{array}$$

$$\begin{array}{lll} f(30,3,G) & = (021)_7 & = 0210210 \\ f(30,5,G) & = (30241)_7 & = 3024130 \\ f(30,3,B) & = (012)_7 & = 0120120 \\ f(30,5,B) & = (20314)_7 & = 2031420 \end{array}$$

$$\begin{array}{lll} f(32,3,G) & = (021)_7 & = 0210210 \\ f(32,5,G) & = (30241)_7 & = 3024130 \\ f(32,3,B) & = (201)_7 & = 2012012 \\ f(32,5,B) & = (42031)_7 & = 4203142 \end{array}$$

$$\begin{array}{lll} f(34,3,G) & = (021)_8 & = 02102102 \\ f(34,5,G) & = (30241)_8 & = 30241302 \\ f(34,3,B) & = (120)_8 & = 1201201 \\ f(34,5,B) & = (14203)_8 & = 14203142 \end{array}$$

Rappel : $NbCol = \left\lfloor \frac{n/2-1}{2} \right\rfloor$

$f(n, 3, G) = (021)_{NbCol}$

$f(n, 5, G) = (30241)_{NbCol}$

$f(n, 3, B) = (012)_{NbCol}$ pour n de la forme *6k*
$f(n, 3, B) = (201)_{NbCol}$ pour n de la forme *6k+2*
$f(n, 3, B) = (120)_{NbCol}$ pour n de la forme *6k+4*

$f(n, 5, B) = (20314)_{NbCol}$ pour n de la forme *10k*
$f(n, 5, B) = (42031)_{NbCol}$ pour n de la forme *10k+2*
$f(n, 5, B) = (14203)_{NbCol}$ pour n de la forme *10k+4*
$f(n, 5, B) = (31420)_{NbCol}$ pour n de la forme *10k+6*
$f(n, 5, B) = (03142)_{NbCol}$ pour n de la forme *10k+8*

Six mots pour les pairs de 50 à 100 (selon les modules 3, 5 et 7)

Les définitions sont reprises à l'identique par rapport aux précédentes pour les modules 3 et 5. Pour le module 7, on a :

$f(n, 7, G) = (5316420)_{NbCol}$
$f(n, 7, B) = (4205316)_{NbCol}$ pour n de la forme *14k*
$f(n, 7, B) = (6420531)_{NbCol}$ pour n de la forme *14k+2*
$f(n, 7, B) = (1642053)_{NbCol}$ pour n de la forme *14k+4*
$f(n, 7, B) = (3164205)_{NbCol}$ pour n de la forme *14k+6*
$f(n, 7, B) = (5316420)_{NbCol}$ pour n de la forme *14k+8*
$f(n, 7, B) = (0531642)_{NbCol}$ pour n de la forme *14k+10*
$f(n, 7, B) = (2053164)_{NbCol}$ pour n de la forme *14k+12*

Conjecture de Goldbach et disjonctions de mots cycliques

Denise Vella-Chemla

11/1/14

1 Introduction

On souhaite trouver une démonstration de la conjecture de Goldbach, qui stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers [1].

On propose dans ce but une modélisation qui associe à chaque nombre pair une matrice booléenne dont les lignes sont des "mots cycliques".

Pour trouver les mots du nombre pair $n+2$ à partir de ceux du nombre pair n, on utilisera la complétion d'un mot par une lettre respectant la cyclicité du mot, à droite ou à gauche, et la troncature de la lettre finale d'un mot.

Il faudra alors caractériser l'existence d'un décomposant de Goldbach d'un nombre pair n par une condition que vérifieront ses mots.

Il faudra aussi fournir un certain "invariant" du processus de passage d'un pair au suivant, qui assurera que l'existence d'un décomposant de Goldbach pour n reste garantie pour $n+2$.

On essaiera enfin de caractériser les mots de nombres pairs particuliers :

- les doubles $2p$ de premiers p, qui vérifient trivialement la conjecture (puisque $2p = p + p$) ;
- les doubles $2.père$ de nombres pairs qui sont tels que $père - 1$ et $père + 1$ sont premiers tous les deux (les "pères de jumeaux").

2 Modélisation

A chaque nombre pair est associé une matrice dont les lignes ont leurs éléments qui sont les lettres de mots cycliques représentant la divisibilité d'entiers successifs.

1. Dans l'égalité $n = p + q$ avec n pair supérieur à 2, p et q premiers, on appellera p et q décomposants de Goldbach de n ou sommants.

Appelons K le nombre de nombres premiers impairs compris entre 3 et $n/2$. Appelons *milieu* le plus grand impair inférieur ou égal à $n/2$.

On peut oublier dans un premier temps l'idée de matrice pour ne garder à l'esprit que le fait qu'à chaque nombre pair n est associé un ensemble de $2K$ mots, qu'on appellera ses mots gris et ses mots bleus.

Sont ainsi associés à n :

- K mots gris, correspondant aux caractères de divisibilité des nombres impairs compris entre 3 et *milieu* inclus, par les nombres premiers impairs compris entre 3 et $\sqrt{n}$;
- K mots bleus, correspondant aux caractères de divisibilité des nombres impairs compris entre $n-3$ et *milieu* inclus, par les nombres premiers impairs compris entre 3 et $\sqrt{n}$.

Tous les mots associés au nombre pair n sont de longueur $\left\lfloor \frac{n/2-1}{2} \right\rfloor$.

Les mots de $n+2$:

- ont le même nombre de lettres que les mots de n si n est un double d'impair ;
- ont une lettre de plus que les mots de n si n est un double de pair.

Fournissons l'exemple des nombres pairs 40 et 42. La notation $f(n,p,G)$ dénote les lettres du mot gris associé à n pour le nombre premier p. La notation $f(n,p,B)$ dénote les lettres du mot bleu associé à n pour le nombre premier p. On a noté en première et dernière lignes en cyan les nombres auxquels correspondent les booléens de divisibilité, pour se repérer un peu.

Mots de 40

	37	35	33	31	29	27	25	23	21
$f(40,5,B)$	0	1	0	0	0	0	1	0	0
$f(40,3,B)$	0	0	1	0	0	1	0	0	1
$f(40,5,G)$	0	1	0	0	0	0	1	0	0
$f(40,3,G)$	1	0	0	1	0	0	1	0	0
	3	5	7	9	11	13	15	17	19

Mots de 42

	39	37	35	33	31	29	27	25	23	21
$f(42,5,B)$	0	0	1	0	0	0	0	1	0	0
$f(42,3,B)$	1	0	0	1	0	0	1	0	0	1
$f(42,5,G)$	0	1	0	0	0	0	1	0	0	0
$f(42,3,G)$	1	0	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21

On reconnaît les séquences périodiques selon lesquelles les nombres sont barrés par l'algorithme d'Erathosthène.

3 Réécriture

Pour connaître les mots d'un nombre existent deux possibilités :

- trouver ses mots bleus à partir de ses mots gris (c'est la vision locale du processus) ;
- trouver ses mots bleus (resp. ses mots gris) à partir des mots bleus (resp. des mots gris) du nombre pair précédent, c'est la vision dynamique du processus).

3.1 Vision globale

Un mot gris du pair $n+2$ est identique pour toutes ses lettres au mot gris du pair précédent n. Si $n = 4k$, on complète ce mot à droite par une lettre en respectant la condition de cyclicité.

Un mot bleu du pair $n+2$ s'obtient toujours par complétion à gauche du mot bleu du pair précédent n. Si $n+2 = 4k$, alors on tronque ce mot en lui ôtant sa dernière lettre pour que le mot obtenu soit de la bonne longueur.

3.2 Vision locale

La première lettre 1 du mot gris $f(n, p, G)$ étant à la position i dans le mot, le mot bleu aura un 1 à la position $i + (n/2 \ mod \ p)$ et les positions des autres 1 de ce mot s'en déduiront pour que soit respectées les conditions de cyclicité.

En annexe sont fournis les mots des nombres pairs de 24 à 50.

4 Invariant

Il faudrait exprimer par un invariant cette perception que l'on a eue en regardant les grilles de divisibilité de "formes" qui restent fixes (dans le cas des formes grises) ou sont translatées à droite (dans le cas des formes bleues) d'un nombre pair au suivant. Cette "invariance de forme" devrait assurer l'existence d'un "mot-colonne" à lettres toutes nulles dans chaque matrice de lettres (cela équivaut à la nullité de la disjonction booléenne des éléments de la colonne).

On n'arrive pas pour l'instant à trouver un tel invariant.

Il faudrait maîtriser la manière dont certaines colonnes de la matrice de n se trouvent comme "permutées" pour devenir d'autres colonnes de la matrice de $n+2$ et pour ça, connaître précisément la combinatoire des permutations de lettres dans les mots booléens.

5 Nombres premiers, nombres pères de jumeaux

Mots de 26 (double de 13 premier)

	23	21	19	17	15	13
$f(26,5,B)$	0	0	0	0	1	0
$f(26,3,B)$	0	1	0	0	1	0
$f(26,5,G)$	0	1	0	0	0	0
$f(26,3,G)$	1	0	0	1	0	0
	3	5	7	9	11	13

Mots de 34 (double de 17 premier)

	31	29	27	25	23	21	19	17
$f(34,5,B)$	0	0	0	1	0	0	0	0
$f(34,3,B)$	0	0	1	0	0	1	0	0
$f(34,5,G)$	0	1	0	0	0	0	1	0
$f(34,3,G)$	1	0	0	1	0	0	1	0
	3	5	7	9	11	13	15	17

On voit que les mots gris et bleus doivent bien sûr se terminer par 0 (puisqu'ils concernent la divisibilité du nombre premier p, qui est par définition non divisible par tous les nombres premiers de 3 à $\sqrt{p}$).

Oublions maintenant les nombres-mémoires cyan et regroupons les mots gris et bleu concernant la divisibilité par 3 et les mots gris et bleu concernant la divisibilité par 5.

$f(34,5,B)$	0	0	0	1	0	0	0	0
$f(34,5,G)$	0	1	0	0	0	0	1	0
$f(34,3,B)$	0	0	1	0	0	1	0	0
$f(34,3,G)$	1	0	0	1	0	0	1	0

Que constatons-nous, après avoir colorié certaines lettres des grilles ? Qu'il y a exactement 3 lettres 0 à l'extrémité droite des mots bleus et gris concernant la divisibilité par 3 et qu'il y a exactement 5 lettres 0 à l'extrémité droite des mots bleus et gris concernant la divisibilité par 5.

En utilisant la vision locale, et si on compte tous les zéros à l'extrémité droite de la grille, on peut regarder la grille du double d'un nombre premier $n = 2p$ comme un goban (un plateau de jeu de go) et voir les lettres 1 comme délimitant une zone de 0 à l'extrémité droite de la grille. Le nombre de zéros appartenant à la zone ainsi délimitée semble toujours égal à la somme de nombres premiers p_k inférieurs à $\sqrt{n}$, i.e. selon chaque p_k, il reste à droite des dernières letres 1 des lignes p_k lettres 0 en tout. Cela est attendu, le nombre de zéros en question comptant exactement le nombre de p_k nombres successifs non-divisibles par p_k, il vaut p_k pour tous les doubles d'impairs lorsque p_k ne divise pas n. Donc, si le nombre de zéros "entourés" par la ligne de 1 est égal à $\sum_{p_k \ premier \ impair \leqslant \sqrt{n}} p_k$, n est un double de premier tandis que si le nombre de zéros est inférieur strictement au nombre en question, n est le double d'un nombre composé impair.

Le comptage des zéros de la zone à l'extrémité droite du goban pour les doubles

de pairs a toujours pour valeur $\sum_{p_k\ premier\ impair\ \leqslant\ \sqrt{n}}(p_k - 1)$. Si de plus, la dernière colonne ne contient que des zéros, n est le double d'un père de jumeaux.

Revenons alors aux nombres de la forme $p^2 + 1$ qui sont ceux pour lesquels il faut ajouter deux mots à l'ensemble de mots par rapport à l'ensemble des mots de leur pair précédent et observons la "petite zone du goban" pour les deux lignes de la divisibilité par le nombre premier p. Sans surprise, on constate que la zone contient "exactement le nombre de zéros qu'il faut", c'est à dire p.

6 Petit détour

Il s'agit ici d'essayer de comprendre à quelle condition une permutation cyclique "garde un zéro" dans le mot résultant de la disjonction booléenne de 2 mots.

On fournit la table de la disjonction booléenne, pour des mots cycliques de longueur impaires (en l'occurrence des mots de longueur 3 ou 5) ne contenant qu'une seule lettre 1). On constate que tout mot obtenu par une telle opération de disjonction contient toujours une lettre 0 au moins.

$\vee$	100	010	001
100	100	110	101
010	110	010	011
001	101	011	001

Mots cycliques de longueur 3 *contenant une seule lettre* 1

$\vee$	10000	01000	00100	00010	00001
10000	10000	11000	10100	10010	10001
01000	11000	01000	01100	01010	01001
00100	10100	01100	00100	00110	00101
00010	10010	01010	00110	00010	00011
00001	10001	01001	00101	00011	00001

Mots cycliques de longueur 5 *contenant une seule lettre* 1

On n'est pas étonné de constater le caractère commutatif de la disjonction booléenne, en voyant que des cases symétriques par rapport à la première diagonale de la table.

On est un peu plus étonné de constater des symétries-miroir entre différentes cases, mais elles s'expliquent vite. Ainsi $10000 \vee 00010 = 10010$ tandis que $01000 \vee 00001 = 01001$, c'est à dire que si on appelle *miroir* la fonction qui associe à un mot booléen son symétrique selon une symétrie-miroir (la première lettre du premier est la dernière lettre du second, la deuxième lettre du premier est l'avant-dernière lettre du second, etc), on a $x \vee y = z$ et $miroir(x) \vee miroir(y) = miroir(z)$.

Annexe : mots des pairs de 24 à 50

24	$3B$	1	0	0	1	0				
	$3G$	1	0	0	1	0				
			×	×		×				
26	$5B$	0	0	0	0	1	0			
	$5G$	0	1	0	0	0	0			
	$3B$	0	1	0	0	1	0			
	$3G$	1	0	0	1	0	0			
				×			×			
28	$5B$	1	0	0	0	0	1			
	$5G$	0	1	0	0	0	0			
	$3B$	0	0	1	0	0	1			
	$3G$	1	0	0	1	0	0			
						×				
30	$5B$	0	1	0	0	0	0	1		
	$5G$	0	1	0	0	0	0	1		
	$3B$	1	0	0	1	0	0	1		
	$3G$	1	0	0	1	0	0	1		
				×		×	×			
32	$5B$	0	0	1	0	0	0	0		
	$5G$	0	1	0	0	0	0	1		
	$3B$	0	1	0	0	1	0	0		
	$3G$	1	0	0	1	0	0	1		
							×			
34	$5B$	0	0	0	1	0	0	0	0	
	$5G$	0	1	0	0	0	0	1	0	
	$3B$	0	0	1	0	0	1	0	0	
	$3G$	1	0	0	1	0	0	1	0	
						×			×	
36	$5B$	0	0	0	0	1	0	0	0	
	$5G$	0	1	0	0	0	0	1	0	
	$3B$	1	0	0	1	0	0	1	0	
	$3G$	1	0	0	1	0	0	1	0	
				×			×		×	
38	$5B$	1	0	0	0	0	1	0	0	0
	$5G$	0	1	0	0	0	0	1	0	0
	$3B$	0	1	0	0	1	0	0	1	0
	$3G$	1	0	0	1	0	0	1	0	0
				×						×
40	$5B$	0	1	0	0	0	0	1	0	0
	$5G$	0	1	0	0	0	0	1	0	0
	$3B$	0	0	1	0	0	1	0	0	1
	$3G$	1	0	0	1	0	0	1	0	0
						×			×	

42	$5B$	0	0	1	0	0	0	0	1	0	0		
	$5G$	0	1	0	0	0	0	1	0	0	0		
	$3B$	1	0	0	1	0	0	1	0	0	1		
	$3G$	1	0	0	1	0	0	1	0	0	1		
						×	×			×			
44	$5B$	0	0	0	1	0	0	0	0	1	0		
	$5G$	0	1	0	0	0	0	1	0	0	0		
	$3B$	0	1	0	0	1	0	0	1	0	0		
	$3G$	1	0	0	1	0	0	1	0	0	1		
				×			×						
46	$5B$	0	0	0	0	1	0	0	0	0	1	0	
	$5G$	0	1	0	0	0	0	1	0	0	0	0	
	$3B$	0	0	1	0	0	1	0	0	1	0	0	
	$3G$	1	0	0	1	0	0	1	0	0	1	0	
									×			×	
48	$5B$	1	0	0	0	0	1	0	0	0	0	1	
	$5G$	0	1	0	0	0	0	1	0	0	0	0	
	$3B$	1	0	0	1	0	0	1	0	0	1	0	
	$3G$	1	0	0	1	0	0	1	0	0	1	0	
				×		×			×	×			
50	$7B$	0	0	0	0	0	0	1	0	0	0	0	0
	$7G$	0	0	1	0	0	0	0	0	0	1	0	0
	$5B$	0	1	0	0	0	0	1	0	0	0	0	1
	$5G$	0	1	0	0	0	0	1	0	0	0	0	1
	$3B$	0	1	0	0	1	0	0	1	0	0	1	0
	$3G$	1	0	0	1	0	0	1	0	0	1	0	0
							×			×			

Une drôle de relation (D.Chemla, 13/1/14)

On voudrait comprendre comment s'étend une certaine relation r entre mots booléens, au fur et à mesure que la longueur des mots augmente.

La relation r est définie de la façon suivante :

$$r(m1, m2) \iff m1 \textit{ et } m2 \textit{ ont au moins une lettre } 0 \textit{ à la même position}$$

Fournissons les tables de r pour les mots de 2 lettres (qui sont au nombre de 4) et 3 lettres (qui sont au nombre de 8).

r	00	01	10	11
00	1	1	1	0
01	1	1	0	0
10	1	0	1	0
11	0	0	0	0

r	000	001	010	011	100	101	110	111
000	1	1	1	1	1	1	1	0
001	1	1	1	1	1	1	0	0
010	1	1	1	1	1	0	1	0
011	1	1	1	1	0	0	0	0
100	1	1	1	0	1	1	1	0
101	1	1	0	0	1	1	0	0
110	1	0	1	0	1	0	1	0
111	0	0	0	0	0	0	0	0

Conjecture de Goldbach, mots booléens et loi de réciprocité quadratique

Denise Vella-Chemla

14/1/14

1 Introduction

On souhaite trouver une démonstration de la conjecture de Goldbach, qui stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers [1].

On se propose dans ce but d'utiliser conjointement deux modélisations :

- l'une qui associe à chaque nombre pair n deux "mots booléens de primalité" m_1 et m_2 qui caractérisent la primalité des nombres impairs x (compris entre 3 et $n/2$) et $n-x$;
- l'autre qui associe à chaque nombre pair n deux "mots booléens de résiduosité quadratique" rq_1 et rq_2 qui caractérisent la résiduosité quadratique des nombres x et $n-x$ à n.

Le nombre pair n a un décomposant de Goldbach si ses mots m_1 et m_2 ont tous les deux une lettre 0 à une position commune.

2 Mots booléens de primalité

Appelons *milieu* le plus grand impair inférieur ou égal à $n/2$.

Deux mots booléens de primalité m_1 et m_2 sont associés à n :

- m_1 correspond aux caractères de primalité (le booléen 0 signifie qu'un nombre est premier et supérieur à $\sqrt{n}$, le booléen 1 signifie qu'il est composé ou premier inférieur à $\sqrt{n}$) des nombres impairs compris entre 3 et *milieu* inclus ;
- m_2 correspond aux caractères de primalité des nombres impairs compris entre $n-3$ et *milieu* inclus.

Les mots m_1 et m_2 associés au nombre pair n sont de longueur $\left\lfloor \frac{n/2-1}{2} \right\rfloor$. La longueur des mots augmente donc de 1 à chaque double d'impair, i.e. une fois sur deux.

1. Dans l'égalité $n = p + q$ avec n pair supérieur à 2, p et q premiers, on appellera p et q décomposants de Goldbach de n ou sommants.

Note : on a pris pour habitude de fournir le mot m_2 en première ligne et le mot m_1 en deuxième ligne (3 en bas à gauche, $n-3$ en haut à gauche).

Exemples :
Mots m_1 et m_2 de 40

	37	35	33	31	29	27	25	23	21
m_2	0	1	1	0	0	1	1	0	1
m_1	1	1	0	1	0	0	1	0	0
	3	5	7	9	11	13	15	17	19

Mots m_1 et m_2 de 42

	39	37	35	33	31	29	27	25	23	21
m_2	1	0	1	1	0	0	1	1	0	1
m_1	1	1	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21

Mots m_1 et m_2 de 44

	41	39	37	35	33	31	29	27	25	23
m_2	0	1	0	1	1	0	0	1	1	0
m_1	1	1	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21

3 Mots booléens de résiduosité quadratique

Deux mots booléens de résiduosité quadratique rq_1 et rq_2 sont associés à n :

- rq_1 correspond aux caractères de résiduosité quadratique à n (le booléen 1 signifie qu'un nombre est résidu quadratique de n, le booléen 0 signifie qu'il ne l'est pas) des nombres impairs compris entre 3 et *milieu* inclus ;
- rq_2 correspond aux caractères de résiduosité quadratique à n des nombres impairs compris entre $n-3$ et *milieu* inclus.

Exemples :
Mots rq_1 et rq_2 de 40 *(*9 *et* 25 *en sont résidus quadratiques)*

	37	35	33	31	29	27	25	23	21
rq_2	0	0	0	0	0	0	1	0	0
rq_1	0	0	0	1	0	0	0	0	0
	3	5	7	9	11	13	15	17	19

Mots rq_1 et rq_2 de 42 *(*$7, 9, 15, 21, 25, 37$ *et* 39 *en sont résidus quadratiques)*

	39	37	35	33	31	29	27	25	23	21
rq_2	1	1	0	0	0	0	0	1	0	1
rq_1	0	0	1	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21

Mots rq_1 et rq_2 de 44 (5, 9, 25, 33 et 37 en sont résidus quadratiques)

	41	39	37	35	33	31	29	27	25	23
rq_2	0	0	1	0	1	0	0	0	1	0
rq_1	0	1	0	1	0	0	0	0	0	0
	3	5	7	9	11	13	15	17	19	21

4 Constats

Rappelons d'abord le contenu de la loi de réciprocité quadratique d'une façon imagée, qui frappe notre aire visuelle. Elle a été démontrée de multiples façons par Gauss (il l'appelait le théorème d'or pour évoquer sa richesse).

Pour les nombres premiers p, il y a exactement $\frac{p-1}{2}$ nombres inférieurs à p qui sont résidus quadratiques de p.

On les note dans les tableaux par un petit trait au-dessus. Ils "sont en face" (leur somme vaut p) lorsque p est de la forme $4k+1$ (dans l'exemple du nombre premier 13 ci-dessous) ou "ne sont pas en face" (auquel cas, il y a un résidu quadratique par colonne) lorsque p est de la forme $4k+3$ (nombre premier 19 ci-dessous).

Résidus quadratiques de 13 de la forme $4k+1$

$\overline{12}$	11	$\overline{10}$	$\overline{9}$	8	7
$\overline{1}$	2	$\overline{3}$	$\overline{4}$	5	6

Résidus quadratiques de 19 de la forme $4k+3$

18	$\overline{17}$	$\overline{16}$	15	14	13	12	$\overline{11}$	10
$\overline{1}$	2	3	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	8	$\overline{9}$

La loi de réciprocité quadratique peut s'exprimer de la façon suivante : soient p et q deux entiers premiers impairs :

- si l'un au moins est de la forme $4k+1$, alors p est résidu quadratique de q si et seulement si q l'est de p ;
- si p et q sont tous deux de la forme $4k+3$ alors p est résidu quadratique de q si et seulement si q n'est pas résidu quadratique de p [2]

Les nombres pairs $2p$ doubles de nombres premiers p de la forme $4k+1$ ont $\frac{p-1}{2}$ résidus quadratiques (26 en a 6) tandis que les doubles de $4k+3$ en ont $\frac{p+1}{2}$ (38 en a 10). Ils sont face à face pour les doubles de premiers de la forme $4k+1$ et il y en a un par colonne pour les doubles de premiers de la forme $4k+3$ (sauf dans la dernière colonne qui fournit le caractère de résiduosité quadratique à $2p$

2. article 151 page 116 des Recherches arithmétiques : "il s'ensuit que la relation de p à q est la même que celle de q à p quand p ou q est de la forme $4k+1$, et qu'elle est inverse quand p et q sont de la forme $4k+3$.

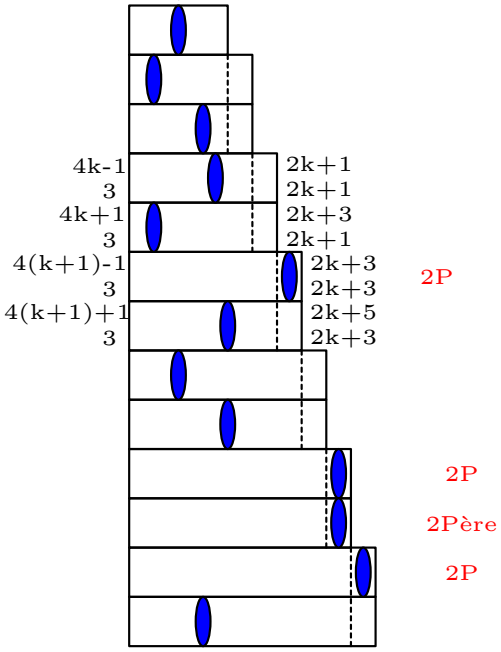
de p, et dans rq_1, et dans rq_2).

Les nombres pairs de la forme p^2+1 ont leurs résidus quadratiques ou non-résidus quadratiques complémentaires à n "face à face", ce quelle que soit leur forme.

Un nombre premier p est résidu quadratique de son double (il se trouve être congru à son propre carré) car $p^2 = \left(\frac{p-1}{2}\right)(2p) + p$.

5 Objectif

Peut-être qu'en mélangeant intelligemment le contenu de ces deux sortes de tableaux, de ces deux types de connaissances que sont, d'une part, le fait que dans le premier cas, on passe des mots m_1 et m_2 d'un nombre pair aux mots m_1 et m_2 du nombre pair suivant uniquement en concaténant à m_1 une lettre à droite et en concaténant à m_2 une lettre à gauche voire en lui en retirant une à droite un coup sur deux, cumulé à d'autre part, tout ce qui est connu des mathématiciens en terme de conséquences de la loi de réciprocité quadratique, pourrait-on parvenir à obtenir une démonstration du fait que les mots m_1 et m_2 ont toujours une lettre 0 à une position commune, ce qui démontrerait la conjecture de Goldbach.
Fournissons ci-dessous une représentation graphique du processus. Les ellipses bleues représentent une décomposition de Goldbach qui irait se déplaçant de pair en pair. Lorsque l'ellipse est en dernière colonne, n est un double de nombre premier. Lorsque 3 dernières colonnes vides se succèdent pour 3 pairs consécutifs, les nombres en question sont deux doubles de nombres premiers encadrant un double de "père de jumeaux".



