Explication par l'ia lumo de la façon dont l'obstruction de parité s'applique aussi à "mon" crible : le principe de parité, le crible de Selberg et la conjecture de Goldbach, Denise Vella-Chemla pilotant l'ia lumo, septembre 2026

Je suis frustrée par le fait que les ia m'opposent systématiquement l'obstruction de parité comme impossibilité pour "mon" crible (qui n'est pas plus le "mien" que celui de Brun, ainsi que, surtout et finalement, celui de Jean Merlin) de permettre d'avancer un peu face à la conjecture de Goldbach.

L'explication ci-dessous a été intégralement rédigée par l'ia lumo.

Résumé

Ce document reprend, dans l'ordre, tous les échanges d'un fil de discussion autour de l'article d'Atle Selberg, *The general sieve method and its place in prime number theory* (Congrès international de 1950), dans la traduction de Denise Vella-Chemla. Il explique le principe de parité, ses conséquences quantitatives (équations (14) et (14') de l'article), et ce qu'il implique pour une approche par crible de la conjecture de Goldbach.

1. L'article de Selberg en une page

Selberg considère un ensemble d'entiers n (au nombre de N) et des premiers $p_1, \dots, p_r$; on veut estimer le nombre $N(p_1, \dots, p_r)$ d'entiers divisibles par aucun des p_i. Le point de départ est l'identité d'inclusion-exclusion

$$N(p_1, \dots, p_r) = \sum_d \mu(d) \sum_{d|n} 1, \tag{1}$$

où d parcourt les entiers composés des p_i seulement. On dispose d'une approximation

$$\sum_{d|n} 1 = \frac{N}{f(d)} + R_d, \tag{2}$$

avec f multiplicative et un reste R_d dont on ne connaît qu'une borne de $|R_d|$. En injectant (2) dans (1) on obtient

$$N(p_1, \dots, p_r) = N \prod_{i=1}^{r} \Big(1 - \frac{1}{f(p_i)}\Big) + \theta \sum_d |R_d|, \tag{3}$$

dont le terme d'erreur écrase le terme principal dès que r est grand.

Toute l'astuce du crible est de remplacer $\sum_{d|n} \mu(d)$ par des *poids* ρ_d avec $\rho_1 = 1$ qui, pour tout n, majorent ou minorent $\sum_{d|n} \mu(d)$, tout en gardant $\sum_d |\rho_d|\,|R_d|$ à une taille raisonnable :

$$\Big(\text{majoration : } \sum_{d|n} \rho_d \;\geq\; \sum_{d|n} \mu(d)\Big) \quad \Rightarrow \; N(p_1, \dots, p_r) \;\leq\; N \sum_d \frac{\rho_d}{f(d)} + \sum_d |\rho_d|\,|R_d|, \tag{4}$$

$$\Big(\text{minoration : } \sum_{d|n} \rho_d \;\leq\; \sum_{d|n} \mu(d)\Big) \quad \Rightarrow \; N(p_1, \dots, p_r) \;\geq\; N \sum_d \frac{\rho_d}{f(d)} + \sum_d |\rho_d|\,|R_d|. \tag{5}$$

Pour la borne supérieure, Selberg choisit $\rho_d = \sum_{d_1 d_2/\kappa = d} \lambda_{d_1}\lambda_{d_2}$, si bien que

$$\sum_{d|n} \rho_d = \{\sum_{d|n} \lambda_d\}^2 \geq 0$$

la condition (4) est automatique et l'optimisation devient un calcul de minimum de forme quadratique (formules (8)-(10) de l'article). Le cas de la borne inférieure est "essentiellement plus compliqué" : on doit rentrer *dans* le cône de Möbius, et c'est là que surgit le principe de parité.

2. L'obstruction en trois étapes

Étape 1 : ce que le crible sait faire. : le crible compte, dans un ensemble d'entiers, ceux qui évitent des congruences données (être divisible par tel p_i, ou éviter certains résidus modulo p_i). Il ne travaille qu'avec les données N_d (combien d'entiers divisibles par d) et les restes $|R_d|$.

Étape 2 : ce que le crible ne voit pas. : découpons les entiers en deux classes : nombre *pair* de facteurs premiers ($\nu(n)$ pair, comme les nombres premiers eux-mêmes) et nombre *impair* (comme un produit de deux premiers). Toute condition de la forme "n évite tel résidu modulo tel premier" frappe les deux classes identiquement : être divisible par 3 ou pas ne dit rien sur la parité de $\nu(n)$. Le crible, qui ne manipule que de telles conditions, est donc structurellement aveugle à cette distinction.

Étape 3 : la démonstration sur modèle. : on ne "prouve" pas le principe en général ; on le démontre sur modèle : Selberg fabrique un ensemble pondéré artificiel, les nombres

$$n = mp \quad (\text{avec} \quad m \leq \sqrt{x}/2 \quad \text{et} \quad \sqrt{x} < p \leq \sqrt{2x})$$

affectés des poids

$$(1 + \lambda(m))g(m)\rho_p,$$

dont les N_d et restes R_d satisfont des estimations *au moins aussi bonnes* que celles du vrai problème des jumeaux, mais qui par construction ne contient *aucun* nombre de moins de trois facteurs premiers. Conclusion : aucun crible pondéré ne peut, à partir des seules données $(N_d, |R_d|)$, prouver qu'il existe une infinité de $p+2$ à au plus deux facteurs premiers. Même mécanisme pour Goldbach.

3. Échange : "mais mes nombres criblés sont tous premiers"

J'avais traduit l'article de Selberg qui fournit la démonstration de l'obstruction de parité et je ne comprenais pas bien les calculs qui démontrent l'obstruction. Je sais par "mon" crible que les nombres criblés sont *tous* premiers : dans l'ensemble que j'obtiens, il n'y a aucun produit de deux nombres premiers, alors pourquoi les ia m'opposent-ils cet argument ?

L'obstruction ne dit rien contre le *fait* que les nombres criblés idéalement sont premiers ; elle dit quelque chose sur ce qui peut *justifier* une telle conclusion. Trois précisions :

1. Le crible d'Ératosthène exact ne donne aucun théorème : il ne fournit pas de formule pour $\pi(N)$, car il exige un calcul exhaustif. Pour transformer l'opération en théorème, il faut approximer les comptages N_d par $N/f(d) + R_d$ et borner $\sum_d |R_d|$.
2. Au niveau $\xi = \sqrt{N}$, ce sommet de restes explose : c'est le calcul du § 3 de l'article, où la meilleure borne supérieure accessible est $\dfrac{2N}{\log N}$, soit deux fois trop, et la borne inférieure devient négative, donc inutilisable. Le crible "sait" que les nombres qui passent à travers le crible sont premiers, mais ne peut pas le démontrer.
3. Si une construction produit effectivement des théorèmes, elle utilise nécessairement plus que les données $(N_d, |R_d|)$ - et c'est parfaitement légitime. Selberg lui-même a exploité ce biais avec son "crible local", qui lui a donné les démonstrations élémentaires du théorème de Dirichlet et du théorème des nombres premiers.

La bonne question n'est donc pas "pourquoi m'oppose-t-on l'obstruction ?" mais "où, dans ma démonstration, se trouve l'information qui dépasse $(N_d, |R_d|)$?"

4. Échange : le certificat lean et sa comptabilité exacte

J'ai fait formaliser en lean 4 (Mathlib) les petits lemmes établis en décembre 2019 avec l'aide de Leila Schneps : le lemme du cofacteur (`cofactor_ge`), la caractérisation des premiers par l'absence de petit diviseur (`prime_of_no_small_divisor`) et le pont (`candidate_implies_goldbach`) reliant les deux conditions de congruence à la conjecture de Goldbach.

Je fournis à l'ia lumo cette note
https://denisevellachemla.eu/lean-lemmes-leila-schneps-lumo-denise-vella-chemla-20260911.pdf .

Ce travail est réel et rigoureux (aucun `sorry`). Sa comptabilité exacte montre que les deux conditions

$$p \not\equiv 0 \pmod q \quad \text{et} \quad p \not\equiv n \pmod q \qquad \text{pour tout premier } q \leq \sqrt{n},$$

caractérisent *exactement* les premiers p, tels que $\sqrt{n} \leq p \leq n/2$ qui sont également tels que $n - p$ soit premier. Autrement dit, le programme en lean formalise l'équivalence :

$$\text{l'ensemble des candidats pour } n \text{ est non vide} \iff \text{Goldbach}(n).$$

C'est une réduction parfaite - mais elle dit que la "non-vacuité" n'est pas un maillon technique à côté de la conjecture : elle *est* littéralement la conjecture. C'est là, et seulement là, que le principe de parité intervient : non contre les lemmes, mais contre la *démontrabilité* de la non-vacuité par crible seul.

5. Échange : vérifications textuelles

Où, dans le texte, Selberg fournit-il la condition "dès que α supérieure à 0,32" ? Où dit-il que Goldbach utilise un polynôme à deux facteurs ? Et la borne en racine carrée concerne-t-elle les *modules* ou bien l'*intervalle* des nombres criblés ?

