Conjecture de Goldbach et nullité du déterminant d'une matrice de Sylvester

Denise Vella-Chemla

1/1/2012

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. Trouver les décomposants de Goldbach d'un nombre pair n équivaut à trouver les racines communes de deux polynômes : le premier polynôme a pour seules racines les nombres premiers impairs inférieurs ou égaux à n ; le second polynôme a pour seules racines leur complémentaire à n. Par exemple, trouver les décomposants de Goldbach de 6 consiste à trouver les racines communes des polynômes $x^2 - 8x + 15 = (x-3)(x-5)$, et $x^2 - 4x + 3 = (x-1)(x-3)$.

Les coefficients et les racines des deux polynômes vérifient les équations de Viète : dans le cas général d'un polynôme unitaire $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2x^2 + a_1x + a_o$:

$x_1 + x_2 + ... + x_n = -a_{n-1}$
$x_1x_2 + x_1x_3 + ... + x_{n-1}x_n = a_{n-2}$ (*somme de tous les produits* 2 à 2)
$x_1x_2x_3 + x_1x_2x_4 + ... + x_{n-2}x_{n-1}x_n = -a_{n-3}$ (*somme de tous les produits* 3 à 3)
...
$x_1x_2...x_k + x_1x_2...x_{k+1} + ... + x_{n-k}x_{n-k+1}...x_n = (-1)^k a_{n-k}$ (*somme de tous les produits* k *à* k)
...
$x_1x_2...x_n = (-1)^n a_o$.

Les coefficients du deuxième polynôme sont les coefficients du développement de Taylor du premier polynôme. Dans le cas du nombre pair $n = 6$, les coefficients du premier polynôme sont :

$$\begin{aligned} a_1 &= 1 \\ a_2 &= -8 \\ a_3 &= 15 \end{aligned}$$

Les coefficients du deuxième polynôme sont :

$$\begin{array}{llll} b_1 = & & & +a_1, \\ b_2 = & & -2a_1n & -a_2, \\ b_3 = & a_1n^2 & +a_2n & +a_3. \end{array}$$

Deux polynômes ont des racines communes si leur résultant (le déterminant de leur matrice de Sylvester) est nul.

On rappelle que la matrice de Sylvester de $P(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$ et $Q(x) = b_0x^n + b_1x^{n-1} + b_2x^{n-2} + \ldots + b_{n-1}x + b_n$ est :

$$\begin{pmatrix} a_0 & 0 & \ldots & 0 & b_0 & 0 & \ldots & 0 \\ a_1 & a_0 & \ddots & 0 & b_1 & b_0 & \ddots & 0 \\ \vdots & a_1 & \ddots & \vdots & \vdots & b_1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 \\ a_n & \vdots & \ddots & a_1 & b_n & \vdots & \ddots & b_1 \\ 0 & a_n & \vdots & \vdots & 0 & b_n & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & a_n & 0 & \ldots & 0 & b_n \end{pmatrix}$$

Dans le cas où $n = 6$, exprimons le résultant uniquement en fonction des coefficients du premier polynôme. C'est le déterminant de la matrice suivante :

$$\begin{pmatrix} a_1 & 0 & b_1 & 0 \\ a_2 & a_1 & b_2 & b_1 \\ a_3 & a_2 & b_3 & b_2 \\ 0 & a_3 & 0 & b_3 \end{pmatrix} = \begin{pmatrix} a_1 & 0 & a_1 & 0 \\ a_2 & a_1 & -2a_1n - a_2 & a_1 \\ a_3 & a_2 & a_1n^2 + a_2n + a_3 & -2a_1n - a_2 \\ 0 & a_3 & 0 & a_1n^2 + a_2n + a_3 \end{pmatrix}$$

Le résultant des deux polynômes dans le cas où $n = 6$ est égal à :

$$a_1^4n^4 + 4a_1^3a_2n^3 + 4a_1^3a_3n^2 + 5a_1^2a_2^2n^2 + 8a_1^2a_2a_3n + 2a_1a_2^3n + 4a_1a_2^2a_3$$

Il se factorise en $(n-6)(n-8)^2(n-10)$ et s'annule donc bien pour 6.

