Analyse critique de deux notes sur le double crible : formalisation topos-théorique et obstruction de parité

Denise Vella-Chemla pilotant claude, septembre 2026

1. Objet et conclusion

Ce document reprend l'analyse de deux notes :

(A) la note sur les *anisotropies modulaires et la structure du site*
https://denisevellachemla.eu/aniso-lumo-dvc-20260919.pdf
(expériences numériques, de Denise Vella-Chemla pilotant l'ia lumo) ;

(B) la note sur le *double crible dans le topos annelé de Monique Hakim*
https://denisevellachemla.eu/topos-annele-lumo-chatgpt-dvc-20260919.pdf
(système projectif $\mathbb{Z}/q^k\mathbb{Z}$, involution $x \mapsto n - x$, comparaison de cinq pistes).

Notations. Pour n pair, $n \geq 6$: $I_n = [3, n/2] \cap \mathbb{Z}$, $R_n = \prod_{q \leq \sqrt{n}} \mathbb{F}_q$, $A_n = \prod_{q \leq \sqrt{n}} (\mathbb{F}_q \setminus \{0, \bar{n}\})$, $\rho_n : I_{nn}$ la réduction diagonale, et $C_n = I_n \times_{R_n} A_n$.

Conclusion. Rien dans cette formalisation ne contourne l'obstruction de parité. Le verdict du § 11 de la note (B) (aucune des cinq pistes ne fournit de théorème nouveau sans supposer la conjecture) est juste, et les raisons en sont exposées ci-dessous.

2. C_n est l'ensemble des candidats retenus par le crible d'Ératosthène

Proposition 1. *On a $C_n = \{p_n \ : \ q \nmid p(n-p)$ pour tout premier $q \leq \sqrt{n}\}$. Si $C_n \neq \varnothing$, alors n est somme de deux nombres premiers.*

Démonstration. Soit p_n. Comme $3 \leq p \leq n/2$ et que p n'a aucun facteur premier $\leq \sqrt{n}$, p est premier (un entier composé $\leq n$ a un facteur premier $\leq \sqrt{n}$). De même $n - p \in [n/2, n-3]$ n'a aucun facteur premier $\leq \sqrt{n}$ et est > 1 : il est premier. □

Remarque : l'implication est à sens unique : un premier $p \leq \sqrt{n}$ est exclu du crible (car $p \equiv 0 \pmod{p}$), même s'il fournit une décomposition.

Le produit fibré $I_n \times_{R_n} A_n$ est donc, comme ensemble, exactement l'ensemble des entiers non éliminés par le crible d'Ératosthène complet, en dimension 2, sur $p(n-p)$. Dans le site $\mathcal{P}_n$, il n'y a aucun morphisme entre premiers distincts : les q ne communiquent pas, et leur seul lien est I_n, qui vit dans la catégorie des ensembles. Le topos reformule le problème sans y ajouter d'information.

La situation est la même que pour les 16 règles du treillis : on recombine des données déjà connues.

3. Ce que la tour projective et l'involution n'apportent pas

La tour $\mathbb{Z}/q^k\mathbb{Z}$. La condition $q \nmid x(x-n)$ ne dépend que de x mod q. Les applications de transition $U_{q,k+1} \to U_{q,k}$ sont donc surjectives (chaque point a q relèvements).

C'est cela, et non la "stabilité par projection", qui rend la condition de Mittag-Leffler triviale (Lemme 4 de la note (B)). La limite projective n'est que l'image réciproque de la condition modulo q (Prop. 2), et le "$\forall k \geq 1$" de la Prop. 3 est redondant avec $k = 1$. La note reconnaît d'ailleurs (§ 11.3) que le crible vit dans un produit fini.

L'involution $\mathbb{Z}/2\mathbb{Z}$.

L'involution $p \mapsto n - p$ est la symétrie de $p(n-p)$, déjà présente dans le crible. Elle regroupe les candidats retenus en paires et divise les comptages par 2 ; elle ne change pas l'existence. Elle n'a aucun rapport avec la "parité" de Selberg, qui porte sur la parité du nombre de facteurs premiers d'un entier.

4. L'obstruction de parité

Les données dont dispose un crible sont des dénombrements de I_n dans des classes de résidus modulo d, avec des restes petits. Le problème de parité (Selberg) exprime que ces données ne permettent pas de distinguer les entiers ayant un nombre pair ou impair de facteurs premiers. Ici, un candidat retenu p donne un produit $p(n-p)$ de exactement deux nombres premiers, donc de parité paire ; un modèle fictif où tous les candidats retenus auraient une parité impaire est indiscernable du modèle réel sur ces seules données.

Quantitativement : dimension $\kappa = 2$, sifting jusqu'à $z = \sqrt{n}$, niveau de distribution D de l'ordre de n (restes $|R_d| \leq 2^{\omega(d)}$), donc

$$s = \frac{\log D}{\log z} \approx 2,$$

alors qu'un minorant positif en dimension 2 exige $s > \beta_2 \approx 4{,}27$ (crible bêta de Iwaniec ; valeur à vérifier dans [3]). C'est pourquoi le meilleur résultat obtenu par crible est le théorème de Chen (P_2, [2]).

Pour franchir la barrière, il faut une information non locale : estimations de sommes exponentielles et de formes bilinéaires (méthode du cercle, identités de type Vaughan), ou annulations sur des corrélations de la fonction de Liouville. Aucune des deux notes n'en fournit.

