Théorie de Galois et Conjecture de Goldbach

Denise Vella-Chemla

4/2/2013

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. 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 $n/2$.

2 Modéliser la recherche des décomposants de Goldbach par des équations algébriques

Chercher un décomposant de Goldbach p d'un nombre pair n consiste à chercher un nombre premier p dont le complémentaire à n est premier.

Après lecture d'un extrait de Galois : *"Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$"*, puis de l'extrait de Libri qui fournit sa méthode exhaustive pour trouver les solutions entières d'une équation polynomiale (cf Annexe), on réalise que les nombres premiers 3, 5, 7 *et* 11, par exemple, sont tout simplement racines de l'équation polynomiale

$$(x-3)(x-5)(x-7)(x-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0.$$

Les coefficients s'obtiennent ainsi :

$$26 = 3+5+7+11.$$
$$236 = 3.5+3.7+3.11+5.7+5.11+7.11.$$
$$886 = 3.5.7+3.5.11+3.7.11+5.7.11.$$
$$1155 = 3.5.7.11.$$

Plus généralement, pour exprimer que x, le nombre à chercher, est premier, on utilise une équation polynomiale de la forme :

$$\pm x^{\pi(n-2)-1} \pm \sigma_1.x^{\pi(n-2)-2} \pm \sigma_2.x^{\pi(n-2)-3} \pm \sigma_3.x^{\pi(n-2)-1} \ldots = 0$$

La plus grande puissance de x est $\pi(n-2)-1$ parce que la décomposition $1+(n-1)$ n'est jamais considérée comme une décomposition de Goldbach, le -1 servant à éliminer le nombre premier 2. Les nombres σ_i désignent respectivement les sommes de produits de i nombres premiers pris parmi tous les nombres premiers considérés. Par exemple, $\sigma_1 = p_1+p_2+p_3+p_4... = 3+5+7+11...$, $\sigma_2 = p_1p_2+p_1p_3+...+p_2p_3+p_2p_4+...$ et le dernier sigma est le produit de tous les nombres premiers inférieurs à $n-2$.

Pour exprimer que $n-x$, le complémentaire du nombre premier cherché doit être l'un des nombres premiers 3, 5, 7 *ou* 11, on remplace x par $(n-x)$ dans l'équation polynomiale ci-dessus ; on obtient l'équation polynomiale suivante :

$$(n-x)^4 - 26(n-x)^3 + 236(n-x)^2 - 886(n-x) + 1155 = 0.$$

Par élévation aux différentes puissances du monôme $n-x$, on obtient :

$$\begin{aligned}(n-x)^4 &= x^4 - 4nx^3 + 6n^2x^2 - 4n^3x + n^4.\\ (n-x)^3 &= -x^3 + 3nx^2 - 3n^2x + n^3.\\ (n-x)^2 &= n^2 - 2nx + x^2.\end{aligned}$$

On reconnaît les coefficients du binôme C_i^j dans l'élévation de $n-x$ à la puissance i.

Les résultats de la théorie de Galois sur la résolubilité des équations polynomiales ne pourraient-ils pas être utilisés ici pour montrer que notre système de deux équations admet toujours une solution en x au moins ?

3 Pgcd des polynômes

Dans la mesure où l'on cherche une racine r qui vérifie et la première et la deuxième équation, le fait que les deux polynômes en question aient un pgcd différent de 1 assurerait l'existence d'une telle racine.

Avec l'outil libre Sage, on expérimente cette idée à la recherche des décomposants de Goldbach de 14.

$Sage : decomp14 = var('x')$
$Sage : eq1 = x^5 - 39 * x^4 + 574 * x^3 - 3954 * x^2 + 12673 * x - 15015$
$Sage : eq2 = -x^5 + 31 * x^4 - 350 * x^3 + 1730 * x^2 - 3489 * x + 2079$
$Sage : eq1.gcd(eq2)$

$Sage :\ x^3 - 21 * x^2 + 131 * x - 231$

$Sage : eq4 = x^3 - 21 * x^2 + 131 * x - 231 == 0$

$Sage : solve([eq4], x)$
$Sage :\ [x == 7, x == 11, x == 3]$

Intéressons-nous maintenant, comme le suggère Galois en proposant comme deuxième équation $x^{p-1} = 1$ dans la phrase *"Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à Fx = 0 et à* $x^{p-1} = 1$*"* au groupe des unités, qui ne contient d'ailleurs que des nombres impairs si n est pair.

4 Le groupe des unités

Rappelons que 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 $(Z/nZ)^\times$ est bien connue. On la trouve notamment dans [3].

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 $\prod C_i$ si $(\mathbb{Z}/n\mathbb{Z})^\times$ est de structure $C2.\prod C_i$.

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 $C_{2^{k-2}}$.

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 leurs groupes respectifs ?

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 expliqué par Galois n'entraîne-t-elle pas automatiquement l'existence d'une solution pour l'équation polynomiale associée à 98 ?

Bibliographie

[1], **Evariste Galois**, *Sur la théorie des nombres*, Bulletin des Sciences mathématiques de M. Férussac, tome XIII, page 42 8, juin 1830. Note de J. Liouville : ce mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques.

[2], **Guillaume Libri**, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématiques*, extraits du *Journal de Mathématiques Pures et Appliquées*, publié par A.L. Crelle, Berlin, 1835, p.44.

[3], **Gilles Bailly-Maitre**, *Arithmétique et Cryptologie*, éditions Ellipses, 2012.