

Pourquoi les antécédents de 1 par la fonction

$$f : x \mapsto (x^4(n-x)^4) \bmod \prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \sqrt{n}}} p_k$$

sont-ils (presque toujours) des décomposants de Goldbach de n ?

Denise Vella-Chemla, octobre 2026.

1. Ce que fait le programme

Pour un entier pair n tel que $6 \leq n \leq 100$, le programme forme le polynôme

$$f_n(x) = x^4(n-x)^4,$$

réduit coefficient par coefficient modulo 210, puis l'évalue aux entiers impairs x de 3 à $n/2$ (arrêt au dernier impair). Le résultat est ensuite réduit modulo la *primorielle*

$$P_n = \prod_{p \text{ premier}, p < \sqrt{n}} p,$$

et l'observation est que les x qui ont pour image 1 modulo P_n sont très souvent des décomposants de Goldbach de n (notés “dg” dans le programme), c'est-à-dire que x et $n-x$ sont premiers.

2. L'explication : la condition $f(x) = 1$ implique la caractérisation $x \not\equiv 0 \pmod{p_k}$ et $x \not\equiv n \pmod{p_k}$ pour tout module p_k premier inférieur ou égal à $\sqrt{n}$

Rappelons la caractérisation établie dans la note [1] <https://denisevellachemla.eu/jade1.pdf> :

Si $3 \leq m \leq n/2$ et si aucun premier $p \leq \sqrt{n}$ ne divise m ni $n-m$, alors m et $n-m$ sont premiers. Autrement dit, tout x impair de la fenêtre $[3, n/2]$ évitant les classes 0 et n modulo chaque $p \leq \sqrt{n}$ est un décomposant de Goldbach de n .

Proposition 1. *Soit x impair, $3 \leq x \leq n/2$, tel que $f_n(x) \equiv 1 \pmod{P_n}$, alors x est un décomposant de Goldbach de n .*

Démonstration. La congruence $f_n(x) \equiv 1 \pmod{P_n}$ dit que $x^4(n-x)^4$ est inversible modulo chaque $p \mid P_n$. En particulier, aucun premier $p < \sqrt{n}$ ne divise x (sinon $p \mid x^4$ et l'image serait $\equiv 0$ modulo p , et non pas à 1), et aucun ne divise $n-x$ (pour la même raison). De plus $p \mid x$ et $p \mid n-x$ entraîneraient $p \mid n$, ce qui est exclu pour p impair. Donc x et $n-x$ n'ont aucun diviseur premier $\leq \sqrt{n}$. Puisque $x \leq n/2$, on a $n-x \geq n/2 \geq \sqrt{n}$, et la caractérisation de [1] s'applique : x et $n-x$ sont premiers. $\square$

Le phénomène n'a donc *rien de mystérieux* : la condition “ $f(x) = 1$ modulo la primorielle” est une condition *plus forte* que la condition caractérisant les décomposants de Goldbach de n supérieurs à $\sqrt{n}$ de [1] (i.e. pour rappel : non congruence à 0 et non congruence à n selon tout module premier inférieur à $\sqrt{n}$). Si elle est vérifiée, on a trouvé un décomposant de Goldbach de n : l'expression polynomiale en x et $n - x$ sert de *détecteur* de la coprimauté aux petits premiers, et la coprimauté aux petits premiers *est* la primalité dans la fenêtre.

2.1. Pourquoi “très souvent” et pas “toujours” : l'artefact de la réduction modulo 210

Le programme ne calcule pas $f_n(x)$ mais le polynôme *réduit modulo 210*, notons-le $\tilde{f}_n$. La réduction soustrait à chaque coefficient un multiple de 210, donc

$$\tilde{f}_n(x) \equiv f_n(x) \pmod{210}.$$

Tout va bien tant que P_n divise 210, c'est-à-dire tant que $\sqrt{n} \leq 11$, soit $n \leq 121$: dans cette zone, image 1 modulo P_n équivaut exactement à la coprimauté de x et $n - x$ aux premiers $< \sqrt{n}$, et le test est exact (vérifié exhaustivement : zéro exception pour $6 \leq n \leq 120$).

