Application double du crible d'Eratosthène pour trouver les décomposants de Goldbach d'un nombre pair

Denise Vella-Chemla

1/12/2012

1 Introduction

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.

Rappelons ici qu'un décomposant de Goldbach d'un nombre pair donné x doit vérifier deux propriétés : la première est qu'il doit être premier, la seconde est qu'il ne doit être congru à x selon aucun nombre premier inférieur ou égal à $\sqrt{x}$, ce qui garantit que son complémentaire à x est premier également*.

2 Exemple du nombre pair 500 : détail de l'application double du crible d'Eratosthène

On détaille ici pour le nombre pair 500 ce qu'on appellera l'application double du crible d'Eratosthène :

1) la première application du crible consiste à éliminer les nombres congrus à 0 selon un module premier inférieur ou égal à $\sqrt{x}$ (de manière à éliminer les nombres composés et les petits premiers inférieurs ou égaux à $\sqrt{x}$) ;

2) la deuxième application du crible consiste à éliminer les nombres congrus à x selon un module premier inférieur ou égal à $\sqrt{x}$.

500 étant congru à 2 selon le module 3, les seuls nombres à considérer sont ceux appartenant à la progression arithmétique $500 - 1 - 6k$, de 7 à 247.

On note dans la deuxième colonne le passage de la première passe du crible (élimination des nombres congrus à 0 selon un module inférieur ou égal à $\sqrt{x} = 22, ...$). Les modules à considérer sont 5, 7, 11, 13, 17, 19.

On note dans la troisième colonne le passage de la seconde passe du crible en spécifiant la congruence partagée avec x.
500 est congru à 0 $(mod\ 5)$, 3 $(mod\ 7)$, 5 $(mod\ 11)$, 6 $(mod\ 13)$, 7 $(mod\ 17)$ *et* 6 $(mod\ 19)$.
Les couleurs permettent de bien visualiser les périodicités.

*Un nombre premier appartient à l'une des deux progressions arithmétiques $6k - 1$ ou $6k + 1$. A cause de la deuxième propriété des décomposants de Goldbach de x, les nombres pairs x divisibles par 3 (les $6k$) peuvent avoir des décomposants de Goldbach dans les deux progressions $x + 1 - 6k$ ou $x - 1 - 6k$. Les nombres congrus à 1 selon le module 3 (les $6k + 4$) n'ont des décomposants que dans la progression arithmétique $x + 1 - 6k$ tandis que ceux congrus à -1 selon le module 3 (les $6k + 2$) n'ont des décomposants que dans la progression arithmétique $x - 1 - 6k$.

7	$0\ (mod\ 7)$	$7\ (mod\ 17)$
13	$0\ (mod\ 13)$	
19	$0\ (mod\ 19)$	$6\ (mod\ 13)$
25	$0\ (mod\ 5)$	$0\ (mod\ 5)$ *et* $6\ (mod\ 19)$
31		$3\ (mod\ 7)$
37		
43		
49	$0\ (mod\ 7)$	$5\ (mod\ 11)$
55	$0\ (mod\ 5$ *et* $11)$	$0\ (mod\ 5)$
61		
67		
73		$3\ (mod\ 7)$
79		
85	$0\ (mod\ 5$ *et* $17)$	$0\ (mod\ 5)$
91	$0\ (mod\ 7$ *et* $13)$	
97		$6\ (mod\ 13)$
103		
109		$7\ (mod\ 17)$
115	$0\ (mod\ 5)$	$0\ (mod\ 5)$ *et* $3\ (mod\ 7)$ *et* $5\ (mod\ 11)$
121	$0\ (mod\ 11)$	
127		
133	$0\ (mod\ 7$ *et* $19)$	
139		$6\ (mod\ 19)$
145	$0\ (mod\ 5)$	$0\ (mod\ 5)$
151		
157		$3\ (mod\ 7)$
163		
169	$0\ (mod\ 13)$	
175	$0\ (mod\ 5$ *et* $7)$	$0\ (mod\ 5)$ *et* $6\ (mod\ 13)$
181		$5\ (mod\ 11)$
187	$0\ (mod\ 11$ *et* $17)$	
193		
199		$3\ (mod\ 7)$
205	$0\ (mod\ 5)$	$0\ (mod\ 5)$
211		$7\ (mod\ 17)$
217	$0\ (mod\ 7)$	
223		
229		
235	$0\ (mod\ 5)$	$0\ (mod\ 5)$
241		$3\ (mod\ 7)$
247	$0\ (mod\ 13$ *et* $19)$	$5\ (mod\ 11)$

Dit familièrement, "pourquoi les congruences à x ne *bouchent-elles pas tous les trous* correspondant aux nombres premiers de l'intervalle initial ?