Annexe 1 : résidus quadratiques des nombres pairs de 24 à 50

24 : 1 9

26 : 1 3 9 13 17 23 25

28 : 1 9 21 25

30 : 1 9 15 19 21 25

32 : 1 9 17 25

34 : 1 9 13 15 17 19 21 25 33

36 : 1 9 13 25

38 : 1 5 7 9 11 17 19 23 25 35

40 : 1 9 25

42 : 1 7 9 15 21 25 37 39

44 : 1 5 9 25 33 37

46 : 1 3 9 13 23 25 27 29 31 35 39 41

48 : 1 9 25 33

50 : 1 9 11 19 21 25 29 31 39 41 49

Annexe 2 : Mots m_1, m_2, rq_1, rq_2 pour les nombres pairs de 24 à 50

24	m_2	1	0	0	1	0			
	m_1	1	0	0	1	0			
	rq_2	0	0	0	0	0			
	rq_1	0	0	0	1	0			
26	m_2	0	1	0	0	1	0		
	m_1	1	1	0	1	0	0		
	rq_2	1	0	0	1	0	1		
	rq_1	1	0	0	1	0	1		
28	m_2	1	0	1	0	0	1		
	m_1	1	1	0	1	0	0		
	rq_2	1	0	1	0	0	0		
	rq_1	0	0	0	1	0	0		
30	m_2	1	1	0	1	0	0	1	
	m_1	1	1	0	1	0	0	1	
	rq_2	0	1	0	1	1	0	1	
	rq_1	0	0	0	1	0	0	1	
32	m_2	0	1	1	0	1	0	0	
	m_1	1	1	0	1	0	0	1	
	rq_2	0	0	1	0	0	0	1	
	rq_1	0	0	0	1	0	0	0	
34	m_2	0	0	1	1	0	1	0	0
	m_1	1	1	0	1	0	0	1	0
	rq_2	0	0	0	1	0	1	1	1
	rq_1	0	0	0	1	0	1	1	1
36	m_2	1	0	0	1	1	0	1	0
	m_1	1	1	0	1	0	0	1	0
	rq_2	0	0	0	0	1	0	0	0
	rq_1	0	0	0	1	0	1	0	0
38	m_2	1	1	0	0	1	1	0	1	0
	m_1	1	1	0	1	0	0	1	0	0
	rq_2	1	0	0	0	0	1	1	0	1
	rq_1	0	1	1	1	1	0	0	1	1
40	m_2	0	1	1	0	0	1	1	0	1
	m_1	1	1	0	1	0	0	1	0	0
	rq_2	0	0	0	0	0	0	1	0	0
	rq_1	0	0	0	1	0	0	0	0	0

42	m_2	1	0	1	1	0	0	1	1	0	1	
	m_1	1	1	0	1	0	0	1	0	0	1	
	rq_2	1	1	0	0	0	0	0	1	0	1	
	rq_1	0	0	1	1	0	0	1	0	0	1	
44	m_2	0	1	0	1	1	0	0	1	1	0	
	m_1	1	1	0	1	0	0	1	0	0	1	
	rq_2	0	0	1	0	1	0	0	0	1	0	
	rq_1	0	1	0	1	0	0	0	0	0	0	
46	m_2	0	0	1	0	1	1	0	0	1	1	0
	m_1	1	1	0	1	0	0	1	0	0	1	0
	rq_2	0	1	1	0	1	0	1	1	1	1	1
	rq_1	1	0	0	1	0	1	0	0	0	0	1
48	m_2	1	0	0	1	0	1	1	0	0	1	1
	m_1	1	1	0	1	0	0	1	0	0	1	0
	rq_2	0	0	0	0	0	0	1	0	0	0	1
	rq_1	0	0	0	1	0	0	0	0	0	0	0
50	m_2	0	1	0	0	1	0	1	1	0	0	1	1
	m_1	1	1	1	1	0	0	1	0	0	1	0	1
	rq_2	0	0	0	1	1	0	0	0	1	1	0	1
	rq_1	0	0	0	1	1	0	0	0	1	1	0	1

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

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

[...]

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

Conjecture de Goldbach, mots booléens et invariant

Denise Vella-Chemla

29/1/14

1 Introduction

On souhaite trouver une démonstration de la conjecture de Goldbach, qui stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers [1].

On se propose dans ce but d'utiliser une modélisation qui associe à chaque nombre pair n un "mot booléen de primalité" m qui code la primalité des nombres impairs x (compris entre 3 et et $n-3$).

On identifiera le processus permettant de passer du mot booléen d'un nombre pair n au mot booléen du nombre pair suivant $n+2$.

On caractérisera l'existence d'un décomposant de Goldbach d'un nombre pair par une condition que vérifie son mot booléen.

On essaiera de trouver une contrainte invariante respectée par les mots booléens des nombres pairs successifs qui assurera que l'existence d'un décomposant de Goldbach est toujours conservée.

2 Mot booléen d'un nombre pair

On choisit de représenter le fait qu'un entier est premier par le booléen 0 et le fait qu'il est composé par le booléen 1.

On appelle $sym(m)$ la fonction qui associe à un mot m son symétrique, i.e. le mot contenant les lettres de m depuis la dernière jusqu'à la première.

Appelons *milieu* le plus grand nombre entier impair inférieur ou égal à $n/2$.

1. Dans l'égalité $n = p + q$ avec n pair supérieur à 2, p et q premiers, on appellera p et q décomposants de Goldbach de n ou sommants.

A chaque nombre pair n sont associés deux mots booléens m_1 et m_2 définis de la façon suivante :

- les lettres de m_1 sont les caractères de primalité des nombres impairs compris entre 3 et *milieu* inclus ;
- les lettres de m_2 sont les caractères de primalité des nombres impairs compris entre $n-3$ et *milieu* inclus.

Les mots m_1 et m_2 associés au nombre pair n sont de longueur $\left\lfloor \frac{n/2-1}{2} \right\rfloor$. La longueur des mots augmente donc de 1 à chaque double d'impair, i.e. une fois sur deux.

Le mot booléen m du nombre pair n est la concaténation des deux mots suivants :

- m_1 ;
- $sym(m_2)$, le symétrique de m_2.

Note : on a pris pour habitude de fournir le mot m_2 en première ligne et le mot m_1 en deuxième ligne (3 en bas à gauche, $n-3$ en haut à gauche). On constate que pour les doubles d'impairs, la lettre codant le caractère de primalité de l'entier *milieu* est doublée.

Exemples : Ci-dessous les mots m_1, m_2 et m des nombres 40, 42 et 44.

40	37	35	33	31	29	27	25	23	21									
m_2	0	1	1	0	0	1	1	0	1									
m_1	0	0	0	1	0	0	1	0	0									
	3	5	7	9	11	13	15	17	19									
m	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0

42	39	37	35	33	31	29	27	25	23	21									
m_2	1	0	1	1	0	0	1	1	0	1									
m_1	0	0	0	1	0	0	1	0	0	1									
	3	5	7	9	11	13	15	17	19	21									
m	0	0	0	1	0	0	1	0	0	1	1	0	1	1	0	0	1	1	0	1

44	41	39	37	35	33	31	29	27	25	23										
m_2	0	1	0	1	1	0	0	1	1	0										
m_1	0	0	0	1	0	0	1	0	0	1										
	3	5	7	9	11	13	15	17	19	21										
m	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0

3 Identifier ce que fait le processus

Reprenons les mots des nombres pairs 24 à 34.

24	m_2	1	0	0	1	0											
	m_1	0	0	0	1	0											
	m	0	0	0	1	0	|	0	1	0	0	1					
26	m_2	0	1	0	0	1	0										
	m_1	0	0	0	1	0	0										
	m	0	0	0	1	0	0	|	0	1	0	0	1	0			
28	m_2	1	0	1	0	0	1										
	m_1	0	0	0	1	0	0										
	m	0	0	0	1	0	0	|	1	0	0	1	0	1			
30	m_2	1	1	0	1	0	0	1									
	m_1	0	0	0	1	0	0	1									
	m	0	0	0	1	0	0	1	|	1	0	0	1	0	1	1	
32	m_2	0	1	1	0	1	0	0									
	m_1	0	0	0	1	0	0	1									
	m	0	0	0	1	0	0	1	|	0	0	1	0	1	1	0	
34	m_2	0	0	1	1	0	1	0	0								
	m_1	0	0	0	1	0	0	1	0								
	m	0	0	0	1	0	0	1	0	|	0	0	1	0	1	1	0	0

On voit que si au nombre pair n est associé un mot booléen de longueur $2i$, le processus qui permet d'obtenir le mot booléen associé au nombre pair $n+2$ effectue plusieurs actions différentes :

- 1) *travail sur la lettre à la position* $i+1$: dans le cas où n est un double d'impair, le mot de $n+2$ est obtenu en enlevant du mot de n la lettre à la position $i+1$; dans le cas où n est un double de pair, le mot de $n+2$ est obtenu en dupliquant cette lettre à la position $i+1$;
- 2) *concaténation en fin du mot :* dans tous les cas, est concaténée à la fin du mot booléen ainsi obtenu la lettre qui caractérise la primalité du nombre entier $2n-3$ pour obtenir le mot de $n+2$.

4 Caractériser une décomposition de Goldbach

Il faut maintenant être capable de caractériser par une condition sur le mot m la présence à une même position dans les mots m_1 et m_2 d'une lettre 0.

Cette caractérisation est simple :

- un double d'impair n se décompose en somme de deux nombres premiers $p = 2i+1$ et $q = 2j-1$ si et seulement si le mot m de n contient une lettre 0 à la position i et une lettre 0 à la position j ;
- un double de pair n se décompose en somme de deux nombres premiers $p = 2i+1$ et $q = 2j+1$ si et seulement si le mot m de n contient une

lettre 0 à la position i et une lettre 0 à la position j.

On note que la somme des positions i et j des deux 0 dans le mot m est toujours un nombre impair.

5 Invariant

Supposons que le mot n admet une décomposition de Goldbach. Essayons de comprendre pourquoi une décomposition va également exister pour $n+2$.

L'invariant est à rechercher dans la liste des positions des 0 successifs dans le mot m.

Si lors de l'étape de concaténation, on concatène la lettre 0 pour obtenir le mot de $n+2$, l'existence d'une décomposition de Goldbach est garantie par le fait que $n+2$ se décompose en $3+(n-1)$.

Dans le cas contraire, si lors de l'étape de concaténation, on concatène un 1 pour obtenir le mot de $n+2$, alors 4 cas sont à considérer, selon que la longueur de la chaîne est conservée ou bien incrémentée de 2 :

- la chaîne conserve sa longueur et on enlève la lettre 0 à la position $i+1$; les mots m_1 et m_2 de $n+2$ ont les formes suivantes :

m_2	1	1	$-$	$-$	$\ldots$	$-$	0	$\ldots$	$-$
m_1	0	0	0	1	$\ldots$	0	$-$	$\ldots$	0

  La lettre 0 en fin de m_1 est justifiée par le fait que si la longueur des mots est conservée, n est forcément un double d'impair premier. On ne voit pas encore ce qui garantit qu'ils contiennent une lettre 0 à une position commune ;

- la chaîne conserve sa longueur et on enlève la lettre 1 à la position $i+1$; les mots m_1 et m_2 de $n+2$ ont les formes suivantes :

m_2	1	$-$	$-$	$-$	$\ldots$	$-$	0	$\ldots$	$-$
m_1	0	0	0	1	$\ldots$	0	$-$	$\ldots$	1

  La lettre 1 en fin de m_1 est justifiée par le fait que si la longueur des mots est conservée, n est forcément un double d'impair composé. On ne voit pas encore ce qui garantit qu'ils contiennent une lettre 0 à une position commune ;

- la chaîne voit sa longueur incrémentée de 2 et la lettre 0 en position $i+1$ est dupliquée ; alors $n+2$ est le double d'un nombre premier p et admet une décomposition de Goldbach triviale $p+p$.

- la chaîne voit sa longueur incrémentée de 2 et la lettre 1 en position $i+1$ est dupliquée ; alors $n+2$ est le double d'un nombre composé, ce qui justifie les lettres 1 en fin des mots m_1 et m_2 ; les mots m_1 et m_2 de $n+2$ ont les formes suivantes :

m_2	1	$-$	$-$	$-$	$\ldots$	$-$	0	$\ldots$	1
m_1	0	0	0	1	$\ldots$	0	$-$	$\ldots$	1

On ne voit pas encore ce qui garantit qu'ils contiennent une lettre 0 à une position commune ;

Annexe : Mots m_1, m_2 des nombres pairs de 24 à 50

24	m_2	1	0	0	1	0										
	m_1	1	0	0	1	0										
26	m_2	0	1	0	0	1	0									
	m_1	1	1	0	1	0	0									
28	m_2	1	0	1	0	0	1									
	m_1	1	1	0	1	0	0									
30	m_2	1	1	0	1	0	0	1								
	m_1	1	1	0	1	0	0	1								
32	m_2	0	1	1	0	1	0	0								
	m_1	1	1	0	1	0	0	1								
34	m_2	0	0	1	1	0	1	0	0							
	m_1	1	1	0	1	0	0	1	0							
36	m_2	1	0	0	1	1	0	1	0							
	m_1	1	1	0	1	0	0	1	0							
38	m_2	1	1	0	0	1	1	0	1	0						
	m_1	1	1	0	1	0	0	1	0	0						
40	m_2	0	1	1	0	0	1	1	0	1						
	m_1	1	1	0	1	0	0	1	0	0						
42	m_2	1	0	1	1	0	0	1	1	0	1					
	m_1	1	1	0	1	0	0	1	0	0	1					
44	m_2	0	1	0	1	1	0	0	1	1	0					
	m_1	1	1	0	1	0	0	1	0	0	1					
46	m_2	0	0	1	0	1	1	0	0	1	1	0				
	m_1	1	1	0	1	0	0	1	0	0	1	0				
48	m_2	1	0	0	1	0	1	1	0	0	1	1				
	m_1	1	1	0	1	0	0	1	0	0	1	0				
50	m_2	0	1	0	0	1	0	1	1	0	0	1	1			
	m_1	1	1	1	1	0	0	1	0	0	1	0	1			
52	m_2	1	0	1	0	0	1	0	1	1	0	0	1			
	m_1	0	0	0	1	0	0	1	0	0	1	0	1			
54	m_2	1	1	0	1	0	0	1	0	1	1	0	0	1		
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1		
56	m_2	0	1	1	0	1	0	0	1	0	1	1	0	0		
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1		
58	m_2	1	0	1	1	0	1	0	0	1	0	1	1	0	0	
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	
60	m_2	1	1	0	1	1	0	1	0	0	1	0	1	1	0	
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	
62	m_2	0	1	1	0	1	1	0	1	0	0	1	0	1	1	0
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0
64	m_2	0	0	1	1	0	1	1	0	1	0	0	1	0	1	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0
66	m_2	1	0	0	1	1	0	1	1	0	1	0	0	1	0	1	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1
68	m_2	1	1	0	0	1	1	0	1	1	0	1	0	0	1	0	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1

70	m_2	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1	0	1						
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1						
72	m_2	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1	0						
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1						
74	m_2	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1	0					
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0					
76	m_2	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1					
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0					
78	m_2	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1				
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1				
80	m_2	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0				
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1				
82	m_2	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0			
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0			
84	m_2	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0			
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0			
86	m_2	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0		
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0		
88	m_2	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1		
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0		
90	m_2	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	
92	m_2	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	
94	m_2	1	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0
96	m_2	1	1	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0
98	m_2	1	1	1	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0	1
100	m_2	0	1	1	1	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0	1

Conjecture de Goldbach, mots booléens, parité, imparité, invariant

Denise Vella-Chemla

2/2/14

1 Introduction

On souhaite trouver une démonstration de la conjecture de Goldbach, qui stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers [1].

On se propose dans ce but d'utiliser une modélisation qui associe à chaque nombre pair n un "mot booléen de primalité" m qui code la primalité des nombres impairs x (compris entre 3 et et $n-3$).

On identifiera le processus permettant de passer du mot booléen d'un nombre pair n au mot booléen du nombre pair suivant $n+2$.

On caractérisera l'existence d'un décomposant de Goldbach d'un nombre pair par une condition que vérifie son mot booléen.

On essaiera de trouver une contrainte invariante respectée par les mots booléens des nombres pairs successifs qui assurera que l'existence d'un décomposant de Goldbach est toujours conservée.

2 Mot booléen d'un nombre pair

On choisit de représenter le fait qu'un entier est premier par le booléen 0 et le fait qu'il est composé par le booléen 1.

On appelle $sym(m)$ la fonction qui associe à un mot m son symétrique, i.e. le mot contenant les lettres de m depuis la dernière jusqu'à la première.

Appelons *milieu* le plus grand nombre entier impair inférieur ou égal à $n/2$.

1. Dans l'égalité $n = p + q$ avec n pair supérieur à 2, p et q premiers, on appellera p et q décomposants de Goldbach de n ou sommants.

A chaque nombre pair n sont associés deux mots booléens m_1 et m_2 définis de la façon suivante :

- les lettres de m_1 sont les caractères de primalité des nombres impairs compris entre 3 et *milieu* inclus ;
- les lettres de m_2 sont les caractères de primalité des nombres impairs compris entre $n-3$ et *milieu* inclus.

Les mots m_1 et m_2 associés au nombre pair n sont de longueur $\left\lfloor \frac{n/2-1}{2} \right\rfloor$. La longueur des mots augmente donc de 1 à chaque double d'impair, i.e. une fois sur deux.

Le mot booléen m du nombre pair n est la concaténation des deux mots suivants :

- m_1 ;
- $sym(m_2)$, le symétrique de m_2.

Note : on a pris pour habitude de fournir le mot m_2 en première ligne et le mot m_1 en deuxième ligne (3 en bas à gauche, $n-3$ en haut à gauche). On constate que pour les doubles d'impairs, la lettre codant le caractère de primalité de l'entier *milieu* est doublée.

Exemples : Ci-dessous les mots m_1, m_2 et m des nombres 40, 42 et 44.

40	37	35	33	31	29	27	25	23	21								
m_2	0	1	1	0	0	1	1	0	1								
m_1	0	0	0	1	0	0	1	0	0								
	3	5	7	9	11	13	15	17	19								
m	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0

42	39	37	35	33	31	29	27	25	23	21									
m_2	1	0	1	1	0	0	1	1	0	1									
m_1	0	0	0	1	0	0	1	0	0	1									
	3	5	7	9	11	13	15	17	19	21									
m	0	0	0	1	0	0	1	0	0	1	1	0	1	1	0	0	1	1	0	1

44	41	39	37	35	33	31	29	27	25	23										
m_2	0	1	0	1	1	0	0	1	1	0										
m_1	0	0	0	1	0	0	1	0	0	1										
	3	5	7	9	11	13	15	17	19	21										
m	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0

3 Identifier ce que fait le processus

Reprenons les mots des nombres pairs 24 à 34.

24	m_2	1	0	0	1	0											
	m_1	0	0	0	1	0											
	m	0	0	0	1	0	|	0	1	0	0	1					
26	m_2	0	1	0	0	1	0										
	m_1	0	0	0	1	0	0										
	m	0	0	0	1	0	0	|	0	1	0	0	1	0			
28	m_2	1	0	1	0	0	1										
	m_1	0	0	0	1	0	0										
	m	0	0	0	1	0	0	|	1	0	0	1	0	1			
30	m_2	1	1	0	1	0	0	1									
	m_1	0	0	0	1	0	0	1									
	m	0	0	0	1	0	0	1	|	1	0	0	1	0	1	1	
32	m_2	0	1	1	0	1	0	0									
	m_1	0	0	0	1	0	0	1									
	m	0	0	0	1	0	0	1	|	0	0	1	0	1	1	0	
34	m_2	0	0	1	1	0	1	0	0								
	m_1	0	0	0	1	0	0	1	0								
	m	0	0	0	1	0	0	1	0	|	0	0	1	0	1	1	0	0

On voit que si au nombre pair n est associé un mot booléen de longueur $2i$, le processus qui permet d'obtenir le mot booléen associé au nombre pair $n+2$ effectue plusieurs actions différentes :

- *travail sur la lettre à la position* $i+1$ (on a coloré cette lettre en bleu dans le tableau ci-dessus) : dans le cas où n est un double d'impair, le mot de $n+2$ est obtenu en enlevant du mot de n la lettre à la position $i+1$; dans le cas où n est un double de pair, le mot de $n+2$ est obtenu en dupliquant cette lettre à la position $i+1$;
- *concaténation en fin du mot :* dans tous les cas, est concaténée à la fin du mot booléen ainsi obtenu la lettre qui caractérise la primalité du nombre entier $2n-3$ pour obtenir le mot de $n+2$. *Remarque :* la concaténation est une opération non-commutative. Par exemple, $1(110) = 1110$ alors que $(110)1 = 1101$.

4 Caractériser l'existence d'une décomposition de Goldbach dans le mot d'un nombre pair

Il faut maintenant être capable de caractériser par une condition sur le mot m la présence à une même position dans les mots m_1 et m_2 d'une lettre 0.

Rappelons quelques éléments de logique booléenne.

La conjonction logique est définie par :

$$1 \wedge 0 = 0 \wedge 1 = 0 \wedge 0 = 0 \text{ et } 1 \wedge 1 = 1.$$

La négation logique est définie par :

$$\neg 0 = 1 \text{ et } \neg 1 = 0.$$

Si l'on appelle $l(m, i)$ la lettre à la position i dans le mot m, alors l'existence d'une décomposition de Goldbach est équivalente à la condition :

$$\Big[\sum_{1 \leqslant i \leqslant \lfloor \frac{n/2-1}{2} \rfloor, i+j=\lfloor \frac{n}{2} \rfloor} \neg l(m,i) \wedge \neg l(m,j) \Big] = 1$$

5 Invariant

Supposons que le mot n admet une décomposition de Goldbach. Essayons de comprendre pourquoi une décomposition va également exister pour $n + 2$.

Les lettres 0 et 1 ne se trouvent pas réparties "n'importe comment" dans les mots m_1 et m_2, au fur et à mesure du déroulement du processus : une condition est toujours vérifiée par les lettres et qui correspond au fait qu'un multiple quelconque d'un nombre non nul est composé. On appelle une telle condition toujours vérifiée un invariant de l'algorithme.

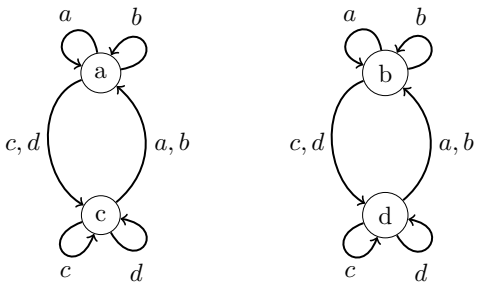
$$\forall\, 0 < i \leqslant n/2,\ \forall k \leqslant n/3, l(m, i + k(2i + 1)) = 1.$$

D'autre part, la condition dont il faut démontrer l'invariance est l'existence de deux lettres 0 à la même position dans les mots m_1 et m_2. On cherche à démontrer cette propriété d'invariance par récurrence (i.e. si n admet une décomposition de Goldbach alors $n + 2$ en admet une aussi). Pour cela, il faut peut-être analyser la manière dont les doublons de lettres à la même position dans les mots m_1 et m_2 de n se combinent lorsqu'ils sont contigus pour engendrer les doublons de lettres à la même position dans les mots m_1 et m_2 de $n+2$.

La table suivante fournit la manière dont les doublons se combinent :

	a $\binom{0}{0}$	b $\binom{0}{1}$	c $\binom{1}{0}$	d $\binom{1}{1}$
a $\binom{0}{0}$	a $\binom{0}{0}$	b $\binom{0}{1}$	a $\binom{0}{0}$	b $\binom{0}{1}$
b $\binom{0}{1}$	a $\binom{0}{0}$	b $\binom{0}{1}$	a $\binom{0}{0}$	b $\binom{0}{1}$
c $\binom{1}{0}$	c $\binom{1}{0}$	d $\binom{1}{1}$	c $\binom{1}{0}$	d $\binom{1}{1}$
d $\binom{1}{1}$	c $\binom{1}{0}$	d $\binom{1}{1}$	c $\binom{1}{0}$	d $\binom{1}{1}$

On peut représenter ces combinaisons d'états par les deux petits automates suivants :



On peut enfin représenter cette même connaissance par les règles de réécriture :

$$
\begin{array}{l}
aa \to a \\
ab \to b \\
ac \to a \\
ad \to b \\
ba \to a \\
bb \to b \\
bc \to a \\
bd \to b \\
ca \to c \\
cb \to d \\
cc \to c \\
cd \to d \\
da \to c \\
db \to d \\
dc \to c \\
dd \to d
\end{array}
$$

Les mots associés aux nombres pairs de 24 à 38 sont (lecture colonne par colonne des mots m_2 et m_1 utilisés plus haut :

6 :	a						
8 :	a						
10 :	a	a					
12 :	c	a					
14 :	a	c	a				
16 :	a	a	c				
18 :	c	a	a	d			
20 :	a	c	a	b			
22 :	a	a	c	b	a		
24 :	c	a	a	d	a		
26 :	a	c	a	b	c	a	
28 :	c	a	c	b	a	c	
30 :	c	c	a	d	a	a	d

Annexe : Mots m_1, m_2 des nombres pairs de 24 à 50

24	m_2	1	0	0	1	0										
	m_1	1	0	0	1	0										
26	m_2	0	1	0	0	1	0									
	m_1	1	1	0	1	0	0									
28	m_2	1	0	1	0	0	1									
	m_1	1	1	0	1	0	0									
30	m_2	1	1	0	1	0	0	1								
	m_1	1	1	0	1	0	0	1								
32	m_2	0	1	1	0	1	0	0								
	m_1	1	1	0	1	0	0	1								
34	m_2	0	0	1	1	0	1	0	0							
	m_1	1	1	0	1	0	0	1	0							
36	m_2	1	0	0	1	1	0	1	0							
	m_1	1	1	0	1	0	0	1	0							
38	m_2	1	1	0	0	1	1	0	1	0						
	m_1	1	1	0	1	0	0	1	0	0						
40	m_2	0	1	1	0	0	1	1	0	1						
	m_1	1	1	0	1	0	0	1	0	0						
42	m_2	1	0	1	1	0	0	1	1	0	1					
	m_1	1	1	0	1	0	0	1	0	0	1					
44	m_2	0	1	0	1	1	0	0	1	1	0					
	m_1	1	1	0	1	0	0	1	0	0	1					
46	m_2	0	0	1	0	1	1	0	0	1	1	0				
	m_1	1	1	0	1	0	0	1	0	0	1	0				
48	m_2	1	0	0	1	0	1	1	0	0	1	1				
	m_1	1	1	0	1	0	0	1	0	0	1	0				
50	m_2	0	1	0	0	1	0	1	1	0	0	1	1			
	m_1	1	1	1	1	0	0	1	0	0	1	0	1			
52	m_2	1	0	1	0	0	1	0	1	1	0	0	1			
	m_1	0	0	0	1	0	0	1	0	0	1	0	1			
54	m_2	1	1	0	1	0	0	1	0	1	1	0	0	1		
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1		
56	m_2	0	1	1	0	1	0	0	1	0	1	1	0	0		
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1		
58	m_2	1	0	1	1	0	1	0	0	1	0	1	1	0	0	
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	
60	m_2	1	1	0	1	1	0	1	0	0	1	0	1	1	0	
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	
62	m_2	0	1	1	0	1	1	0	1	0	0	1	0	1	1	0
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0
64	m_2	0	0	1	1	0	1	1	0	1	0	0	1	0	1	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0
66	m_2	1	0	0	1	1	0	1	1	0	1	0	0	1	0	1	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1
68	m_2	1	1	0	0	1	1	0	1	1	0	1	0	0	1	0	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1

70	m_2	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1	0	1						
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1						
72	m_2	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1	0						
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1						
74	m_2	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1	0					
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0					
76	m_2	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1					
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0					
78	m_2	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1				
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1				
80	m_2	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0				
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1				
82	m_2	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0			
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0			
84	m_2	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0			
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0			
86	m_2	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0		
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0		
88	m_2	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1		
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0		
90	m_2	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	1	
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	
92	m_2	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0	
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	
94	m_2	1	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1	0
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0
96	m_2	1	1	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0
98	m_2	1	1	1	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0	1
100	m_2	0	1	1	1	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1
	m_1	0	0	0	1	0	0	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	0	1

Le maillage permet la visualisation des règles de réécriture

(Denise Vella-Chemla - 7/2/14)

En octobre 2005, on avait trouvé un maillage qui semblait intéressant pour visualiser les décompositions de Goldbach.

Puis on l'avait abandonné sous prétexte qu'il ne rendait pas visibles les classes de congruences d'appartenance des entiers dans les différents corps premiers.

Il s'avère que ce maillage fournit la visualisation des règles de réécriture sur les mots d'un langage à 4 lettres qu'on vient tout juste de découvrir.

