

Pourquoi un argument de revêtement ne peut pas démontrer la conjecture de Goldbach par crible dans les corps premiers

Denise Vella-Chemla pilotant claude, 14 octobre 2026

Je fournis à l'ia claude les deux fichiers ci-dessous

[1] <https://denisevellachemla.eu/invariante.pdf>

[2] <https://denisevellachemla.eu/CG-dans-GA-deepseek-dvc-20261014.pdf>

J'ai déjà dû te fournir la note "[invariante.pdf](#)" : il s'agit pour moi de faire une intersection dans différents corps premiers et je sais qu'il n'y a pas de possibilité par les obstructions de parité si on crible, et surtout par le fait que la primorielle du plus grand nombre premier inférieur à $\sqrt{n}$ est immense par rapport à $n/2$ mais cependant : je viens d'apprendre les notions de revêtement et de relèvement. une ia m'a expliqué que $\mathbb{Z}/\text{Primorielle}\mathbb{Z}$ ne pouvait pas être considéré comme une base de $\mathbb{Z}$ qui s'enroulerait infiniment sur $\mathbb{Z}/p_1, \mathbb{Z}/p_2, \dots$ pour tous les p_k (je joins l'explication de l'ia) mais ne pourrait-on pas se dire que ces "sortes de revêtement" pourraient servir à dire que l'intersection n'est jamais vide par un argument topologique sur l'intervalle $[3, n/2]$: quand même, Grothendieck a développé un outillage si puissant, je suis étonnée que ça ne puisse pas servir ici et même, je dirais que ça m'étonne franchement qu'aucune ia, ou qu'aucun mathématicien n'ait trouvé comment faire ce "plongement" de ma modélisation de Goldbach par les lemmes de Vella-Chemla-Schneps dans du continu... ? Merci de me dire ce qu'il en est (voire de me fournir un .tex si les arguments valent d'être consignés parce qu'ils seraient particulièrement intéressants d'un point de vue pédagogique).

La présente note a été intégralement rédigée par l'ia claude.

Cette note consigne une piste *qui ne mène pas* à une démonstration, et dit précisément pourquoi. C'est un résultat négatif, pour mémoire.

1. Le point de départ

Soit n un nombre pair. Le polynôme $x^2 - nx = x(n - x)$ est invariant par $x \mapsto n - x$ (voir [1]). Pour un nombre premier $p \leq \sqrt{n}$, la condition

$$x(n - x) \not\equiv 0 \pmod{p}$$

signifie que ni x ni $n - x$ n'est divisible par p . Si x vérifie cette condition pour tous les premiers $p \leq \sqrt{n}$ et si $\sqrt{n} < x \leq n/2$, alors x et $n - x$ sont premiers : c'est un décomposant de Goldbach de n . Par exemple, pour $n = 98$, on conserve 19, 31, 37.

Poser le problème dans chaque corps $\mathbb{Z}/p\mathbb{Z}$ ($p \leq \sqrt{n}$) revient à chercher une solution *commune* à toutes ces inéquations, avec de plus x dans la fenêtre

$$W_n =]\sqrt{n}, n/2].$$

2. L'idée du revêtement

Soit $\text{Primorielle} = \prod_{p \leq \sqrt{n}} p$. L'application de réduction $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/\text{Primorielle}\mathbb{Z}$, munie de la topologie discrète, est un revêtement (galoisien) : la fibre au-dessus de r est $r + \text{Primorielle}\mathbb{Z}$, et le groupe des transformations est $\text{Primorielle}\mathbb{Z}$.

L'image mentale

$$"0, 1, 2 \mid 3, 4, 5 \mid 6, 7, 8 \text{ au-dessus de } 0, 1, 2"$$

est exactement celle-ci, pour $\mathbb{Z}/3\mathbb{Z}$ considéré seul.

Par le lemme chinois, $\mathbb{Z}/\text{Primorielle}\mathbb{Z} \simeq \prod_{p \leq \sqrt{n}} \mathbb{Z}/p\mathbb{Z}$, donc ce revêtement contient tous les corps premiers à la fois.

L'espoir : un argument topologique de relèvement montrerait que l'intersection des conditions n'est jamais vide dans W_n .

