Equations polynomiales modulaires et Conjecture de Goldbach

Denise Vella-Chemla

5/2/2013

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

1 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, 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 de degré 4 :

$$(1) \qquad x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0.$$

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, un décomposant de Goldbach de n, est premier, on utilise une équation polynomiale de la forme :

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

En utilisant la notation $\pi(n)$ pour la fonction de décompte des nombres premiers inférieurs ou égaux à n, 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 et qu'on souhaite éliminer le nombre premier pair 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 impairs inférieurs à $n-2$.

Pour trouver par exemple les décomposants de Goldbach des nombres pairs compris entre les nombres premiers 11 et 13, 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 (1) 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 :

$$(n-x)^4 = x^4 - 4nx^3 + 6n^2x^2 - 4n^3x + n^4.$$
$$(n-x)^3 = -x^3 + 3nx^2 - 3n^2x + n^3.$$
$$(n-x)^2 = n^2 - 2nx + x^2.$$

Remplaçons n par 12, on obtient le polynôme $x^4 - 22x^3 + 164x^2 - 458x + 315 = 0$, qui est bien le développement de $(x-1)(x-5)(x-7)(x-9)$ dont chaque racine est le complémentaire à 12 d'un nombre premier inférieur à 12.

En annexe 1 sont fournis les 2 polynômes dont les racines sont soit les nombres premiers inférieurs à n, soit leur complémentaire à n pour les nombres n compris entre 6 et 18 (ainsi que leur pgcd étudié dans la section suivante).

2 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, et ainsi l'existence d'un décomposant de Goldbach pour n.

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

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

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

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

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

Comme attendu, les racines du polynôme pgcd sont bien les décomposants de Goldbach de 14.

3 Factorisation modulo p

Lors d'une conférence donnée dans le cadre du bicentenaire de la naissance de Galois, Alain Connes présente la théorie de Galois et fournit deux exemples de factorisation de polynômes modulo différents nombres premiers. Testons cette factorisation sur les polynômes pgcd trouvés dans la section précédente.

Pour $n = 8$, le pgcd des polynômes est $x^2 - 8x + 15$.
Dans $\mathbb{Z}/3\mathbb{Z}$, ce polynôme est égal à $x^2 + x$ qui est trivialement annulable donc 3 est décomposant de Goldbach de 8.
De même, dans $\mathbb{Z}/5\mathbb{Z}$, le polynôme pgcd est égal à $x^2 + 2x$ qui est trivialement annulable donc 5 est décomposant de Goldbach de 8.

Pour $n = 10$, le pgcd des polynômes est $x^3 - 15x^2 + 71x - 105$.
Dans $\mathbb{Z}/3\mathbb{Z}$, ce polynôme est égal à $x^3 + 2x$ qui est trivialement annulable donc 3 est décomposant de Goldbach de 10.

De même, dans $\mathbb{Z}/5\mathbb{Z}$, le polynôme pgcd est égal à $x^3 + x$ qui est trivialement annulable donc 5 est décomposant de Goldbach de 10 (décomposition de Goldbach dite triviale).

Pour $n = 12$, le pgcd des polynômes est $x^2 - 12x + 35$.
Dans $\mathbb{Z}/5\mathbb{Z}$, ce polynôme est égal à $x^2 + 3x$ qui est trivialement annulable donc 5 est décomposant de Goldbach de 12.

Pour $n = 14$, le pgcd des polynômes est $x^3 - 21x^2 + 131x - 231$.
Dans $\mathbb{Z}/3\mathbb{Z}$, ce polynôme est égal à $x^3 + 2x$ qui est trivialement annulable donc 3 est décomposant de Goldbach de 14.
Par contre, dans $\mathbb{Z}/5\mathbb{Z}$, le polynôme pgcd est égal à $x^3 + 4x^2 + x + 4$ qui n'est pas annulable par un entier et donc 5 n'est pas décomposant de Goldbach de 8.

Pour $n = 16$, le pgcd des polynômes est $x^4 - 32x^3 + 350x^2 - 1504x + 2145$.
Dans $\mathbb{Z}/3\mathbb{Z}$, ce polynôme est égal à $x^4+x^3+2x^2+2x$ qui est trivialement annulable donc 3 est décomposant de Goldbach de 16.
De même, dans $\mathbb{Z}/5\mathbb{Z}$, le polynôme pgcd devient $x^4 + 3x^3 + x$ qui est trivialement annulable donc 5 est décomposant de Goldbach de 16.
Par contre, dans $\mathbb{Z}/7\mathbb{Z}$, le polynôme pgcd est égal à $x^4 + 3x^3 + x + 4$ qui n'est pas annulable par un entier donc 7 n'est pas décomposant de Goldbach de 16.

Pour $n = 18$, le pgcd des polynômes est $x^4 - 36x^3 + 466x^2 - 2556x + 5005$.
Dans $\mathbb{Z}/5\mathbb{Z}$, ce polynôme est égal à $x^4+4x^3+x^2+4x$ qui est trivialement annulable donc 5 est décomposant de Goldbach de 18.
De même, dans $\mathbb{Z}/7\mathbb{Z}$, le polynôme pgcd est égal à $x^4+6x^3+4x^2+6x$ qui est trivialement annulable donc 5 est décomposant de Goldbach de 8.