On rappelle :

- que la lettre a est utilisée pour symboliser une décomposition de n de la forme $p+q$ avec p et q premiers et $p \leqslant n/2$;
- que la lettre b est utilisée pour symboliser une décomposition de n de la forme $p+q$ avec p composé et q premier et $p \leqslant n/2$;
- que la lettre c est utilisée pour symboliser une décomposition de n de la forme $p+q$ avec p premier et q composé et $p \leqslant n/2$;
- que la lettre d est utilisée pour symboliser une décomposition de n de la forme $p+q$ avec p et q composés et $p \leqslant n/2$;

Les quatre lettres sont représentées par les petits symboles suivants :

lettre a :

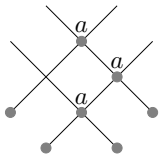
lettre b :

lettre c :

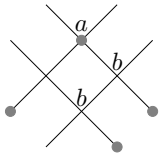
lettre d :

Les 16 règles de réécriture sont alors aisées à retrouver :

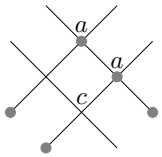
1) règle $aa \to a$:



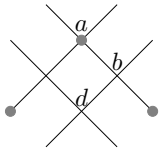
2) règle $ab \to b$:



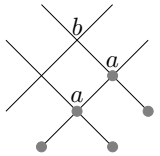
3) règle $ac \to a$:



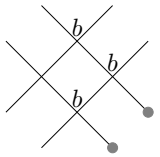
4) règle $ad \to b$:



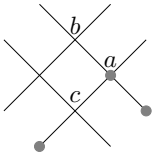
5) règle $ba \to a$:



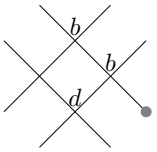
6) règle $bb \to b$:



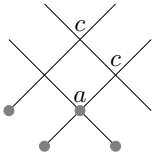
7) règle $bc \to a$:



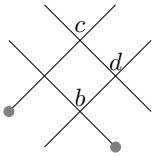
8) règle $bd \to b$:



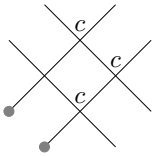
9) règle $ca \to c$:



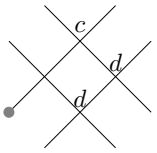
10) règle $cb \to d$:



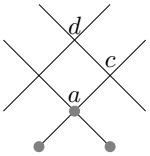
11) règle $cc \to c$:



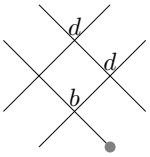
12) règle $cd \to d$:



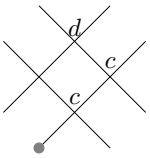
13) règle $da \to c$:



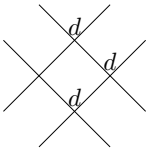
14) règle $db \to d$:



15) règle $dc \to c$:



16) règle $dd \to d$:



On peut ainsi “lire verticalement” les mots sur notre alphabet de 4 lettres associés aux nombres pairs successifs (les décompositions de Goldbach sont indiquées par les lettres a rouges).

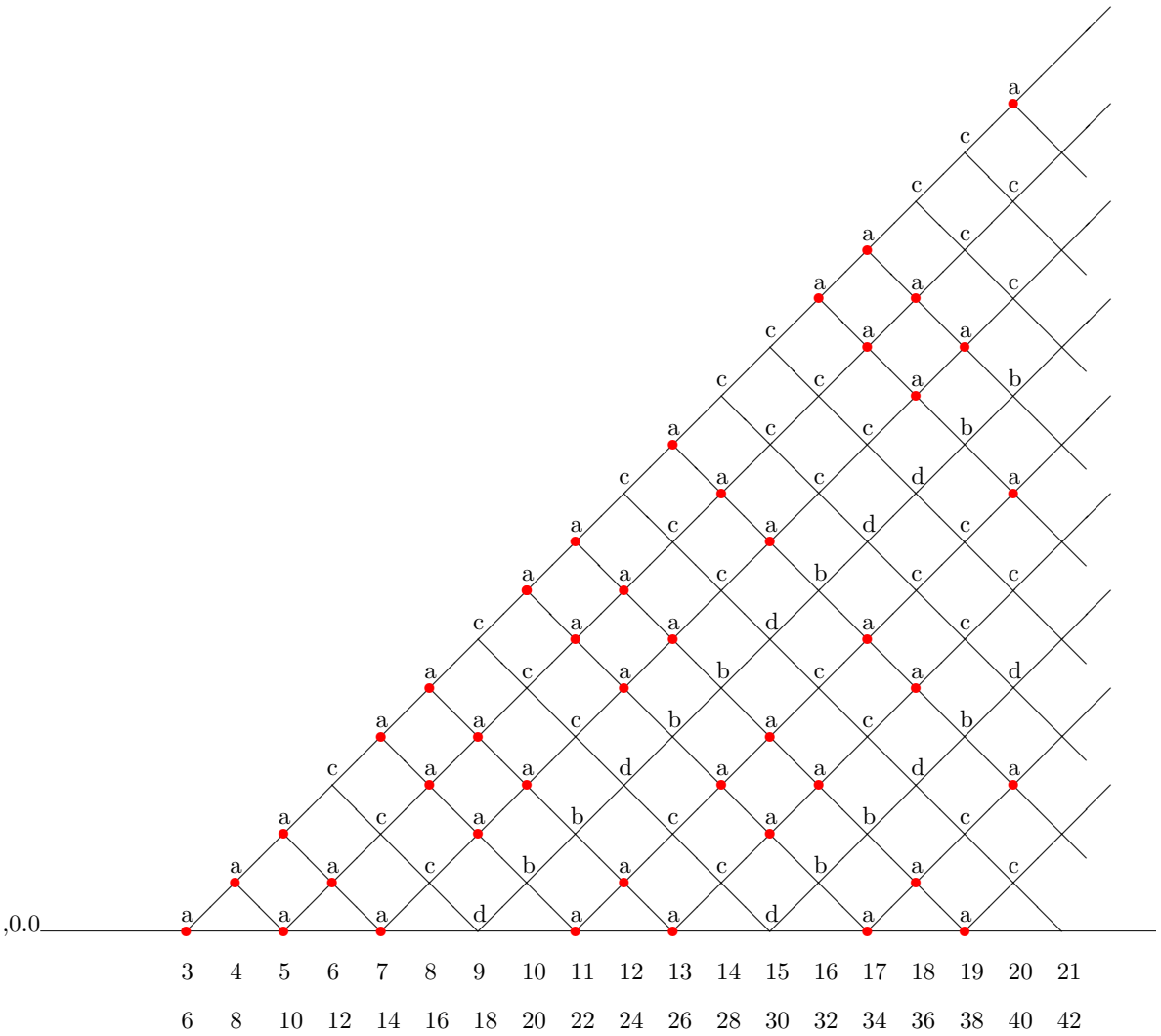


FIGURE 1 – Le treillis Goldbach

Conjecture de Goldbach, langage, réécriture

Denise Vella-Chemla

9/2/14

1 Introduction

On souhaite trouver une démonstration de la conjecture de Goldbach, qui stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers [1].

On se propose dans ce but d'utiliser une modélisation qui associe à chaque nombre pair n un mot d'un langage à 4 lettres qui code la primalité des nombres impairs x (compris entre 3 et et $n/2$) et de leur complémentaire.

On identifiera le processus permettant de passer du mot d'un nombre pair n au mot du nombre pair suivant $n+2$.

On caractérisera l'existence d'un décomposant de Goldbach d'un nombre pair par une simple condition que vérifie son mot.

On essaiera de trouver une contrainte invariante respectée par les mots des nombres pairs successifs qui assurera que l'existence d'un décomposant de Goldbach est toujours conservée.

2 Mots d'un nombre pair

On choisit de représenter le fait qu'un entier est premier par le booléen 0 et le fait qu'il est composé par le booléen 1.

On appelle $sym(m)$ la fonction qui associe à un mot m son symétrique, i.e. le mot contenant les lettres de m depuis la dernière jusqu'à la première.

Appelons *milieu* le plus grand nombre entier impair inférieur ou égal à $n/2$.

1. Dans l'égalité $n = p + q$ avec n pair supérieur à 2, p et q premiers, on appellera p et q décomposants de Goldbach de n ou sommants.

A chaque nombre pair n sont associés deux mots booléens m_1 et m_2 définis de la façon suivante :

- les lettres de m_1 sont les caractères de primalité des nombres impairs compris entre 3 et *milieu* inclus ;
- les lettres de m_2 sont les caractères de primalité des nombres impairs compris entre $n-3$ et *milieu* inclus.

Les mots m_1 et m_2 associés au nombre pair n sont de longueur $\left\lfloor \frac{n/2-1}{2} \right\rfloor$. La longueur des mots augmente donc de 1 à chaque double d'impair, i.e. une fois sur deux.

Le mot booléen m du nombre pair n est la concaténation des deux mots suivants :

- m_1 ;
- $sym(m_2)$, le symétrique de m_2.

Note : on a pris pour habitude de fournir le mot m_2 en première ligne et le mot m_1 en deuxième ligne (3 en bas à gauche, $n-3$ en haut à gauche). On constate que pour les doubles d'impairs, la lettre codant le caractère de primalité de l'entier *milieu* est doublée.

On associe d'autre part à n un mot d'un langage à 4 lettres m_{abcd}, dont chaque lettre code les colonnes de lettres des mots m_2 et m_1.

La lettre a code la colonne $\binom{0}{0}$. La lettre b code la colonne $\binom{0}{1}$. La lettre c code la colonne $\binom{1}{0}$. La lettre d code la colonne $\binom{1}{1}$.

Exemples : Ci-dessous les mots m_1, m_2, m et m_{abcd} des nombres 40, 42 et 44.

40	37	35	33	31	29	27	25	23	21									
m_2	0	1	1	0	0	1	1	0	1									
m_1	0	0	0	1	0	0	1	0	0									
	3	5	7	9	11	13	15	17	19									
m	0	0	0	1	0	0	1	0	0	|	1	0	1	1	0	0	1	1	0
m_{abcd}	a	c	c	b	a	c	d	a	c									

42	39	37	35	33	31	29	27	25	23	21										
m_2	1	0	1	1	0	0	1	1	0	1										
m_1	0	0	0	1	0	0	1	0	0	1										
	3	5	7	9	11	13	15	17	19	21										
m	0	0	0	1	0	0	1	0	0	1	|	1	0	1	1	0	0	1	1	0	1
m_{abcd}	c	a	c	d	a	a	d	c	a	d										

44	41	39	37	35	33	31	29	27	25	23											
m_2	0	1	0	1	1	0	0	1	1	0											
m_1	0	0	0	1	0	0	1	0	0	1											
	3	5	7	9	11	13	15	17	19	21											
m	0	0	0	1	0	0	1	0	0	1	|	0	1	1	0	0	1	1	0	1	0
m_{abcd}	a	c	a	d	c	a	b	c	c	b											

3 Identifier ce que fait le processus

Reprenons les mots m_1, m_2 et m des nombres pairs 24 à 34.

24	m_2	1	0	0	1	0									
	m_1	0	0	0	1	0									
	m	0	0	0	1	0	|	0	1	0	0	1			
26	m_2	0	1	0	0	1	0								
	m_1	0	0	0	1	0	0								
	m	0	0	0	1	0	0	|	0	1	0	0	1	0	
28	m_2	1	0	1	0	0	1								
	m_1	0	0	0	1	0	0								
	m	0	0	0	1	0	0	|	1	0	0	1	0	1	
30	m_2	1	1	0	1	0	0	1							
	m_1	0	0	0	1	0	0	1							
	m	0	0	0	1	0	0	1	|	1	0	0	1	0	1	1
32	m_2	0	1	1	0	1	0	0							
	m_1	0	0	0	1	0	0	1							
	m	0	0	0	1	0	0	1	|	0	0	1	0	1	1	0
34	m_2	0	0	1	1	0	1	0	0							
	m_1	0	0	0	1	0	0	1	0							
	m	0	0	0	1	0	0	1	0	|	0	0	1	0	1	1	0	0

On voit que si au nombre pair n est associé un mot booléen de longueur $2i$, le processus qui permet d'obtenir le mot booléen associé au nombre pair $n+2$ effectue plusieurs actions différentes :

- *travail sur la lettre à la position* $i+1$ (on a coloré cette lettre en bleu dans le tableau ci-dessus) : dans le cas où n est un double d'impair, le mot de $n+2$ est obtenu en enlevant du mot de n la lettre à la position $i+1$; dans le cas où n est un double de pair, le mot de $n+2$ est obtenu en dupliquant cette lettre à la position $i+1$;
- *concaténation en fin du mot :* dans tous les cas, est concaténée à la fin du mot booléen ainsi obtenu la lettre qui caractérise la primalité du nombre entier $2n-3$ pour obtenir le mot de $n+2$. *Remarque :* la concaténation est une opération non-commutative. Par exemple, $1(110) = 1110$ alors que $(110)1 = 1101$.

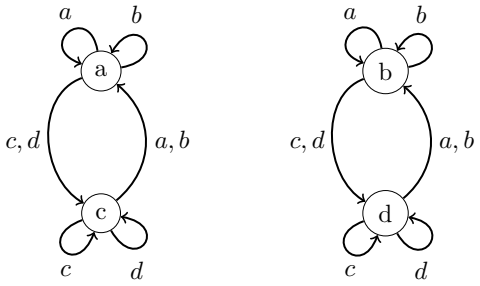
Si on considère maintenant la représentation par les mots du langage à 4 lettres, celui du nombre pair $n+2$ s'obtient de la façon suivante à partir de celui de n :

- la première lettre du mot de $n+2$ est a si $n-3$ est premier et c sinon (cette première lettre est la seule qui introduit de l'indéterminisme car elle n'appartient pas au mot du langage à 4 lettres de n ou ne se déduit pas des lettres de ce dernier) ;
- les lettres suivantes du mot de $n+2$ sont obtenues par réécriture du mot de n selon les règles ci-dessous :

$$
\begin{aligned}
aa &\to a \\
ab &\to b \\
ac &\to a \\
ad &\to b \\
ba &\to a \\
bb &\to b \\
bc &\to a \\
bd &\to b \\
ca &\to c \\
cb &\to d \\
cc &\to c \\
cd &\to d \\
da &\to c \\
db &\to d \\
dc &\to c \\
dd &\to d
\end{aligned}
$$

  On note que 4 règles de réécriture ($aa \to a,\ ac \to a,\ ba \to a,\ bc \to a$) assurent d'obtenir une lettre a au moins dans le mot de $n+2$.

  On peut représenter ces règles de réécriture par les deux petits automates déterministes suivants (l'opérateur est à gauche) :



- enfin, la concaténation d'une lettre en fin de mot, dans le cas où n est un double de pair obéit à la règle suivante :
  - si n a a ou b comme dernière lettre, après avoir obtenu le mot de $n+2$ en appliquant les règles de réécriture, on lui concatène la lettre a ;
  - si n a c ou d comme dernière lettre, après avoir obtenu le mot de $n+2$ en appliquant les règles de réécriture, on lui concatène la lettre d.

4 Loi de composition de Ritz-Rydberg

On teste ici sur deux exemples la loi de composition de Ritz-Rydberg, qui a pour conséquence que la composition des règles de réécriture (α, β) et (β, γ) a le même effet que la règle de réécriture (α, γ).

$ab/bc \to bba \to ba \to a$ permet d'obtenir le même résultat que $ac \to a$.

$cd/da \to ddc \to dc \to c$ permet d'obtenir le même résultat que $ca \to c$.

En annexe 2, sont fournies les 64 règles de composition qui vérifient le principe de Ritz-Rydberg.

5 Caractériser l'existence d'une décomposition de Goldbach dans le mot d'un nombre pair

Il faut maintenant être capable de caractériser par une condition sur le mot m la présence à une même position dans les mots m_1 et m_2 d'une lettre 0.

Rappelons quelques éléments de logique booléenne.

La conjonction logique est définie par :

$$1 \wedge 0 = 0 \wedge 1 = 0 \wedge 0 = 0 \text{ et } 1 \wedge 1 = 1.$$

La négation logique est définie par :

$$\neg 0 = 1 \text{ et } \neg 1 = 0.$$

Si l'on appelle $l(m, i)$ la lettre à la position i dans le mot m, alors l'existence d'une décomposition de Goldbach est équivalente à la condition :

$$\Big[\sum_{1 \leqslant i \leqslant \lfloor \frac{n/2-1}{2} \rfloor, i+j=\lfloor \frac{n}{2} \rfloor} \neg l(m,i) \wedge \neg l(m,j) \Big] = 1$$

En utilisant la représentation par les mots du langage à 4 lettres, l'existence d'une décomposition de Goldbach est simplement la présence d'une lettre a dans le mot du nombre pair considéré.

Le double d'un nombre impair dont le mot m_{abcd} se termine par une lettre a est un double de nombre premier, qui vérifie donc trivialement la conjecture de Goldbach (ex : 46 dont le mot m_{abcd} est *aacbccbacda* se terminant par une lettre a est le double de 23, premier).

Le double d'un nombre pair dont le mot m_{abcd} se termine par une lettre a est le double d'un "père de jumeau" (ex : 36 dont le mot m_{abcd} est *acabca* se terminant par une lettre a est le double de 18, un père de jumeau, i.e. un nombre pair compris entre deux nombres premiers, en l'occurrence 17 et 19).

6 Invariant

Rappelons un fait qui peut peut-être être utile : tous les mots m_{abcd} des nombres pairs que nous considérerons ne pourront jamais contenir une suite de 3 lettres a consécutives : cela provient du fait que 3, 5 et 7 sont les seuls trois nombres premiers consécutifs puisque toute suite de trois impairs consécutifs contient un nombre divisible par 3.

On constate dans l'annexe que les mots contiennent des "lettres alignées" selon des verticales ou des diagonales descendantes, que ce soit des b ou d d'une part, ou des a ou c d'autre part.

Ces lignes sont vite identifiées comme correspondant aux décompositions successives faisant soit intervenir le même premier sommant, soit intervenir le même deuxième sommant. La quatrième ligne verticale de lettres par exemple, qui commence par les lettres *dbbdbbdb*... correspond aux décompositions $9 + 9$, $9 + 11$, $9 + 13$, ... La sixième diagonale descendante, à partir de la première lettre du mot de 18, et qui contient les lettres *cccdccd* correspond aux décompositions $3 + 15$, $5 + 15$, $7 + 15$, $9 + 15$, ...

On peut donc de manière imagée, considérer que le mot m_{abcd} d'un nombre pair est une sorte de sandwich multi-couches, qui contient une première tranche de lettres a ou c en début de mot, suivie d'un certain nombre de tranches alternées, les unes ne contenant que des lettres b ou d et les autres ne contenant que des lettres a ou c, et que les tranches voient les positions de leur première et dernière lettre fixées une fois pour toutes, même si leur composition varie au fur et à mesure du processus.

Supposons qu'un mot $n + 2$ n'admette pas de décomposition de Goldbach. Ce mot ne doit contenir que des lettres c, b ou d. On note ce mot de la façon suivante, par abus de notation : $(c^*(b \vee d)^*)^*$.

Essayons de trouver d'où pourrait provenir la contradiction si on prend comme hypothèse l'existence d'un tel mot.

Pour cela, essayons d'imaginer la composition du mot m_{abcd} associé au nombre pair précédent qui est n. Il pourrait contenir des lettres a mais elles devraient forcément être en "fin des tranches" $(c \vee a)$ puisque sinon, toute occurence du doublon de lettres ac entraînerait la présence d'une lettre a dans le mot du nombre pair $n + 2$, ce qui serait contraire à l'hypothèse. Un raisonnement similaire oblige les lettres d à être à la fin des tranches $(b \vee d)$. Le mot du nombre pair n serait donc obligatoirement de la forme $(c^*a(b \vee d)^*d)^*$. Il contiendrait des lettres a. On n'arrive pas à aboutir à une contradiction pour l'instant.

Pour regarder autrement le processus, voyons comment les règles de réécriture se combinent entre elles, dans un tableau de concaténation : si on concatène xy avec zt, on va s'intéresser à la lettre obtenue par le "jointure" des deux doublons de lettres, c'est à dire qu'on notera dans le tableau le résultat de la règle de réécriture qui a les lettres yz en partie gauche :

	ab	ad	bb	bd	ca	cb	cc	cd	da	db	dc	dd
ab	a	a	b	b	a	a	a	a	b	b	b	b
ad	c	c	d	d	c	c	c	c	d	d	d	d
bb	a	a	b	b	a	a	a	a	b	b	b	b
bd	c	c	d	d	c	c	c	c	d	d	d	d
ca	a	a	b	b	a	a	a	a	b	b	b	b
cb	a	a	b	b	a	a	a	a	b	b	b	b
cc	c	c	d	d	c	c	c	c	d	d	d	d
cd	c	c	d	d	c	c	c	c	d	d	d	d
da	a	a	b	b	a	a	a	a	b	b	b	b
db	a	a	b	b	a	a	a	a	b	b	b	b
dc	c	c	d	d	c	c	c	c	d	d	d	d
dd	c	c	d	d	c	c	c	c	d	d	d	d

On n'arrive pas à avancer dans cette voie-là non plus.

Si on calcule la proportion de lettres a (de décompositions de Goldbach donc) dans les mots m_{abcd} de n valant certaines puissances de 10, on trouve qu'elle est égale à $5402/249999 = 0.0216$ pour $n = 10^6$, $38807/2499999 = 0.0155$ pour $n = 10^7$ et $291400/249999 = 0.0116$ pour $n = 10^8$. Elle semble ne même pas être divisée par 2 lorsqu'on multiplie n par 10 mais cela ne prouve rien.

Si enfin on compte simplement le nombre d'occurrences de chaque lettre en partie gauche ou droite des règles de réécriture, les lettres sont bien sûr présentes 8 fois en tout dans les 16 parties gauches, et équitablement 4 fois chacune en partie droite des règles. Mais les règles sont comme "entremêlées" ce qui empêche de trouver une fonction qui permettrait d'identifier certaines d'entre elles (les lettres a et b par exemple, se comportent de la même manière en tant que préfixes des parties gauches, mais totalement différemment en tant que suffixes).

Annexe 1 : mots du langage à 4 lettres associés aux nombres pairs de 6 à 100

6 : a
8 : a
10 : $a\ a$
12 : $c\ a$
14 : $a\ c\ a$
16 : $a\ a\ c$
18 : $c\ a\ a\ d$
20 : $a\ c\ a\ b$
22 : $a\ a\ c\ b\ a$
24 : $c\ a\ a\ d\ a$
26 : $a\ c\ a\ b\ c\ a$
28 : $c\ a\ c\ b\ a\ c$
30 : $c\ c\ a\ d\ a\ a\ d$
32 : $a\ c\ c\ b\ c\ a\ b$
34 : $a\ a\ c\ d\ a\ c\ b\ a$
36 : $c\ a\ a\ d\ c\ a\ d\ a$
38 : $c\ c\ a\ b\ c\ c\ b\ c\ a$
40 : $a\ c\ c\ b\ a\ c\ d\ a\ c$
42 : $c\ a\ c\ d\ a\ a\ d\ c\ a\ d$
44 : $a\ c\ a\ d\ c\ a\ b\ c\ c\ b$
46 : $a\ a\ c\ b\ c\ c\ b\ a\ c\ d\ a$
48 : $c\ a\ a\ d\ a\ c\ d\ a\ a\ d\ c$
50 : $a\ c\ a\ b\ c\ a\ d\ c\ a\ b\ c\ d$
52 : $c\ a\ c\ b\ a\ c\ b\ c\ c\ b\ a\ d$
54 : $c\ c\ a\ d\ a\ a\ d\ a\ c\ d\ a\ b\ d$
56 : $a\ c\ c\ b\ c\ a\ b\ c\ a\ d\ c\ b\ b$
58 : $c\ a\ c\ d\ a\ c\ b\ a\ c\ b\ c\ d\ b\ a$
60 : $c\ c\ a\ d\ c\ a\ d\ a\ a\ d\ a\ d\ d\ a$
62 : $a\ c\ c\ b\ c\ c\ b\ c\ a\ b\ c\ b\ d\ c\ a$
64 : $a\ a\ c\ d\ a\ c\ d\ a\ c\ b\ a\ d\ b\ c\ c$
66 : $c\ a\ a\ d\ c\ a\ d\ c\ a\ d\ a\ b\ d\ a\ c\ d$
68 : $c\ c\ a\ b\ c\ c\ b\ c\ c\ b\ c\ b\ b\ c\ a\ d$
70 : $a\ c\ c\ b\ a\ c\ d\ a\ c\ d\ a\ d\ b\ a\ c\ b\ d$
72 : $c\ a\ c\ d\ a\ a\ d\ c\ a\ d\ c\ b\ d\ a\ a\ d\ b$
74 : $a\ c\ a\ d\ c\ a\ b\ c\ c\ b\ c\ d\ b\ c\ a\ b\ d\ a$
76 : $a\ a\ c\ b\ c\ c\ b\ a\ c\ d\ a\ d\ d\ a\ c\ b\ b\ c$
78 : $c\ a\ a\ d\ a\ c\ d\ a\ a\ d\ c\ b\ d\ c\ a\ d\ b\ a\ d$
80 : $c\ c\ a\ b\ c\ a\ d\ c\ a\ b\ c\ d\ b\ c\ c\ b\ d\ a\ b$
82 : $a\ c\ c\ b\ a\ c\ b\ c\ c\ b\ a\ d\ d\ a\ c\ d\ b\ c\ b\ a$
84 : $c\ a\ c\ d\ a\ a\ d\ a\ c\ d\ a\ b\ d\ c\ a\ d\ d\ a\ d\ a$
86 : $a\ c\ a\ d\ c\ a\ b\ c\ a\ d\ c\ b\ b\ c\ c\ b\ d\ c\ b\ c\ a$
88 : $c\ a\ c\ b\ c\ c\ b\ a\ c\ b\ c\ d\ b\ a\ c\ d\ b\ c\ d\ a\ c$
90 : $c\ c\ a\ d\ a\ c\ d\ a\ a\ d\ a\ d\ d\ a\ a\ d\ d\ a\ d\ c\ a\ d$
92 : $a\ c\ c\ b\ c\ a\ d\ c\ a\ b\ c\ b\ d\ c\ a\ b\ d\ c\ b\ c\ c\ b$
94 : $c\ a\ c\ d\ a\ c\ b\ c\ c\ b\ a\ d\ b\ c\ c\ b\ b\ c\ d\ a\ c\ d\ a$
96 : $c\ c\ a\ d\ c\ a\ d\ a\ c\ d\ a\ b\ d\ a\ c\ d\ b\ a\ d\ c\ a\ d\ c$
98 : $c\ c\ c\ b\ c\ c\ b\ c\ a\ d\ c\ b\ b\ c\ a\ d\ d\ a\ b\ c\ c\ b\ c\ d$
100 : $a\ c\ c\ d\ a\ c\ d\ a\ c\ d\ b\ c\ d\ b\ a\ c\ b\ d\ c\ b\ a\ c\ d\ a\ d$

Annexe 2 : Application de la loi de composition de Ritz-Rydberg aux règles de réécriture

$aa/aa \to aaa \to aa \to a$ permet d'obtenir le même résultat que $aa \to a$.
$aa/ab \to aab \to ab \to b$ permet d'obtenir le même résultat que $ab \to b$.
$aa/ac \to aaa \to aa \to a$ permet d'obtenir le même résultat que $ac \to a$.
$aa/ad \to aab \to ab \to b$ permet d'obtenir le même résultat que $ad \to b$.
$ab/ba \to bba \to ba \to a$ permet d'obtenir le même résultat que $aa \to a$.
$ab/bb \to bbb \to bb \to b$ permet d'obtenir le même résultat que $ab \to b$.
$ab/bc \to bba \to ba \to a$ permet d'obtenir le même résultat que $ac \to a$.
$ab/bd \to bbb \to bb \to b$ permet d'obtenir le même résultat que $ad \to b$.
$ac/ca \to acc \to ac \to a$ permet d'obtenir le même résultat que $aa \to a$.
$ac/cb \to acd \to ad \to b$ permet d'obtenir le même résultat que $ab \to b$.
$ac/cc \to acc \to ac \to a$ permet d'obtenir le même résultat que $ac \to a$.
$ac/cd \to acd \to ad \to b$ permet d'obtenir le même résultat que $ad \to b$.
$ad/da \to bdc \to bc \to a$ permet d'obtenir le même résultat que $aa \to a$.
$ad/db \to bdd \to bd \to b$ permet d'obtenir le même résultat que $ab \to b$.
$ad/dc \to bdc \to bc \to a$ permet d'obtenir le même résultat que $ac \to a$.
$ad/dd \to bdd \to bd \to b$ permet d'obtenir le même résultat que $ad \to b$.