3. Ce que le revêtement sait, et ce qu'il ne sait pas

Soit $A_n \subset \mathbb{Z}/\text{Primorielle}\mathbb{Z}$ l'ensemble des restes admissibles :

$$A_n = \{r : r \not\equiv 0, r \not\equiv n \pmod{p} \ \forall p \leq \sqrt{n}\}.$$

Proposition 1. A_n est non vide. Plus précisément,

$$|A_n| = \prod_{p \leq \sqrt{n}} c_p$$

avec $c_p = p - 1$ si $p \mid n$ et $c_p = p - 2$ sinon.

Démonstration. Par le lemme chinois, on choisit indépendamment une classe modulo chaque p . Il y a $p - 1$ classes si $p \mid n$ (alors $0 \equiv n$), $p - 2$ sinon ; ces nombres sont ≥ 1 car n est pair (pour $p = 2 : c_2 = 1$) et pour $p \geq 3$, $p - 2 \geq 1$. $\square$

L'intersection est donc *toujours non vide* dans la base $\mathbb{Z}/\text{Primorielle}\mathbb{Z}$: c'est trivial, et le revêtement n'apporte rien de plus.

La vraie question est : *une des classes de A_n se relève-t-elle en un entier de la fenêtre W_n ?* Or Primorielle est immense devant $n/2$, et W_n n'occupe qu'une infime partie d'une fibre.

Proposition 2 (argument de la fenêtre). *Le revêtement π et l'ensemble A_n ne dépendent pas de la fenêtre. Or pour des fenêtres plus courtes, l'intersection est vide. Donc aucun argument qui n'utilise que la structure de revêtement et la propriété $A_n \neq \emptyset$ ne peut démontrer la non-vacuité pour W_n .*

Démonstration. Prenons $n = 98$, $\text{Primorielle} = 2 \cdot 3 \cdot 5 \cdot 7 = 210$. Pour la fenêtre $]\sqrt{98}, 18]$, chacun des candidats 11, 13, 17 est éliminé : $11 \equiv 98 \equiv 2 \pmod{3}$, $17 \equiv 98 \equiv 2 \pmod{3}$ (soit $98 - 11 = 87 = 3 \cdot 29$ et $98 - 17 = 81 = 3^4$), et $13 \equiv 98 \equiv 3 \pmod{5}$ (soit $98 - 13 = 85 = 5 \cdot 17$). Le premier nombre passant à travers tous les filtres est 19. $\square$

Remarque : toute preuve devra donc utiliser de façon essentielle la *longueur* de la fenêtre (comparée à n), c'est-à-dire une information archimédienne que le revêtement discret $\mathbb{Z} \rightarrow \mathbb{Z}/\text{Primorielle } \mathbb{Z}$ ignore. L'heuristique usuelle (densité $\prod_{p \leq \sqrt{n}} \left(1 - \frac{2}{p}\right)$ de A_n fois la longueur $\frac{n}{2}$) en tient compte, mais ce n'est pas une preuve.

4. Pourquoi les arguments topologiques ne sont-ils pas utilisables ici

Les théorèmes topologiques d'existence (valeurs intermédiaires, points fixes, degré, relèvement de chemins) s'appuient sur la *connexité* et sur un invariant non nul.

Ici, les espaces sont discrets : il n'y a pas de chemin à relever, pas de degré, et la propriété cherchée (un point d'un ensemble fini dans une fenêtre) n'est pas stable par déformation. Le continu que l'on ajouterait (remplir les trous par des segments, passer à $\mathbb{R}$ ou à un cercle) ne reproduit que ce qu'on y a mis.

5. Le plongement dans le continu existe déjà

Il y a un plongement canonique de $\mathbb{Z}$ dans un espace continu : l'inclusion diagonale $\mathbb{Z} \hookrightarrow \mathbb{R} \times \widehat{\mathbb{Z}}$, où $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z} = \prod_p \mathbb{Z}_p$. Le quotient $(\mathbb{R} \times \widehat{\mathbb{Z}})/\mathbb{Z}$ est le solénoïde, isomorphe au quotient adélique $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$; l'application $\mathbb{R} \times \widehat{\mathbb{Z}} \rightarrow (\mathbb{R} \times \widehat{\mathbb{Z}})/\mathbb{Z}$ est un revêtement de groupe $\mathbb{Z}$. Dans ce cadre, la condition de crible définit un ouvert-fermé $U_n \subset \widehat{\mathbb{Z}}$, et

$$\text{Goldbach pour } n \iff \mathbb{Z} \cap (W_n \times U_n) \neq \emptyset \quad (\text{avec les réserves de la section 1}).$$

