Conjecture de Goldbach et résidus quadratiques

Denise Vella-Chemla

28/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.
On rappelle que p est un décomposant de Goldbach de n si p est un nombre premier incongru* à n selon tout module premier inférieur à $\sqrt{n}$.

$$\forall\ n \geq 6,\ \ n\ =\ p+q,\ p\ et\ q\ premiers\ impairs \iff \forall\ q \leq \sqrt{n},\quad p \not\equiv n\ (mod\ q)^{\dagger}$$

Un décomposant de Goldbach de n, s'il existe, est un élément du groupe des unités $(\mathbb{Z}/n\mathbb{Z})^*$. Son complémentaire à n appartient lui aussi au groupe des unités. Le groupe des unités forme un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, \times)$. Son ordre divise l'ordre du groupe en question. Il y a donc au plus $\varphi(n)/2$ décompositions qui sont constituées de deux sommants qui sont tous les deux des unités. Par le principe des tiroirs, cela entraîne dans la plupart des cas qu'il y a au plus un résidu quadratique par colonne (ou inversement, au moins un non-résidu par colonne) ; remarque : cela n'est pas le cas lorsque les résidus quadratiques sont *"en face"*, ce qui arrive à chaque fois que n est de la forme $2p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_i^{\alpha_i}$ avec tous les p_i de forme $4n+1$.
Dans la plupart des cas donc, une décomposition de Goldbach a l'un de ses deux sommants qui est un non-résidu quadratique (cf en Annexe 2 les décompositions de Goldbach des nombres pairs n de 8 à 100 constituées d'un sommant non-résidu quadratique de n).

2 Tentative de démonstration

Il reste à comprendre, et c'est là l'essentiel, pourquoi l'un des nombres premiers non-résidus de n est forcément incongru à n selon tous les nombres premiers impairs inférieurs à $\sqrt{n}$.
Pour cela, on aimerait utiliser un extrait du Mémoire sur la théorie des nombres de Libri [1] (4° de la page en annexe) qui énonce *En multipliant le résidu quadratique a_r, successivement par tous les non-résidus quadratiques,*

$$b_1, b_2, b_3, \ldots, b_u, \ldots, b_p,$$

on aura de nouveau, après avoir divisé tous les produits par n, p restes différents, qui seront tous les non-résidus quadratiques de n.

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

†Par exemple, 98 a pour plus petit décomposant de Goldbach 19 parce que 3, 5, 7, 11, 13 et 17 sont tous congrus à 98 selon "quelqu'un".

$$98 = 2.7^2.$$
$$98 \equiv 3\ (mod\ 5).$$
$$98 \equiv 5\ (mod\ 3).$$
$$98 \equiv 7\ (mod\ 7).$$
$$98 \equiv 11\ (mod\ 3).$$
$$98 \equiv 13\ (mod\ 5).$$
$$98 \equiv 17\ (mod\ 3).$$

On peut représenter cela de la manière suivante :

$$r.\begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix} = \begin{pmatrix} n'_1 \\ n'_2 \\ \vdots \\ n'_k \end{pmatrix} \begin{matrix} (mod\ n) \\ (mod\ n) \\ \vdots \\ (mod\ n) \end{matrix}$$

avec r désignant un résidu quadratique de n, $n_1, \ldots, n_k$ désignant les non-résidus quadratiques de n et les n'_i étant une substitution des n_i.
Si l'on note $f_r : \mathcal{N}_n \to \mathcal{N}_n$ la substitution en question, au bout d'un certain nombre d'applications de f_r, on va retrouver l'ensemble de non-résidus dans l'ordre initial, ce que l'on écrit :

$$\exists m, (f_r)^m = 1_{\mathcal{N}_n}.$$

La contradiction pourrait peut-être venir du fait que n étant un résidu quadratique particulier de n, on peut multiplier l'ensemble des non-résidus par ce résidu particulier en place de r, mais comme $n \equiv 0\ (mod\ n)$, les non-résidus vont "être absorbés" par cette multiplication par n et on ne va pas pouvoir trouver tous les non-résidus, à de multiples substitutions près, au fur et à mesure de l'application de f_r.

On pourrait alors dire qu'il existe un nombre premier (il se trouve que c'est un non-résidu quadratique de n) incongru à n selon tout nombre premier inférieur à $\sqrt{n}$ (Le problème vient ici du fait qu'on n'a pas travaillé modulo des nombres premiers inférieurs à $\sqrt{n}$ mais modulo n, ce qui ne va pas.). Si on trouvait le moyen d'aboutir à une contradiction en partant de l'hypothèse que tous les nombres premiers non-résidus quadratiques de n ne peuvent être simultanément congrus à n selon un certain module chacun, un nombre premier non-résidu quadratique de n aurait son complémentaire à n qui serait premier également et il fournirait une décomposition de Goldbach de n.

Bibliographie

[1], **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.