$ba/aa \to aaa \to aa \to a$ permet d'obtenir le même résultat que $ba \to a$.
$ba/ab \to aab \to ab \to b$ permet d'obtenir le même résultat que $bb \to b$.
$ba/ac \to aaa \to aa \to a$ permet d'obtenir le même résultat que $bc \to a$.
$ba/ad \to aab \to ab \to b$ permet d'obtenir le même résultat que $bd \to b$.
$bb/ba \to bba \to ba \to a$ permet d'obtenir le même résultat que $ba \to a$.
$bb/bb \to bbb \to bb \to b$ permet d'obtenir le même résultat que $bb \to b$.
$bb/bc \to bba \to ba \to a$ permet d'obtenir le même résultat que $bc \to a$.
$bb/bd \to bbb \to bb \to b$ permet d'obtenir le même résultat que $bd \to b$.
$bc/ca \to acc \to ac \to a$ permet d'obtenir le même résultat que $ba \to a$.
$bc/cb \to acd \to ad \to b$ permet d'obtenir le même résultat que $bb \to b$.
$bc/cc \to acc \to ac \to a$ permet d'obtenir le même résultat que $bc \to a$.
$bc/cd \to acd \to ad \to b$ permet d'obtenir le même résultat que $bd \to b$.
$bd/da \to bdc \to bc \to a$ permet d'obtenir le même résultat que $ba \to a$.
$bd/db \to bdd \to bd \to b$ permet d'obtenir le même résultat que $bb \to b$.
$bd/dc \to bdc \to bc \to a$ permet d'obtenir le même résultat que $bc \to a$.
$bd/dd \to bdd \to bd \to b$ permet d'obtenir le même résultat que $bd \to b$.

$ca/aa \to caa \to ca \to c$ permet d'obtenir le même résultat que $ca \to c$.
$ca/ab \to cab \to cb \to d$ permet d'obtenir le même résultat que $cb \to d$.
$ca/ac \to caa \to ca \to c$ permet d'obtenir le même résultat que $cc \to c$.
$ca/ad \to cab \to cb \to d$ permet d'obtenir le même résultat que $cd \to d$.
$cb/ba \to dba \to da \to c$ permet d'obtenir le même résultat que $ca \to c$.
$cb/bb \to dbb \to db \to d$ permet d'obtenir le même résultat que $cb \to d$.
$cb/bc \to dba \to da \to c$ permet d'obtenir le même résultat que $cc \to c$.
$cb/bd \to dbb \to db \to d$ permet d'obtenir le même résultat que $cd \to d$.
$cc/ca \to ccc \to cc \to c$ permet d'obtenir le même résultat que $ca \to c$.
$cc/cb \to ccd \to cd \to d$ permet d'obtenir le même résultat que $cb \to d$.
$cc/cc \to ccc \to cc \to c$ permet d'obtenir le même résultat que $cc \to c$.
$cc/cd \to ccd \to cd \to d$ permet d'obtenir le même résultat que $cd \to d$.

$cd/da \to ddc \to dc \to c$ permet d'obtenir le même résultat que $ca \to c$.
$cd/db \to ddd \to dd \to d$ permet d'obtenir le même résultat que $cb \to d$.
$cd/dc \to ddc \to dc \to c$ permet d'obtenir le même résultat que $cc \to c$.
$cd/dd \to ddd \to dd \to d$ permet d'obtenir le même résultat que $cd \to d$.

$da/aa \to caa \to ca \to c$ permet d'obtenir le même résultat que $da \to c$.
$da/ab \to cab \to cb \to d$ permet d'obtenir le même résultat que $db \to d$.
$da/ac \to caa \to ca \to c$ permet d'obtenir le même résultat que $dc \to c$.
$da/ad \to cab \to cb \to d$ permet d'obtenir le même résultat que $dd \to d$.
$db/aa \to dba \to da \to c$ permet d'obtenir le même résultat que $da \to c$.
$db/ab \to dbb \to db \to d$ permet d'obtenir le même résultat que $db \to d$.
$db/ac \to dba \to da \to c$ permet d'obtenir le même résultat que $dc \to c$.
$db/ad \to dbb \to db \to d$ permet d'obtenir le même résultat que $dd \to d$.
$dc/aa \to ccc \to cc \to c$ permet d'obtenir le même résultat que $da \to c$.
$dc/ab \to ccd \to cd \to d$ permet d'obtenir le même résultat que $db \to d$.
$dc/ac \to ccc \to cc \to c$ permet d'obtenir le même résultat que $dc \to c$.
$dc/ad \to ccd \to cd \to d$ permet d'obtenir le même résultat que $dd \to d$.
$dd/aa \to ddc \to dc \to c$ permet d'obtenir le même résultat que $da \to c$.
$dd/ab \to ddd \to dd \to d$ permet d'obtenir le même résultat que $db \to d$.
$dd/ac \to ddc \to dc \to c$ permet d'obtenir le même résultat que $dc \to c$.
$dd/ad \to ddd \to dd \to d$ permet d'obtenir le même résultat que $dd \to d$.

Ci-dessous un extrait d'une conférence de Serge Haroche "La physique quantique" à l'Université de tous les savoirs en 2000 (DV, 16/2/2014)

Lien vers la conférence :
http ://www.canal-u.tv/video/universite$_d$e$_t$ous$_l$es$_s$avoirs/la$_p$hysique$_q$uantique$_s$erge$_h$aroche.1065

En raison des imperfections de la cavité, d'une certaine rugosité du miroir, de temps en temps, un photon va s'échapper, et partir dans l'environnement. Dès que le photon est parti, c'en est fini de la cohérence quantique. Le premier photon qui s'échappe sert d'espion pour vous dire que vous êtes dans un chemin et pas dans l'autre. Le temps que le premier photon va mettre à disparaître est extrêmement court. Si vous avez un milliard de photons et un temps de relaxation d'une milliseconde, il vous faudra un milliardième de millisecondes pour que le premier photon s'échappe et la cohérence quantique aura disparu. On comprend que les cohérences macroscopiques disparaissent très très vite pour des champs macroscopiques et on ne peut faire des expériences que si n n'est pas trop grand. On a fait une telle expérience qui "saisit la décohérence au vol". Les cohérences quantiques sont extrêmement fragiles, elles s'évanouissent dès qu'un quantum s'est perdu dans l'environnement.

A relier à ceci, paru le 27 janvier 2014 :
http ://www2.cnrs.fr/presse/communique/3415.htm

Il a pris de mes nouvelles à distance depuis Helsinki et Vordingborg. A chaque fois qu'il le fait, mon cerveau se met en mouvement, c'est un bon catalyseur. Il a bien compris que je suis une sorte de particule quantique : mon état est complètement modifié quand on m'observe, je ne suis bien que là où je ne suis pas et je lui sais gré d'essayer de me perturber le moins possible.

En ce moment, c'est très difficile d'avancer, j'aimerais pouvoir m'isoler mais il y a trop de sollicitations. J'ai décidé que moi aussi, j'aurai une exigence : je chercherai une idée qui appartienne à mon domaine : bits, données, instructions, programmes, invariant, preuve. C'était nul d'aller fouiller leurs plates-bandes, elles sont si foisonnantes, si compliquées, je ne vois pas leur lumière, j'ai besoin de simplicité.

J'aimerais tant bénéficier de l'effet tunnel : en tant que particule quantique, je suis coincée dans une sorte de bol depuis 8 ans, je n'arrête pas de me cogner contre les parois, vraiment comme une mouche frappe bêtement contre une vitre une journée durant sous prétexte qu'elle voit la lumière derrière. Mon énergie est très inférieure à l'énergie minimum qu'il faudrait pour sauter par-dessus les parois du bol : je n'ai aucun bagage, c'est comme si j'escaladais les parois à mains nues, et nombreux sont ceux qui se sont moqués de moi. Il y a une probabilité infime que je passe de l'autre côté, que je trouve l'explication.

(DV, 4/1/14)

En mai 2009, j'avais proposé une méthode permettant de trouver les décomposants de Goldbach d'un nombre pair en calculant des produits de sinusoïdes. J'ai à nouveau présenté cette méthode sur un forum l'hiver dernier mais sans résultat.

J'ai enfin trouvé des références à propos de ces produits de sinus mais ils ne me permettent pas davantage d'avancer sur ce chemin-là :

- dans le fichier Berard-texte.pdf, à la page 3 sont présentés des exemples en dimension 1 : le problème de Dirichlet (sur la corde-segment) et le problème fermé (sur le cercle) ;

- dans le fichier Berard-transp.pdf, on voit apparaître le produit de sinus dans la page 8 concernant l'équation des ondes ; pages 13 et 14 sont présentés le problème de Dirichlet et le problème fermé ;

(DV, 3/1/14)

Notes sur En cherchant Majorana d'Etienne Klein
(Denise Chemla - 26/12/2013)

(p.54) Mais le mécanisme de cette radioactivité est incompréhensible dans le cadre de la physique classique. Et c'est là que Gamow et Majorana franchissent un seuil. Selon les lois classiques, il est impossible qu'une particule alpha sorte d'un noyau atomique, qui représente pour elle une cuvette aux parois infranchissables, autrement dit une "barrière de potentiel". Ce que Gamow comprend et que Majorana démontre formellement, c'est qu'une telle interdiction peut être déjouée par les lois quantiques. Appliquées à une particule alpha prétendument prisonnière d'un noyau, elles lui permetttent d'apparaître... à l'extérieur du noyau ! Elles lui offrent en effet une probabilité non nulle de traverser la barrière de potentiel. Initialement confinée, la particule alpha se déplace très vite, ne cesse d'abord de se cogner et de rebondir sur la paroi intérieure du noyau ; puis, après de multiples tentatives infructueuses, profitant du jeu des probabilités et de la multiplicité des occasions, elle finit par passer au travers - d'où le terme d'"effet tunnel" inventé par Gamow.

Mon interprétation : je suis une particule alpha et j'ai une probabilité infime d'échapper à ma condition, à force de m'être cognée à CG, et de réussir peut-être à la démontrer, par "effet tunnel" !!!

(p.108) Majorana dans son dernier article émet l'hypothèse que certaines particules dépourvues de charge électrique pourraient être leur propre antiparticule - une hypothèse à l'origine de recherches menées aujourd'hui sur des particules fascinantes et fantomatiques, les neutrinos.

(P.110) L'équation de Dirac recèle quelque chose d'étrange : certaines des solutions de son équation correspondent à des particules d'énergie... négative ! Or toutes les particules connues sont dotées d'une énergie positive, y compris lorsqu'elles sont immobiles, puisque leur énergie est alors égale à leur énergie de masse mc^2. Si ces particules d'énergie négative existaient, elles auraient donc une masse négative. Cela impliquerait que, sous l'action d'une force, elles se déplaceraient dans le sens contraire à celui des particules ordinaires, toutes dotées d'une masse positive.[...] Ce nouvel objet microscopique est l'"antiparticule de l'électron", qui sera bientôt baptisée le "positron". Dirac démontre en outre qu'un électron et un positron ne peuvent apparaître qu'ensemble, c'est à dire par paire, un peu comme des frères jumeaux.

(p.112) Majorana montre d'abord, de façon très élégante, qu'on peut déduire l'équation de Dirac d'un principe plus fondamental, en fait plus symétrique, que celui dont est parti le théoricien anglais. Il montre ensuite qu'on peut donner une autre forme à cette équation et qu'alors certaines de ses solutions correspondent à des particules qui sont... leur propre antiparticule ! Majorana pour cela identifie d'autres matrices que celles de Dirac satisfaisant aux règles de la même algèbre (de Clifford), les "matrices de Majorana" dont toutes les composantes sont des nombres imaginaires purs (de partie réelle nulle), ce qui permet à la nouvelle équation ainsi obtenue d'avoir des solutions réelles (au sens où elles ne sont pas complexes). Ces solutions réelles correspondent à des particules qui sont leur propre antiparticule.

Mon interprétation : Les particules qui sont leur propre antiparticule sont les nombres premiers. Les électrons et les positrons qui vont par deux correspondent à mes caractères de divisibilité dans les grilles. On n'aura qu'à affecter aux nombres jusqu'à $n/2$ des électrons seulement et aux nombres de $n/2$ à n les positrons correspondants.

Ci-dessous un extrait de l'Essai d'Albert Einstein Comment je vois le monde (p.34 de l'édition Champs Sciences chez Flammarion) (DC, 30/11/2013)

Il ne suffit pas d'apprendre à l'homme une spécialité. Car il devient ainsi une machine utilisable mais non une personnalité. Il importe qu'il acquière un sentiment, un sens pratique de ce qui vaut la peine d'être entrepris, de ce qui est beau, de ce qui est moralement droit. Sinon, il ressemble davantage, avec ses connaissances professionnelles, à un chien savant qu'à une créature harmonieusement développée. Il doit apprendre à comprendre les motivations des hommes, leurs chimères et leurs angoisses pour déterminer son rôle exact vis-à-vis des proches et de la communauté.

Ces réflexions essentielles livrées à la jeune génération, grâce au contact vivant avec les professeurs, ne s'écrivent absolument pas dans les manuels. Ainsi s'exprime et se forme d'abord toute culture. Quand je conseille ardemment ≪ Les Humanités ≫, c'est cette culture vivante que je recommande, et non pas un savoir desséché, surtout en histoire et en philosophie.

Les excès du système de compétition et de spécialisation prématurée sous le fallacieux prétexte d'efficacité, assassinent l'esprit, interdisent toute vie culturelle et suppriment même les progrès dans les sciences d'avenir. Il importe enfin, pour la réalisation d'une parfaite éducation, de développer l'esprit critique dans l'intelligence du jeune homme. Or la surcharge de l'esprit, par le système de notes, entrave et transforme nécessairement la recherche en superficialité et absence de culture.

L'enseignement devrait être ainsi : celui qui le reçoit le recueille comme un don inestimable mais jamais comme une contrainte pénible.

(p. 158 Principes de la recherche)

Mais regardons à nouveau ceux qui ont trouvé grâce aux yeux de l'ange. Ils se révèlent singuliers, peu communicatifs, solitaires et malgré ces points communs se ressemblent moins que ceux qui ont été expulsés. Qu'est-ce qui les a conduits au Temple (de la Science) ? La réponse n'est pas facile à fournir et ne peut assurément pas s'appliquer uniformément à tous. Mais d'abord en premier lieu, avec Schopenhauer, je m'imagine qu'une des motivations les plus puissantes qui incitent à une œuvre artistique ou scientifique consiste en une volonté d'évasion du quotidien dans sa rigueur cruelle et sa monotonie désespérante, en un besoin d'échapper aux chaînes des désirs propres éternellement instables. Cela pousse les êtres sensibles à se dégager de leur existence personnelle pour chercher l'univers de la contemplation et de la compréhension objectives. Cette motivation ressemble à la nostalgie qui attire le citadin loin de son environnement bruyant et compliqué vers les paisibles paysages de la haute montagne, où le regard vagabonde à travers une atmosphère calme et pure, et se perd dans les perspectives reposantes semblant avoir été créées pour l'éternité.

A cette motivation d'ordre négatif s'en associe une autre plus positive. L'homme cherche à se former de quelque manière que ce soit, mais selon sa propre logique, une image du monde **simple et claire**.

Ainsi surmonte-t-il l'univers du vécu parce qu'il s'efforce dans une certaine mesure de le remplacer par cette image. Chacun à sa façon procède de cette manière, qu'il s'agisse d'un peintre, d'un poète, d'un philosophe spéculatif ou d'un physicien. A cette image et à sa réalisation, il consacre l'essentiel de sa vie affective pour acquérir ainsi la paix et la force qu'il ne peut pas obtenir dans les limites trop restreintes de l'expérience tourbillonnante et subjective.

La méthode du théoricien implique qu'il utilise comme base dans toutes les hypothèses ce qu'on appelle des principes, à partir desquels il peut déduire des conséquences. Son activité se divise donc essentiellement en deux parties. Il doit rechercher d'abord ces principes et ensuite développer les conséquences qui leur sont inhérentes. Pour l'exécution de ce second travail, il reçoit à l'école un outillage excellent. Si donc la première de ces tâches est déjà accomplie dans un certain domaine ou pour un certain ensemble de relations, il ne manquera pas de réussir par un travail et un raisonnement persévérants. Mais la première clef de ces tâches, c'est-à-dire celle d'établir les principes qui serviront de base à sa déduction, se présente de manière toute différente. Car ici il n'existe pas de méthode qu'on puisse apprendre ou systématiquement appliquer pour atteindre un objectif. Le chercheur doit plutôt épier, si l'on peut dire, dans la nature ces principes généraux, pendant qu'il dégage à travers les grands ensembles de faits expérimentaux des traits généraux et certains, qui peuvent être explicités nettement.

[...]
En plus, objectivement, mon exercice d'aujourd'hui pourrait trouver une justification en ce sens : ne serait-il point intéressant de connaître ce que pense de sa science un homme qui, sa vie durant, s'est exercé de toute son énergie à en éclaircir et à en perfectionner les éléments de base ? Sa façon d'appréhender l'évolution ancienne et contemporaine pourrait influencer terriblement ce qu'il attend de l'avenir et donc ce qu'il vise comme objectif immédiat. Mais c'est là le destin de tout individu qui se donne passionnément au monde des idées.

[...]
Cette conception exerçait sur moi une véritable fascination sans que j'y trouve une base possible pour une théorie nouvelle.

[...]
La **simplicité** me conseillait de...

[...]
Cette évidence ne coïncidait pas avec la vieille expérience m'affirmant que tous les corps subissent dans un champ de gravitation la même accélération. Ce principe, dont la formulation se traduit par l'égalité des masses inertes et des masses pesantes, m'apparut alors dans sa signification essentielle. Au sens le plus fort du terme, je le découvris et son existence m'amena à deviner qu'il incluait probablement la clef pour une intelligence meilleure et plus profonde de l'inertie et de la gravitation.

[...]
Par conséquent, je devais fonder une théorie dont les équations garderaient leur forme dans le cas de transformations non linéaires de coordonnées. J'ignorais, à ce moment de ma recherche, si elle s'appliquerait à des transformations de coordonnées tout à fait ordinaires (continues), ou bien seulement à certaines.

Je remarquais vite qu'avec l'introduction, exigée par le principe d'équivalence, des transformations non linéaires, l'explication simplement physique des coordonnées devait disparaître, c'est-à-dire que je ne pouvais plus attendre que les différences de coordonnées expriment les résultats immédiats des mesures réalisées avec des règles et des horloges idéales. Cette évidence me gênait terriblement car pendant longtemps, je n'arrivais pas à situer la place réelle et nécessaire des coordonnées en physique. Je n'ai vraiment résolu ce dilemme qu'en 1912.

[...]
Ces erreurs de jugement durèrent deux années de travail singulièrement ardu. Je reconnus enfin que je m'étais trompé à la fin de 1915...

[...]
Exemple : un archéologue d'une future civilisation découvre un traité de géométrie d'Euclide, mais sans figures. Par la lecture des théorèmes, il reconstituera bien l'emploi des mots "point", "droite", "plan". Il reconstruira aussi la chaîne des théorèmes et même, d'après les règles connues, il pourra en inventer de nouveaux. Mais cette élaboration de théorèmes restera pour lui un vrai jeu avec des mots, tant qu'il ne "pourra pas se figurer quelque chose" avec les expressions "point", "droite", "plan", etc. Mais s'il le peut et seulement s'il le peut, la géométrie deviendra pour lui un réel contenu. Le même raisonnement s'applique à la mécanique analytique et en général à toutes les sciences logico-déductives.

Qu'est-ce que je veux dire par "pouvoir se figurer quelque chose avec les expressions "point", "droite", "plan", etc." ? D'abord je précise qu'il faut exprimer la matière des expériences sensibles auxquelles ces mots renvoient. Ce problème extra-logique restera le problème clef que l'archéologue ne pourra résoudre que par intuition, puisant dans ses expériences pour y chercher s'il y trouverait quelque chose d'analogue à ces expressions primitives de la théorie et de ces axiomes, bases mêmes des règles du jeu. Voilà comment, absolument, il faut poser la question de l'existence d'une chose représentée abstraitement.

[...]
Les méthodes inductives, d'usage dans la Science, correspondant en réalité à la jeunesse de la Science, sont éliminées pour une méthode déductive précautionneuse. Une combinaison théorique de ce genre doit présenter un haut degré de perfection pour pouvoir déboucher sur des conséquences qui, en dernière analyse, seront confrontées à l'expérience. Là encore, le juge suprême, avouons-le, reste le fait expérimental ;

mais la reconnaissance par le fait expérimental évalue aussi le travail terriblement long et complexe et souligne les ponts établis entre les immenses conséquences vérifiables et les axiomes qui les ont permis. Le théoricien doit exécuter ce travail de Titan avec la claire certitude qu'il n'a d'autre ambition de préparer peut-être l'assassinat de sa propre théorie. On ne doit jamais critiquer le théoricien quand il entreprend un tel travail et le taxer de fantaisiste. Il faut estimer cette fantaisie. Car elle représente pour lui le seul itinéraire qui mène au but. Assurément il ne s'agit pas d'une plaisanterie, mais d'une patiente recherche en vue des possibilités **logiquement les plus simples**, et en vue de leurs conséquences.

[...]
Aussi Kepler devait-il avoir une singulière conviction en ces lois pour qu'il puisse, des dizaines d'années durant, y consacrer toutes ses forces par un travail obstiné et suprêmement compliqué.

[...]
Il est seul. Nul ne le soutient ni ne le comprend.

[...]
Mais Newton veut répondre à la question précise : existe-t-il **une règle simple** ?

[...]
Ces lois concernent le mouvement en tant qu'ensemble. Elles ne répondent pas à la question : "Comment de l'état de mouvement d'un système découle le mouvement qui lui succède immédiatement dans la durée ?".

[...]
L'effort vers la connaissance, par sa nature propre, nous pousse en même temps à l'intelligence de l'extrême variété de l'expérience et à la maîtrise de la **simplicité** économique des hypothèses fondamentales. L'accord final de ces objectifs représente dans le premier moment de nos recherches un acte de foi. Sans cette foi, la conviction de la valeur indépendante de la connaissance n'existerait pas, cohérente et indestructible.

Cette attitude profondément religieuse de l'homme scientifique face à la vérité rejaillit sur toute sa personnalité. En effet, en deux domaines les résultats de l'expérience et les lois de la pensée commandent par eux-mêmes. Et donc le chercheur, en principe, ne se fonde sur aucune autorité dont les décisions ou les communications pourraient prétendre à la vérité. D'où le violent paradoxe suivant : un homme livre toute son énergie à des expériences objectives et il se transforme, dès qu'on l'envisage en sa fonction sociale, en un individualiste extrême qui, théoriquement du moins, ne se fierait qu'à son propre jugement. On pourrait presque dire que l'individualisme intellectuel et la recherche scientifique naissent ensemble historiquement, et que depuis ils ne se séparent plus.

Or l'homme scientifique présenté ainsi, qu'est-il d'autre qu'une simple abstraction, invisible dans le monde réel, mais comparable à l'*homme oeconomicus* de l'économie classique ? Or, dans la réalité, la science concrète, celle de notre quotidien, ne se serait jamais créée et maintenue vivace si cet homme de science n'était apparu, au moins dans ses grandes lignes, dans un grand nombre d'individus et pendant de longs siècles.

Evidemment, je ne considère pas automatiquement comme un homme scientifique celui qui sait se servir d'instruments et de méthodes jugés scientifiques. Je ne pense qu'à ceux dont l'esprit se révèle vraiment scientifique.

Extraits de *Et si le temps n'existait pas ?* de Carlo Rovelli (DC 24/11/13)

(p. 13) Enfant, je lisais les fables d'un écrivain italien pour enfants, Gianni Rodari. L'une d'elles raconte l'histoire de Giovannino et de la route qui ne mène nulle part. Giovannino vivait dans un village où il y avait une route qui, d'après tout le monde, ne menait nulle part. Mais Giovannino était curieux et têtu et, malgré ce que tout le monde disait, il voulait aller voir. Il y alla, et bien sûr il trouva un château et une princesse, qui le couvrit de pierres précieuses. Quand il rentra au village, ainsi nanti, tout le monde se précipita sur la route, mais personne n'y trouva plus le moindre trésor.

J'ai lu cet extrait jeudi soir ; le matin-même, avec les élèves de CE1 que j'ai en classe, nous avions lu dans leur manuel de lecture une autre histoire de Gianni Rodari, celle de l'enfant qui posait ses questions à l'envers "Pourquoi les tiroirs ont-ils des tables ?".

(p. 67 et 68) La vieille idée aristotélicienne et cartésienne voit l'espace comme relation.

Une théorie complète de la gravitation quantique ne sera probablement construite qu'en abandonnant complètement l'idée newtonienne de l'espace comme entité. L'espace n'est pas une entité dans laquelle les objets sont localisés : l'entité "espace" n'existe pas. [...] Ce sont les relations qui constituent l'espace.

La base même de la science est donc la pensée critique : la conscience forte que nos visions du monde sont toujours partielles, subjectives, imprécises, provinciales et simplistes. Il faut sans cesse chercher à comprendre mieux. A ouvrir des horizons. A trouver un point de vue plus large. Cela n'est ni commode ni naturel car, d'une certaine façon, nous sommes prisonniers de nos pensées. Il est par définition impossible de sortir de notre propre pensée. On ne peut pas la regarder du dehors et la modifier. C'est de l'intérieur de nos erreurs qu'il faut travailler pour découvrir *où* nous sommes en train de nous tromper. Cela revient, pour utiliser une belle et célèbre image, à reconstruire son bateau tout en naviguant. La science, c'est cela : un effort continu pour reconstruire et restructurer notre propre pensée alors même que nous sommes en train de penser.

(p. 81 et 82) Dès mon arrivée, Wheeler est venu me voir dans le Bed and breakfast où j'avais trouvé à me loger. Nous avons pris le petit-déjeuner ensemble et puis il m'a accompagné dans une longue promenade à travers le campus. Je lui ai expliqué les résultats de nos calculs, tandis que lui me racontait ses histoires extraordinaires : Bohr, la bombe atomique... "Tu vois, Carlo, me disait-il, quand Einstein est arrivé ici la première fois, fuyant l'Allemagne nazie, je suis allé le chercher au petit matin, comme je viens de le faire avec toi, et nous nous sommes promenés le long du même parcours...". Pourquoi le voisinage, même indirect, des hommes qui ont laissé le plus de traces dans notre pensée nous donne-t-il tant d'émotion ? Ce sont des hommes comme les autres, bien sûr, avec leurs faiblesses et leur humanité comme tout le monde, mais la fascination que nous avons éprouvée pour leurs idées leur confère une aura qui nous enchante. Ils nous ont ouvert des chemins que nous avons le privilège de pouvoir suivre, et de ce fait éveillent admiration, gratitude et affection.

(p. 94 et 95) Revenons-en aux principes. Ce qu'il faut comprendre pour commencer, c'est que lorsque deux événements se déroulent en des endroits suffisamment éloignés, il n'y a pas de sens, en général, à dire lequel des deux arrive *le premier*. Et il n'y a pas de sens non plus à demander ce qui arrive *en ce moment précis* dans la galaxie d'Andromède, par exemple. La raison en est que le temps ne s'écoule pas partout de la même manière. Nous avons notre temps, et la galaxie d'Andromède a le sien, et de manière générale ces deux temps ne peuvent pas être mis en relation.

La seule chose qu'on puisse faire, c'est échanger des signaux, mais ceux-ci vont prendre des millions d'années pour faire l'aller-retour entre ici et Andromède. Imaginez un extra-terrestre qui nous envoie un signal depuis Andromède. Nous recevons ce message *aujourd'hui* et nous y répondons immédiatement. Nous pouvons dire que le moment où l'extra-terrestre a envoyé le signal se place *avant* aujourd'hui, et que le moment où il recevra la réponse viendra *après* aujourd'hui. Mais pendant les millions d'années qui s'écoulent entre l'envoi du signal par l'extra-terrestre et sa réception de notre réponse, il n'existe pas de moment particulier sur Andromède qui corresponde à cet "aujourd'hui" sur la Terre.

Tout cela pour dire que nous ne devons pas penser au temps comme s'il existait une horloge cosmique rythmant la vie de l'univers. Nous devons y penser comme à quelque chose de local : chaque objet dans l'univers possède son propre temps. La façon dont les temps de chacun s'articulent lorsque des objets se

rencontrent ou échangent des signaux peut être décrite précisément. Mais pour le faire, dans la description mathématique du monde, on ne parle pas de “temps” et d”’espace”, mais d’une union des deux appelée “espace-temps”.

(p. 106) Quand un scientifique formule une idée, il tend généralement à croire qu’elle est correcte. Si personne d’autre n’approuve, il continuera souvent à croire qu’il a raison et que les autres ont tort... mais il aura quelques doutes. S’il découvre que quelqu’un d’autre a trouvé la même idée indépendamment de lui, la tentation de croire que “nous” avons raison et que les autres “ne comprennent rien” devient irrésistible...