Présentons une idée qui peut être intéressante : on peut considérer que l'élimination des nombres dans la troisième colonne consiste à appliquer le crible d'Eratosthène, moyennant une translation adéquate à partir du nombre origine 0. On remplace chaque congruence à un nombre non-nul (telle que $x \equiv r\ (mod\ m)$) par la congruence correspondante $x + \delta \equiv 0\ (mod\ m)$ avec δ bien choisi.
Pour l'exemple du nombre pair 500, le système de congruences permettant de trouver l'intervalle "translaté" est le suivant :

$$\begin{cases} x \equiv 1\ (mod\ 6) \\ x \equiv 0\ (mod\ 17) \\ x + 12 \equiv 0\ (mod\ 13) \\ x + 18 \equiv 0\ (mod\ 19) \\ x + 24 \equiv 0\ (mod\ 7) \\ x + 42 \equiv 0\ (mod\ 11) \end{cases}$$

Ce système est équivalent au système : $\begin{cases} x \equiv 1 \ (mod\ 6) \\ x \equiv 4 \ (mod\ 7) \\ x \equiv 2 \ (mod\ 11) \\ x \equiv 1 \ (mod\ 13) \\ x \equiv 0 \ (mod\ 17) \\ x \equiv 1 \ (mod\ 19) \end{cases}$ de plus petite solution le nombre 646153.

On voit ainsi apparaître une judicieuse bijection entre les nombres x de l'intervalle initial $[7, 247]$ et les nombres $y = x + 646146$ de l'intervalle $[646153, 646393]$ telle que $x \equiv r \ (mod\ m) \iff y \equiv 0 \ (mod\ m)$.

7	$7 \ (mod\ 17)$	646153	$0 \ (mod\ 17)$
13		646159	
19	$6 \ (mod\ 13)$	646165	$0 \ (mod\ 13)$
25	$6 \ (mod\ 19)$	646171	$0 \ (mod\ 19)$
31	$3 \ (mod\ 7)$	646177	$0 \ (mod\ 7)$
37		646183	
43		646189	
49	$5 \ (mod\ 11)$	646195	$0 \ (mod\ 11)$
55		646201	
61		646207	
67		646213	
73	$3 \ (mod\ 7)$	646219	$0 \ (mod\ 7)$
79		646225	
85		646231	
91		646237	
97	$6 \ (mod\ 13)$	646243	$0 \ (mod\ 13)$
103		646249	
109	$7 \ (mod\ 17)$	646255	$0 \ (mod\ 17)$
115	$3 \ (mod\ 7)$ *et* $0 \ (mod\ 11)$	646261	$0 \ (mod\ 7)$ *et* $0 \ (mod\ 11)$
121		646267	
127		646273	
133		646279	
139	$6 \ (mod\ 19)$	646285	$0 \ (mod\ 19)$
145		646291	
151		646297	
157	$3 \ (mod\ 7)$	646303	$0 \ (mod\ 7)$
163		646309	
169		646315	
175	$6 \ (mod\ 13)$	646321	$0 \ (mod\ 13)$
181	$5 \ (mod\ 11)$	646327	$0 \ (mod\ 11)$
187		646333	
193		646339	
199	$3 \ (mod\ 7)$	646345	$0 \ (mod\ 7)$
205		646351	
211	$7 \ (mod\ 17)$	646357	$0 \ (mod\ 17)$
217		646363	
223		646369	
229		646375	
235		646381	
241	$3 \ (mod\ 7)$	646387	$0 \ (mod\ 7)$
247	$5 \ (mod\ 11)$	646393	$0 \ (mod\ 11)$

On peut donc considérer qu'on élimine sensiblement la même quantité de nombres dans les deux passes du crible. Le détail de la quantité de nombres éliminée selon chaque module est fourni dans le tableau ci-après. Le lemme de Gauss de l'article 127 des Recherches arithmétiques nous indique cela si ce n'est que les nombres sont consécutifs au lieu d'appartenir à des progressions arithmétiques (on aurait pu de toute façon ici se ramener à des suites de nombres consécutifs, les progressions arithmétiques en $6k$ n'étant utiles que pour alléger la présentation de cet exemple).

module	5	7	11	13	17	19
quantité de nbs éliminés par la première passe	8	6	3	4	2	3
quantité de nbs éliminés par la deuxième passe	8	6	3	3	3	2

On élimine 19 nombres sur 41 dans la colonne de gauche et 22 nombres sur 41 dans celle de droite. Il faudrait être capable de dénombrer les chevauchements pour montrer que même dans le cas où il y aurait le moins de chevauchements possibles, il resterait des nombres décomposants de Goldbach de x.

