Conjecture de Goldbach et résidus quadratiques

Denise Vella-Chemla

25/9/11

1 Quelles incongruences de second degré permettent de garantir les incongruences de premier degré souhaitées ?

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.
Cette conjecture est trivialement vérifiée par les nombres pairs doubles de 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 $\sqrt{n}$.

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

Dans la suite, on utilise la notation de Gauss : $a\ R\ b$ représente le fait que a est résidu quadratique de b tandis que $a\ N\ b$ représente le fait que a est non-résidu quadratique de b.

Posons $n\ =\ 2^{\alpha_0}A$ avec $A\ =\ p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_i^{\alpha_i}$.

On cherche à démontrer qu'il existe toujours un nombre premier q qui est non-résidu de tout diviseur premier impair p_k de n ($q\ N\ p_k$) et qui fournit une décomposition de Goldbach de n ($n\ =\ q+r$, avec q et r deux nombres premiers impairs).

Théorème‡ :

$$q\ N\ p_k \implies q\ N\ p_k^{\alpha_k}$$

En vertu de la règle des produits (le produit de deux résidus ou de deux non-résidus est un résidu, le produit d'un résidu et d'un non-résidu est un non-résidu), deux cas sont à considérer selon que i est pair ou impair.

1) i est pair $\implies q\ R\ A$.
On étudie alors la relation quadratique qui lie q à 2^{α_0}.
On utilise les résultats de l'article 103 des Recherches Arithmétiques (voir en annexe 2.).

- Si $\alpha_0 = 1$, si $q\ N\ 2$ alors $q\ N\ n$;
- Si $\alpha_0 = 2$, il faut trouver q de forme $4l+3$ pour que $q\ N\ 2^{\alpha_0} = 4$ et par conséquent $q\ N\ n$;

*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".

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

‡article 101 des Recherches Arithmétiques (voir en annexe 2.)

- Si $\alpha_0 \geq 3$, il faut qu'on trouve q de forme $8l+3$, $8l+5$ ou $8l+7$ de façon à ce que $q\ N\ 2^{\alpha_0}$ et par conséquent $q\ N\ n$;

2) i est impair $\implies q\ N\ A$. On étudie alors la relation quadratique qui lie q à 2^{α_0}.

- Si $\alpha_0 = 1$, $q\ R\ 2^{\alpha_0} = 2$ et par conséquent $q\ N\ n$;
- Si $\alpha_0 = 2$, il faut qu'on trouve q de forme $4l+1$ pour que $q\ R\ 2^{\alpha_0} = 4$ et par conséquent $q\ N\ n$;
- Si $\alpha_0 \geq 3$, il faut qu'on trouve q de forme $8l+1$ pour que $q\ R\ 2^{\alpha_0}$ et par conséquent $q\ N\ n$.

Dans tous les cas où on a pu aboutir à la conclusion $q\ N\ n$, tous les non-résidus quadratiques de n ne pouvant être simultanément congrus à n, l'un d'entre eux est non-congru à n[§], son complémentaire à n est premier également et il fournit une décomposition de Goldbach de n.

Annexe 1 : Illustration de l'énoncé "un nombre premier non-résidu de tous les diviseurs impairs du nombre pair n fournit une décomposition de Goldbach de n" pour les nombres pairs de 8 à 100

8, diviseur 2, 3N2, 3+5
12, diviseur 3, 5N3, 5+7
16, diviseur 2, 3N2, 3+13
18, diviseur 3, 5N3, 5+13
20, diviseur 5, 3N5, 3+17
24, diviseur 3, 5N3, 5+19
28, diviseur 7, 5N7, 5+23
30, diviseurs 3 et 5, 17N3, 17N5, 17+13
32, diviseur 2, 3N2, 3+29
36, diviseur 3, 5N3, 5+31
40, diviseur 5, 3N5, 3+37
42, diviseurs 3 et 7, 5N3, 5N7, 5+37
44, diviseur 11, 7N11, 7+37
48, diviseur 3, 5N3, 5+43
50, diviseur 5, 3N5, 3+47
52, diviseurs 3 et 13, 5N3, 5N13, 5+47
54, diviseur 3, 11N3, 11+43
56, diviseur 7, 3N7, 3+47
60, diviseurs 3 et 5, 17N3, 17N5, 17+43
64, diviseur 2, 3N2, 3+61
66, diviseurs 3 et 11, 29N3, 29N11, 29+47
68, diviseur 17, 7N17, 7+61
70, diviseurs 5 et 7, 17N5, 17N7, 17+53
72, diviseur 3, 5N3, 5+67
76, diviseur 19, 23N19, 23+53
78, diviseurs 3 et 13, 5N3, 5N13, 5+73
80, diviseur 5, 7N5, 7+73
84, diviseurs 3 et 7, 5N3, 5N7, 5+79
88, diviseur 11, 17N11, 17+71
90, diviseurs 3 et 5, 17N3, 17N5, 17+73
92, diviseur 23, 19N23, 19+73
96, diviseur 3, 17N3, 17+79
98, diviseur 7, 19N7, 19+79
100, diviseur 5, 3N5, 3+97.

