Utiliser les congruences quadratiques pour trouver un décomposant de Goldbach d'un nombre pair

Denise Vella-Chemla

7/9/11

1 Introduction

Dans cette note, on se propose de montrer comment utiliser les congruences quadratiques pour trouver un décomposant de Goldbach d'un nombre pair donné. La conjecture de Goldbach (7 juin 1742), reformulée par Euler, stipule que tout nombre pair (supérieur à 4) est la somme de deux nombres premiers impairs.

2 Rappels

On fournit ci-dessous la table de la relation *est résidu quadratique de*. On rappelle que p est résidu quadratique de q si p est congru à un carré modulo q (i.e. si p est le reste d'une division euclidienne d'un carré par q). Cette table est la table II fournie par Gauss en annexe des Recherches Arithmétiques[1].

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
2	×			×			×		×		×		×		×
3	×	×			×	×			×			×			×
5	×		×		×			×		×	×		×		
7	×	×		×				×		×	×	×			×
11	×		×	×	×			×				×		×	
13	×	×				×	×		×	×				×	
17	×					×	×	×						×	×
19	×	×	×				×	×			×				
23	×			×	×	×		×	×	×			×	×	
29	×		×	×		×			×	×					
31	×	×	×		×				×		×		×	×	
37	×	×		×	×							×	×		×
41	×		×						×		×	×	×	×	
43	×	×		×		×	×	×					×	×	
47	×				×		×	×	×		×	×		×	×

Ci-dessous, on rappelle quelques théorèmes de la Section Quatrième des Recherches Arithmétiques de Gauss.

page 73, fin de l'article 98 :
On peut aussi faire usage des deux méthodes pour démontrer ce THÉORÈME[2] : *la valeur de l'expression* $\frac{a}{b}$ $(mod\ p)$*, sera un résidu, quand les nombres* a *et* b *seront tous les deux résidus ou non-résidus. Elle sera un non-résidu, quand l'un des nombres* a *et* b *sera résidu et l'autre non-résidu.*

[1] Dans la table fournie ici, inversement de celle fournie par Gauss, p est à lire en tête d'une ligne tandis que q est à lire en tête d'une colonne

[2] Ici, le mot est calligraphié en petites capitales bien que ces dernières ne soient pas utilisées par Gauss dans les Recherches Arithmétiques dans la mesure où il ne fournit pas la démonstration de ce théorème.

page 80, article 109 : en effet, il est évident que si r est un résidu, $\frac{1}{r}$ $(mod\ p)$ en sera un aussi.

page 84, article 116 : Au reste on tire facilement de ce qui précède la règle générale suivante : $+2$ est résidu de tout nombre qui n'est divisible ni par 4 ni par aucun nombre premier de la forme $8n+3$ ou $8n+5$, et non-résidu de tous les autres, par exemple, de tous ceux de la forme $8n+3$, $8n+5$, tant premiers que composés.

Dans la suite, on utilise la notation de Gauss, plutôt que le symbole de Legendre usité habituellement pour représenter la relation de congruence quadratique qui relie deux nombres : on notera $a\ R\ b$ le fait que a est résidu quadratique de b et $a\ N\ b$ le fait que a est non-résidu de b[3].

3 Mise en oeuvre

On cherche

$$p \not\equiv n\ (mod\ p_i),\ \forall\ p_i < \sqrt{n}.$$

Posons $n = a^2b$ avec a le plus grand carré divisant n et $b = \gamma_1\gamma_2\ldots\gamma_k$ le produit de tous les facteurs premiers de la factorisation de n de puissance impaire.
On cherche p tel que $\frac{1}{b}.p \not\equiv a^2\ (mod\ p_i)$.
En vertu du théorème sur les inverses (de l'article 109), cela équivaut à chercher p tel que $bp\ N\ p_i$, quel que soit p_i nombre premier impair inférieur à $\sqrt{n}$.

Pour chaque nombre premier impair p_i inférieur ou égal à $\sqrt{n}$, si $b\ R\ p_i$, il faut que $p\ N\ p_i$ et inversement, si $b\ N\ p_i$, il faut que $p\ R\ p_i$ pour que $bp\ N\ p_i$.

4 Application de notre méthode pour les nombres pairs inférieurs à 100

Dans la première démonstration de Gauss concernant le caractère de résiduosité quadratique de 2 selon n'importe quel nombre premier (article 112), il utilise une récurrence qui s'appuie sur le caractère de résiduosité quadratique de 2 selon les nombres premiers inférieurs à 100.
Dans sa première démonstration de la Loi de Réciprocité Quadratique, Gauss utilise à nouveau une démonstration par récurrence (article 136 et suivants).
Dans la dernière note (n^o 146) de son journal mathématique, il parle également du fait que Dedekind a vérifié une certaine propriété pour tous les nombres premiers inférieurs à 100.
Enfin, Euler, dans un superbe article "Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs" établit le bien-fondé de ses calculs en fournissant leur résultat pour les nombres jusqu'à 100.
En suivant leur enseignement, voyons ici comment appliquer notre méthode pour les nombres inférieurs à 100 et essayons d'en induire une généralisation[4].