L'Homme magnétique. — L'Homme non magnétique.

L'homme robuste, gai, bien équilibré, conscient de sa force et du rôle important qu'il joue dans l'humanité ne ressemble en rien au pauvre mélancolique constamment en proie à la plus sombre tristesse et redoutant sans cesse des malheurs qui n'auront peut-être pas le temps de lui arriver. C'est que notre état physique et notre état moral sont solidaires l'un de l'autre et que, si l'un est sérieusement affecté, l'autre souffre toujours plus ou moins. La force silencieuse de la pensée agissant constamment dans le même sens, façonne notre corps, burine nos traits, dirige nos manières, assure nos gestes et règle notre démarche. En imprimant à tout notre être physique une série de mouvements correspondant à ceux de notre état mental, elle nous rend agréables, attractifs et sympathiques ou désagréables, répulsifs et antipathiques ; et les empreintes de ces qualités et de ces défauts se voient constamment sur notre physionomie, dans nos manières, dans notre attitude, dans notre allure, tout autant que ces qualités elles-mêmes se sentent, car elles sont directement perçues par un sens de l'esprit dont nous ne faisons que soupçonner l'existence.

S'il en est ainsi, on peut donc définir à l'avance le type de l'homme attractif dont la personnalité magnétique, est développée à un certain degré, et Turnbull nous trace ainsi qu'il suit dans son Cours de Magnétisme personnel les traits caractéristiques de chacun d'eux ; voyons, d'abord, l'homme magnétique :

l'homme magnétique. — Quand vous vous trouvez en compagnie de l'homme consciemment magnétique, le premier effet qu'il vous fait est celui d'être au repos : il n'est point nerveux, il ne s'agite pas. Vous éprouvez, ensuite, le sentiment qu'il a en lui, une force en réserve quelque part, une force dont vous ne pouvez pas fixer l'endroit. Elle ne se trouve pas précisément dans son regard, ni dans ses manières, ni dans son parler, ni dans ses actions ; mais elle est là, elle existe et semble faire partie de lui. Voilà exactement le fait : c'est une partie de lui, et quelques minutes auparavant, tout singulier que cela vous paraisse, c'était dans une petite mesure une partie de vous ! Un peu de cette force d'attraction qu'il montre et dont vous êtes conscient est allé de vous à lui sans que vous le sachiez...

Examinons l'homme d'un peu plus près afin de connaître le secret de la fascination qu'il exerce sur vous. Observez, d'abord, son regard. Ses yeux vous dominant quoiqu'il ne vous regarde pas fixement. Il ne regarde pas dans vos yeux ni dans l'un plutôt que dans l'autre : il regarde juste entre les deux, là où votre nez prend racine. Son regard semble vous percer avec intention — un regard fixe et pénétrant, mais dans lequel il n'y a rien de désagréable. Vous sentez qu'il n'est pas, qu'il ne peut pas être impertinent. Remarquez également qu'il ne vous regarde pas ainsi quand vous parlez : il attend votre communication puis il vous envoie la sienne. Quand il parle, il vous regarde de cette manière déterminée, dominatrice et, cependant, bienveillante, mais il ne se fait, pas valoir...

Il vous écoute avec politesse ; mais vous recevez l'impression d'une volonté inflexible, vous percevez une puissance dans lui. C'est l'homme qui doit être obéi ; en un mot, l'impression qu'il vous laisse est celle de quelqu'un qui sait exactement ce qu'il veut et qui n'est pas pressé parce qu'il est certain de l'obtenir... Voilà, donc, pourquoi il est si calme, si assuré ! Le savoir est une Force et il sait que son état dépend des Lois de Cause, et d'Effet.

Analysons sa conversation. Vous a-t-il appris quelque chose ? Très peu, et rien qu'on puisse considérer comme vain ou prétentieux. Ce qu'il donne n'est généralement point important, quoique vous semblez croire cela tandis que vous l'écoutez.

Il n'est pas empressé. Il vous fait plutôt sentir que, s'il le voulait, il pourrait en dire long. Ainsi, il pique un peu votre curiosité..., mais il ne vous tend pas un piège pour chercher à se faire admirer...

Quand cet homme a attiré vers lui la popularité, l'influence, le succès, il a accepté ces dons : il les a considérés comme son dû..., puis il a continué son chemin... Il a acquis la richesse de la même façon qu'il a acquis la popularité : par la domination. Il a dominé par le magnétisme ; il a attiré les hommes à lui...

Quelle impression cet homme vous a-t-il faite ? — Celle-ci : vous désirez le connaître mieux parce que vous sentez qu'il vous est sympathique, d'une façon mystérieuse et que vous ne pouvez définir. Il vous tient selon l'expression courante, et vous ne pouvez vous soustraire à son influence, même après que vous avez pris congé de lui.

Il se sert de votre force. Si vous voulez bien observer ce qui se passe entre lui et vous, vous verrez que vous êtes celui qui a fait montre de vos connaissances, que vous êtes celui qui a cherché à plaire: en un mot, vous êtes celui qui a donné. Oui, c'est précisément cela : vous avez donné ; il a reçu. S'il avait voulu que ce fût autrement, lui, fort de son savoir conscient, et vous, faible et dépourvu, vous auriez été obligé de recevoir tout ce qu'il aurait voulu vous donner en fait d'impulsions, d'ordres ou d'idées... Mais il ne l'a pas voulu ; il s'est permis, simplement, de vous faire une bonne impression. Puis, il est parti après vous avoir pris un peu de magnétisme, comme l'abeille s'envole après avoir pris te miel de la fleur.

l'homme non magnétique. — Après avoir, ainsi, décrit la caractéristique de l'homme magnétique qui va de succès en succès, le même auteur décrit celle de l'homme non magnétique qui personnifie l'insuccès ; puis il les compare l'un à l'autre.

Il vous irrite ; si vous êtes acariâtre vous-même, il augmente votre mauvaise humeur ; si vous avez des dispositions, être morbide, il obscurcit votre horizon encore plus ; si vous vous sentez heureux, sa présence semble avoir l'effet de peser sur vous. Oui, c'est un poids, et vous avez à le soulever. Il vous demande de la sympathie ; il dit qu'on ne le comprend pas ; il se plaint du sort, du temps, d'une personne quelconque.

C'est un mécontent, un bavard ; il vous communique ses secrets ; il veut que vous preniez part à ses ennuis. C'est un impulsif sans discrétion, manquant de calme, de jugement de mesure et d'intérêt. Flattez-le et laissez-le s'en aller ! Vous pouvez le prendre de la manière la plus aisée en flattant son égoïsme : parlez-lui en, débarrassez-vous de lui... et... n'y pensez plus.

Vous vous sentez heureux dès qu'il est parti. Sa présence a pesé horriblement sur vous parce que vous ne saviez pas comment vous soustraire à son influence. Si vous l'aviez su, vous auriez pu, non seulement vous épargner une perte de magnétisme, mais même tirer, si vous l'aviez voulu, quelque chose de sa faiblesse.

Pourquoi donc, est-il dépourvu de dispositions attractives ? — La raison en est bien simple. C'est un négatif ; il dépend d'autrui ; il a des griefs à exposer... Pouvez-vous vous figurer l'homme magnétique que nous venons de décrire, comme ayant, lui aussi, des griefs ? Essayez donc de vous le représenter ainsi . — Non, ce serait absurde. Notre homme magnétique est une force parce qu'il s'est rendu maître des circonstances, parce qu'il a gardé une attitude d'esprit qui soumet les événements, qui domine ce qui est autour de lui.

Voici notre homme non magnétique personnifiant l'insuccès, de son propre aveu, quoiqu'il ne le sache peut-être pas ; il est faible ; il se plaint ; l'attitude de son esprit appelle l'insuccès ; il gaspille la pensée et l'énergie. D'après la Loi immuable de Cause et d'Effet, un tel être ne peut qu'échouer...

Voilà nos deux types en présence. Etudiez les attentivement. Que le premier vous serve de modèle et le second d'avis. Observez ces grands préceptes et qu'ils tintent, toujours, à vos oreilles : « N'exposez pas vos griefs, ne recherchez ni la sympathie ni la flatterie. Découvrez la force qui agit dans tous les désirs et appropriez-vous cette force. »

Pour ne pas diminuer l'importance de cette magistrale description, je n'ajouterai rien à la caractéristique de l'homme magnétique comparée à celle de l'homme non magnétique.

Conjecture de Goldbach : écrire, réécrire, compter

Denise Vella-Chemla

16/2/14

1 Introduction

On souhaite trouver une démonstration de la conjecture de Goldbach, qui stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers [*].

On se propose dans ce but d'utiliser une modélisation qui associe à chaque nombre pair n un mot d'un langage à 4 lettres $m_{abcd}(n)$ qui code la primalité des nombres impairs x (compris entre 3 et et $n/2$) et de leur complémentaire.

On identifiera le processus permettant de passer du mot d'un nombre pair n au mot du nombre pair suivant $n+2$.

On caractérisera l'existence d'un décomposant de Goldbach d'un nombre pair par une simple condition que vérifie son mot.

On essaiera de trouver une formule récurrente qui permet de passer du nombre de décompositions de Goldbach $dg(n)$ d'un nombre pair n au nombre de décompositions de Goldbach $dg(n+2)$ du nombre pair suivant $n+2$.

2 Mot d'un nombre pair

On choisit de représenter le fait qu'un entier est premier par le booléen 0 et le fait qu'il est composé par le booléen 1.

On rappelle :

- que la lettre a est utilisée pour symboliser une décomposition de n de la forme $p+q$ avec p et q premiers et $p \leqslant n/2$;
- que la lettre b est utilisée pour symboliser une décomposition de n de la forme $p+q$ avec p composé et q premier et $p \leqslant n/2$;
- que la lettre c est utilisée pour symboliser une décomposition de n de la forme $p+q$ avec p premier et q composé et $p \leqslant n/2$;

∗. Dans l'égalité $n = p+q$ avec n pair supérieur à 2, p et q premiers, on appellera p et q décomposants de Goldbach de n ou sommants.

– que la lettre d est utilisée pour symboliser une décomposition de n de la forme $p+q$ avec p et q composés et $p \leqslant n/2$;

Exemples : Ci-dessous les mot $m_{abcd}(40)$, $m_{abcd}(42)$ et $m_{abcd}(44)$.

40	37	35	33	31	29	27	25	23	21
	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0
	3	5	7	9	11	13	15	17	19
$m_{abcd}(40)$	a	c	c	b	a	c	d	a	c

42	39	37	35	33	31	29	27	25	23	21
	1	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21
$m_{abcd}(42)$	c	a	c	d	a	a	d	c	a	d

44	41	39	37	35	33	31	29	27	25	23
	0	1	0	1	1	0	0	1	1	0
	0	0	0	1	0	0	1	0	0	1
	3	5	7	9	11	13	15	17	19	21
$m_{abcd}(44)$	a	c	a	d	c	a	b	c	c	b

3 Identifier ce que fait le processus

Le mot m_{abcd} du nombre pair $n+2$ s'obtient de la façon suivante à partir de celui de n :

– la première lettre du mot de $n+2$ est a si $n-3$ est premier et c sinon (cette première lettre est la seule qui introduit de l'indéterminisme car elle n'appartient pas au mot du langage à 4 lettres $m_{abcd}(n)$ ou ne se déduit pas des lettres de ce dernier) ;

– les lettres suivantes du mot de $n+2$ sont obtenues par réécriture du mot

de n selon les règles ci-dessous :

$$
\begin{array}{l}
aa \to a \\
ab \to b \\
ac \to a \\
ad \to b \\
ba \to a \\
bb \to b \\
bc \to a \\
bd \to b \\
ca \to c \\
cb \to d \\
cc \to c \\
cd \to d \\
da \to c \\
db \to d \\
dc \to c \\
dd \to d
\end{array}
$$

On note que 4 règles de réécriture ($aa \to a,\ ac \to a,\ ba \to a,\ bc \to a$) assurent d'obtenir une lettre a au moins dans le mot de $n + 2$.

- enfin, la concaténation d'une lettre en fin de mot, dans le cas où n est un double de pair obéit à la règle suivante :
  - si n a a ou b comme dernière lettre, après avoir obtenu le mot de $n + 2$ en appliquant les règles de réécriture, on lui concatène la lettre a ;
  - si n a c ou d comme dernière lettre, après avoir obtenu le mot de $n + 2$ en appliquant les règles de réécriture, on lui concatène la lettre d.

En annexe 2, on montre qu'on a toujours $x^2 = x$ par application réitérée de chacune des 16 règles de réécriture.

4 Caractériser l'existence d'une décomposition de Goldbach dans le mot d'un nombre pair

n admet une décomposition de Goldbach si son mot contient une lettre a.

Le double d'un nombre impair dont le mot m_{abcd} se termine par une lettre a est un double de nombre premier, qui vérifie donc trivialement la conjecture de Goldbach (ex : 46 dont le mot m_{abcd} est *aacbccbacda* se terminant par une lettre a est le double de 23, premier).

Le double d'un nombre pair dont le mot m_{abcd} se termine par une lettre a est le double d'un "père de jumeau" (ex : 36 dont le mot m_{abcd} est *acabca* se terminant par une lettre a est le double de 18, un père de jumeau, i.e. un nombre pair compris entre deux nombres premiers, en l'occurrence 17 et 19).

5 Formule récurrente

On cherche une formule récurrente [†] qui permettrait de "compter les lettres a". Dans ce but, on observe attentivement les règles de réécriture.

Par abus de langage (!), on dira que les règles $aa \to a$, $ad \to b$ ainsi même que $ab \to b$ [‡], éliminent un a à gauche. On dira également que les règles $ca \to c$ et $da \to c$ éliminent quant à elles un a à droite.

Si l'on note $X_{\alpha\beta}$ le nombre d'occurrences du sous-mot $\alpha\beta$ dans le mot de $m_{abcd}(n)$, alors il semblerait que l'inégalité suivante soit toujours vérifiée :

$$\begin{aligned} dg(n+2) \geqslant dg(n) \quad & -X_{aa} - X_{ab} - X_{ad} - X_{ca} - X_{da} \\ & +X_{bc} + X_{dac} \\ & +X_{caa} + X_{daa} + X_{cad} + X_{dad} + X_{cab} + X_{dab} \end{aligned}$$

Cette formule garantit peut-être qu'au-delà d'un certain entier, le nombre de a du mot d'un nombre pair (i.e. le nombre de décompositions de Goldbach du nombre pair en question) ne peut jamais devenir nul.

†. On est conforté dans l'idée qu'une telle formule récurrente existe par l'article d'Euler *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs* dans lequel il trouve une telle formule pour la somme des diviseurs d'un entier.

‡. bien que cette dernière ne le fasse que par combinaison avec une autre règle.

Annexe 1 : mots du langage à 4 lettres associés aux nombres pairs de 6 à 100

6 : a
8 : a
10 : $a\ a$
12 : $c\ a$
14 : $a\ c\ a$
16 : $a\ a\ c$
18 : $c\ a\ a\ d$
20 : $a\ c\ a\ b$
22 : $a\ a\ c\ b\ a$
24 : $c\ a\ a\ d\ a$
26 : $a\ c\ a\ b\ c\ a$
28 : $c\ a\ c\ b\ a\ c$
30 : $c\ c\ a\ d\ a\ a\ d$
32 : $a\ c\ c\ b\ c\ a\ b$
34 : $a\ a\ c\ d\ a\ c\ b\ a$
36 : $c\ a\ a\ d\ c\ a\ d\ a$
38 : $c\ c\ a\ b\ c\ c\ b\ c\ a$
40 : $a\ c\ c\ b\ a\ c\ d\ a\ c$
42 : $c\ a\ c\ d\ a\ a\ d\ c\ a\ d$
44 : $a\ c\ a\ d\ c\ a\ b\ c\ c\ b$
46 : $a\ a\ c\ b\ c\ c\ b\ a\ c\ d\ a$
48 : $c\ a\ a\ d\ a\ c\ d\ a\ a\ d\ c$
50 : $a\ c\ a\ b\ c\ a\ d\ c\ a\ b\ c\ d$
52 : $c\ a\ c\ b\ a\ c\ b\ c\ c\ b\ a\ d$
54 : $c\ c\ a\ d\ a\ a\ d\ a\ c\ d\ a\ b\ d$
56 : $a\ c\ c\ b\ c\ a\ b\ c\ a\ d\ c\ b\ b$
58 : $c\ a\ c\ d\ a\ c\ b\ a\ c\ b\ c\ d\ b\ a$
60 : $c\ c\ a\ d\ c\ a\ d\ a\ a\ d\ a\ d\ d\ a$
62 : $a\ c\ c\ b\ c\ c\ b\ c\ a\ b\ c\ b\ d\ c\ a$
64 : $a\ a\ c\ d\ a\ c\ d\ a\ c\ b\ a\ d\ b\ c\ c$
66 : $c\ a\ a\ d\ c\ a\ d\ c\ a\ d\ a\ b\ d\ a\ c\ d$
68 : $c\ c\ a\ b\ c\ c\ b\ c\ c\ b\ c\ b\ b\ c\ a\ d$
70 : $a\ c\ c\ b\ a\ c\ d\ a\ c\ d\ a\ d\ b\ a\ c\ b\ d$
72 : $c\ a\ c\ d\ a\ a\ d\ c\ a\ d\ c\ b\ d\ a\ a\ d\ b$
74 : $a\ c\ a\ d\ c\ a\ b\ c\ c\ b\ c\ d\ b\ c\ a\ b\ d\ a$
76 : $a\ a\ c\ b\ c\ c\ b\ a\ c\ d\ a\ d\ d\ a\ c\ b\ b\ c$
78 : $c\ a\ a\ d\ a\ c\ d\ a\ a\ d\ c\ b\ d\ c\ a\ d\ b\ a\ d$
80 : $c\ c\ a\ b\ c\ a\ d\ c\ a\ b\ c\ d\ b\ c\ c\ b\ d\ a\ b$
82 : $a\ c\ c\ b\ a\ c\ b\ c\ c\ b\ a\ d\ d\ a\ c\ d\ b\ c\ b\ a$
84 : $c\ a\ c\ d\ a\ a\ d\ a\ c\ d\ a\ b\ d\ c\ a\ d\ d\ a\ d\ a$
86 : $a\ c\ a\ d\ c\ a\ b\ c\ a\ d\ c\ b\ b\ c\ c\ b\ d\ c\ b\ c\ a$
88 : $c\ a\ c\ b\ c\ c\ b\ a\ c\ b\ c\ d\ b\ a\ c\ d\ b\ c\ d\ a\ c$
90 : $c\ c\ a\ d\ a\ c\ d\ a\ a\ d\ a\ d\ d\ a\ a\ d\ d\ a\ d\ c\ a\ d$
92 : $a\ c\ c\ b\ c\ a\ d\ c\ a\ b\ c\ b\ d\ c\ a\ b\ d\ c\ b\ c\ c\ b$
94 : $c\ a\ c\ d\ a\ c\ b\ c\ c\ b\ a\ d\ b\ c\ c\ b\ b\ c\ d\ a\ c\ d\ a$
96 : $c\ c\ a\ d\ c\ a\ d\ a\ c\ d\ a\ b\ d\ a\ c\ d\ b\ a\ d\ c\ a\ d\ c$
98 : $c\ c\ c\ b\ c\ c\ b\ c\ a\ d\ c\ b\ b\ c\ a\ d\ d\ a\ b\ c\ c\ b\ c\ d$
100 : $a\ c\ c\ d\ a\ c\ d\ a\ c\ b\ c\ d\ b\ a\ c\ b\ d\ c\ b\ a\ c\ d\ a\ d$

Annexe 2 : $x^2 = x$ pour chaque règle de réécriture

aa/aa	$\to aaa$	$\to aa$
ab/ab	$\to bab$	$\to ab$
ac/ac	$\to aca$	$\to ac$
ad/ad	$\to bcb$	$\to ad$
ba/ba	$\to aba$	$\to ba$
bb/bb	$\to bbb$	$\to bb$
bc/bc	$\to ada$	$\to bc$
bd/bd	$\to bdb$	$\to bd$
ca/ca	$\to cac$	$\to ca$
cb/cb	$\to dad$	$\to cb$
cc/cc	$\to ccc$	$\to cc$
cd/cd	$\to dcd$	$\to cd$
da/da	$\to cbc$	$\to da$
db/db	$\to dbd$	$\to db$
dc/dc	$\to cdc$	$\to dc$
dd/dd	$\to ddd$	$\to dd$

Le petit baluchon

Denise Vella-Chemla

21 février 2014

On voudrait rassembler ici les cailloux trouvés durant la promenade.

1 Sinusoïdes

On s'est intéressé à elles en réalisant que $sin(5\pi x)$ s'annule 4 fois sur l'intervalle $]0,1[$, pour les fractions $\frac{1}{5},\frac{2}{5},\frac{3}{5},\frac{4}{5}$. De même, la sinusoïde $sin(p\pi x)$ s'annule exactement $p-1$ fois sur l'intervalle $]0,1[$ et ce jamais sur un point sur lequel s'annule la sinusoïde d'un nombre premier p' inférieur à $\sqrt{p}$. On saisit ainsi bien l'infinité de l'intervalle $]0,1[$, les sinusoïdes d'une infinité de nombres premiers réussissant à s'intercaler sans les toucher entre toutes les sinusoïdes correspondant à des nombres premiers plus petits et déjà placées sur l'intervalle.

Si on se place sur la droite réelle habituelle au lieu de se focaliser sur l'intervalle $]0,1[$, les décomposants de Goldbach se calculent très simplement ; ce sont les seuls nombres entiers inférieurs à $n/2$ qui n'annulent pas le produit suivant :

$$\prod_{p\ un\ nb\ 1^{er} \leqslant \sqrt{n}} sin\left(\frac{x\pi}{p}\right).sin\left(\frac{(n-x)\pi}{p}\right)$$

En annexe sont fournis de tels produits de sinusoïdes présentant le fait que 5 est décomposant de Goldbach de 16, que $7, 11, 17$ et 19 sont décomposants de Goldbach de 48 ou encore que $19, 31$ et 37 sont décomposants de Goldbach de 98.

On est tenté de relier ces interférences entre sinusoïdes à l'expérience de mécanique quantique dite des "fentes de Young".

2 Essayer de suivre les professeurs : rechercher la limpidité et la sincérité

Nathalie Charraud signale le souci du style de présentation des résultats et de la transmission qui motive Cantor. Il insiste en effet sur l"'effort de présenter le cheminement de pensée aussi clairement que possible" et admire particulièrement les exposés d'Hermite pour leur limpidité : "Le style personnel de Cantor va avec le souci de communiquer de la façon la plus transparente possible le processus et les étapes de sa découverte.".

Ce souci de limpidité se retrouve chez Hilbert, dans un extrait de sa conférence de 1900 : "On peut néanmoins se demander s'il n'existe pas des attributs généraux caractérisant un bon problème de mathématiques. Un mathématicien des temps passés a dit : "une théorie mathématique ne doit être regardée comme parfaite que si elle a été rendue tellement claire qu'on puisse la faire comprendre au premier individu rencontré dans la rue". Cette clarté, cette limpidité si énergiquement exigée ici d'une théorie mathématique, je l'exigerai encore davantage d'un problème mathématique parfait ; ce qui est clair et limpide nous attire en effet, ce qui est embrouillé nous rebute".

L'extrait particulièrement émouvant de Galois : "On doit prévoir que, traitant des sujets aussi nouveaux, hasardé dans une voie aussi insolite, bien souvent des difficultés se sont présentées que je n'ai su vaincre.

Aussi, dans ces deux mémoires et surtout dans le second qui est plus récent, trouvera-t-on souvent la formule : "Je ne sais pas". La classe des lecteurs dont j'ai parlé au commencement ne manquera pas d'y trouver à rire. C'est que malheureusement on ne se doute pas que le livre le plus précieux du plus savant serait celui où il dirait tout ce qu'il ne sait pas, c'est qu'on ne se doute pas qu'un auteur ne nuit jamais tant à ses lecteurs que quand il dissimule une difficulté. Quand la concurrence, c'est à dire l'égoïsme, ne règnera plus dans les sciences, quand on s'associera pour étudier, au lieu d'envoyer aux Académies des paquets cachetés, on s'empressera de publier les moindres observations pour peu qu'elles soient nouvelles, et on ajoutera : Je ne sais pas le reste.".

En cherchant à suivre Galois, on a trouvé que les décomposants de Goldbach de n sont les solutions communes et inférieures à $n/2$ de l'inéquation $x^2 - nx \neq 0$ que l'on doit résoudre simultanément dans tous les corps premiers $\mathbb{Z}/p_i\mathbb{Z}$ avec p_i un nombre premier quelconque inférieur à $\sqrt{n}$.

Traitons l'exemple de la recherche des décompositions de Goldbach de 98.
Le polynôme $x^2 - 98x$ est égal à $x^2 - 2x$ dans $\mathbb{Z}/3\mathbb{Z}$ tandis qu'il est égal à $x^2 - 3x$ dans $\mathbb{Z}/5\mathbb{Z}$, ou encore égal à x^2 tout simplement dans $\mathbb{Z}/7\mathbb{Z}$ puisque 7 divise 98.

Notons dans un tableau pour les nombres premiers supérieurs à $\sqrt{98}$ et inférieurs à 49 la moitié de 98 les valeurs des polynômes en question et voyons ceux qui sont éliminés dans chacun des corps premiers.

	11	13	17	19	23	29	31	37	41	43	47
x^2 (dont on teste la nullité dans $\mathbb{Z}/7\mathbb{Z}$)	121	169	289	361	529	841	961	1369	1681	1849	2209
$x^2 - 2x$ (dont on teste la nullité dans $\mathbb{Z}/3\mathbb{Z}$)	~~99~~	143	~~255~~	323	~~483~~	~~783~~	899	1295	~~1599~~	1763	~~2115~~
$x^2 - 3x$ (dont on teste la nullité dans $\mathbb{Z}/5\mathbb{Z}$)	88	~~130~~	238	304	~~460~~	754	868	1258	1558	~~1720~~	2068

On voit que ne sont conservés que les nombres 19, 31 et 37 qui sont comme attendu les décomposants de Goldbach de 98.

3 Somme des diviseurs d'Euler [1], minimiser / maximiser

L'article d'Euler *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs* est magique. On reste subjugué par la manière dont le mathématicien a trouvé la formule récurrente de la somme des diviseurs. Même le fait de la programmer la laisse hermétique. On trouve particulièrement esthétique la manière dont les nombres pentagonaux surgissent de la combinaison par différence de la suite des entiers et de la suite des impairs. Ci-dessous une formule récurrente plus simple que celle d'Euler pour calculer la somme des diviseurs d'un entier $\sigma(n)$.

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

On peut voir les nombres premiers comme des minima locaux de la fonction somme des diviseurs.

Puisque la somme des diviseurs d'un nombre premier p vaut $p+1$, $p+q$ est une décomposition de Goldbach de n si et seulement si $\sigma(p) + \sigma(q) = n + 2$. Les décomposants de Goldbach minimisent donc la somme de la somme des diviseurs de p et de la somme des diviseurs de q.

L'idée duale consiste à trouver les décomposants de Goldbach en maximisant le produit des indicateurs d'Euler des deux décomposants. Dominique Ceugniet a vérifié cette idée par programme jusqu'à 7.10^6 [2].

1. M. Giard, qui fournit cette formule récurrente différente de celle d'Euler sur la toile dans les notes de la séquence A000203 de l'OEIS fournit comme explication que cette formule provient d'un résultat de Chazy mais ceci serait à confirmer par des spécialistes des fonctions modulaires.
2. une cacahuète devant l'infini.

4 Ma conjecture

Tout nombre pair supérieur à 14 partage un décomposant de Goldbach avec $n - 6$.

5 Addition disjointe

La définition récursive $x \oplus y = x + y - xy$ simplifie considérablement les calculs provenant de l'application du principe d'inclusion-exclusion.

