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

Denise Vella-Chemla

Décembre 2012

1 Introduction

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

Un décomposant de Goldbach d'un nombre pair x ne peut être congru à x selon aucun module premier m inférieur ou égal à $\sqrt{x}$, cette condition garantissant que son complémentaire q à x est premier également (et ce quel que soit r $(mod\ m)$ le reste de x).

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

Ci-après, pour le nombre pair 500, nous montrons comment procéde la double utilisation du crible d'Eratosthène :

1) la première application du crible consiste à éliminer les nombres congrus à 0 modulo un nombre premier inférieur ou égal à $\sqrt{x}$;

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

500 étant congru à 2 modulo 3, les seuls nombres à considérer sont ceux appartenant à la progression arithmétique $6k+1$, de 7 à 247. Tous les nombres appartenant à la progression arithmétique $6k-1$ sont congrus à 500 $(mod\ 6)$ et sont donc composés.

Nous notons dans la deuxième colonne les congruences éliminées lors de la première passe du crible (congruences à 0 modulo un nombre premier inférieur ou égal à $\sqrt{500} = 22, ...$). Les modules devant être considérés sont 5, 7, 11, 13, 17, 19.

Nous notons dans la troisième colonne les congruences éliminées lors de la deuxième passe du crible (congruences partagées 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.

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* $19)$	$5\ (mod\ 11)$

Présentons une idée qui devrait être intéressante : on peut considérer que l'élimination des nombres dans la troisième colonne consiste à appliquer le crible d'Eratosthène sur un autre intervalle de la droite des entiers, obtenu par une translation adéquate depuis le nombre origine 0. Remplaçons chaque congruence à un nombre non nul (telle que $x \equiv r\ (mod\ m), r \neq 0$) par la congruence correspondante $x + \delta \equiv 0\ (mod\ m)$ avec δ convenablement choisi.

Pour l'exemple du nombre pair 500, le système de congruences qui permet de trouver l'intervalle translaté est :

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

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

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

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	$0\ (mod\ 11)$

La réponse à notre question familière "Pourquoi les congruences à x ne *remplissent-elles pas tous les trous* correspondant aux nombres premiers de l'intervalle initial ?" est que l'on ne peut obtenir une bijection entre des congruences à $r\ (mod\ m), r \neq 0$ et des congruences à $0\ (mod\ m)$ en restant sur un même intervalle, le seul moyen d'obtenir une telle bijection est de changer d'intervalle, comme présenté dans la table page 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 ce nombre premier est un décomposant de Goldbach de x.