$100 = 2^2.5^2$. On cherche p tel que $p\ N\ 3$, $p\ N\ 5$ et $p\ N\ 7$.
17 remplit ces trois conditions et fournit une décomposition de 100.

$98 = 2.7^2$. On cherche p tel que $2p\ N\ 3$, $2p\ N\ 5$ et $2p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
19 remplit ces trois conditinos et fournit une décomposition de 98.

$96 = 2^5.3$. On cherche p tel que $6p\ N\ 3$, $6p\ N\ 5$, et $6p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $3\ R\ 3$, $3\ N\ 5$, et $3\ N\ 7$. Il faut donc que $p\ R\ 3$, $p\ N\ 5$ et $p\ R\ 7$.

[3] En utilisant le symbole de Legendre, : $a\ R\ b$ équivaut à $\left(\frac{a}{b}\right) = +1$ tandis que $a\ N\ b$ équivaut à $\left(\frac{a}{b}\right) = -1$
[4] On ne traite pas les nombres pairs doubles de nombres premiers qui vérifient trivialement la conjecture.

7 remplit ces trois conditions et fournit une décomposition de 96.

$92 = 2^2.23$. On cherche p tel que $23p\ N\ 3$, $23p\ N\ 5$, et $23p\ N\ 7$. Or $23\ N\ 3$, $23\ N\ 5$, et $23\ R\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
19 remplit ces trois conditions et fournit une décomposition de 92.

$90 = 2.3^2.5$. On cherche p tel que $10p\ N\ 3$, $10p\ N\ 5$, et $10p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $5\ N\ 3$, $5\ R\ 5$, et $5\ N\ 7$. Et donc, $10\ R\ 3$, $10\ N\ 5$, et $10\ N\ 7$. Il faut donc que $p\ N\ 3$, $p\ R\ 5$ et $p\ R\ 7$.
11 remplit ces trois conditions et fournit une décomposition de 90.

$88 = 2^3.11$. On cherche p tel que $22p\ N\ 3$, $22p\ N\ 5$, et $22p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $11\ N\ 3$, $11\ R\ 5$, et $11\ R\ 7$. Et donc, $22\ R\ 3$, $22\ N\ 5$, et $22\ R\ 7$. Il faut donc que $p\ N\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
5 remplit ces trois conditions et fournit une décomposition de 88.

$84 = 2^2.3.7$. On cherche p tel que $21p\ N\ 3$, $21p\ N\ 5$, et $21p\ N\ 7$. Or $3\ R\ 3$, $3\ N\ 5$, et $3\ N\ 7$. Et $7\ R\ 3$, $7\ N\ 5$, et $7\ R\ 7$. Et donc, $21\ R\ 3$, $21\ R\ 5$, et $21\ N\ 7$. Il faut donc que $p\ N\ 3$, $p\ N\ 5$ et $p\ R\ 7$.
23 remplit ces trois conditions et fournit une décomposition de 84.

$80 = 2^4.5$. On cherche p tel que $5p\ N\ 3$, $5p\ N\ 5$, et $5p\ N\ 7$. Or $5\ N\ 3$, $5\ R\ 5$, et $5\ N\ 7$. Il faut donc que $p\ R\ 3$, $p\ N\ 5$ et $p\ R\ 7$.
7 remplit ces trois conditions et fournit une décomposition de 80.

$78 = 2.3.13$. On cherche p tel que $78p\ N\ 3$, $78p\ N\ 5$, et $78p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $3\ R\ 3$, $3\ N\ 5$, et $3\ N\ 7$. Et $13\ R\ 3$, $13\ N\ 5$, et $13\ N\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
19 remplit ces trois conditions et fournit une décomposition de 78.

$76 = 2^2.19$. On cherche p tel que $19p\ N\ 3$, $19p\ N\ 5$, et $19p\ N\ 7$. Or $19\ R\ 3$, $19\ R\ 5$, et $19\ N\ 7$. Il faut donc que $p\ N\ 3$, $p\ N\ 5$ et $p\ R\ 7$.
23 remplit ces trois conditions et fournit une décomposition de 76.

$72 = 2^3.3^2$. On cherche p tel que $2p\ N\ 3$, $2p\ N\ 5$, et $2p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
19 remplit ces trois conditions et fournit une décomposition de 72.