Par exemple,

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

6 Rêves d'un prince

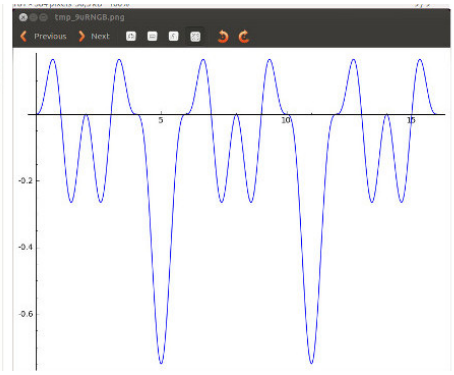
On peut trouver sur la toile le journal mathématique de Gauss. On y lit que Gauss a étudié la conjecture de Goldbach le 14 mai 1796 à Göttingen. On peut imaginer que les deux premières lettres mystérieuses du mot GEGAN qui apparaît dans la citation "Vicimus GEGAN" du 11 octobre 1796 sont les initiales respectives de Goldbach et Euler...

Ci-dessous l'extrait de la lettre qu'il a adressée à Sophie Germain, qui s'était fait passer pour un homme M. Leblanc, pour lui envoyer les résultats de ses travaux en théorie des nombres.

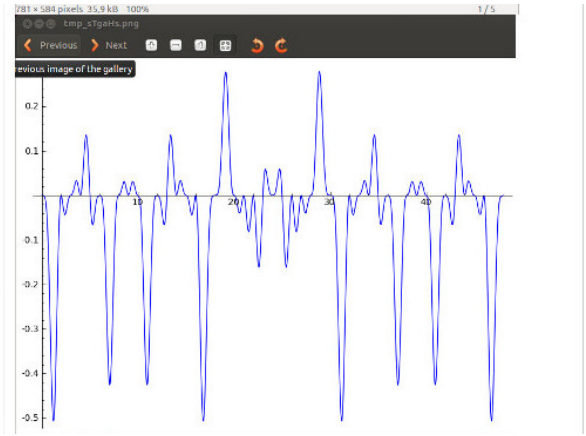
"Le goût pour les sciences abstraites en général et surtout pour les mystères des nombres est fort rare : on ne s'en étonne pas ; les charmes enchanteurs de cette sublime science ne se décèlent dans toute leur beauté qu'à ceux qui ont le courage de les approfondir. Mais lorsqu'une personne de ce sexe, qui, par nos moeurs et par nos préjugés, doit rencontrer infiniment plus d'obstacles et de difficultés que les hommes à se familiariser avec ces recherches épineuses, sait néanmoins franchir ces entraves et pénétrer ce qu'elles ont de plus caché, il faut sans doute qu'elle ait le plus noble courage, des talents tout à fait extraordinaires, le génie supérieur. En effet, rien ne pourrait me prouver d'une manière plus flatteuse et moins équivoque, que les attraits de cette science, qui ont embelli ma vie de tant de jouissances, ne sont pas chimériques, que la prédilection dont vous l'avez honorée."

Annexe : 3 exemples de calculs de produits de sinusoïdes pour trouver les décomposants de Goldbach des nombres pairs 16, 48 et 98

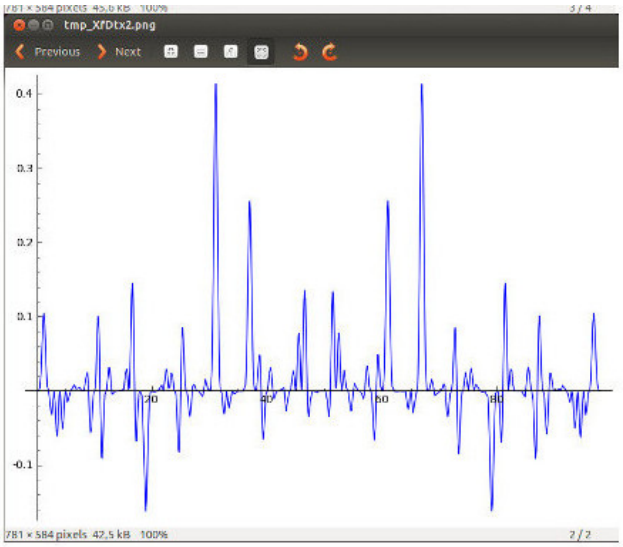
5 est décomposant de Goldbach de 16.



7, 11, 17 et 19 sont décomposants de Goldbach de 48.



19, 31 et 37 sont décomposants de Goldbach de 98.



Avoir entendu parler des idées de la physique quantique (DV - 1/3/2014)

On peut écouter sur la toile d'excellentes conférences au sujet de la mécanique quantique par Alain Aspect, Serge Haroche, Nicolas Gisin ou Michel Spiro, aux adresses suivantes :

http ://www.canal-u.tv/video/universite$_t$$oulouse_i$$i_l$$e_m$$irail/la_p$$hysique_q$$uantique_{al}$$epreuve_d$$e_l$$experience_a$$lain_a$$spect$.12026

http ://www.canal-u.tv/video/universite$_d$$e_t$$ous_l$$es_s$$avoirs/les_t$$ests_e$$t_e$$ffets_d$$e_l$$a_p$$hysique_q$$uantique$.1066

http ://www.youtube.com/watch ?v=tWeGIxnbcHk

http ://www.youtube.com/watch ?v=yA-OzMoMSXA

http ://public.weconext.eu/academie-sciences/2014-01-14/video$_i$$d_0$01/

http ://www.futura-sciences.com/magazines/matiere/infos/actu/d/physique-mecanique-quantique-faille-eliminee-experience-aspect-47262/

http ://www.youtube.com/watch ?v=tWeGIxnbcHk

http ://www.canal-u.tv/video/universitedetouslessavoirs/laphysiquequantiquesergeharoche.1065

http ://www.canal-u.tv/video/cerimes/electrodynamique$_q$$uantique_e$$n_c$$avite_s$$erge_h$$aroche$.7699

http ://www.youtube.com/watch ?v=mghV2Fl6iLE

http ://www.youtube.com/watch ?v=GA8LR4w2Q90

http ://www.youtube.com/watch ?v=ysYWnXpAMqg

http ://www.unige.ch/communication/archives/2013/gisin.html

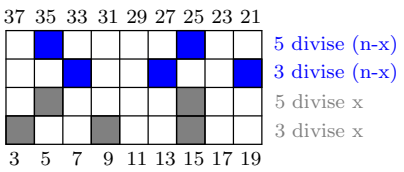
http ://vimeo.com/61521690

http ://www.youtube.com/watch ?v=qsk74xrXPjM

Et un lien vers un petit dessin animé :

http ://www.youtube.com/watch ?v=La64$_l$$UHfqs$
c
On peut établir des analogies entre la conjecture de Goldbach telle qu'on l'a modélisée et plusieurs notions du paradigme quantique.

Il semble naturel de penser que, selon le principe de quantification, chaque entier admettant des multiples entiers, les nombres premiers ne peuvent occuper que certaines positions bien particulières sur la droite des entiers, et que ces positions correspondent aux raies d'un spectre. De même, les décomposants de Goldbach d'un entier pair n, ne partageant aucun de leurs restes avec n dans chaque corps premier $\mathbb{Z}/p_i\mathbb{Z}$ ($p_i \leqslant \sqrt{n}$), peuvent être vus eux-aussi comme correspondant aux raies d'un spectre associé à n (et constituent comme une sorte de signature de n, de même que ses restes dans les différents corps premiers peuvent être considérés comme une telle signature puisque si on fixe leur nombre, ils caractérisent totalement cet entier par le théorème des restes chinois).



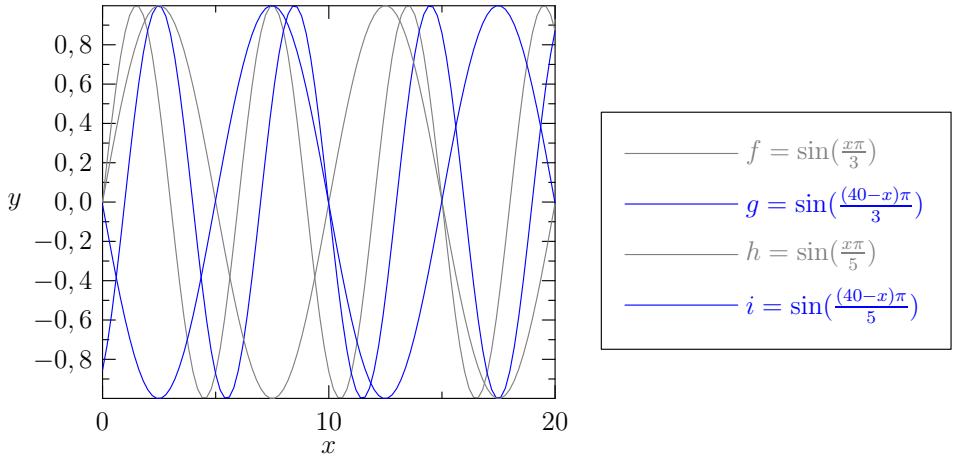
On ne réexplique pas ici la représentation par les grilles de divisibilité qui nous a permis de mieux comprendre la conjecture de Goldbach et dont l'exemple du nombre pair 40 est représenté ci-dessus. 11 et 17, qui ne sont divisibles ni par 3 ni par 5 et qui ne partagent avec 40 aucun de leur reste dans des divisions euclidiennes par 3 ou 5 (i.e. dont la colonne ne contient pas de case colorée) sont des décomposants de Goldbach de 40.

On a proposé à partir de ces grilles la possibilité de trouver les décomposants de Goldbach en calculant des produits de sinusoïdes.

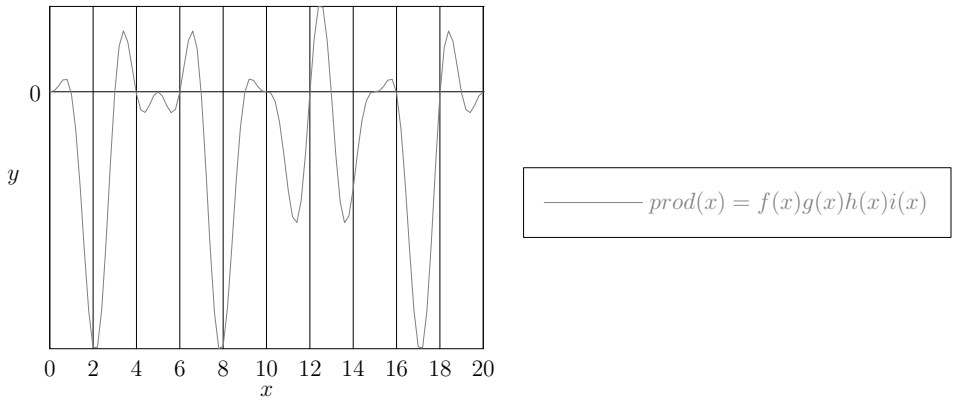
Les décomposants de Goldbach de n sont en effet les seuls nombres entiers impairs inférieurs à $n/2$ qui n'annulent pas le produit suivant :

$$\prod_{3 \leqslant p \ un \ nb \ 1^{er} \leqslant \sqrt{n}} sin\left(\frac{x\pi}{p}\right).sin\left(\frac{(n-x)\pi}{p}\right)$$

Les sinusoïdes correspondant au cas du nombre pair 40 (se reporter à la grille de divisibilité ci-dessus) sont :



Leur produit ne s'annule effectivement pas pour les nombres entiers impairs 11 et 17.



On peut établir une analogie entre ces sinusoïdes et les fonctions d'onde de la mécanique quantique. En poussant l'analogie, on peut imaginer qu'on puisse établir une probabilité qu'un nombre pair ait un décomposant de Goldbach sans pouvoir établir sa valeur, selon une sorte de principe d'incertitude.

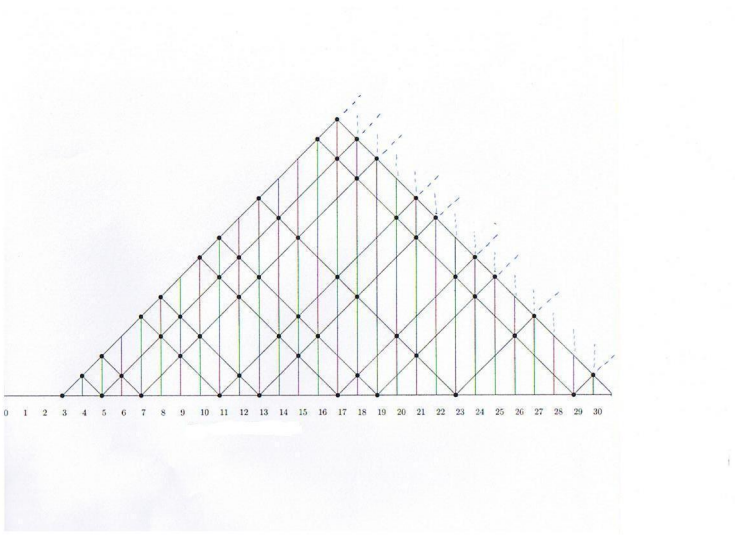
Enfin, si on souhaite établir une analogie avec la propriété d'*intrication quantique* : on associe à chaque case de la grille de divisibilité ci-dessus un q-bit qui est simultanément dans les états 0 et 1. On peut imaginer cette grille comme de taille infinie si on considère tous les nombres pairs d'un même coup. Le fait de fixer

le nombre pair n donne leur valeur à chacun des q-bits. L'intrication quantique entre q-bits doit être capable d'exprimer le fait que le q-bit associé au caractère de divisibilité $p|x$ doit être intriqué avec tout q-bit associé au caractère de divisibilité $p|ax+b$ avec $a > 0$ et $0 < b < p$, p étant un nombre premier quelconque.

Ces analogies semblent vaines : notre schéma de pensée est trop influencé par une "forte éducation au déterminisme". On va donc réitérer encore, en "s'accrochant" à un domaine bien connu, celui de la théorie des langages, des systèmes de réécriture, du "pattern-matching", notre langage à 4 lettres a, b, c, d, tout récemment trouvé, n'étant pas sans rappeler le langage même de l'ADN et ses A, C, T, G.

Cependant, à l'écoute de la conférence de Nicolas Gisin, et à la lecture de son livre *"L'impensable hasard"*, il y a un élément qui s'avère très troublant : il s'agit du jeu de Bell, un jeu qui se joue selon certaines règles particulières, et auquel il est possible de "gagner" plus souvent que 3 fois sur 4.

Il s'avère qu'au tout début de ces recherches, en regardant intensément le "maillage" qui représente les décompositions de Goldbach ci-dessous, on avait réalisé qu'il "couvrait bien les entiers" ; on pensait alors "le treillis couvre approximativement les 3/4 des entiers de sa base". On s'était amusé à calculer un "coefficient de ratage", qu'on va présenter à nouveau ici, et qui valait à peu près 3/4.



On calculait le "coefficient de ratage" de la façon suivante : pour chaque premier p, appelons x le plus petit entier tel que $2x$ n'est pas obtenable par somme de deux premiers inférieurs ou égaux à p. Ainsi, 8 est le plus petit pair non obtenable avec seulement le nombre premier 3, le ratio correspondant à cet échec est $4/3 > 1$. 12 est le plus petit pair non-obtenable avec les nombres premiers 3 et 5, on obtient le ratio 6/5. Ratio suivant 8/7 car 16 est le plus petit pair non-obtenable avec les seuls premiers 3,5,7, etc. Jusqu'à 10^6, par programme, le plus petit ratio s'est avéré être 22/29 (c'est le ratio correspondant au fait que 44 est le plus petit pair non-obtenable par somme de deux premiers inférieurs ou égaux à 29).

On avait alors retrouvé l'inverse de ce ratio égal à $29/22 = 1.31818...$ à l'adresse :
http ://hyperphysics.phy-astr.gsu.edu/hbase/MPII/P3402Hw12b.html
qui fournit toute une série de constantes physiques.
Ce ratio était présenté comme la densité du photon par nanomètre-cube, vraisemblablement dans un certain contexte.

La question, alors lancinante, revient en force en étudiant, autant que faire se peut, ces conférences et livres de vulgarisation de physique quantique.

Pourrait-on imaginer trouver une justification provenant de la physique quantique de la véracité de la conjecture de Goldbach ? Pour cela, il faudrait réussir à établir un pont entre notre langage à 4 lettres, et le jeu de Bell.

Conjecture de Goldbach : un monoïde, deux booléens, quatre lettres, seize règles, un invariant et des changements de parité

Denise Vella-Chemla

16/3/14

1 Transposition

On considère un alphabet fini de 4 lettres $A = \{a, b, c, d\}$.
On appelle mot une suite finie d'éléments de A.
L'ensemble des mots sur A est muni par la concaténation d'une structure de monoïde.
Ainsi défini, cet ensemble, noté A^*, est le monoïde libre.
On appelle longueur d'un mot le nombre de lettres qui le composent. les lettres d'un mot m sont notées $m_1, m_2, \ldots, m_l$ dans leur ordre d'occurrence dans le mot si l est la longueur de m. La lettre a code la matrice $\binom{0}{0}$, et respectivement b $\binom{0}{1}$, c $\binom{1}{0}$ et enfin d $\binom{1}{1}$ [*].

Dans la suite, on utilise l'opération définie sur les matrices :

$$\binom{x_1}{x_2}.\binom{y_1}{y_2} = \binom{x_1}{y_2}$$

L'opération de multiplication des matrices fournit 16 règles de réécriture de couples de lettres (règles dénotées par la lettre r ci-après), qui semblent pertinentes pour l'étude de la conjecture de Goldbach :

1) $aa \to a$	5) $ba \to a$	9) $ca \to c$	13) $da \to c$
2) $ab \to b$	6) $bb \to b$	10) $cb \to d$	14) $db \to d$
3) $ac \to a$	7) $bc \to a$	11) $cc \to c$	15) $dc \to c$
4) $ad \to b$	8) $bd \to b$	12) $cd \to d$	16) $dd \to d$

∗. Pour disposer d'un moyen de distinguer les 4 lettres à toutes fins utiles, on considère l'application f qui à la matrice $M = \binom{x}{y}$ associe l'entier $f(M) = x - \frac{1}{2}y$.
Cette application f envoie $\binom{0}{0}$ sur 0, $\binom{0}{1}$ sur 1, $\binom{1}{0}$ sur $-\frac{1}{2}$ et $\binom{1}{1}$ sur $\frac{1}{2}$.
On peut également considérer la fonction g telle que $g(M) = 2y - x$ qui associe aux matrices une classe d'équivalence de $\mathbb{Z}/4\mathbb{Z}$ en envoyant $\binom{0}{0}$ sur 0, $\binom{0}{1}$ sur 2, $\binom{1}{0}$ sur $-1 = 3$ et $\binom{1}{1}$ sur 1.

Si le mot associé au nombre pair n est noté $m_n = m_1 m_2 \dots m_l$, le mot associé au nombre pair $n+2$ est $m_{n+2} = m'_1 m'_2 \dots m'_{l'}$ avec $l' = l$ si n est un double d'impair et $l' = l+1$ sinon ; dans le cas où n est un double d'impair, les règles de concaténation d'une lettre en fin de mot de la forme $m'_{l'} = r'(m_l)$ pour les nombres n doubles de pairs sont $r'(a) = r'(b) = a$ et $r'(c) = r'(d) = d$.

D'autre part, l'application des règles de réécriture s'écrit :

$$\forall i \in \mathbb{N}, 2 \leqslant i \leqslant l, m'_i = r(m_{i-1} m_i).$$

Enfin, la "règle de la première lettre" (qui est la seule règle indéterministe à appliquer) est : $m'_1 = a$ si $n-1$ est un nombre premier et $m'_1 = c$ sinon.

On rappelle qu'on cherche un invariant qui garantirait qu'*"on ne perd jamais la lettre a"* au fur et à mesure du déroulement de l'algorithme.

On analyse localement les règles de réécriture :
- les règles 1, 2, 4 font "perdre un a" (la règle 4 fait en outre perdre un d) tandis que la règle 3 fait perdre un c ;
- les règles 5, 6, 7 font "perdre un b" (la règle 7 fait en outre perdre un c) tandis que la règle 8 fait perdre un d ;
- les règles 10, 11, 12 font "perdre un c" (la règle 10 fait en outre perdre un b) tandis que la règle 9 fait perdre un a ;
- enfin, les règles 13, 15, 16 font "perdre un d" (la règle 13 fait en outre perdre un a) tandis que la règle 14 fait perdre un b ;
- d'autre part, la règle 4 fait gagner un b, la règle 7 fait gagner un a, la règle 10 fait gagner un d et la règle 13 fait gagner un c.

De façon un peu plus générale, les règles 1, 2, 3, 4, 9, 10, 11, 12 laissent la somme $N_b + N_d$ constante tandis que les règles 5, 6, 7, 8, 13, 14, 15 et 16 laissent la somme $N_a + N_c$ constante (si on note N_α le nombre de lettres α du mot sur lequel sont appliquées simultanément toutes les règles de réécriture possibles).

Si on considère une sorte de "permutation de lettres à la Galois", on constate qu'à un renommage de a en d et inversement près, ainsi qu'à un renommage de b en c et inversement près, il y a une parfaite symétrie entre les règles 1 et 16, 2 et 15, 3 et 14, 4 et 13, etc. i.e. entre les règles i et $17-i$.

On trouve un invariant de la façon suivante : il faut considérer les mots associés aux nombres pairs privés de leur première lettre [†] présentant le fait que les mots utilisés ici "codent" les décompositions d'un nombre pair en somme de deux impairs dont le plus petit sommant est compris entre 3 et $n/2$ inclus). Il s'agit alors de coder le nombre de lettres a, b, c et d par des nombres notés N_a, N_b, N_c et N_d. Puis on calcule les nombres $N_a + N_d$ d'une part et $N_b + N_c$ d'autre part et on étudie le changement de parité des sommes en question lors du passage d'un nombre pair au nombre pair suivant. A cause de la manière dont les règles de réécriture affectent l'une ou l'autre de ces sommes, lors du passage d'un double de pair à un double d'impair, seule l'une des deux parités change, tandis que lors du passage d'un double d'impair à un double de pair, soit les parités des

†. cf une note précédente à l'adresse http ://denise.vella.chemla.free.fr/ecrreecc.pdf.

deux sommes en question changent, soit aucune d'entre elles. En annexe 2, sont fournis les nombres de lettres, les valeurs des sommes $N_a + N_d$ et $N_b + N_c$, on a noté les changements de parité en utilisant la couleur rouge.

Le problème est qu'on ne sait pas combien de règles de chacune des deux sortes sont applicables sur un mot donné, qui permettrait de déduire que tout mot contient forcément une lettre a (les lettres a correspondent aux décompositions de Goldbach).

On constate cependant que la fonction $N_a + N_c$ est une fonction en espalier qui augmente simplement de 1 à chaque fois que n est le double d'un nombre premier.

2 Un espace double

On se place avec cette modélisation dans une sorte d'*espace double* qui rappelle les tirettes que présentait Laisant dans la note *"Sur un procédé de vérification expérimentale du théorème de Goldbach"* du Bulletin de la SMF [‡].

La droite des entiers est doublée et "mise en face" d'elle-même à une certaine position translatée de $n/2$ de manière à ce que x se trouve associé à $n - x$.

3 Des causes différentes produisent les mêmes effets

On pourrait s'interroger sur l'intérêt de présenter une n-ième modélisation du problème binaire de Goldbach.

La modélisation proposée ici peut être intéressante car elle ne considère plus les nombres selon leurs propriétés, comme la divisibilité par exemple, ou bien encore les distances qui les séparent, mais selon leur position relative les uns par rapport aux autres dans un certain repère variant selon le nombre pair dont on cherche une décomposition de Goldbach [§].

Ainsi, dans l'annexe 1, les deux sous-mots bleus *acd* que l'on trouve dans les mots des nombres pairs 34 et 70 correspondent aux décompositions $5+29, 7+27, 9+25$ pour 34 et $17 + 53, 19 + 51, 21 + 49$ pour 70 et n'ont en quelque sorte "rien à voir". Mais par réécriture, ces décompositions se "comporteront" de la même façon au fur et à mesure du déroulement de l'algorithme.

De la même façon, si on utilise une modélisation par points dont les coordonnées sont des restes modulaires dans les corps finis $\mathbb{Z}/p\mathbb{Z}$, on avait trouvé un bel

‡. cf Charles-Ange Laisant, *"Sur un procédé de vérification expérimentale du théorème de Goldbach"*, Bulletin de la Société Mathématique de France, n° 25, p. 108, 1/12/1897.

§. En cela, c'est une approche topologique au sens décrit par la professeur Eva Bayer-Fluckiger dans la conférence à l'adresse $http://www.canal-u.tv/video/universite_de_tous_les_savoirs/theorie_des_noeuds.1023$ au sujet de la théorie des noeuds.

exemple dans le Davis et Hersh de nombres partageant des décomposants de Goldbach en partageant peu de coordonnées modulaires : ils se "comportaient" eux-aussi de la même façon avec chacun des décomposants de Goldbach partagé (ils n'avaient aucune coordonnée commune avec lui) en n'ayant "rien à voir" l'un avec l'autre (selon un ensemble de relations qu'on pourrait résumer par $a \neq c$ et $b \neq c$ et cependant $a \neq b$).

On peut noter l'analogie suivante entre la conjecture de Goldbach et la conjecture des nombres premiers jumeaux si l'on utilise la modélisation par points de coordonnées les restes : un décomposant de Goldbach p d'un nombre pair n ne partage aucune de ses coordonnées ni avec le point origine (de coordonnées toutes nulles) puisqu'il est premier, ni avec n (puisque son complémentaire est premier). Un décomposant de Goldbach de n dépend de n, ce qui semble normal. Un "père de jumeau" (i.e. le double d'un nombre pair, "coincé" entre deux nombres premiers) de façon similaire n'a aucune coordonnée égale à 1 ou bien à $p-1$ dans le corps $\mathbb{Z}/p\mathbb{Z}$. On pourrait dire en quelque sorte que la conjecture de Goldbach est un problème relatif quand la conjecture des nombres premiers jumeaux est un problème absolu mais il s'agit dans les deux cas d'éliminer deux coordonnées (voire une lorsqu'elles sont confondues) dans chaque corps premier $\mathbb{Z}/p\mathbb{Z}$.