Dès que $\sqrt{n} > 11$, la primorielle contient le facteur 11 (puis 13, 17, ...), qui ne divise pas 210. Modulo ces grands premiers, $\tilde{f}_n \not\equiv f_n$, et la congruence $\tilde{f}_n(x) \equiv 1 \pmod{11}$ ne dit plus rien sur la divisibilité de x ou $n - x$ par 11. C'est de là, et de là seulement, que viennent les exceptions. Vérification exhaustive pour $6 \leq n \leq 300$ (5550 couples (n, x) testés, dont 1133 décomposants de Goldbach) :

- 104 couples donnent image 1 ; 101 sont des décomposants de Goldbach ;
- les 3 exceptions sont $n = 162, x = 19$ (car $n - x = 143 = 11 \times 13$), $n = 166, x = 23$ (car $n - x = 143 = 11 \times 13$) et $n = 252, x = 43$ (car $n - x = 209 = 11 \times 19$) ;
- dans les trois cas le coupable est le premier 11, premier nombre premier ne divisant pas 210, et le facteur 11 de $n - x$ est invisible pour le polynôme tronqué.

En sens inverse, la condition image 1 est *beaucoup* plus forte que nécessaire : sur les 1133 décomposants de Goldbach de la plage, seuls 101 la satisfont. La raison est un phénomène de petite arithmétique : modulo p , tout résidu inversible u vérifie $u^4 \equiv 1$ pour $p = 3$ et $p = 5$ (le groupe des inversibles est d'ordre $p - 1 \in \{2, 4\}$), mais pas modulo 7 (ordre 6) : il faut alors $x(n - x) \equiv \pm 1 \pmod{7}$, une restriction supplémentaire qui élimine des décomposants de Goldbach parfaitement valides. La condition image 1 n'est donc ni nécessaire ni, au-delà de $n = 121$, suffisante : c'est un détecteur avec bruit, pas une caractérisation.

2.2. Remarque : si l'on supprimait la réduction modulo 210

Avec le polynôme exact f_n , la proposition ci-dessus donne un test *toujours* exact :

$$f_n(x) \equiv 1 \pmod{P_n} \implies x \text{ et } n - x \text{ premiers.}$$

Le module 210 n'apporte rien : il complique même le test en le corrompant au-delà de $n = 121$. La version honnête du programme est : “chercher x tel que $x^4(n - x)^4$ soit inversible modulo P_n ” — et l'inversibilité, pas la valeur 1, suffit.

3. Cela peut-il servir à une démonstration ?

Non, et c'est le point central. La chaîne logique est :

$$\exists x \in [3, n/2] : f_n(x) \equiv 1 \pmod{P_n} \implies \exists x \in [3, n/2] \text{ candidat}$$

$$\implies n \text{ vérifie la conjecture de Goldbach.}$$

Mais la première flèche est la plus difficile des deux : prouver qu'il *existe* un x de la fenêtre dont l'image vaut exactement 1 modulo la primorielle est un problème plus dur que la non-vacuité de l'ensemble des candidats, puisqu'il exige en plus l'équirépartition de f_n parmi les valeurs inversibles. Or la non-vacuité des candidats est précisément le maillon manquant, identifié dans la note [1] : c'est la barrière de parité, le même mur que pour les premiers jumeaux - la distribution des classes de congruences qui passent à travers tous les filtres dans les progressions arithmétiques au-delà de $\sqrt{n}$.

L'idée proposée ne crée donc pas d'information nouvelle : elle *ré-encode* la condition de candidat sous forme polynomiale. C'est un détecteur, pas un générateur d'existence. On retrouve l'obstruction déjà décrite :

- le monde profini (les congruences modulo la primorielle) dit "si un point de la roue tombe dans la fenêtre, c'est un décomposant de Goldbach" ;
- la place archimédienne (la fenêtre $[3, n/2]$) décide de l'existence, et le monde profini y est aveugle.

4. Enseignement

1. un nombre a pour image 1 modulo la primorielle
 $\implies x$ et $n - x$ sont premiers à tous les nombres premiers $< \sqrt{n}$
 $\implies$ décomposants de Goldbach par la note [1] :
le phénomène observé est une conséquence directe de la caractérisation de la note en question ;
2. Le "très souvent" est un artefact de la réduction des coefficients modulo 210 : exact pour $n \leq 121$, trois fausses alertes pour $6 \leq n \leq 300$, toutes causées par le premier 11, invisible pour un polynôme tronqué modulo 210.
3. Le test est très loin d'être nécessaire (101 décomposants de Goldbach détectés sur 1133) : la contrainte $u^4 \equiv 1$ modulo 7 élimine des décomposants de Goldbach valides.
4. Pour une démonstration, la condition est plus forte que la condition de candidat, donc au moins aussi difficile à satisfaire : elle ne contourne pas la barrière de parité, elle utilise une condition sur un polynôme qui n'est pas nécessaire et suffisante.