$70 = 2.5.7$. On cherche p tel que $70p\ N\ 3$, $70p\ N\ 5$, et $70p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $5\ N\ 3$, $5\ R\ 5$, et $5\ N\ 7$. Et $7\ R\ 3$, $7\ N\ 5$, et $7\ R\ 7$. Il faut donc que $p\ N\ 3$, $p\ N\ 5$ et $p\ R\ 7$.
23 remplit ces trois conditions et fournit une décomposition de 70.

$66 = 2.3.11$. On cherche p tel que $66p\ N\ 3$, $66p\ N\ 5$, et $66p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $3\ R\ 3$, $3\ N\ 5$, et $3\ N\ 7$. Et $11\ N\ 3$, $11\ R\ 5$, et $11\ R\ 7$. Il faut donc que $p\ N\ 3$, $p\ N\ 5$ et $p\ R\ 7$.
23 remplit ces trois conditions et fournit une décomposition de 66.

$64 = 2^6$. On cherche p tel que $p\ N\ 3$, $p\ N\ 5$ et $p\ N\ 7$.
17 remplit ces trois conditions et fournit une décomposition de 64.

$60 = 2^2.3.5$. On cherche p tel que $15p\ N\ 3$, $15p\ N\ 5$, et $15p\ N\ 7$. Or $3\ R\ 3$, $3\ N\ 5$, et $3\ N\ 7$. Et $5\ N\ 3$, $5\ R\ 5$, et $5\ N\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
19 remplit ces trois conditions et fournit une décomposition de 60.

$56 = 2^3.7$. On cherche p tel que $14p\ N\ 3$, $14p\ N\ 5$, et $14p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $7\ R\ 3$, $7\ N\ 5$, et $7\ R\ 7$. Il faut donc que $p\ R\ 3$, $p\ N\ 5$ et $p\ N\ 7$.
3 remplit ces trois conditions et fournit une décomposition de 53.

$54 = 2.3^3$. On cherche p tel que $6p\ N\ 3$, $6p\ N\ 5$, et $6p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $3\ R\ 3$, $3\ N\ 5$, et $3\ N\ 7$. Il faut donc que $p\ R\ 3$, $p\ N\ 5$ et $p\ R\ 7$.
7 remplit ces trois conditions et fournit une décomposition de 54.

$52 = 2^2.13$. On cherche p tel que $13p\ N\ 3$, $13p\ N\ 5$, et $13p\ N\ 7$. Or $13\ R\ 3$, $13\ N\ 5$, et $13\ N\ 7$. Il faut donc que $p\ N\ 3$, $p\ R\ 5$ et $p\ R\ 7$.
11 remplit ces trois conditions et fournit une décomposition de 52.

$50 = 2.5^2$. On cherche p tel que $2p\ N\ 3$, $2p\ N\ 5$, et $2p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
19 remplit ces trois conditions et fournit une décomposition de 50.

$48 = 2^4.3$. On cherche p tel que $3p\ N\ 3$ et $3p\ N\ 5$. Or $3\ R\ 3$ et $3\ N\ 5$. Il faut donc que $p\ N\ 3$ et $p\ R\ 5$.
5 remplit ces deux conditions et fournit une décomposition de 48.

$44 = 2^2.11$. On cherche p tel que $11p\ N\ 3$ et $11p\ N\ 5$. Or $11\ N\ 3$ et $11\ R\ 5$. Il faut donc que $p\ R\ 3$ et $p\ N\ 5$.
3 remplit ces deux conditions et fournit une décomposition de 44.

$42 = 2.3.7$. On cherche p tel que $42p\ N\ 3$ et $42p\ N\ 5$. Or $2\ N\ 3$ et $2\ N\ 5$. Et $3\ R\ 3$ et $3\ N\ 5$. Et $7\ R\ 3$ et $7\ N\ 5$. Il faut donc que $p\ R\ 3$ et $p\ R\ 5$.
19 remplit ces deux conditions et fournit une décomposition de 42.

$40 = 2^3.5$. On cherche p tel que $10p\ N\ 3$ et $10p\ N\ 5$. Or $2\ N\ 3$ et $2\ N\ 5$. Et $5\ N\ 3$ et $5\ R\ 5$. Il faut donc que $p\ N\ 3$ et $p\ R\ 5$.
11 remplit ces deux conditions et fournit une décomposition de 40.

$36 = 2^2.3^2$. On cherche p tel que $p\ N\ 3$ et $p\ N\ 5$.
17 remplit ces deux conditions et fournit une décomposition de 36.

$32 = 2^5$. On cherche p tel que $2p\ N\ 3$ et $2p\ N\ 5$. Or $2\ N\ 3$ et $2\ N\ 5$. Il faut donc que $p\ R\ 3$ et $p\ R\ 5$.
19 remplit ces deux conditions et fournit une décomposition de 32.