Annexe 1 : mots du langage à 4 lettres associés aux nombres pairs de 6 à 100

6 : a
8 : a
10 : $a\ a$
12 : $c\ a$
14 : $a\ c\ a$
16 : $a\ a\ c$
18 : $c\ a\ a\ d$
20 : $a\ c\ a\ b$
22 : $a\ a\ c\ b\ a$
24 : $c\ a\ a\ d\ a$
26 : $a\ c\ a\ b\ c\ a$
28 : $c\ a\ c\ b\ a\ c$
30 : $c\ c\ a\ d\ a\ a\ d$
32 : $a\ c\ c\ b\ c\ a\ b$
34 : $a\ a\ c\ d\ a\ c\ b\ a$
36 : $c\ a\ a\ d\ c\ a\ d\ a$
38 : $c\ c\ a\ b\ c\ c\ b\ c\ a$
40 : $a\ c\ c\ b\ a\ c\ d\ a\ c$
42 : $c\ a\ c\ d\ a\ a\ d\ c\ a\ d$
44 : $a\ c\ a\ d\ c\ a\ b\ c\ c\ b$
46 : $a\ a\ c\ b\ c\ c\ b\ a\ c\ d\ a$
48 : $c\ a\ a\ d\ a\ c\ d\ a\ a\ d\ c$
50 : $a\ c\ a\ b\ c\ a\ d\ c\ a\ b\ c\ d$
52 : $c\ a\ c\ b\ a\ c\ b\ c\ c\ b\ a\ d$
54 : $c\ c\ a\ d\ a\ a\ d\ a\ c\ d\ a\ b\ d$
56 : $a\ c\ c\ b\ c\ a\ b\ c\ a\ d\ c\ b\ b$
58 : $c\ a\ c\ d\ a\ c\ b\ a\ c\ b\ c\ d\ b\ a$
60 : $c\ c\ a\ d\ c\ a\ d\ a\ a\ d\ a\ d\ d\ a$
62 : $a\ c\ c\ b\ c\ c\ b\ c\ a\ b\ c\ b\ d\ c\ a$
64 : $a\ a\ c\ d\ a\ c\ d\ a\ c\ b\ a\ d\ b\ c\ c$
66 : $c\ a\ a\ d\ c\ a\ d\ c\ a\ d\ a\ b\ d\ a\ c\ d$
68 : $c\ c\ a\ b\ c\ c\ b\ c\ c\ b\ c\ b\ b\ c\ a\ d$
70 : $a\ c\ c\ b\ a\ c\ d\ a\ c\ d\ a\ d\ b\ a\ c\ b\ d$
72 : $c\ a\ c\ d\ a\ a\ d\ c\ a\ d\ c\ b\ d\ a\ a\ d\ b$
74 : $a\ c\ a\ d\ c\ a\ b\ c\ c\ b\ c\ d\ b\ c\ a\ b\ d\ a$
76 : $a\ a\ c\ b\ c\ c\ b\ a\ c\ d\ a\ d\ d\ a\ c\ b\ b\ c$
78 : $c\ a\ a\ d\ a\ c\ d\ a\ a\ d\ c\ b\ d\ c\ a\ d\ b\ a\ d$
80 : $c\ c\ a\ b\ c\ a\ d\ c\ a\ b\ c\ d\ b\ c\ c\ b\ d\ a\ b$
82 : $a\ c\ c\ b\ a\ c\ b\ c\ c\ b\ a\ d\ d\ a\ c\ d\ b\ c\ b\ a$
84 : $c\ a\ c\ d\ a\ a\ d\ a\ c\ d\ a\ b\ d\ c\ a\ d\ d\ a\ d\ a$
86 : $a\ c\ a\ d\ c\ a\ b\ c\ a\ d\ c\ b\ b\ c\ c\ b\ d\ c\ b\ c\ a$
88 : $c\ a\ c\ b\ c\ c\ b\ a\ c\ b\ c\ d\ b\ a\ c\ d\ b\ c\ d\ a\ c$
90 : $c\ c\ a\ d\ a\ c\ d\ a\ a\ d\ a\ d\ d\ a\ a\ d\ d\ a\ d\ c\ a\ d$
92 : $a\ c\ c\ b\ c\ a\ d\ c\ a\ b\ c\ b\ d\ c\ a\ b\ d\ c\ b\ c\ c\ b$
94 : $c\ a\ c\ d\ a\ c\ b\ c\ c\ b\ a\ d\ b\ c\ c\ b\ b\ c\ d\ a\ c\ d\ a$
96 : $c\ c\ a\ d\ c\ a\ d\ a\ c\ d\ a\ b\ d\ a\ c\ d\ b\ a\ d\ c\ a\ d\ c$
98 : $c\ c\ c\ b\ c\ c\ b\ c\ a\ d\ c\ b\ b\ c\ a\ d\ d\ a\ b\ c\ c\ b\ c\ d$
100 : $a\ c\ c\ d\ a\ c\ d\ a\ c\ b\ c\ d\ b\ a\ c\ b\ d\ c\ b\ a\ c\ d\ a\ d$

Annexe 2 : Invariant de parités pour les nombres pairs compris entre 12 et 50

14 :	a	c	a								$1a0b1c0d$	11
16 :	a	a	c								$1a0b1c0d$	11
18 :	c	a	a	d							$2a0b0c1d$	30
20 :	a	c	a	b							$1a1b1c0d$	12
22 :	a	a	c	b	a						$2a1b1c0d$	22
24 :	c	a	a	d	a						$3a0b0c1d$	40
26 :	a	c	a	b	c	a					$2a1b2c0d$	23
28 :	c	a	c	b	a	c					$2a1b2c0d$	23
30 :	c	c	a	d	a	a	d				$3a0b1c2d$	51
32 :	a	c	c	b	c	a	b				$1a2b3c0d$	15
34 :	a	a	c	d	a	c	b	a			$3a1b2c1d$	43
36 :	c	a	a	d	c	a	d	a			$4a0b1c2d$	61
38 :	c	c	a	b	c	c	b	c	a		$2a2b4c0d$	26
40 :	a	c	c	b	a	c	d	a	c		$2a1b4c1d$	35
42 :	c	a	c	d	a	a	d	c	a	d	$4a0b2c3d$	72
44 :	a	c	a	d	c	a	b	c	c	b	$2a2b4c1d$	36
46 :	a	a	c	b	c	c	b	a	c	d	$3a2b4c1d$	46
48 :	c	a	a	d	a	c	d	a	a	d	$5a0b2c3d$	82

Conjecture de Goldbach : 16 règles de réécriture si bizarres

Denise Vella-Chemla

19/3/14

1 Des règles de réécriture si bizarres

On rappelle qu'on a choisi de représenter le fait qu'un entier est premier par le booléen 0 et le fait qu'il est composé par le booléen 1.

On a également pris comme conventions :

- que la lettre a est utilisée pour symboliser une décomposition de n de la forme $p+q$ avec p et q premiers et $p \leqslant n/2$;
- que la lettre b est utilisée pour symboliser une décomposition de n de la forme $p+q$ avec p composé et q premier et $p \leqslant n/2$;
- que la lettre c est utilisée pour symboliser une décomposition de n de la forme $p+q$ avec p premier et q composé et $p \leqslant n/2$;
- que la lettre d est utilisée pour symboliser une décomposition de n de la forme $p+q$ avec p et q composés et $p \leqslant n/2$;

La lettre a code la matrice $\begin{pmatrix}0\\0\end{pmatrix}$, et respectivement $b\begin{pmatrix}0\\1\end{pmatrix}$, $c\begin{pmatrix}1\\0\end{pmatrix}$ et enfin $d\begin{pmatrix}1\\1\end{pmatrix}$

Exemples : Ci-dessous le mot $m_{abcd}(40)$.

40	37	35	33	31	29	27	25	23	21
	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0
	3	5	7	9	11	13	15	17	19
$m_{abcd}(40)$	a	c	c	b	a	c	d	a	c

Dans la suite, on utilise l'opération définie sur les matrices :

$$\begin{pmatrix}x_1\\x_2\end{pmatrix}.\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{pmatrix}x_1\\y_2\end{pmatrix}$$

L'opération de multiplication des matrices fournit 16 règles de réécriture de couples de lettres, qui semblent pertinentes pour l'étude de la conjecture de Goldbach :

1)	$aa \to a$	5)	$ba \to a$	9)	$ca \to c$	13)	$da \to c$
2)	$ab \to b$	6)	$bb \to b$	10)	$cb \to d$	14)	$db \to d$
3)	$ac \to a$	7)	$bc \to a$	11)	$cc \to c$	15)	$dc \to c$
4)	$ad \to b$	8)	$bd \to b$	12)	$cd \to d$	16)	$dd \to d$

Observons les règles 1 à 4 : elle consistent à appliquer une sorte d'opérateur a à gauche.

Réécrivons la règle 1 en terme d'opérations dans l'algèbre de Boole :

$$\begin{pmatrix}0\\0\end{pmatrix}.\begin{pmatrix}0\\0\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$$
$$\begin{pmatrix}0\\0\end{pmatrix}.\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$$
$$\begin{pmatrix}0\\0\end{pmatrix}.\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$$
$$\begin{pmatrix}0\\0\end{pmatrix}.\begin{pmatrix}1\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$$

Cette règle, appliquée à deux doublons $\begin{pmatrix}x_1\\y_1\end{pmatrix}$ et $\begin{pmatrix}x_2\\y_2\end{pmatrix}$ fournit le doublon $\begin{pmatrix}x_1\wedge x_2\\y_1\vee y_2\end{pmatrix}$.
La règle 2 (opérateur b "appliqué à gauche") devient dans l'algèbre de Boole :

$$\begin{pmatrix}0\\1\end{pmatrix}.\begin{pmatrix}0\\0\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$$
$$\begin{pmatrix}0\\1\end{pmatrix}.\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$$
$$\begin{pmatrix}0\\1\end{pmatrix}.\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$$
$$\begin{pmatrix}0\\1\end{pmatrix}.\begin{pmatrix}1\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$$

Cette règle, appliquée à deux doublons $\begin{pmatrix}x_1\\y_1\end{pmatrix}$ et $\begin{pmatrix}x_2\\y_2\end{pmatrix}$ fournit le doublon $\begin{pmatrix}x_1\wedge x_2\\y_1\wedge y_2\end{pmatrix}$.

La règle 3 (opérateur c "appliqué à gauche") devient dans l'algèbre de Boole :

$$\begin{pmatrix}1\\0\end{pmatrix}.\begin{pmatrix}0\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$$
$$\begin{pmatrix}1\\0\end{pmatrix}.\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\\1\end{pmatrix}$$
$$\begin{pmatrix}1\\0\end{pmatrix}.\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$$
$$\begin{pmatrix}1\\0\end{pmatrix}.\begin{pmatrix}1\\1\end{pmatrix}=\begin{pmatrix}1\\1\end{pmatrix}$$

Cette règle, appliquée à deux doublons $\begin{pmatrix}x_1\\y_1\end{pmatrix}$ et $\begin{pmatrix}x_2\\y_2\end{pmatrix}$ fournit le doublon $\begin{pmatrix}x_1\vee x_2\\y_1\vee y_2\end{pmatrix}$.

Enfin, la règle 4 (opérateur d "appliqué à gauche") devient dans l'algèbre de Boole :

$$\begin{pmatrix}1\\1\end{pmatrix}.\begin{pmatrix}0\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$$
$$\begin{pmatrix}1\\1\end{pmatrix}.\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\\1\end{pmatrix}$$
$$\begin{pmatrix}1\\1\end{pmatrix}.\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$$
$$\begin{pmatrix}1\\1\end{pmatrix}.\begin{pmatrix}1\\1\end{pmatrix}=\begin{pmatrix}1\\1\end{pmatrix}$$

Cette règle, appliquée à deux doublons $\binom{x_1}{x_2}$ et $\binom{y_1}{y_2}$ fournit le doublon $\binom{x_1 \vee x_2}{y_1 \wedge y_2}$.

Si l'on regarde maintenant ensemble les règles en considérant les opérateurs à droite plutôt qu'à gauche, en mettant ensemble les règles 1, 5, 9 et 13, (resp. 2, 6, 10 et 14 ensemble, 3, 7, 11 et 15 ensemble et enfin, 4, 8, 12, et 16 ensemble), on constate les choses suivantes, comme attendu totalement "symétriques" de ce qu'on a obtenu à gauche :

- le a appliqué à droite d'un doublon $\binom{x_1}{x_2}$ permet d'obtenir $\binom{x_1 \vee 0}{x_2 \wedge 0}$;
- le b appliqué à droite d'un doublon $\binom{x_1}{x_2}$ permet d'obtenir $\binom{x_1 \vee 1}{x_2 \vee 0}$;
- le c appliqué à droite d'un doublon $\binom{x_1}{x_2}$ permet d'obtenir $\binom{x_1 \wedge 0}{x_2 \wedge 1}$;
- le d appliqué à droite d'un doublon $\binom{x_1}{x_2}$ permet d'obtenir $\binom{x_1 \wedge 1}{x_2 \vee 1}$.

Les règles sont complètement décourageantes, on imagine mal ce que peut donner l'application simultanée de plusieurs d'entre elles à un même mot, sans avoir aucune connaissance du nombre d'applications de chacune. On désespère de jamais comprendre pourquoi *"tout mot contient un a"*.

En outre, et cela est vraisemblablement complètement rédhibitoire, on n'arrive toujours pas à lever l'indéterminisme patent qui porte sur la première lettre des mots utilisés ; or, c'est cet indéterminisme qui "engendre tout le reste".

Conjecture de Goldbach et somme des diviseurs : utiliser une récurrence mystérieuse

Denise Vella-Chemla

22/3/14

On peut trouver sur la toile une récurrence toute simple qui permet de calculer la somme des diviseurs d'un nombre. Un nombre premier p a pour somme des diviseurs $\sigma(p) = p + 1$. On utilise cette condition pour tester la primalité. Les décomposants de Goldbach p et q d'un nombre pair n (i.e. les nombres premiers p et q dont n est la somme) s'avèrent ainsi être les nombres qui minimisent la somme $\sigma(p) + \sigma(q)$ en la rendant égale à $n + 2$ [1].

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

int main (int argc, char* argv[]) {
  int n, k, somme, i ;
  int sigma[100] ;

  sigma[1] = 1 ;
  std::cout << "sigma[1]=1\n" ;
  for (n=2 ; n <= 100 ; n++) {
      somme = 0 ;
      for (k=1 ; k < n ; k++)
         somme = somme+(-(n*n)+5*k*n-5*k*k)*sigma[k]*sigma[n-k] ;
      sigma[n] = (12*somme)/(n*n*(n-1)) ;
      std::cout << "premier(" << n << ") = " ;
      std::cout << (sigma[n]==(n+1)) << "\n" ;
  }

  for (n=6 ; n <= 100 ; n=n+2)
    for (i=3 ; i <= n/2 ; i=i+2)
      if ((sigma[i]+sigma[n-i])==n+2) {
    std::cout << n << " = " << i << "+" << n-i ;
    std::cout << " est une décomposition de Goldbach de " << n << "\n" ;
  }
}
```

1. On a découvert qu'inversement, il semblerait que les décomposants de Goldbach maximisent le produit des indicateurs d'Euler $\varphi(p)\varphi(q)$.

Conjecture de Goldbach et indicatrice d'Euler

Denise Vella-Chemla

22/3/14

L'indicatrice d'Euler est une fonction arithmétique multiplicative. Un nombre premier p a pour indicatrice d'Euler $\varphi(p) = p - 1$.

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

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

int main (int argc, char* argv[])
{
  int n, k, produit, NbPremiersA ;
  int phi[100] ;

  for (n=1 ; n <= 100 ; n=n+1) {
    NbPremiersA = 0 ;
    for (k=1 ; k <= n ; k++)
      if (pgcd(n,k)==1) NbPremiersA++ ;
    phi[n]=NbPremiersA ;
  }

  for (n=6 ; n <= 100 ; n=n+2)
    for (k=3 ; k <= n/2 ; k=k+2)
      if ((phi[k]*phi[n-k]) == (k-1)*(n-k-1) {
    std::cout << k << "+" << n-k ;
    std::cout << " est une décomposition de Goldbach de " << n << "\n" ;
  }
}
```

Les décomposants de Goldbach p et q d'un nombre pair n (i.e. les nombres premiers p et q dont n est la somme) s'avèrent ainsi être les nombres dont le produit des indicatrices d'Euler $\varphi(p) * \varphi(q)$ est égal à $(p-1)(n-p-1)$.

Conjecture de Goldbach et mouvement brownien

Denise Vella-Chemla

22/3/14

On se place dans la suite dans un espace cartésien à deux dimensions.

On va associer à chaque nombre pair un *"déplacement global dans le plan"*, qui sera constitué de la suite des déplacements associés aux différentes décompositions de ce nombre pair comme somme de deux nombres impairs [1]. Le déplacement associé à tout nombre pair aura comme origine le point $(0, 0)$.

On codera :

- une décomposition de n de la forme $p + q$ avec p et q premiers et $p \leqslant n/2$ par l'augmentation de 1 de l'abscisse du point sur lequel on se trouve ;
- une décomposition de n de la forme $p + q$ avec p impair composé et q premier et $p \leqslant n/2$ par l'augmentation de 1 de l'ordonnée du point sur lequel on se trouve ;
- une décomposition de n de la forme $p + q$ avec p premier et q impair composé et $p \leqslant n/2$ par la diminution de 1 de l'ordonnée du point sur lequel on se trouve ;
- une décomposition de n de la forme $p + q$ avec p et q impairs composés et $p \leqslant n/2$ par la diminution de 1 de l'abscisse du point sur lequel on se trouve.

Ainsi, des conditions identiques de primalité pour p et pour $n - p$ son complémentaire se traduiront par des déplacements horizontaux (le vecteur $(1, 0)$ correspond à deux nombres premiers [2] et le vecteur $(-1, 0)$ correspond à deux nombres composés [3]). Des conditions différentes de primalité pour p et pour $n-p$ son complémentaire se traduiront quant à elles par des déplacements verticaux (le vecteur $(0, 1)$ correspond aux sommes $p + q$ avec p impair composé $\leqslant n/2$ et q premier [4] et le vecteur $(0, -1)$ correspond aux sommes $p + q$ avec p premier $\leqslant n/2$ et q impair composé [5]).

Exemple : déplacement global associé au nombre pair 48
Le nombre 48 admet 11 décompositions comme somme de deux impairs :

- les décompositions $5+43$, $7+41$, $11+37$, $17+41$, $19+29$, faisant intervenir deux nombres premiers sont codées par 5 déplacements à droite ;

1. On omet la décomposition $1 + (n - 1)$.
2. la lettre a de notes récentes.
3. la lettre d de notes récentes.
4. la lettre b de notes récentes.
5. la lettre c de notes récentes.

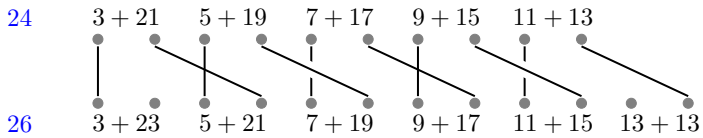
– les décompositions $3+45$, $13+35$, $23+25$ faisant intervenir un nombre premier et un impair composé sont codées par 3 déplacements vers le bas ;
– les décompositions $9+39$, $15+43$, $21+27$, faisant intervenir un impair composé et un nombre premier sont codées par 3 déplacements vers le haut.

On s'est déplacé du point origine $(0,0)$ au point $(2,-3)$.

En annexe, sont fournis les déplacements associés aux nombres pairs de 10 à 100.

On constate que ce codage permet de trouver très aisément les pairs doubles de nombres premiers : leur "déplacement global" consiste en un unique déplacement vers le bas ou bien en un unique déplacement vers la droite.

Cela se comprend par la théorie des tresses : le passage d'un double de composé à un double de premier consistant à appliquer des permutations suivant toujours le même schéma, du fait de l'ajout artificiel du nombre premier en question dans la décomposition triviale $2p = p+p$; présentons l'exemple des nombres pairs 24 et 26 ci-dessous :



Ce codage permet d'autre part de trouver très aisément les pairs doubles de ces nombres qu'on désigne sous le nom de "pères de jumeaux" (i.e. un père de jumeau est un nombre pair k tel que $k-1$ et $k+1$ sont simultanément premiers) : leur "déplacement global" consiste en un unique déplacement à la fois vers le bas et vers la gauche (i.e. $(-1,-1)$, cf. annexe 3).

La proposition ci-dessus est codée par le programme suivant ; son résultat est fourni en annexe.

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

int prime(int p) {
  bool notfound=true ;
  unsigned long k = 2 ;

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

int main (int argc, char* argv[]) {
  int n, k, x, y, xprec, yprec ;

  x = 0 ;
  y = 0 ;
  for (n=14 ; n <= 1000 ; n=n+2) {
    xprec = x ;
    yprec = y ;
    x = 0 ;
    y = 0 ;
    for (k=3 ; k <= n/2 ; k=k+2) {
      if (prime(k) && prime(n-k)) x=x+1 ;
      else if (prime(k) && (not(prime(n-k)))) y=y-1 ;
      else if ((not(prime(k))) && prime(n-k)) y=y+1 ;
      else if ((not(prime(k))) && (not(prime(n-k)))) x=x-1 ;
    }
    std::cout << n << " : x = " << x << " y = " << y << "\n" ;
    if ((((x-xprec) == 1) && ((y-yprec) == 0))
        || (((x-xprec) == 0) && ((y-yprec) == -1)))
      std::cout << "je descends ou vais à droite pour " << n/2 << "\n" ;
  }
}
```

Annexe 1 : déplacements associés aux nombres pairs de 10 à 100

10	$2(1,0)+0(-1,0)+0(0,1)+1(0,-1)$	$(2,0)$
12	$1(1,0)+0(-1,0)+0(0,1)+1(0,-1)$	$(1,-1)$
14	$2(1,0)+0(-1,0)+0(0,1)+1(0,-1)$	$(2,-1)$
16	$2(1,0)+0(-1,0)+0(0,1)+1(0,-1)$	$(2,-1)$
18	$2(1,0)+1(-1,0)+0(0,1)+1(0,-1)$	$(1,-1)$
20	$2(1,0)+0(-1,0)+1(0,1)+1(0,-1)$	$(2,0)$
22	$3(1,0)+0(-1,0)+1(0,1)+1(0,-1)$	$(3,0)$
24	$3(1,0)+1(-1,0)+0(0,1)+1(0,-1)$	$(2,-1)$
26	$3(1,0)+0(-1,0)+1(0,1)+2(0,-1)$	$(3,-1)$
28	$2(1,0)+0(-1,0)+1(0,1)+3(0,-1)$	$(2,-2)$
30	$3(1,0)+2(-1,0)+0(0,1)+2(0,-1)$	$(1,-2)$
32	$2(1,0)+0(-1,0)+2(0,1)+3(0,-1)$	$(2,-1)$
34	$4(1,0)+1(-1,0)+1(0,1)+2(0,-1)$	$(3,-1)$
36	$4(1,0)+2(-1,0)+0(0,1)+2(0,-1)$	$(2,-2)$
38	$2(1,0)+0(-1,0)+2(0,1)+5(0,-1)$	$(2,-3)$
40	$3(1,0)+1(-1,0)+1(0,1)+4(0,-1)$	$(2,-3)$
42	$4(1,0)+3(-1,0)+0(0,1)+3(0,-1)$	$(1,-3)$
44	$3(1,0)+1(-1,0)+2(0,1)+4(0,-1)$	$(2,-2)$
46	$4(1,0)+1(-1,0)+2(0,1)+4(0,-1)$	$(3,-2)$
48	$5(1,0)+3(-1,0)+0(0,1)+3(0,-1)$	$(2,-3)$
50	$4(1,0)+2(-1,0)+2(0,1)+4(0,-1)$	$(2,-2)$
52	$3(1,0)+1(-1,0)+3(0,1)+5(0,-1)$	$(2,-2)$
54	$5(1,0)+4(-1,0)+1(0,1)+3(0,-1)$	$(1,-2)$
56	$3(1,0)+1(-1,0)+4(0,1)+5(0,-1)$	$(2,-1)$
58	$4(1,0)+2(-1,0)+3(0,1)+5(0,-1)$	$(2,-2)$
60	$6(1,0)+5(-1,0)+0(0,1)+3(0,-1)$	$(1,-3)$
62	$3(1,0)+1(-1,0)+4(0,1)+7(0,-1)$	$(2,-3)$
64	$5(1,0)+3(-1,0)+2(0,1)+5(0,-1)$	$(2,-3)$
66	$6(1,0)+5(-1,0)+1(0,1)+4(0,-1)$	$(1,-3)$
68	$2(1,0)+1(-1,0)+5(0,1)+8(0,-1)$	$(1,-3)$
70	$5(1,0)+4(-1,0)+3(0,1)+5(0,-1)$	$(1,-2)$
72	$6(1,0)+5(-1,0)+2(0,1)+4(0,-1)$	$(1,-2)$
74	$5(1,0)+3(-1,0)+4(0,1)+6(0,-1)$	$(2,-2)$
76	$5(1,0)+3(-1,0)+4(0,1)+6(0,-1)$	$(2,-2)$
78	$7(1,0)+6(-1,0)+2(0,1)+4(0,-1)$	$(1,-2)$
80	$4(1,0)+3(-1,0)+5(0,1)+7(0,-1)$	$(1,-2)$
82	$5(1,0)+3(-1,0)+5(0,1)+7(0,-1)$	$(2,-2)$
84	$8(1,0)+7(-1,0)+1(0,1)+4(0,-1)$	$(1,-3)$
86	$5(1,0)+3(-1,0)+5(0,1)+8(0,-1)$	$(2,-3)$
88	$4(1,0)+3(-1,0)+5(0,1)+9(0,-1)$	$(1,-4)$
90	$9(1,0)+9(-1,0)+0(0,1)+4(0,-1)$	$(0,-4)$
92	$4(1,0)+3(-1,0)+6(0,1)+9(0,-1)$	$(1,-3)$
94	$5(1,0)+4(-1,0)+5(0,1)+9(0,-1)$	$(1,-4)$
96	$7(1,0)+7(-1,0)+2(0,1)+7(0,-1)$	$(0,-5)$
98	$3(1,0)+4(-1,0)+6(0,1)+11(0,-1)$	$(-1,-5)$
100	$6(1,0)+6(-1,0)+4(0,1)+8(0,-1)$	$(0,-4)$

Annexe 2 : déplacements des doubles de premiers ($(1,0)$ ou $(0,-1)$)

```
14 : x = 2 y = -1
16 : x = 2 y = -1
18 : x = 1 y = -1
20 : x = 2 y = 0
22 : x = 3 y = 0
je descends ou je vais à droite pour 11
24 : x = 2 y = -1
26 : x = 3 y = -1
je descends ou je vais à droite pour 13
28 : x = 2 y = -2
30 : x = 1 y = -2
32 : x = 2 y = -1
34 : x = 3 y = -1
je descends ou je vais à droite pour 17
36 : x = 2 y = -2
38 : x = 2 y = -3
je descends ou je vais à droite pour 19
40 : x = 2 y = -3
42 : x = 1 y = -3
44 : x = 2 y = -2
46 : x = 3 y = -2
je descends ou je vais à droite pour 23
48 : x = 2 y = -3
50 : x = 2 y = -2
52 : x = 2 y = -2
54 : x = 1 y = -2
56 : x = 2 y = -1
58 : x = 2 y = -2
je descends ou je vais à droite pour 29
60 : x = 1 y = -3
62 : x = 2 y = -3
je descends ou je vais à droite pour 31
64 : x = 2 y = -3
66 : x = 1 y = -3
68 : x = 1 y = -3
70 : x = 1 y = -2
72 : x = 1 y = -2
74 : x = 2 y = -2
je descends ou je vais à droite pour 37
76 : x = 2 y = -2
78 : x = 1 y = -2
80 : x = 1 y = -2
82 : x = 2 y = -2
je descends ou je vais à droite pour 41
84 : x = 1 y = -3
86 : x = 2 y = -3
je descends ou je vais à droite pour 43
88 : x = 1 y = -4
90 : x = 0 y = -4
92 : x = 1 y = -3
94 : x = 1 y = -4
je descends ou je vais à droite pour 47
96 : x = 0 y = -5
98 : x = -1 y = -5
100 : x = 0 y = -4
```

Annexe 3 : déplacements des doubles de “pères de jumeau” ($(-1, -1)$)

```
24 : x = 2 y = -1
24 : xprec = 3 yprec = 0

36 : x = 2 y = -2
36 : xprec = 3 yprec = -1

60 : x = 1 y = -3
60 : xprec = 2 yprec = -2

84 : x = 1 y = -3
84 : xprec = 2 yprec = -2

120 : x = 0 y = -3
120 : xprec = 1 yprec = -2

144 : x = -2 y = -5
144 : xprec = -1 yprec = -4

204 : x = -5 y = -5
204 : xprec = -4 yprec = -4

216 : x = -7 y = -8
216 : xprec = -6 yprec = -7

276 : x = -11 y = -7
276 : xprec = -10 yprec = -6

300 : x = -13 y = -7
300 : xprec = -12 yprec = -6
```

Goldbach conjecture and Brownian motion

Denise Vella-Chemla

March 22, 2014

In the following, one is located in a two-dimensional cartesian space.

We associate to each even integer a *"global motion in the plane"*, that is constituted of several moves associated to this even integer decompositions as a sum of two odd integers [1]. Every motion has $(0, 0)$ point as origin.

We code :

- an n decomposition of the form $p+q$ in which p and q are two primes and $p \leqslant n/2$ by an increase of 1 of the current point abscissa ;
- an n decomposition of the form $p + q$ in which p is an odd compound integer and q is a prime and $p \leqslant n/2$ by an increase of 1 of the current point ordinate ;
- an n decomposition of the form $p + q$ in which p is a prime and q is an odd compound integer and $p \leqslant n/2$ by a decreasing by 1 of the current point ordinate ;
- an n decomposition of the form $p + q$ in which p and q are two odd compound integers and $p \leqslant n/2$ by a decreasing by 1 of the current point abscissa.

Example : global move associated with even integer 48
48 admits 11 decompositions as a sum of two odd integers :

- $5+43$, $7+41$, $11+37$, $17+41$, $19+29$ decompositions, adding two primes, are coded by 5 moves to the right ;
- $3 + 45$, $13 + 35$, $23 + 25$ decompositions, adding a prime and an odd compound integer are coded by 3 moves to the bottom ;
- $9+39$, $15+43$, $21+27$ decompositions, adding an odd compound integer are coded by par 3 moves to the top.

One has moved from origin point $(0, 0)$ to point $(2, -3)$.

We can see that this choice allows finding easily even numbers that are of the form $2p$ with p prime : their "global move" consists only in a unique move to the bottom or to the right.

1. $1 + (n - 1)$ decomposition is omitted.

The proposal we made can be coded in c++ to verify this result concerning prime doubles :

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

int prime(int atester) {
  unsigned long diviseur=2;
  bool pastrouve=true;
  unsigned long k = 2;
  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve) {
    if ((k * k) > atester) return 1;
    else if ((atester % k) == 0) { return 0 ; }
         else k++;
  }
}

int main (int argc, char* argv[]) {
  int n, k, x, y, xprec, yprec ;

  x = 0 ;
  y = 0 ;
  for (n=14 ; n <= 1000 ; n=n+2) {
    xprec = x ;
    yprec = y ;
    x = 0 ;
    y = 0 ;
    for (k=3 ; k <= n/2 ; k=k+2) {
      if (prime(k) && prime(n-k)) x=x+1 ;
      else if (prime(k) && (not(prime(n-k)))) y=y-1 ;
      else if ((not(prime(k))) && prime(n-k)) y=y+1 ;
      else if ((not(prime(k))) && (not(prime(n-k)))) x=x-1 ;
    }
    if ((((x-xprec) == 1) && ((y-yprec) == 0))
        || (((x-xprec) == 0) && ((y-yprec) == -1)))
      std::cout << "only one step bottom or right for integer " << n/2 <<
           "\n" ;
  }
}
```

Programme de la somme des diviseurs d'Euler

Denise Vella-Chemla

26/3/14

L'article d'Euler *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs* est magique. On reste subjugué par la manière dont le mathématicien a trouvé la formule récurrente de la somme des diviseurs. Même le fait de la programmer la laisse hermétique. On trouve particulièrement esthétique la manière dont les nombres pentagonaux surgissent de la combinaison par différence de la suite des entiers et de la suite des impairs.