Considérons maintenant les nombres premiers de l'intervalle "translaté". A chacun d'eux correspond par bijection un nombre de l'intervalle initial $[7, 247]$. Chacun de ces nombres, s'il est premier, constituera un décomposant de Goldbach de x.
A 646159, premier, correspond 13, qui ne nous intéresse pas car inférieur à $\sqrt{500} = 22, ...$
A 646183, premier, correspond le nombre premier 37, décomposant de Goldbach de 500.
A 646189, premier, correspond le nombre premier 43, décomposant de Goldbach de 500.
A 646237, premier, correspond 91 qui n'est pas premier.
A 646267, premier, correspond 121 qui n'est pas premier.
A 646273, premier, correspond le nombre premier 127, décomposant de Goldbach de 500.
A 646309, premier, correspond le nombre premier 163, décomposant de Goldbach de 500.
A 646339, premier, correspond le nombre premier 193, décomposant de Goldbach de 500.

Les autres décomposants de Goldbach trouvés pour 500 ne sont pas en bijection avec des nombres premiers de l'intervalle translaté ; peut-être pourrions-nous nous passer d'eux pour aboutir à une démonstration...

Il est important de noter que le théorème des restes chinois nous assure de l'existence d'une infinité d"'intervalles translatés", qui peuvent être associés à l'intervalle initial.

Par exemple, pour le nombre pair 200, le même traitement fournit comme premier intervalle translaté l'intervalle $[2807, 2907]$ qui par bijection ne fournira que des nombres pairs de l'intervalle initial, qui ne peuvent donc trivialement pas être des décomposants de Goldbach de x. L'intervalle translaté suivant $[5813, 5913]$ (obtenu par addition de $3 \times 7 \times 11 \times 13$ nous fournira une certaine quantité de nombres premiers que l'on pourra "ramener" par translation dans l'intervalle initial à la recherche de nombres premiers plus petits susceptibles d'être des décomposants de Goldbach de x.
A 5813, premier, correspond le nombre premier 7, décomposant de Goldbach de 200.
A 5821, premier, correspond le nombre premier 15, qui n'est pas premier.
A 5827, premier, correspond le nombre premier 21, qui n'est pas premier.
A 5839, premier, correspond le nombre premier 33, qui n'est pas premier.
A 5843, premier, correspond le nombre premier 37, décomposant de Goldbach de 200.
A 5849, premier, correspond le nombre premier 43, décomposant de Goldbach de 200.
A 5851, premier, correspond le nombre premier 45, qui n'est pas premier.
A 5857, premier, correspond le nombre premier 51, qui n'est pas premier.
A 5861, premier, correspond le nombre premier 55, qui n'est pas premier.
A 5867, premier, correspond le nombre premier 61, décomposant de Goldbach de 200.
A 5869, premier, correspond le nombre premier 63, qui n'est pas premier.
A 5879, premier, correspond le nombre premier 73, décomposant de Goldbach de 200.
A 5881, premier, correspond le nombre premier 75, qui n'est pas premier.
A 5897, premier, correspond le nombre premier 91, qui n'est pas premier.
A 5903, premier, correspond le nombre premier 97, décomposant de Goldbach de 200.

Pour le nombre pair 100, le premier intervalle translaté possible, correspondant au système de congruences $\{x \equiv 2 \ (mod\ 3), x \equiv \ 1 \ (mod\ 7)\}$ commence au nombre 8 mais ne nous permet par translation vers l'intervalle initial de n'atteindre que des nombres pairs. On utilise donc le deuxième intervalle translaté fourni par le théorème des restes chinois, qui débute à 29, et qui nous permet par translation de 26 en arrière de trouver les décomposants de Goldbach de 100 que sont 11, 17, 41 *et* 47, qui sont à distance 26

des nombres premiers de cet intervalle $[29, 79]$ que sont $37,\ 43,\ 67$ *et* 73.

Il est étrange de lier ainsi les décomposants de Goldbach d'un nombre aux nombres premiers qui se trouvent appartenir à un intervalle de nombres plus grands que lui sur la droite numérique.

Il faudrait généraliser cette approche et s'assurer que cette nouvelle manière de concevoir la conjecture de Goldbach peut amener à une démonstration.

La réponse à notre question familière "pourquoi les congruences à x ne *bouchent-elles pas tous les trous* correspondant aux nombres premiers de l'intervalle initial ?" est qu'on ne peut obtenir une bijection entre des congruences à r $(mod\ m)$ et des congruences à 0 $(mod\ m)$ en restant sur le même intervalle, le seul moyen d'obtenir une telle bijection est de changer d'intervalle, comme présenté dans le tableau 3. C'est pour cette raison qu'il y a au moins un nombre premier qui, vérifiant toutes les incongruences à x nécessaires, a son complémentaire à x qui est premier également et le nombre premier en question fournit ainsi une décomposition de Goldbach de x.