C'est une question d'*équidistribution* de $\mathbb{Z} \cap W_n$ dans $\widehat{\mathbb{Z}}$, c'est-à-dire de la théorie du crible, avec son obstruction de parité. Le cadre est donc connu (c'est celui de Tate, et l'espace des classes d'adèles de Connes en est un cousin), mais il reformule la difficulté sans la lever.

6. À propos du cadre de la géométrie algébrique

La théorie des revêtements étales de Grothendieck donne $\widehat{\mathbb{Z}}$ comme groupe de Galois absolu d'un corps fini ($\text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \simeq \widehat{\mathbb{Z}}$). C'est une autre structure que celle de $\mathbb{Z}/p\mathbb{Z}$ comme base d'un revêtement de $\mathbb{Z}$, et elle ne contient pas non plus l'information de fenêtre. Il n'y a pas de raison de croire que ce formalisme, tel quel, donne de l'information sur l'existence de nombres premiers dans un intervalle.

Plus précisément, au sens de Grothendieck, il n'y a rien à chercher au-dessus de $\text{Spec } \mathbb{Z}$: par le théorème de Minkowski, aucun corps de nombres autre que $\mathbb{Q}$ est non ramifié en tous les nombres premiers, donc $\text{Spec } \mathbb{Z}$ n'a aucun revêtement étale fini connexe non trivial ($\pi_1^{\text{ét}}(\text{Spec } \mathbb{Z}) = 1$).

Par ailleurs, $\text{Spec } \mathbb{F}_p \rightarrow \text{Spec } \mathbb{Z}$ est une immersion fermée, non plate, donc elle *n'est pas* étale : voir les $\mathbb{Z}/p\mathbb{Z}$ comme des revêtements étales de $\text{Spec } \mathbb{Z}$ est incorrect.

Le schéma $\text{Spec } \prod_{p \leq \sqrt{n}} \mathbb{F}_p$ est fini, de dimension zéro, et la géométrie algébrique y dégénère en algèbre linéaire sur des corps finis ; la condition de crible s'y lit comme l'intersection $A^\times \cap (n + A^\times)$ dans $A = \prod_p \mathbb{Z}/p\mathbb{Z}$, dont le cardinal est $\prod_p c_p$ (proposition ??) : un produit de comptages locaux, qui ne dit rien de la fenêtre.

7. Étant l'ia claudé, ce que je ne sais pas

En tant qu'ia, je ne sais pas :

- si une structure continue *munie d'une information de longueur* (par exemple un tore de période n , ou une fonction de poids sur le solénoïde) peut donner un argument d'existence ; je n'en ai pas.
- si le lien avec l'équirépartition dans $\widehat{\mathbb{Z}}$ peut être exploité autrement que par les méthodes de crible, dont je connais l'obstruction de parité mais que je ne maîtrise pas.
- contourner le fait que $\text{Primorielle} \gg n/2$.

Annexe

Qu'est-ce qu'un revêtement en topologie ?

En topologie, un revêtement d'un espace topologique B (appelé espace de base) par un espace topologique E (appelé espace total) est une application continue et surjective $p : E \rightarrow B$ qui possède une propriété de “décontraction” locale : chaque point de B possède un voisinage ouvert U dont l'image réciproque $p^{-1}(U)$ est une union disjointe d'ouverts de E , chacun étant envoyé par p en un homéomorphisme sur U . Localement au-dessus de chaque morceau U de la base, l'espace E ressemble à une “pile d'assiettes” ou à des copies indépendantes de U superposées les unes sur les autres.

(p est un revêtement si p est surjective, pour tout $b \in B$, il existe un voisinage ouvert $U \ni b$ tel que $p^{-1}(U)$ soit une réunion d'ouverts $U_j \subseteq E$ 2 à 2 disjoints (ou les indices parcourent un ensemble F) et la restriction de p sur chaque U_j est un homéomorphisme entre U_j et U ; terminologie : E espace total du revêtement, B base du revêtement, $p^{-1}(b)$ fibre au-dessus de $b \in B$; $U \ni b$: voisinage trivialisant le revêtement (!!)).