4 A quelle condition le pgcd factorisé dans un certain corps premier est-il trivialement annulable ?

On voit aisément que le polynôme pgcd sera trivialement annulable dans un corps premier $\mathbb{Z}/p\mathbb{Z}$ à chaque fois qu'on réussira à éliminer la constante, habituellement dénotée a_0 du polynôme de la forme $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$.

A quoi est égale la constante a_0 du polynôme pgcd ? Etudions quelques exemples :

- pour $n = 6$, la constante a_0 est égale à $\frac{3.5}{1.3} = 3$;
- pour $n = 8$, la constante a_0 est égale à $\frac{3.5.7}{1.3.5} = 15$;
- pour $n = 10$, la constante a_0 est égale à $\frac{3.5.7}{3.5.7} = 105$;
- pour $n = 12$, la constante a_0 est égale à $\frac{3.5.7.11}{1.5.7.9} = 35$;
- pour $n = 14$, la constante a_0 est égale à $\frac{3.5.7.11.13}{1.3.7.9.11} = 231$;
- pour $n = 16$, la constante a_0 est égale à $\frac{3.5.7.11.13}{3.5.9.11.13} = 2145$;
- pour $n = 18$, la constante a_0 est égale à $\frac{3.5.7.11.13.17}{1.5.7.11.13.15} = 5005$;

La constante a_0 est le produit des décomposants de Goldbach de n. Il faudrait être capable de prouver que cette constante n'est jamais égale à 1.

5 Résumé et obstacle

On prend l'équation polynômiale $Fx = 0$ avec Fx produit des $(x - p_i)$ avec p_i un nombre premier impair inférieur à n, le nombre pair dont on cherche des décompositions de Goldbach.

On utilise le générateur $x \mapsto n - x$ qui envoie trivialement les décomposants de Goldbach les uns sur les autres.

Le polynôme Fx s'annule pour les nombres premiers ainsi que pour leur complémentaire, obtenu par le générateur, lorsque ce complémentaire est premier. Il ne s'annule pas pour les valeurs des complémentaires lorsque ceux-ci sont des nombres composés. Il faudrait être capable de démontrer que le groupe de Galois associé au polynôme Fx rend ce polynôme obligatoirement réductible modulo l'un des p_i. Malheureusement, parmi les unités $\mathbb{Z}/n\mathbb{Z}$, les nombres premiers pris seuls ne forment pas un sous-groupe (est une unité tout nombre qui est premier à n, les nombres premiers ne divisant pas n sont des unités mais les nombres composés premiers à n sont des unités également).

Il faudrait être capable de trouver un autre polynôme, qui serait invariant par le générateur proposé et qui serait tel que, comme le dit Galois, $Fx = 0$ et $x^{\varphi(n)} = 1$ auraient un facteur commun qui soit de degré 1 ou plus.

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] **Alain Connes**, *Conférence donnée à l'Académie des Sciences à l'occasion du bicentenaire de la naissance d'Evariste Galois*, vidéo visionnable à l'adresse $http://www.youtube.com/watch?v=rMb9UE5msH8$ et transparents téléchargeables à l'adresse $http://www.alainconnes.org/fr/downloads.php$ sous l'entrée Conférence Galois de la section Autres conférences.

Annexe : polynômes pour n compris entre 6 et 18 et leur pgcd

- $n = 6$

$$\begin{cases} x^2 - 8x + 15 = 0 \\ x^2 - 4x + 3 = 0 \end{cases} \longrightarrow\!\!\!\!\rightarrow \quad pgcd : x - 3$$

- $n = 8$

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 9x^2 - 23x + 15 = 0 \end{cases} \longrightarrow\!\!\!\!\rightarrow \quad pgcd = x^2 - 8x + 15 = 0$$

- $n = 10$

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 15x^2 - 71x + 105 = 0 \end{cases} \longrightarrow\!\!\!\!\rightarrow \quad pgcd = x^3 - 15x^2 + 71x - 105 = 0$$

- $n = 12$

$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 - 22x^3 + 164x^2 - 458x + 315 = 0 \end{cases} \longrightarrow\!\!\!\!\rightarrow \quad pgcd = x^2 - 12x + 35 = 0$$

- $n = 14$

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 31x^4 - 350x^3 + 1730x^2 - 3489x + 2079 = 0 \end{cases}$$
$$\longrightarrow \quad pgcd = x^3 - 21x^2 + 131x - 231 = 0$$

- $n = 16$

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 41x^4 - 638x^3 + 4654x^2 + 15681x - 19305 = 0 \end{cases}$$
$$\longrightarrow \quad pgcd = x^4 - 32x^3 + 350x^2 - 1504x + 2145 = 0$$

- $n = 18$

$$\begin{cases} x^6 - 56x^5 + 1237x^4 - 13712x^3 + 79891x^2 - 230456x + 255255 = 0 \\ x^6 - 52x^5 + 1057x^4 - 10552x^3 + 52891x^2 - 118420x + 75075 = 0 \end{cases}$$
$$\longrightarrow \quad pgcd = x^4 - 36x^3 + 466x^2 - 2556x + 5005 = 0$$