

Autour de la conjecture de Goldbach : produit de corps finis et géométrie algébrique

Denise Vella-Chemla pilotant l'ia deepseek, 14 octobre 2026

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

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

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

Je lui demande quelle serait la traduction de cette façon de voir la conjecture de Goldbach dans le domaine de la géométrie algébrique de Grothendieck.

1. Le cadre initial : produit cartésien de corps finis

1.1. Notation $\prod$ et $\coprod$

Le symbole

$$\prod_{k=1}^K \mathbb{Z}/p_k\mathbb{Z}$$

désigne le *produit cartésien* (aussi appelé produit direct) des anneaux $\mathbb{Z}/p_1\mathbb{Z}, \dots, \mathbb{Z}/p_K\mathbb{Z}$. Concrètement, un élément de cet ensemble est un k -uplet

$$(m_1, m_2, \dots, m_K), \quad m_k \in \mathbb{Z}/p_k\mathbb{Z}.$$

La loi d'addition et la loi de multiplication se font composante par composante :

$$(m_1, \dots, m_K) + (m'_1, \dots, m'_K) = (m_1 + m'_1, \dots, m_K + m'_K),$$

et de même pour la multiplication. Muni de ces lois, l'ensemble $\prod_{k=1}^K \mathbb{Z}/p_k\mathbb{Z}$ est un anneau commutatif unitaire.

Il ne faut pas confondre le produit cartésien (représenté par le symbole $\prod$) avec la *réunion disjointe* représentée par le symbole $\coprod$, qui désigne . En théorie des schémas, on a l'identification

$$\mathrm{Spec} \left(\prod_{k=1}^K \mathbb{Z}/p_k\mathbb{Z} \right) \cong \prod_{k=1}^K \mathrm{Spec} (\mathbb{Z}/p_k\mathbb{Z}).$$

Autrement dit : le spectre d'un produit d'anneaux est la réunion disjointe des spectres.

C'est exactement ce qui apparaît dans le problème de la conjecture de Goldbach (on cherche dans chacun des $\mathbb{Z}/p_k\mathbb{Z}$ les nombres qui ne sont ni 0 ni n le nombre pair dont on cherche les décomposants de Goldbach).

1.2. Propriétés algébriques

L'anneau $A := \prod_{k=1}^K \mathbb{Z}/p_k\mathbb{Z}$ est :

- **fini** (de cardinal $\prod_{k=1}^K p_k$) ;
- **artinien** (tout anneau fini l'est) ;
- **réduit** (sans nilpotents non nuls), car chaque $\mathbb{Z}/p_k\mathbb{Z}$ est un corps ;
- **non intègre** dès que $K \geq 2$, car il possède des diviseurs de zéro : par exemple $(1, 0, \dots, 0) \cdot (0, 1, \dots, 0) = 0$.

Ce *n'est donc pas* un corps. C'est un produit de corps.

Par le théorème des restes chinois, si l'on note Primorielle $= \prod_{k=1}^K p_k$, on a un isomorphisme canonique

$$A \cong \mathbb{Z}/\text{Primorielle}\mathbb{Z}.$$

Ainsi, travailler dans $\prod_{k=1}^K \mathbb{Z}/p_k\mathbb{Z}$ revient à travailler modulo Primorielle, avec la décomposition en composantes premières.

1.3. Votre condition

Vous cherchez $m = (m_1, \dots, m_k) \in A$ tel que, pour chaque k ,

$$m_k \not\equiv 0 \pmod{p_k} \quad \text{et} \quad m_k \not\equiv n_k \pmod{p_k},$$

où $n = (n_1, \dots, n_k)$ est un élément fixé de A (chaque n_k est le résidu modulaire de n selon le module p_k).

En d'autres termes, m_k doit éviter deux valeurs dans $\mathbb{F}_{p_k}$, à savoir 0 et n_k . Cela équivaut à :

$$m \in A^\times \quad \text{et} \quad m - n \in A^\times,$$

où $A^\times = \prod_{k=1}^K (\mathbb{Z}/p_k\mathbb{Z})^\times$ désigne le groupe des unités de A .

