Un algorithme d'obtention des décomposants de Goldbach d'un nombre pair

Denise Vella-Chemla

Décembre 2012

1 Introduction

La conjecture de Goldbach stipule que tout nombre pair n plus grand que 2 est la somme de deux nombres premiers. Ces nombres premiers p et q sont appelés décomposants de Goldbach de n. Assumons ici que la conjecture de Goldbach est vraie.

Rappelons quatre faits :

1) Les nombres premiers plus grands que 3 sont de la forme $6k \pm 1$.

2) n étant un nombre pair plus grand que 2 ne peut être le carré d'un nombre premier qui est impair. Si $p_1, p_2, \ldots, p_r$ sont des nombres premiers plus grands que $\sqrt{n}$, l'un d'entre eux au plus (peut-être aucun) appartient à la décomposition euclidienne de n en facteurs premiers puisque le produit de deux d'entre eux est supérieur à n.

3) Les décomposants de Goldbach de n sont à trouver parmi les unités du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z}, \times)$. Ces unités sont premières à n, elles sont en nombre pair et la moitié d'entre elles sont inférieures ou égales à $n/2$.

4) Si un nombre premier $p \leq n/2$ est congru à n modulo un nombre premier $m_i < \sqrt{n}$ $(n = p + \lambda m_i)$, son complémentaire à n, q, est composé parce que $q = n - p = \lambda m_i$ est congru à 0 $(mod\ m_i)$. Dans ce cas, le nombre premier p ne peut être un décomposant de Goldbach de n.

2 Algorithme

Prendre en compte ces faits élémentaires amène une procédure qui permet d'obtenir un ensemble de nombres qui sont des décomposants de Goldbach de n.

Notons m_i $(i = 1, \ldots, j(n))$, les nombres premiers $3 < m_i \leq \sqrt{n}$.

La procédure consiste d'abord à éliminer les nombres $p \leq n/2$ congrus à 0 $(mod\ m_i)$ puis à éliminer les nombres p congrus à n $(mod\ m_i)$.

Le crible d'Eratosthène est utilisé pour ces éliminations.

3 Etude d'un exemple

Appliquons la procédure au nombre pair $n = 500$.

Notons d'abord que $500 \equiv 2$ $(mod\ 3)$. Puisque $6k - 1 = 3k' + 2$, tous les nombres premiers de la forme $6k - 1$ sont congrus à 500 $(mod\ 3)$, de telle manière que leur complémentaire à 500 est composé. Nous n'avons pas à prendre en compte ces nombres. Aussi, nous ne considérons que les $\left\lfloor \dfrac{500}{12} \right\rfloor$ nombres de la forme $6k+1$ inférieurs ou égaux à $500/2$. Ils sont compris entre 7 et 247 (première colonne du tableau).

Puisque $\lfloor\sqrt{500}\rfloor = 22$, les modules premiers m_i différents de 2 et 3 sont $5, 7, 11, 13, 17, 19$. Appelons-les m_i où $i = 1, 2, 3, 4, 5, 6$.

La seconde colonne du tableau fournit le résultat de la première passe du crible : elle élimine les nombres congrus à 0 $(mod\ m_i)$ quelque soit i.

La troisième colonne du tableau fournit le résultat de la deuxième passe du crible : elle élimine les nombres congrus à n ($mod\ m_i$) quelque soit i.

Tous les modules inférieurs à $\sqrt{n}$ sauf ceux de la factorisation de n apparaissent en troisième colonne (pour les modules qui divisent n, la première et la deuxième passe éliminent les mêmes nombres).

$500 = 2^2.5^3$. Le module 5 n'apparaît pas en troisième colonne.

Un même module ne peut apparaître sur la même ligne en deuxième et troisième colonne.

500 est congru à 0 (mod 5), 3 (mod 7), 5 (mod 11), 6 (mod 13), 7 (mod 17) et 6 (mod 19).

$a_k = 6k+1$	*congruence(s) à 0 éliminant* a_k	*congruence(s) à* r $\neq 0$ *éliminant* a_k (*i.e. congruence(s) à* n)	n-a_k	*nombres restants*
7 (p)	0 (mod 7)	7 (mod 17)	493	
13 (p)	0 (mod 13)		487 (p)	
19 (p)	0 (mod 19)	6 (mod 13)	481	
25	0 (mod 5)	6 (mod 19)	475	
31 (p)		3 (mod 7)	469	
37 (p)			463 (p)	37
43 (p)			457 (p)	43
49	0 (mod 7)	5 (mod 11)	451	
55	0 (mod 5 *and* 11)		445	
61 (p)			439 (p)	61
67 (p)			433 (p)	67
73 (p)		3 (mod 7)	427	
79 (p)			421 (p)	79
85	0 (mod 5 *and* 17)		415	
91	0 (mod 7 *and* 13)		409 (p)	
97 (p)		6 (mod 13)	403	
103 (p)			397 (p)	103
109 (p)		7 (mod 17)	391	
115	0 (mod 5)	3 (mod 7) *and* 5 (mod 11)	385	
121	0 (mod 11)		379 (p)	
127 (p)			373 (p)	127
133	0 (mod 7 *and* 19)		367 (p)	
139 (p)		6 (mod 19)	361	
145	0 (mod 5)		355	
151 (p)			349 (p)	151
157 (p)		3 (mod 7)	343	
163 (p)			337 (p)	163
169	0 (mod 13)		331	
175	0 (mod 5 *and* 7)	6 (mod 13)	325	
181 (p)		5 (mod 11)	319	
187	0 (mod 11 *and* 17)		313 (p)	
193 (p)			307 (p)	193
199 (p)		3 (mod 7)	301	
205	0 (mod 5)		295	
211 (p)		7 (mod 17)	289	
217	0 (mod 7)		283 (p)	
223 (p)			277 (p)	223
229 (p)			271 (p)	229
235	0 (mod 5)		265	
241 (p)		3 (mod 7)	259	
247	0 (mod 13 *and* 19)	5 (mod 11)	253	

Remarque : revenons sur la première partie de l'algorithme, qui élimine les nombres p congrus à 0 ($mod\ m_i$) quelque soit i. Son résultat consiste à éliminer tous les nombres composés qui ont un quelconque m_i dans leur décomposition euclidienne, n en faisant éventuellement partie, à éliminer également tous les nombres premiers plus petits que $\sqrt{n}$, mais à conserver tous les nombres premiers supérieurs ou égaux à $\sqrt{n}$ qui est plus petit que $n/4+1$.

La seconde partie de l'algorithme élimine les nombres p dont le complémentaire à n est composé parce qu'ils partagent une congruence avec n ($p \equiv n \ (mod\ m_i)$ pour un i donné). La seconde partie de l'algorithme élimine les nombres p de la forme $n = p + \lambda m_i$ quelque soit i. Si $n = \mu_i m_i$, aucun nombre premier ne peut satisfaire la relation précédente. Puisque n est pair, $\mu_i = 2\nu_i$, la conjecture implique $\nu_i = 1$. Si $n \neq \mu_i m_i$, la conjecture implique qu'il existe un nombre premier p tel que, pour un i donné, $n = p + \lambda m_i$ qui peut être réécrit en $n \equiv p \ (mod\ m_i)\ or\ n - p \equiv 0 \ (mod\ m_i)$.

Les deux passes de l'algorithme peuvent être menées indépendamment l'une de l'autre.

Bibiographie

[1] **C.F. Gauss**, *Recherches arithmétiques*, 1807, Ed. Jacques Gabay, 1989.

[2] **J.F. Gold, D.H. Tucker**, *On A Conjecture of Erdös*, Proceedings - NCUR VIII. (1994), Vol. II, pp. 794-798.