$30 = 2.3.5$. On cherche p tel que $30p\ N\ 3$ et $30p\ N\ 5$. Or $2\ N\ 3$ et $2\ N\ 5$. Et $3\ R\ 3$ et $3\ N\ 5$. Et $5\ N\ 3$ et $5\ R\ 5$.Il faut donc que $p\ N\ 3$ et $p\ N\ 5$.
17 remplit ces deux conditions et fournit une décomposition de 30.

$28 = 2^2.7$. On cherche p tel que $7p\ N\ 3$ et $7p\ N\ 5$. Or $7\ R\ 3$ et $7\ N\ 5$. Il faut donc que $p\ N\ 3$ et $p\ R\ 5$.
5 remplit ces deux conditions et fournit une décomposition de 28.

$24 = 2^3.3$. On cherche p tel que $6p\ N\ 3$. Or $2\ N\ 3$ et $3\ R\ 3$. Il faut donc que $p\ R\ 3$.
7 remplit cette condition et fournit une décomposition de 24.

$20 = 2^2.5$. On cherche p tel que $5p\ N\ 3$. Or $5\ N\ 3$. Il faut donc que $p\ R\ 3$.
3 remplit cette condition et fournit une décomposition de 20.

$18 = 2.3^2$. On cherche p tel que $2p\ N\ 3$. Or $2\ N\ 3$. Il faut donc que $p\ R\ 3$.
7 remplit cette condition et fournit une décomposition de 18.

$16 = 2^4$. On cherche p tel que $p\ N\ 3$.
5 remplit cette condition et fournit une décomposition de 16.

$12 = 2^2.3$. On cherche p tel que $3p\ N\ 3$. Or $3\ R\ 3$. Il faut donc que $p\ N\ 3$.
5 remplit cette condition et fournit une décomposition de 12.

On remarquera qu'on n'a pas traité le cas du nombre pair 68. En effet, il met en défaut la méthode de la façon suivante :
$68 = 2^2.17$. On cherche p tel que $17p\ N\ 3$, $17p\ N\ 5$, et $17p\ N\ 7$. Or $17\ N\ 3$, $17\ N\ 5$, et $17\ N\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ R\ 7$.
Et là, aucun nombre premier ne vérifie les trois congruences quadratiques souhaitées.

Annexe : un extrait de la biographie *Poincaré : philosophe et mathématicien* d'Umberto Bottazzini aux éditions Belin Pour la Science

Au sujet du raisonnement par récurrence : le terrain le plus naturel et le plus favorable pour cette étude est l'arithmétique élémentaire, c'est à dire les opérations mettant en jeu des nombres entiers. Quand nous analysons des opérations telles que l'addition et la multiplication, nous nous rendons compte qu'un type de raisonnement se *retrouve à chaque pas*, c'est la démonstration *par récurrence* : on établit d'abord un théorème pour n égal à 1 ; on montre ensuite que, s'il est vrai de $n-1$, il est vrai de n, et on en conclut qu'il est vrai pour tous les nombres entiers. C'est là le raisonnement mathématique par excellence, déclare Poincaré. Sa particularité est qu'il contient, sous une forme condensée, une infinité de syllogismes, et qu'il permet de passer du particulier au général, du fini à l'infini, concept qui apparaît dès les premiers pas de l'arithmétique élémentaire et sans lequel il n'y aurait pas de science parce qu'il n'y aurait rien de général, mais uniquement des énoncés particuliers. D'où nous vient ce raisonnement pas récurrence, s'interroge Poincaré ? Certainement pas de l'expérience. Celle-ci peut nous suggérer que la règle est vraie pour les dix ou les cent premiers nombres, mais elle est désarmée face à l'infinité de tous les nombres naturels. Le principe de contradiction (on dirait aujourd'hui le raisonnement par l'absurde) est aussi impuissant : il nous permet d'obtenir certaines vérités, mais non d'en enfermer une infinité en une seule formule. Cette règle (le raisonnement par récurrence), inaccessible à la démonstration analytique et à l'expérience, est le véritable type du jugement synthétique a priori, conclut Poincaré. L'irrésistible évidence avec laquelle ce principe s'impose n'est autre que l'affirmation de la puissance de l'esprit qui se sait capable de concevoir la répétition indéfinie d'un même acte dès que cet acte est une fois possible.

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.

[3] **R. Cuculière**, *Histoire de la Loi de Réciprocité Quadratique : Gauss et Tate*, Groupe de travail d'analyse ultramétrique, tome 7-8 (1979-1981), exp. n^o 36, p. 1-14.