Annexe 1 : page 44 du Mémoire sur la théorie des nombres de Guillaume Libri

$$b_1,\ b_2,\ b_3,\ \ldots\ b_u,\ \ldots\ b_p,$$

les p non-résidus quadratiques, on aura les équations

$$\sum_{x=1}^{x=n}\cos\frac{2x^2\pi}{n}=2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n};\quad \sum_{x=1}^{x=n}\sin\frac{2x^2\pi}{n}=2\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n};$$

$$\sum_{u=1}^{u=p+1}\left(\cos\frac{2a_u\pi}{n}+\cos 2\frac{b_u\pi}{n}\right)=\sum_{\gamma=1}^{\gamma=n}\cos\frac{2\gamma\pi}{n};\quad \sum_{u=1}^{u=p+1}\left(\sin\frac{2a_u\pi}{n}+\sin\frac{2b_u\pi}{n}\right)=\sum_{\gamma=1}^{\gamma=n}\sin\frac{2\gamma\pi}{n}.$$

3°. En multipliant successivement un résidu quadratique quelconque a_r, par tous les autres, on aura la série

$$a_r a_1,\ a_r a_2,\ a_r a_3,\ \ldots\ a_r a_p,$$

qui fournira de nouveau, en divisant tous ses termes par n, p restes différens, qui seront tous les résidus quadratiques de n disposés dans un ordre quelconque; d'où l'on déduira

$$30.\quad \begin{cases}\displaystyle\sum_{x=1}^{x=n}\cos\frac{2a_r x^2\pi}{n}=2\sum_{u=1}^{u=p+1}\cos\frac{2a_r a_u\pi}{n}=2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n};\\ \displaystyle\sum_{x=1}^{x=n}\sin\frac{2a_r x^2\pi}{n}=2\sum_{u=1}^{u=p+1}\sin\frac{2a_r a_u\pi}{n}=2\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}.\end{cases}$$

4°. En multipliant le résidu quadratique a_r, successivement par tous les non-résidus quadratiques

$$b_1,\ b_2,\ b_3,\ \ldots\ b_u,\ \ldots\ b_p,$$

on aura de nouveau, après avoir divisé tous les produits par n, p restes différens, qui seront tous les non-résidus quadratiques de n, et on trouvera

$$31.\quad \begin{cases}\displaystyle\sum_{u=1}^{u=p+1}\cos\frac{2a_r b_u\pi}{n}=\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n};\\ \displaystyle\sum_{u=1}^{u=p+1}\sin\frac{2a_r b_u\pi}{n}=\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}.\end{cases}$$

5°. En multipliant le non-résidu quadratique b_r, successivement par tous les résidus quadratiques

$$a_1,\ a_2,\ a_3,\ \ldots\ a_u,\ \ldots\ a_p,$$

et divisant tous les produits par n, on aura pour restes tous les non-résidus quadratiques; et par conséquent on obtiendra

$$32.\quad \begin{cases}\displaystyle\sum_{u=1}^{u=p+1}\cos\frac{2b_r a_u\pi}{n}=\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n};\\ \displaystyle\sum_{u=1}^{u=p+1}\sin\frac{2b_r a_u\pi}{n}=\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}.\end{cases}$$

6°. Enfin en multipliant successivement un non-résidu quadratique quelconque b_r, par tous les non-résidus quadratiques

$$b_1,\ b_2,\ b_3,\ \ldots\ b_u,\ \ldots\ b_p,$$

Annexe 2 : Illustration de l'énoncé "On trouve toujours un nombre premier non-résidu de n qui fournisse une décomposition de Goldbach de n" pour les nombres pairs de 8 à 100

8, 3 N 8, 3+5.
12, 5 N 12, 5+7.
16, 3 N 16, 3+13.
18, 5 N 18, 5+13.
20, 3 N 20, 3+17.
24, 5 N 24, 5+19.
28, 5 N 28, 5+23.
30, 17 N 30, 17+13.
32, 3 N 32, 3+29.
36, 5 N 36, 5+31.
40, 3 N 40, 3+37.
42, 5 N 42, 5+37.
44, 3 N 44, 3+41.
48, 5 N 48, 5+43.
50, 3 N 50, 3+47.
52, 5 N 52, 5+47.
54, 11 N 54, 11+43.
56, 3 N 56, 3+53.
60, 17 N 60, 17+43.
64, 3 N 64, 3+61.
66, 29 N 66, 29+37.
68, 7 N 68, 7+61.
70, 17 N 70, 17+73.
72, 5 N 72, 5+67.
76, 23 N 76, 23+53.
78, 5 N 78, 5+73.
80, 7 N 80, 7+73.
84, 5 N 84, 5+79.
88, 17 N 88, 17+71.
90, 17 N 90, 17+73.
92, 19 N 92, 19+73.
96, 17 N 96, 17+79.
98, 19 N 98, 19+79.
100, 3 N 100, 3+97.