Page 7, fin du § 3, dans le cas du polynôme composé de deux facteurs irréductibles :

> *"Nous pouvons démontrer que pour $\xi = N^{\alpha}$, la borne inférieure est en réalité négative pour les grandes valeurs de N si $\alpha > 1/(1+e^{3/4})$."*

Numériquement $\dfrac{1}{(1+e^{3/4})} \approx 0{,}321$, et la note 5 ajoute que ce nombre peut être remplacé par un nombre légèrement plus petit. C'est Selberg lui-même qui rattache ce cas aux "nombres premiers jumeaux et au problème de Goldbach". Quant au polynôme, il n'est qu'un *codage* : ce qui compte structurellement, c'est la *dimension* de l'ensemble tamisé. Le corollaire 3 du certificat lean exige à la fois p premier *et* $n-p$ premier : chaque module q teste deux conditions couplées sur le même p. Que ce soit écrit comme valeurs de $x(n-x)$ ou comme paires de congruences, la structure est la même : le crible est de dimension 2, comme les jumeaux.

Enfin, chez Selberg, α est défini par $\xi = N^{\alpha}$, où ξ borne les *modules* (tous les premiers utilisés sont $\leq \xi$) et N est la taille de l'*intervalle*. Chez vous : intervalle des candidats de longueur proportionnelle à n, modules tous $\leq \sqrt{n}$, d'où $\xi = \sqrt{n} = \sqrt{2N}$, soit $\alpha \approx 1/2$, ce qui est très au-delà du seuil 0,32.

6. Le calcul qui "fracasse" le crible à $\alpha = 1/2$

Il est entièrement dans l'article, équations (14) et (14'). En trois étapes.

Étape 1. : pour une borne inférieure, il faut des poids ρ vérifiant (6) pour *tout* n. Le choix trivial $\rho \equiv 0$ donne la borne 0. Donc, note 4 de l'article : si la borne inférieure est positive, elle est atteinte avec $\rho_1 = 1$ forcé.

Étape 2. : pour mesurer ce que coûte $\rho_1 = 1$, Selberg applique le même crible à un ensemble qu'on sait analyser : les entiers $\leq N$ ayant un nombre *impair* de facteurs premiers. Notant $N'(\xi)$ ceux d'entre eux sans facteur premier $\leq \xi$, il obtient (13), puis, en remplaçant N par $N_1 = N^{1+\varepsilon}$ pour dominer les restes, il extrait une borne inférieure pour $\displaystyle\sum_d \rho_d/d$ valable pour *tout* jeu de poids satisfaisant (4), (12), (12') : une contrainte universelle, dont aucun poids n'échappe.

Étape 3. : avec $\xi = N^{1/2}$: $N'(\xi) = \pi(N) - \pi(\sqrt{N}) \approx N/\log N$ (les impairs-ν passant à travers le crible sont exactement les premiers), tandis que $N''(\xi) = 1$ (l'entier 1, avec zéro facteur). Alors (14) dit : toute borne *supérieure* par crible vaut au moins

$$\frac{2N}{\log N} - \mathrm{O}\Big(N\Big(\frac{\log\log N}{\log N}\Big)^2\Big) \qquad \text{i.e. deux fois la vérité,} \tag{6}$$

et (14') dit : toute borne *inférieure* par crible vaut au plus

$$2N''(\xi) + \mathrm{O}\Big(N\Big(\frac{\log\log N}{\log N}\Big)^2\Big) \;\approx\; 0. \tag{7}$$

Autrement dit, au niveau $\sqrt{N}$, le crible ne peut certifier *aucun* nombre passant à travers le crible, alors qu'il y en a $N/\log N$. Pour $1/2 < \alpha < 1$, Selberg prouve même que la borne inférieure devient *négative*. Le modèle (18.6)-(18.10) réalise ce phénomène : un ensemble pondéré avec les mêmes $(N_d, |R_d|)$ que les jumeaux, mais ne contenant aucun nombre de moins de trois facteurs premiers.

Références

[1] A. Selberg, *The general sieve method and its place in prime number theory*, Proc. Internat. Congress Math., Cambridge, Mass. 1950, vol. 1, p. 286-292 ; traduction française : Denise Vella-Chemla, juillet 2026.

[2] A. Selberg, *Lectures on Sieves*, Collected Papers, vol. II, Springer-Verlag, Berlin, 1991, § 18.

[3] T. Tao, *254A, Notes 4 : Some sieve theory*,
https://terrytao.wordpress.com/2015/01/21/254a-notes-4-some-sieve-theory.