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

const int taille=100;
int a[taille];
int h[taille];
int euler[taille];

int f(int x) { return (3 * x * x - x) / 2; }

int g(int x) { return (3 * x * x + x) / 2; }

int remplis_h()
{int i,y;

  for (i=1; i<=taille; i++)
    if (i % 2 == 0) h[i]=f(i/2);
    else h[i]=g((i-1)/2);
}

int remplis_a()
{int i;

  for (i=1; i<=taille; i++)
    if ((i % 4 == 1) || (i % 4 == 2)) a[i]=1;
    else a[i]=-1;
}
```

```
int calcule_euler()
{int x, y, somme;

  euler[1]=1;
  for (x=2; x<=taille; x++)
    {
      somme = 0; y=0;
      while (x-h[y] >= 0)
        {
    if (x == h[y]) somme = somme + a[y-1] * x;
    else somme = somme + a[y-1] * euler[x-h[y]];
    y++;
  }
      euler[x]=somme;
    }
}

int main (int argc, char* argv[])
{
  int i;

  remplis_a();
  remplis_h();
  calcule_euler();
  for (i=1 ; i <= taille ; i++)
    std::cout << i << " : " << euler[i] << "\n" ;
}
```

On peut voir les nombres premiers comme des minima locaux de la fonction somme des diviseurs.

Puisque la somme des diviseurs d'un nombre premier p vaut $p+1$, $p+(n-p)$ est une décomposition de Goldbach de n si et seulement si $\sigma(p)+\sigma(n-p) = n+2$. Les décomposants de Goldbach minimisent donc la somme des sommes des diviseurs de p et $n-p$.

Conjecture de Goldbach : mots bouclés

Denise Vella-Chemla

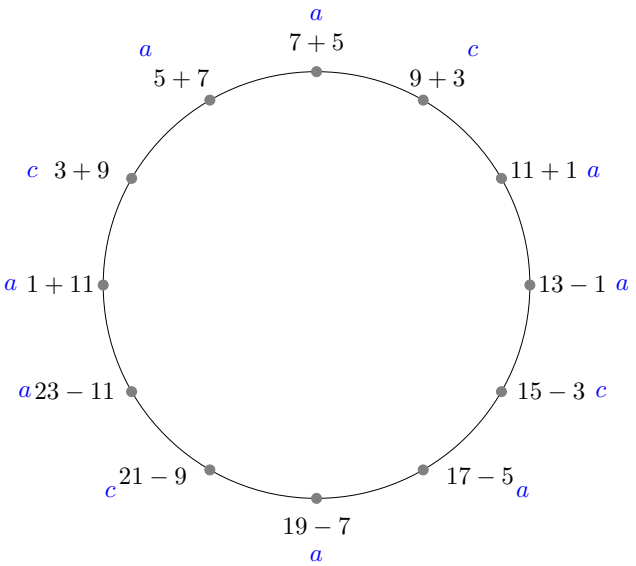
27/3/14

1 Pourquoi des mots de longueurs finies ?

On a présenté dans plusieurs notes récentes comment associer à chaque nombre pair un mot de longueur fini, sur un alphabet à 4 lettres (cf $http://denise.vella.chemla.free.fr/transposition$).

Un peu de réflexion supplémentaire nous oblige à nous interroger : pourquoi utiliser des mots de longueur finie ? Pourquoi ne coder pour le nombre 26 par exemple que les seules décompositions $3+23$, $5+21$, $7+19$, $9+17$, $11+15$ et $13+13$ et oublier une décomposition comme $29-3$ par exemple ?

On s'est trouvé complètement bloqué par l'indéterminisme portant sur la première lettre des mots utilisés dans la précédente modélisation. On va s'intéresser également aux décompositions soustractives en voyant les décompositions comme des points de boucles.



On prend comme convention, comme Cantor, que le nombre 1 est premier. On utilise deux lettres : la lettre a pour signifier qu'une décomposition fait intervenir deux nombres premiers, qu'elle soit additive ou soustractive et la lettre c

pour signifier que la décomposition fait intervenir au moins un nombre composé.

Ci-dessus, le cercle des décompositions associé au nombre pair 12.

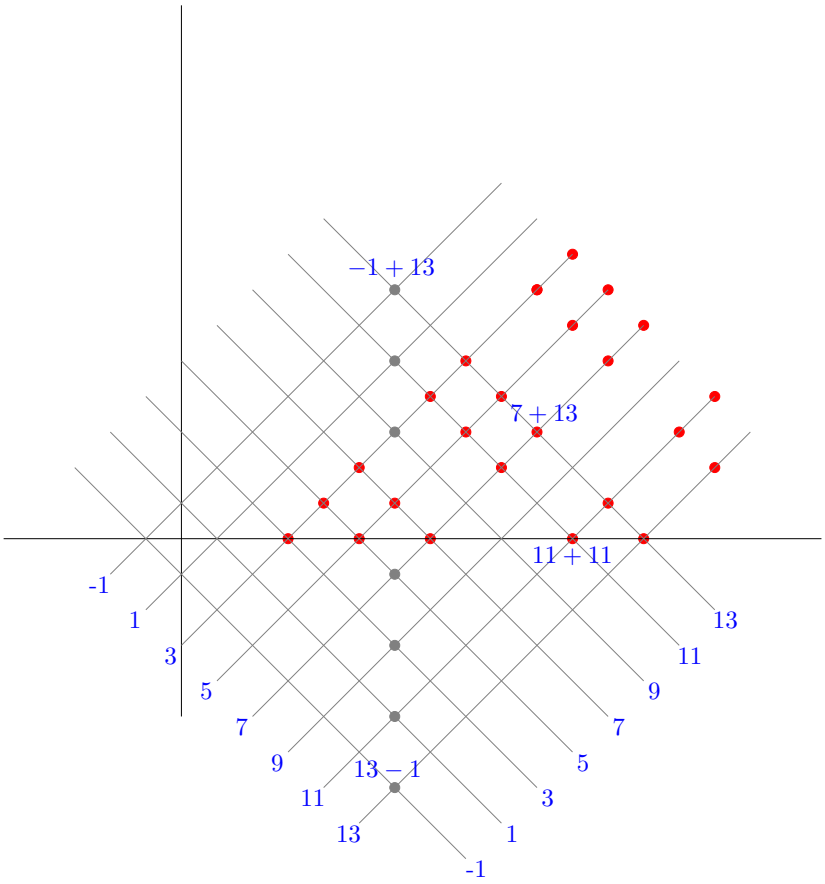
Conjecture de Goldbach : revenir au maillage

Denise Vella-Chemla

28/3/14

Les points commutent-ils ?

Sur le maillage ci-dessous, les décompositions de Goldbach (de nombres pairs comme sommes de deux nombres premiers) sont représentées par des points rouges.



On a représenté par des points gris certaines décompositions du nombre pair 12 de $-1+13$ en haut à $13-1$ en bas. L'unique décomposition de Goldbach de 12

qu'est $5+7$ a été représentée par un point rouge.

La décomposition $a+b$ est représentée par le point de coordonnées $\left(\frac{a+b}{2}, \frac{a-b}{2}\right)$. Ainsi, même si $-1+13 = 13-1$, à ces deux décompositions ne sont pas associés les mêmes points. Cette particularité est engendrée par le fait qu'on a choisi une orientation de notre espace, en s'intéressant aux deux diagonales descendantes en bas à gauche et en bas à droite à partir d'un point et vers l'axe des abscisses. Un autre choix arbitraire aurait pu être fait.

Extrait de la biographie *Alan Turing ou l'énigme de l'intelligence* d'Andrew Hodges (DC 30/12/13)

(p. 218) Ce n'était pas le seul parallèle entre les travaux de Claude Shannon et ceux d'Alan Turing. Il existait entre eux comme une sorte de réciprocité. Alan, dont le point fort était plutôt la logique des machines, s'était néanmoins plongé dans l'étude de l'information.

Shannon, de son côté, s'était également intéressé au concept de machine logique. Alan lui fit lire ses *Nombres calculables* et ils parlèrent d'une idée très présente dans l'article de Turing, à savoir la reproduction mécanique du cerveau. De 1936 à 1938, Shannon avait travaillé sur l'analyseur différentiel du Massachussetts Institute of Technology et, ayant étudié la neurologie au même titre que les mathématiques et la logique, il avait vu dans cette recherche un premier pas vers la machine pensante. Ils se rendirent compte qu'ils partageaient une même conception des choses : le cerveau n'avait rien de sacré, et si une machine parvenait un jour à faire aussi bien qu'un cerveau, alors elle serait effectivement douée de la faculté de *penser*. Ni l'un ni l'autre ne proposait cependant de moyen d'y arriver.

C'était là, au moins, un sujet dont ils pouvaient parler librement. Alan s'étonna un jour : "Shannon ne veut pas entrer seulement des *données* dans un cerveau, il veut lui donner de la *culture* ! Il veut lui faire écouter de la *musique* !". Une autre fois, à la cantine, alors qu'il dissertait sur les possibilités d'une "machine pensante", sa voix haut perchée commença à dominer le brouhaha général des jeunes cadres dynamiques en quête de promotion au sein des Bell Labs. Tous l'entendirent bientôt affirmer : "Non, ce qui m'intéresse, ce n'est pas de mettre au point un cerveau puissant. Je ne cherche rien d'autre qu'un cerveau médiocre, dans le genre de celui du président de l'American Telephone and Telegraph Company.". La salle entière fut pétrifiée, mais Alan continua nonchalamment à exposer son idée : fournir à la machine toutes les données concernant les cours de la bourse et les matières premières puis lui poser simplement la question : "J'achète ou je vends ?". Le téléphone sonna ensuite tout l'après-midi dans son laboratoire et l'on ne cessa de lui demander qui diable il pouvait bien être.

Note : Alan Turing avait inventé bien avant l'heure le trading haute-fréquence...

Conjecture de Goldbach, réécriture, contradiction

Denise Vella-Chemla

30/3/14

1 16 règles de réécriture

On rappelle qu'on a choisi de représenter le fait qu'un entier est premier par le booléen 0 et le fait qu'il est composé par le booléen 1.

On a également pris comme conventions d'utiliser ($p \leqslant n/2$) :

- la lettre a pour symboliser une décomposition de n de la forme $p+q$ avec p et q premiers ;
- la lettre b pour symboliser une décomposition de n de la forme $p+q$ avec p composé et q premier ;
- la lettre c pour symboliser une décomposition de n de la forme $p+q$ avec p premier et q composé ;
- la lettre d pour symboliser une décomposition de n de la forme $p+q$ avec p et q composés.

La lettre a code la matrice $\begin{pmatrix}0\\0\end{pmatrix}$, et respectivement $b\begin{pmatrix}0\\1\end{pmatrix}$, $c\begin{pmatrix}1\\0\end{pmatrix}$ et enfin $d\begin{pmatrix}1\\1\end{pmatrix}$

Exemple : Ci-dessous le mot $m_{abcd}(40)$.

40	37	35	33	31	29	27	25	23	21
	0	1	1	0	0	1	1	0	1
	0	0	0	1	0	0	1	0	0
	3	5	7	9	11	13	15	17	19
$m_{abcd}(40)$	a	c	c	b	a	c	d	a	c

Dans la suite, on utilise l'opération ainsi définie sur les matrices :

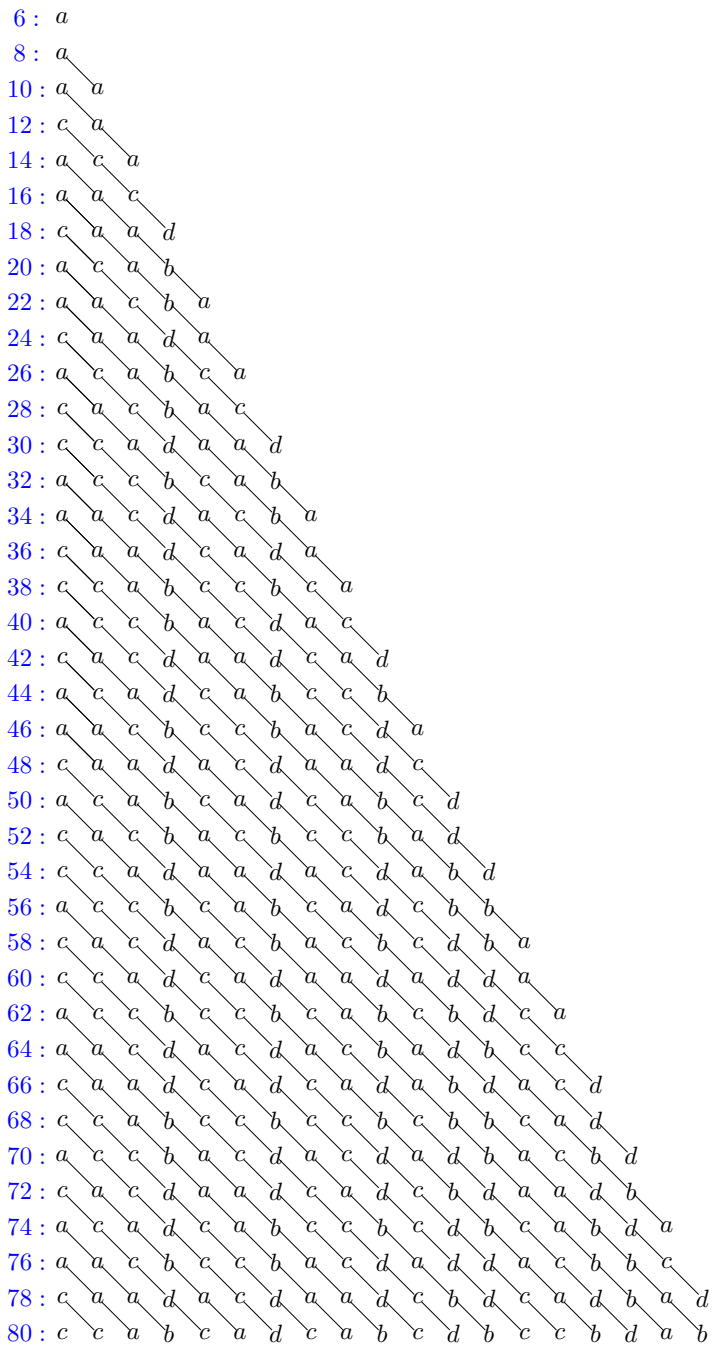
$$\begin{pmatrix}x_1\\x_2\end{pmatrix}.\begin{pmatrix}y_1\\y_2\end{pmatrix} = \begin{pmatrix}x_1\\y_2\end{pmatrix}$$

L'opération ci-dessus fournit 16 règles de réécriture de couples de lettres, qui semblent pertinentes pour l'étude de la conjecture de Goldbach :

1) $aa \to a$	5) $ba \to a$	9) $ca \to c$	13) $da \to c$
2) $ab \to b$	6) $bb \to b$	10) $cb \to d$	14) $db \to d$
3) $ac \to a$	7) $bc \to a$	11) $cc \to c$	15) $dc \to c$
4) $ad \to b$	8) $bd \to b$	12) $cd \to d$	16) $dd \to d$

2 Observer les mots

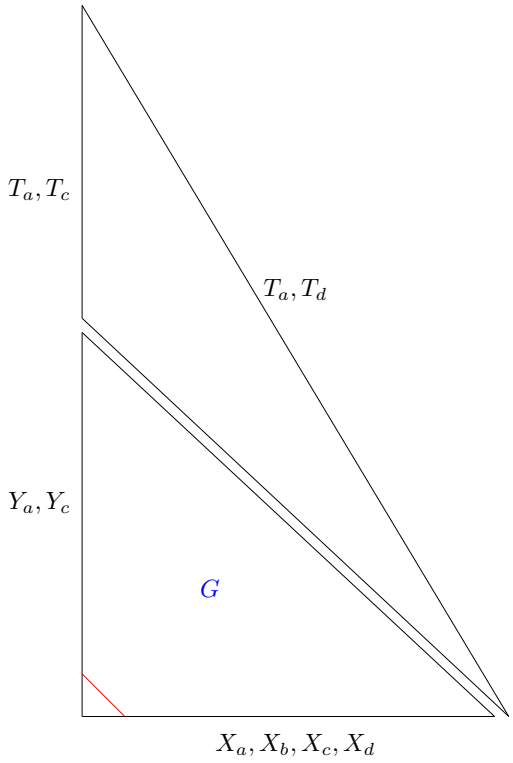
Observons les mots associés aux nombres pairs compris entre 6 et 80.



On constate que les diagonales de lettres à partir des premières lettres des mots sont constituées soit de lettres a et b exclusivement, soit de lettres c et d exclusivement.

3 Quelques régularités

On observe quelques régularités facilement explicables, qui lient entre eux les nombres de lettres de chaque sorte apparaissant dans un mot et dans une portion de la colonne des premières lettres, ou bien qui lient entre eux les nombres de dernières lettres des mots des doubles d'impairs et une autre portion de la colonne des premières lettres, selon le schéma suivant :



Le triangle global contient les mots associés aux nombres pairs de 6 à n.

X_a, X_b, X_c et X_d comptent le nombre de a, b, c ou d du mot associé à n privé de ses première et dernière lettres.

T_a et T_c comptent le nombre de lettres a ou c qui sont premières lettres des mots associés aux nombres pairs compris entre 3 et $n/2+3$. T_d compte le nombre de lettres d qui sont dernières lettres de mots associés à des nombres pairs compris entre 6 et n et qui sont doubles d'impairs.

Y_a et Y_c comptent le nombre de lettres a ou c qui sont premières lettres de mots associés aux nombres pairs compris entre $n/2+5$ et $n-2$.

Les contraintes suivantes sont toujours vérifiées :

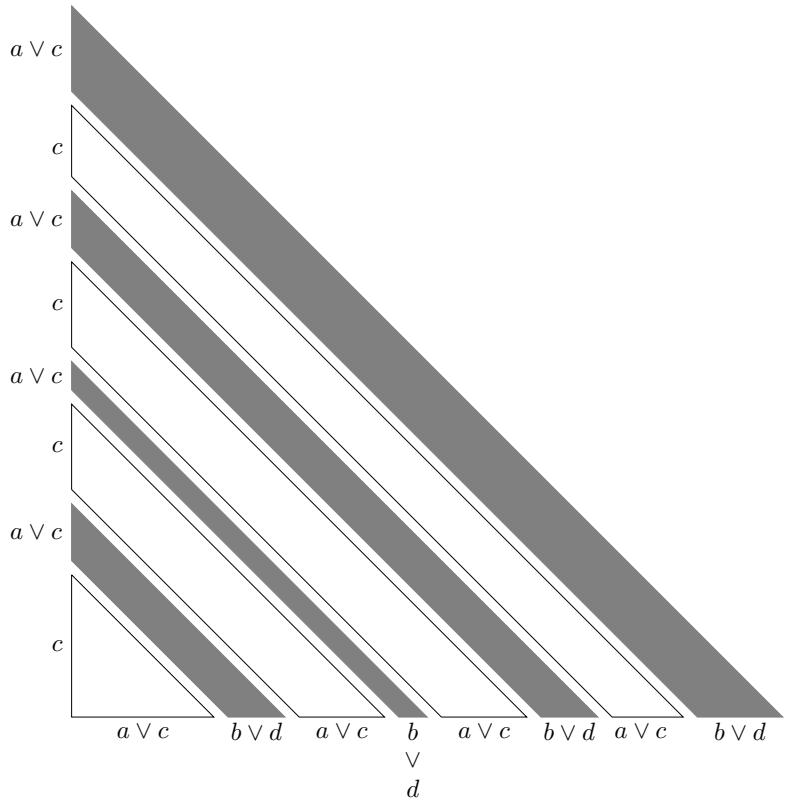
$$\begin{aligned} T_c &= T_d \\ Y_a &= X_a + X_b \\ Y_c &= X_c + X_d \end{aligned}$$

Les lettres des différents mots sont ainsi très intriquées mais ces éléments ne semblent pas permettre de comprendre davantage pourquoi tout mot contient un a.

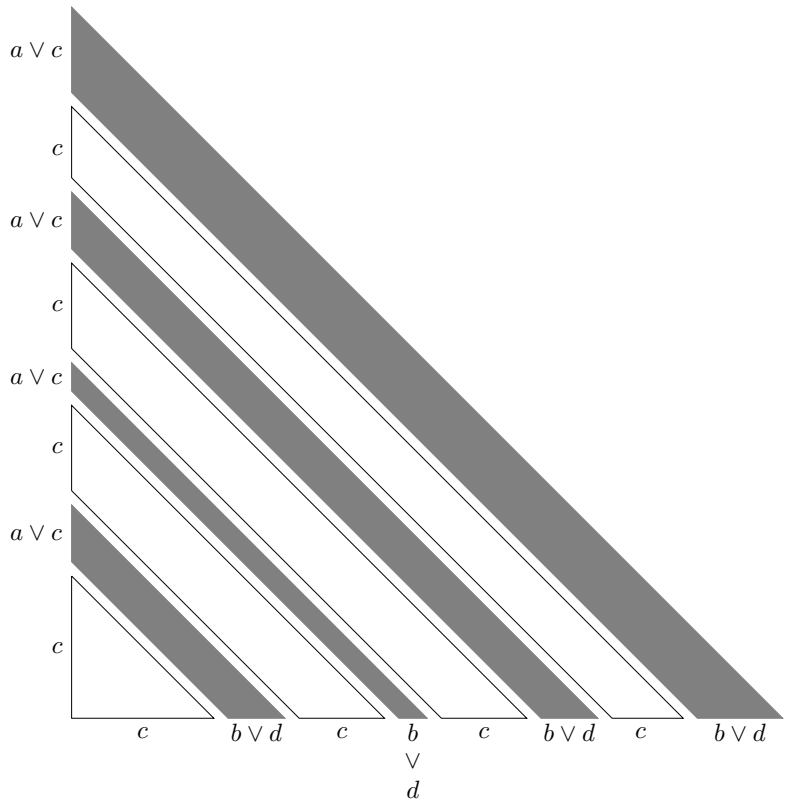
On va plutôt examiner les conséquences de l'absence de a dans un mot pour trouver une contradiction.

4 Rechercher une contradiction

Intéressons-nous pour cela à la partie que nous avons appelé G dans le schéma ci-dessus, de forme triangle isocèle. Elle est en quelque sorte constituée de "tranches de lettres" que l'on a symbolisées par des bandes blanches ou grises dans le schéma ci-dessous :



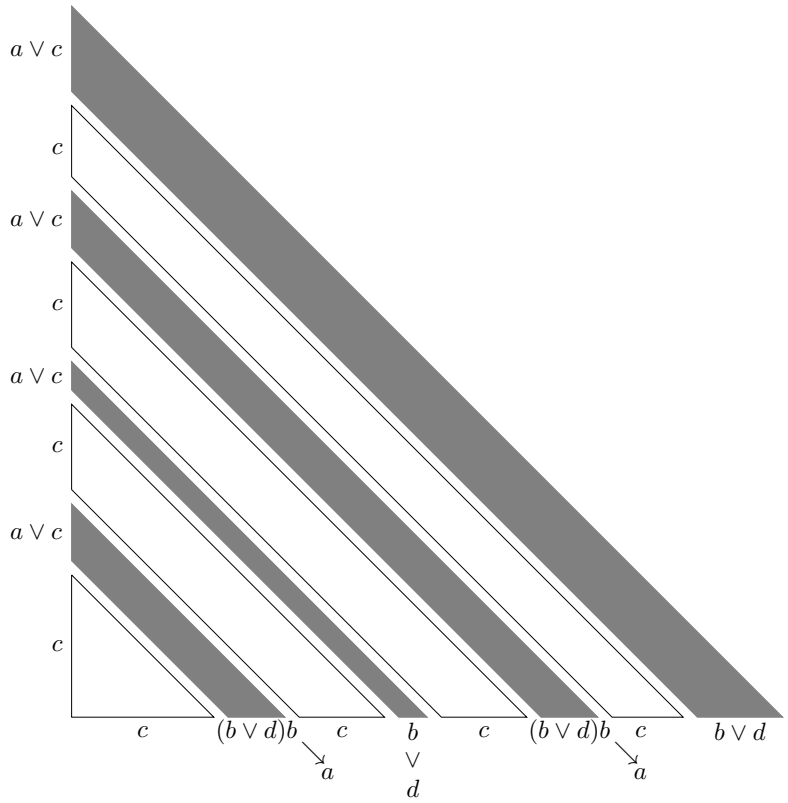
Imaginons que le mot m_n est associé à un nombre n qui contredit la conjecture de Goldbach, i.e. m_n ne contient aucune lettre a, la lettre a symbolisant on le rappelle la somme de deux nombres premiers. Cette configuration peut être représentée par le schéma ci-dessous (les lettres a ont disparu dans la ligne de lettres en bas du triangle isocèle) :



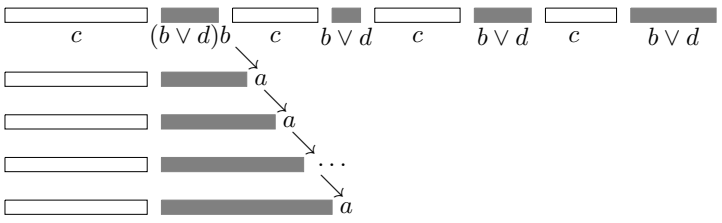
Si le mot m_n ne contient que des lettres b, c ou d, les seules règles de réécriture qui lui sont applicables sont les suivantes :

6) $bb \to b$	10) $cb \to d$	14) $db \to d$
7) $bc \to a$	11) $cc \to c$	15) $dc \to c$
8) $bd \to b$	12) $cd \to d$	16) $dd \to d$

Cela a une conséquence sur les seules positions possibles des lettres a dans le mot m_{n+2} du nombre pair $n+2$, m_{n+2} étant engendré en appliquant les seules règles de réécriture identifiées ci-dessus à m_n : les lettres a doivent obligatoirement se trouver dans m_{n+2} juste après les dernières positions des tranches $b \vee d$ et sont obligatoirement toutes seules entre d'autres lettres des 3 sortes b, c ou d. En effet, la seule règle de réécriture applicable à notre mot contredisant la conjecture de Goldbach est la règle 7 : $bc \to a$. Elle pourrait être utilisée sur la dernière lettre b éventuelle d'une tranche de $b \vee d$ associée à la première lettre c de la tranche de c qui la suit. On note cela par des petites flèches vers des lettres a pour deux tranches quelconques de $b \vee d$ sur le schéma ci-dessous :



Intéressons-nous à la première lettre a et voyons comment elle se comporte par application successive des règles de réécriture : elle reste seule et avance le long d'une diagonale de liaison un certain nombre de fois. Cela a pour conséquence que la tranche $b \vee d$ qui la précède s'allonge, ce qui est impossible. Symbolisons cela par le schéma suivant :



On a ainsi abouti à une contradiction qui serait conséquence de l'absence de a dans un mot. Cela entraîne l'impossibilité qu'un nombre pair contredise la conjecture de Goldbach. Les règles de réécriture fonctionnent de telle manière qu'elles préservent les "longueurs des tranches".