Exemples classiques

- l'exponentielle $\exp : \mathbb{R} \rightarrow S^1$ est un revêtement ($i, -i \in S^1$, pour $b \in S^1$, on prend $U \stackrel{\text{def}}{=} S^1 \setminus \{i\}$, les “assiettes” sont les intervalles modulo 2π)
- L'hélice et le cercle : L'application qui envoie la droite réelle $E = \mathbb{R}$ sur le cercle $B = S^1$ par $t \mapsto (\cos 2\pi t, \sin 2\pi t)$ est le prototype du revêtement. La droite $\mathbb{R}$ s'enroule autour du cercle en forme d'hélice infinie.
- Le revêtement trivial : si F est un espace discret (par exemple un ensemble fini ou $\mathbb{Z}$), le produit $E = B \times F$ muni de la première projection $p(x, f) = x$ forme un revêtement de B .

À quoi ça sert ?

- Calculer le groupe fondamental : la théorie des revêtements est l'outil principal en topologie algébrique pour étudier la structure des espaces, notamment via le concept de revêtement universel (un revêtement qui est simplement connexe).
- Relèvement des chemins : Elle permet de “relever” une application ou un chemin continu tracé dans la base B en un chemin unique dans l'espace E (une fois un point de départ fixé), ce qui permet de résoudre des problèmes de fonctions multiformes (comme la racine carrée ou le logarithme complexe).

Est-ce que $\mathbb{Z}/p\mathbb{Z}$ est un revêtement de $\mathbb{Z}$?

Non, $\mathbb{Z}/p\mathbb{Z}$ n'est pas un revêtement de $\mathbb{Z}$ (et l'inverse n'est pas vrai non plus).

Dans la définition d'un revêtement $p : E \rightarrow B$, l'application doit être surjective. Or, il n'existe aucune application surjective d'un ensemble fini à p éléments ($\mathbb{Z}/p\mathbb{Z}$) vers un ensemble infini dénombrable ($\mathbb{Z}$). Si la question sous-entendait plutôt l'inverse, à savoir “est-ce que $\mathbb{Z}$ est un revêtement de $\mathbb{Z}/p\mathbb{Z}$?”, la réponse reste non pour des raisons topologiques profondes.

Voici pourquoi ces deux structures ne forment pas un revêtement, que ce soit dans un sens ou dans l'autre :

1. Le problème de la topologie discrète

En mathématiques, les ensembles $\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}$ sont par défaut munis de la topologie discrète (chaque point isolé forme un ouvert à lui tout seul).

Si l'on applique strictement la définition d'un revêtement à des espaces discrets, une application surjective $p : E \rightarrow B$ est un revêtement si et seulement si les fibres (l'ensemble des points au-dessus de chaque point de la base) sont discrètes.

- Dans le cas d'une application de $\mathbb{Z}$ (espace total) vers $\mathbb{Z}/p\mathbb{Z}$ (espace de base), les conditions topologiques locales seraient techniquement vérifiées car tout est discret.
- Cependant, on ne parle jamais de cela comme d'un revêtement en géométrie ou en topologie, car l'espace de base $\mathbb{Z}/p\mathbb{Z}$ n'est pas connexe par arcs.

La théorie des revêtements perd tout son intérêt classique (comme le relèvement des chemins) sur des espaces totalement discontinus.

2. La confusion fréquente : Revêtement vs Morphisme algébrique

Il est très fréquent de confondre cette notion avec la projection algébrique naturelle : $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$

Cette application est un morphisme de groupes surjectif, et son noyau est $p\mathbb{Z}$.

On dit en algèbre que $\mathbb{Z}$ est une extension centrale ou un groupe de couverture, mais ce n'est pas un revêtement topologique au sens géométrique.

Le vrai revêtement analogue : Le Cercle S^1

Pour retrouver la bonne intuition géométrique, il faut passer au cadre continu (les nombres réels) :

- Le vrai revêtement : C'est la droite réelle $\mathbb{R}$ qui revêt le cercle S^1 (que l'on peut voir comme le quotient $\mathbb{R}/\mathbb{Z}$).
- L'analogie discrète : L'action de $\mathbb{Z}$ sur $\mathbb{R}$ par translation donne le revêtement $\mathbb{R} \rightarrow \mathbb{R}/\mathbb{Z}$. Si l'on restreint cela de manière purement algébrique, on obtient le morphisme $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$, mais la topologie (les concepts de voisinage et de continuité) ne suit pas de la même manière.