Passons au cas des nombres pairs 8 et 10, compris entre les nombres premiers 7 et 11. Les 3 nombres premiers impairs que sont $3, 5$ *et* 7 fournissent les valeurs suivantes des coefficients des deux polynômes :

$$\begin{array}{lrrrr} a_1 = & & & & 1 \\ a_2 = & & & & -15 \\ a_3 = & & & & 71 \\ a_4 = & & & & -105 \\ b_4 = & -a_1n^3 & -a_2n^2 & -a_3n & -a_4 \\ b_3 = & & 3a_1n^2 & +2a_2n & +a_3 \\ b_2 = & & & -3a_1n & -a_2 \\ b_1 = & & & & +a_1 \end{array}$$

Dans les cas où $n = 8$ *ou* 10, exprimons le résultant uniquement en fonction des coefficients du premier polynôme. C'est le déterminant de la matrice $\begin{pmatrix} a_1 & 0 & 0 & b_1 & 0 & 0 \\ a_2 & a_1 & 0 & b_2 & b_1 & 0 \\ a_3 & a_2 & a_1 & b_3 & b_2 & b_1 \\ a_4 & a_3 & a_2 & b_4 & b_3 & b_2 \\ 0 & a_4 & a_3 & 0 & b_4 & b_3 \\ 0 & 0 & a_4 & 0 & 0 & b_4 \end{pmatrix}$ qui vaut :

$$\begin{pmatrix} a_1 & 0 & 0 & a_1 & 0 & 0 \\ a_2 & a_1 & 0 & -3a_1n - a_2 & a_1 & 0 \\ a_3 & a_2 & a_1 & 3a_1n^2 + 2a_2n + a_3 & -3a_1n - a_2 & a_1 \\ a_4 & a_3 & a_2 & -a_1n^3 - a_2n^2 - a_3n - a_4 & 3a_1n^2 + 2a_2n + a_3 & -3a_1n - a_2 \\ 0 & a_4 & a_3 & 0 & -a_1n^3 - a_2n^2 - a_3n - a_4 & 3a_1n^2 + 2a_2n + a_3 \\ 0 & 0 & a_4 & 0 & 0 & -a_1n^3 - a_2n^2 - a_3n - a_4 \end{pmatrix}$$

Le résultant des deux polynômes en fonction de n vaut :

$$-n^9+90n^8-3576n^7+82320n^6-1209744n^5+11767200n^4-75743744n^3+311032320n^2-739123200n+774144000$$

et se factorise en :

$$-(n-6)(n-8)^2(n-10)^3(n-12)^2(n-14)$$

Le résultant s'annule bien en 8 et 10.
Les racines multiples sont dûes au fait qu'en combinant de toutes les manières possibles les nombres premiers $3, 5$ *et* 7, on obtient les sommes suivantes : $3+3=6, 3+5=8, 3+7=10, 5+3=8, 5+5=10, 5+7=12, 7+3=10, 7+5=12, 7+7=14$. On a bien deux manières différentes d'obtenir 8, trois d'obtenir 10, 2 d'obtenir 12 et une manière d'obtenir les deux extrema 6 et 14. Le résultant contient donc en substance toute l'information concernant des décompositions de Goldbach de nombres pairs (pas tous, cela sera vu dans le cas suivant) compris entre deux nombres premiers successifs.

