

Une reformulation tensorielle du crible de Goldbach via un cube de congruences

Denise Vella-Chemla, pilotant l'IA claude

27 juin 2026

1 Motivation

On cherche à détecter, pour un entier pair n , l'existence de *décomposants de Goldbach* $p > \sqrt{n}$, c'est-à-dire des entiers $p \in (\sqrt{n}, n - \sqrt{n})$ tels que ni p ni $n - p$ ne soit divisible par un nombre premier $z \leq \sqrt{n}$. Un tel p , s'il existe, est automatiquement premier (par construction il n'a aucun facteur $\leq \sqrt{n}$, et $n - p$ non plus), et $n = p + (n - p)$ est alors une décomposition de Goldbach.

L'idée de départ est d'encoder la relation de congruence dans un objet à trois indices, puis d'examiner si des opérations algébriques usuelles (produit matriciel, déterminant, spectre) permettent de *lire* l'existence d'un tel p .

2 Le cube de congruences

Définition 1 Pour $x, y, z \geq 1$, on définit le cube booléen $M \in \{0, 1\}^{N \times N \times N}$ par

$$M[x - 1, y - 1, z - 1] = \begin{cases} 1 & \text{si } x \equiv y \pmod{z}, \\ 0 & \text{sinon.} \end{cases}$$

Le décalage d'indices (-1 partout) sert uniquement à éviter la ligne/colonne 0 qui n'a pas de sens arithmétique pour un module.

Pour z fixé, on note M_z la tranche matricielle $M_z[x, y] = M[x, y, z]$. C'est la matrice d'adjacence de la relation « même classe résiduelle modulo z » sur $\{1, \dots, N\}$: une matrice de bloc constante par classes, étroitement liée aux matrices circulantes (chaque M_z est en fait une somme de matrices de permutation circulantes correspondant aux décalages multiples de z).

3 Extraction de la condition de Goldbach

Définition 2 Pour z premier et $p \in \{1, \dots, n - 1\}$, on pose

$$v_z[p] = (1 - M_z[p, 0]) \cdot (1 - M_z[p, n]) = \mathcal{K}[p \not\equiv 0 \pmod{z}] \cdot \mathcal{K}[p \not\equiv n \pmod{z}].$$

Le vecteur v_z est lu directement dans deux colonnes de la tranche M_z (colonnes d'indices 0 et n). En notant $\mathcal{P} = \{z \text{ premier} : z \leq \sqrt{n}\}$, on forme le produit de Hadamard (coordonnée par coordonnée) :

$$w = \bigodot_{z \in \mathcal{P}} v_z, \quad \text{et} \quad N(n) = \sum_{p=\lceil \sqrt{n} \rceil}^{n-\lceil \sqrt{n} \rceil} w[p].$$

Remarque 1 $N(n)$ compte exactement les entiers p vérifiant la condition de l'énoncé : pour tout $z \leq \sqrt{n}$ premier, $p \not\equiv 0$ et $p \not\equiv n \pmod{z}$. C'est une identité exacte, pas une approximation : $N(n) > 0$ si et seulement s'il existe un décomposant de Goldbach de n au-delà de \sqrt{n} .

4 Développement par inclusion-exclusion

En développant chaque facteur $v_z = 1 - \mathcal{K}[p \equiv 0] - \mathcal{K}[p \equiv n] + \mathcal{K}[p \equiv 0 \text{ et } p \equiv n \pmod{z}]$ (le dernier terme étant nul dès que $z \nmid n$), le produit sur \mathcal{P} se développe en somme sur les parties $S \subseteq \mathcal{P}$:

$$N(n) = \sum_{S \subseteq \mathcal{P}} (-1)^{|S|} \cdot \#\left\{p \in I_n : \forall z \in S, p \equiv 0 \text{ ou } p \equiv n \pmod{z}\right\},$$

où $I_n = [\sqrt{n}, n - \sqrt{n}]$. Par le théorème des restes chinois (les éléments de \mathcal{P} étant premiers entre eux), pour S fixé il y a exactement $2^{|S|}$ classes résiduelles modulo $\prod_{z \in S} z$ qui satisfont la condition, chacune contenant environ $|I_n| / \prod_{z \in S} z$ entiers. D'où l'approximation

$$N(n) \approx n \prod_{z \in \mathcal{P}} \left(1 - \frac{2}{z}\right),$$

qui est, à la constante de singularité près (laquelle dépend des facteurs premiers de n), l'**heuristique de Hardy–Littlewood** pour la fonction de Goldbach.

5 Diagnostic

Proposition 1 (Ce que le cube apporte) *L'identité d'inclusion-exclusion du §4 est exacte et correctement encodée par les opérations sur M : $N(n)$ s'obtient par lecture de coordonnées précises (colonnes 0 et n de chaque tranche M_z) suivies d'un produit de Hadamard et d'une somme. Aucune approximation n'intervient à ce stade.*

Proposition 2 (Ce que le cube ne résout pas) *Le passage de la somme exacte sur $2^{|\mathcal{P}|}$ parties à l'approximation $n \prod (1 - 2/z)$ introduit une erreur cumulée de l'ordre de $2^{|\mathcal{P}|} \sim 2^{2\sqrt{n}/\ln n}$ (par le théorème des nombres premiers, $|\mathcal{P}| = \pi(\sqrt{n}) \sim 2\sqrt{n}/\ln n$), qui domine largement le terme principal n . C'est exactement l'obstruction classique du crible de Legendre, celle que les cribles tronqués de Brun et Selberg contournent partiellement (ils permettent par exemple le théorème de Chen) mais qui reste, dans sa forme « pure », bloquée par l'obstruction de parité : aucune opération linéaire ou spectrale sur M (produit MM^\top , déterminant, valeurs propres) ne peut distinguer un entier premier d'un entier ayant exactement deux facteurs premiers, car ces opérations agrègent une information globale sur les indices alors que la distinction recherchée est de nature locale et multiplicative.*

6 Conclusion

Le cube M constitue une reformulation fidèle et élégante du crible d’Eratosthène–Legendre appliqué simultanément autour de 0 et de n . Il ne fournit cependant pas de mécanisme nouveau permettant de franchir l’obstruction de parité : la difficulté de la conjecture de Goldbach ne réside pas dans la représentation de l’information arithmétique, mais dans le volume d’erreur inhérent à toute somme d’inclusion-exclusion non tronquée sur l’ensemble des petits nombres premiers.