Limite de cette affirmation. On ne peut pas prouver qu'aucun cadre futur n'y parviendra ; on affirme seulement que toute preuve n'utilisant que la structure locale modulo q reste soumise à la barrière.

5. Hypothèses qui réintroduisent la conjecture

Transversalité (Déf. 5 et § 6.3 de la note (B)). Si l'on demande que les ouverts locaux U_q s'intersectent dans le produit, c'est vrai par le théorème chinois des restes, mais cela ne permet pas de conclure. Si l'on demande que l'intersection rencontre $\rho_n(I_n)$, c'est la conjecture elle-même. Le théorème Lean "via Mittag-Leffler" est donc soit non démontrable, soit circulaire.

Densité interne (piste 1).

Pour $n = 10^4$, on a $|I_n| = 4998$ alors que $|R_n| = 97\# \approx 2{,}3 \times 10^{36}$. L'image $\rho_n(I_n)$ est une partie infime de R_n. Son équirépartition vers A_n est exactement le contenu de la conjecture : le nombre attendu de candidats retenus est $|I_n|\,|A_n|/|R_n|$, et le démontrer est le problème.

6. Erreurs et points de rigueur

(1) **Lemme 8(2), note (B).** $\alpha_q(x) = \bar{n} - x$ n'est pas un (anti)automorphisme d'anneau. On a $\alpha_q(x + y) = \bar{n} - x - y$, qui diffère de $\alpha_q(x) + \alpha_q(y)$ sauf si $\bar{n} = 0$, et $\alpha_q(xy) = \bar{n} - xy$, qui diffère de $(\bar{n} - x)(\bar{n} - y)$. C'est une réflexion de l'ensemble $\mathbb{F}_q$. La suite (Prop. 10, Th. 12) n'en dépend pas.

(2) **Lemme 19, note (B).** L'argument "le seul point fixe possible est $0 \notin A_q$" ne vaut que pour $q \mid n$. Si q est impair et ne divise pas n, alors $\bar{n}/2 \neq 0$ est bien dans A_q. Ainsi α a un point fixe dans A_n si et seulement si aucun premier impair $q \leq \sqrt{n}$ ne divise n. Exemple : $n = 14$, $A_2 = \{1\}$, $A_3 = \{1\}$, et $(1, 1) \in A_{14}$ est fixe (c'est la classe de $n/2 = 7$). L'affirmation "aucune orbite fixe" et le facteur 2 exact sont donc faux en général.

(3) **§ 2.2, note (B).** Un cumul des éliminations supérieur à 240 % ne témoigne pas de "corrélations arithmétiques" : la somme des fractions éliminées dépasse 100 % même pour des conditions indépendantes. La quantité pertinente est $\prod_q (1 - f_q)$.

(4) **Expérience 2, note (A).** Retirer des premiers du crible ne peut qu'agrandir C_n (moins de conditions), jamais le vider : la question "faut-il tous les q pour garantir $C_n \neq \varnothing$?" va dans le mauvais sens de monotonie. Ce que l'on mesure probablement, c'est le nombre de q nécessaires pour éliminer tous les faux positifs, et la réponse (presque tous) traduit le fait élémentaire qu'il faut tous les premiers $\leq \sqrt{n}$ pour certifier la primalité jusqu'à n. De plus, un algorithme glouton fournit une borne supérieure sur la taille minimale, pas une preuve de minimalité. Le protocole exact n'est pas reconstituable d'après la note.

(5) **Expérience 1, note (A).** L'anisotropie est le facteur local $(q-1)/(q-2)$ de la série singulière de Hardy–Littlewood [1], que la note cite elle-même. Les chiffres sont cohérents : $2{,}54/2{,}04 \approx 1{,}25 \approx (4/3)/(16/15)$. Cela confirme un fait connu, sans le dépasser.

(6) **§ 5.2, note (A).** La colonne "Match ?" est vide. Pour $n = 102$ et $n = 1002$, le ratio (1,14 et 1,16) est loin de la correction (2,13 et 2,00). Le tableau ne soutient donc pas l'affirmation "70 à 80 % de la variance expliquée", et la colonne "Heuristique" (7,0 pour $n = 102$) n'est pas reconstituable.

7. Avis d'ensemble

L'apport réel de la note (B) est la clarification du problème et la formalisation de la symétrie ; le vocabulaire Mittag-Leffler et topos est surtout décoratif. La quatrième "prochaine étape" (arguments analytiques classiques) est la seule direction réaliste, ce qui rejoint la conclusion selon laquelle densité et spectralité se ramènent à la méthode du cercle.

Pour la partie Lean, `ZMod 2` et `Multiplicative (ZMod 2)` existent déjà dans Mathlib : il est préférable de les utiliser plutôt que de redéfinir le groupe avec des `sorry`.

Pour que les notes résistent à un lecteur extérieur, il est conseillé d'y ajouter un court paragraphe posant l'égalité "C_n = candidats retenus par le crible d'Ératosthène" et la barrière de parité, afin de ne pas attendre du topos ce qu'il ne peut pas donner.

Références

[1] G. H. Hardy, J. E. Littlewood, *Some problems of "Partitio numerorum"; III : On the expression of a number as a sum of primes*, Acta Mathematica 44 (1923).

[2] J.-R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica 16 (1973), 157–176.

[3] J. Friedlander, H. Iwaniec, *Opera de Cribro*, AMS Colloquium Publications 57, 2010.