Passons au nombre pair 12. Les nombres premiers impairs sont $3, 5, 7$ *et* 11 fournissent les valeurs suivantes des coefficients des deux polynômes :

$$\begin{array}{lrrrrr}
a_1 = & & & & & 1 \\
a_2 = & & & & & -26 \\
a_3 = & & & & & 236 \\
a_4 = & & & & & -886 \\
a_5 = & & & & & 1155 \\
b_5 = & a_1n^4 & +a_2n^3 & +a_3n^2 & +a_4n & +a_5 \\
b_4 = & & -4a_1n^3 & -3a_2n^2 & -2a_3n & -a_4 \\
b_3 = & & & 6a_1n^2 & +3a_2n & +a_3 \\
b_2 = & & & & -4a_1n & -a_2 \\
b_1 = & & & & & a_1
\end{array}$$

Le résultant des deux polynômes vaut :

$$\begin{aligned}
n^{16} &- 208 * n^{15} + 20140 * n^{14} - 1204960 * n^{13} + 49855072 * n^{12} - 1512487936 * n^{11} + 34800798080 * n^{10} \\
&-619431879680 * n^9 + 8618909904128 * n^8 - 94050771759104 * n^7 + 802095988997120 * n^6 \\
&-5289268303093760 * n^5 + 26434722173927424 * n^4 - 96780810002890752 * n^3 \\
&+244741340434268160 * n^2 - 381863291623833600 * n + 276876106924032000
\end{aligned}$$

Il se factorise en $(n-6)(n-8)^2(n-10)^3(n-12)^2(n-14)^3(n-16)^2(n-18)^2(n-22)$ et s'annule bien en 12.
Par contre, ce résultant ne s'annule pas en 20 : en combinant les seuls nombres premiers $3, 5, 7$ et 11, on ne peut obtenir 20 dont les décompositions de Goldbach sont $3+17$ et $7+13$.

Pour $n = 14$, écrivons seulement les coefficients de la deuxième équation en fonction de ceux de la première.

$$\begin{array}{lrrrrrr}
b_6 = & -a_1n^5 & -a_2n^4 & -a_3n^3 & -a_4n^2 & -a_5n & -a_6 \\
b_5 = & & 5a_1n^4 & +4a_2n^3 & +3a_3n^2 & +2a_4n & +a_5 \\
b_4 = & & & -10a_1n^3 & -6a_2n^2 & -3a_3n & -a_4 \\
b_3 = & & & & +10a_1n^2 & +4a_2n & +a_3 \\
b_2 = & & & & & -5a_1n & -a_2 \\
b_1 = & & & & & & +a_1
\end{array}$$

Cela nous permet de voir apparaître en diagonale les coefficients du binôme de Newton.

En résumé, un même résultant fonction de n dont on doit démontrer la nullité intervient pour tous les nombres pairs compris entre deux nombres premiers successifs.

On constate que dans les factorisations des polynômes trouvées,

$$\begin{array}{l}
(n-6)(n-8)^2(n-10) \\
-(n-6)(n-8)^2(n-10)^3(n-12)^2(n-14) \\
(n-6)(n-8)^2(n-10)^3(n-12)^2(n-14)^3(n-16)^2(n-18)^2(n-22)
\end{array}$$

du fait de la commutativité de l'addition, les facteurs de la forme $(n-2p)$ avec p premier apparaissent à une puissance impaire tandis que les facteurs de la forme $(n-2c)$ avec c composé apparaissent à une puissance paire. On passe d'un résultant au résultant "suivant" en multipliant la factorisation par $2n+1$ facteurs supplémentaires, le $+1$ correspondant à l'ajout du facteur $(n-2p)$, p étant le dernier nombre premier ajouté à la liste. Si l'on cherche une sorte d'"'invariant de boucle"[*] lors du passage d'un nombre pair au suivant, il faudrait montrer que le nombre de racines du polynôme résultant inférieures à un certain nombre k est toujours supérieur au nombre de nombres pairs plus petits que k "à couvrir", ou dit autrement que lorsqu'on ajoute un nouveau nombre premier, on ne peut pas engendrer de "trou" dans la liste ordonnée des nombres pairs (un nombre pair sans décomposition de Goldbach)[†].

[*] notion intervenant dans les preuves de programmes de Hoare.

[†] On pourrait même envisager de simplement démontrer que le passage d'un résultant au résultant suivant permet d'obtenir seulement la décomposition de Goldbach d'un nombre pair de plus et alors la conjecture serait démontrée.