2. Traduction géométrique : schéma fini étale

2.1. Le schéma associé

Posons

$$X = \text{Spec}(A) = \prod_{k=1}^K \text{Spec}(\mathbb{F}_{p_k}).$$

C'est un schéma de *dimension zéro* : chacun des $\text{Spec}(\mathbb{F}_{p_k})$ est un point fermé. Le schéma X est *fini* et *étale* sur $\text{Spec}(\mathbb{Z})$ (étale car chaque $\mathbb{F}_{p_k}$ est une extension finie séparable de $\mathbb{F}_{p_k}$ lui-même, et le morphisme structural est non ramifié).

Le faisceau structural $\mathcal{O}_X$ vérifie

$$\mathcal{O}_X(X) = A, \quad \mathcal{O}_X^\times(X) = A^\times.$$

2.2. Votre condition en langage de faisceaux

Considérons le morphisme de faisceaux

$$f_n : \mathcal{O}_X \rightarrow \mathcal{O}_X, \quad x \mapsto x - n.$$

Alors votre condition se réécrit :

$$m \in \mathcal{O}_X^\times(X) \quad \text{et} \quad f_n(m) \in \mathcal{O}_X^\times(X).$$

C'est une condition *ouverte* en chaque point : sur un schéma fini, un point est ouvert, donc “être non nul” et “être différent de n ” sont des conditions ouvertes triviales.

2.3. Riemann-Roch-Grothendieck et caractère de Chern

Sur un schéma de dimension zéro, ces outils dégénèrent :

- la cohomologie des faisceaux cohérents est concentrée en degré 0 :

$$H^i(X, \mathcal{F}) = 0 \quad \text{pour } i \geq 1.$$

Donc la caractéristique d'Euler $\chi(X, \mathcal{F}) = \sum_i (-1)^i \dim H^i(X, \mathcal{F})$ se réduit à $\dim H^0(X, \mathcal{F})$.

- le théorème de Riemann-Roch-Grothendieck, qui s'écrit

$$\text{ch}(f_! \mathcal{F}) \cdot \text{td}(T_f) = f_* (\text{ch}(\mathcal{F}) \cdot \text{td}(T_X)),$$

devient une égalité triviale de rangs.

- le groupe de Grothendieck $K_0(X)$ est isomorphe à $\mathbb{Z}^k$: un faisceau cohérent sur X est la donnée d'un $\mathbb{F}_{p^k}$ -espace vectoriel de dimension finie en chaque point k .
- le caractère de Chern ch envoie $K_0(X)$ dans $H^\bullet(X, \mathbb{Q})$, qui est concentré en degré 0 : c'est simplement l'application rang.

Remarque : la géométrie algébrique sur un schéma fini étale de dimension zéro est donc *équivalente* à de l'algèbre linéaire sur des corps finis. Elle ne peut pas, à elle seule, capturer un énoncé additif global comme Goldbach.

3. Piste plus judicieuse : intersection de sous-schémas dans $\mathbb{A}_{\mathbb{Z}}^2$

Cette section présente, à titre indicatif, la direction qui aurait le plus de sens pour attaquer Goldbach par la géométrie algébrique. Elle est volontairement esquissée : elle met en jeu des outils lourds (cohomologie ℓ -adique, motifs, fonctions L), difficiles à implémenter informatiquement, mais qui peut intéresser un lecteur mathématicien.

3.1. Reformulation de Goldbach

La conjecture de Goldbach affirme : tout entier pair $n \geq 4$ s'écrit $n = p + q$ avec p, q premiers.

Fixons n pair. On considère dans le plan affine $\mathbb{A}_{\mathbb{Z}}^2 = \text{Spec}(\mathbb{Z}[x, y])$ les sous-schémas suivants :

$$\begin{aligned} D_n : & \quad x + y = n, \\ P_x : & \quad x \text{ premier}, \\ P_y : & \quad y \text{ premier}. \end{aligned}$$

La conjecture équivaut à : pour tout n pair ