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 $109 + (-11)$.