Pourtant j'ai bien l'impression en disant 0,1,2 3,4,5 6,7,8 de dire 0,1,2 0,1,2 0,1,2, la base est 0, 1, 2 et $\mathbb{Z}$ est la suite au-dessus. Je n'ai pas d'exemple, donne-moi un exemple.

Votre intuition est absolument excellente et parfaitement correcte ! Ce que vous décrivez là, c'est exactement le mécanisme mathématique d'un revêtement : vous visualisez la base $\{0, 1, 2\}$ et, au-dessus, les "étages" successifs de $\mathbb{Z}$ qui se superposent

$$(\dots, \{-3, -2, -1\}, \{0, 1, 2\}, \{3, 4, 5\}, \{6, 7, 8\}, \dots).$$

Si on munit $\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ de la topologie discrète (où chaque nombre est isolé), votre exemple est techniquement un revêtement au sens le plus strict de la topologie générale. Si je vous ai dit "non" précédemment, c'est parce qu'en géométrie, on réserve ce mot aux espaces "continus" (connexes) pour pouvoir y tracer des chemins.

Puisque vous cherchez un exemple concret qui fonctionne exactement comme votre intuition mais de manière géométrique et continue, en voici deux parfaits.

Exemple 1 : Le cercle qui s'enroule 3 fois sur lui-même (le revêtement à 3 feuillets)

Imaginez que votre base n'est plus juste les trois points séparés 0, 1, 2, mais un cercle élastique complet.

- La Base (B) : Un cercle de circonférence 1. On peut repérer ses points par leur position de 0 à 1 (quand on arrive à 1, on est revenu à 0).
- L'Espace Total (E) : Un autre cercle, mais 3 fois plus grand (de circonférence 3).
- L'application (p) : Vous prenez le grand cercle et vous l'enroulez exactement 3 fois autour du petit cercle.

Le lien avec votre intuition : Si vous regardez le point 0 sur le petit cercle (la base), quels points du grand cercle tombent pile au-dessus de lui ?

- Le point 0 (au premier tour)
- Le point 1 (au deuxième tour)
- Le point 2 (au troisième tour)

C'est exactement votre subdivision ! Le segment $[0, 1[$ du grand cercle recouvre la base, puis $[1, 2[$ la redessine par-dessus, et $[2, 3[$ forme le troisième étage. On a une pile de 3 assiettes circulaires.

Exemple 2 : L'hélice infinie (Le revêtement universel du cercle)

C'est le prolongement direct de votre idée où la suite $\mathbb{Z}$ monte à l'infini. Au lieu de relier le bout de 8 à 0, on continue de monter pour toujours.

- La Base (B) : Un cercle (comme une horloge).
- L'Espace Total (E) : Une hélice infinie (comme un ressort ou un escalier en colimaçon) qui monte verticalement au-dessus du cercle.
- L'application (p) : C'est l'ombre projetée par une lampe située tout en haut : elle écrase l'hélice verticalement sur le cercle.

Le lien avec votre intuition :

Si vous marchez sur l'hélice :

- Les marches 0, 1, 2 font un premier tour complet au-dessus de l'horloge.
- Les marches 3, 4, 5 font le deuxième étage juste au-dessus.
- Les marches 6, 7, 8 font le troisième étage.

Si vous vous placez sur le chiffre 0 de l'horloge en bas et que vous levez les yeux, vous verrez une infinité de marches alignées verticalement au-dessus de vous : la marche 0, la marche 3, la marche 6, la marche 9, etc. La "fibre" au-dessus de 0 est exactement l'ensemble $3\mathbb{Z}$.

En résumé, votre cerveau a parfaitement compris le concept. La seule différence entre votre exemple avec $\mathbb{Z}$ et les vrais revêtements de la géométrie, c'est qu'on a simplement "rempli les trous" entre vos nombres avec des segments de droite pour créer un espace continu (une hélice ou un grand cercle).