[§]Là, le bât blesse, je crois, il doit être non congru à n selon tout les p_i inférieurs à $\sqrt{n}$ alors qu'il ne l'est là que selon les nombres premiers impairs divisant n.

Annexe 2 : Extraits des articles 101 et 103 des Recherches Arithmétiques

page 74, article 101 : Tout nombre non-divisible par p, qui est résidu de p, sera aussi résidu de p^n ; celui qui ne sera pas résidu de p ne le sera pas non plus de p^n.
La seconde partie de cette proposition est évidente par elle-même ; ainsi si la première n'était pas vraie, parmi les nombres plus petits que p^n et non-divisibles par p, il y en aurait plus qui fussent résidus de p qu'il n'y en aurait qui le fussent de p^n, c'est-à-dire plus de $\frac{1}{2}p^{n-1}(p-1)$. Mais on peut voir sans peine que le nombre des résidus de p qui se trouvent entre 1 et p^n, est précisément $\frac{1}{2}p^{n-1}(p-1)$.
Il est tout aussi facile de trouver effectivement un carré qui soit congru à un résidu donné, suivant le module p^n, si l'on connaît un carré congru à ce résidu suivant le module p.
Soit en effet a^2 un carré congru au résidu donné A, suivant le module p^μ, on en déduira, de la manière suivante, un carré $\equiv A$, suivant le module p^ν, ν étant $> \mu$ et non plus grand que 2μ. Supposons que la racine du carré cherché soit $\pm a + xp^\mu$; et il est aisé de s'assurer que c'est là la forme qu'elle doit avoir. Il faut donc qu'on ait $a^2 \pm 2axp^\mu + x^2p^{2\mu} \equiv A \ (mod\ p^\nu)$, ou comme $2\mu > \nu$, on aura $\pm 2axp^\mu \equiv A - a^2 \ (mod\ p^\nu)$. Soit $A - a^2 = p^\mu.d$, on aura $\pm 2ax \equiv d \ (mod\ p^{\nu-\mu})$; donc x sera la valeur de l'expression $\pm\frac{d}{2a} \ (mod\ p^{\nu-\mu})$. Ainsi étant donné un carré congru à A, suivant le module p, on en déduira un carré congru à A, suivant le module p^2 ; de là au module p^4, au module p^8, etc.
Exemple. Etant proposé le résidu 6 congru au carré 1, suivant le module 5, on trouve le carré 9^2 auquel il est congru suivant le module 25, 16^2 auquel il est congru suivant le module 125, etc.

page 76, article 103 : Comme nous avons commencé (n^o 100) par exclure le cas où $p = 2$, il faut ajouter quelque chose à ce sujet. Quand 2 est module, tous les nombres sont résidus, et il n'y en a point de non-résidus. Quand le module est 4, tous les nombres impairs de la forme $4k + 1$ sont résidus, et tous ceux de la forme $4k + 3$ sont non-résidus. Enfin, quand le module est 8 ou une plus haute puissance de 2, tous les nombres impairs de la forme $8k + 1$ sont résidus, et les autres, ou ceux de la forme $8k + 3$, $8k + 5$, $8k + 7$ sont non-résidus ;

Bibliographie

[1] **C. F. Gauss**, *Recherches Arithmétiques*, Editions Jacques Gabay, 1801.

[2] **G. Cantor**, *Vérification jusqu'à 1000 du théorème empirique de Goldbach*, Congrès de Caen de l'A.F.A.S. (Association Française pour l'Avancement des Sciences) du 10 août 1894, p.117 à 134.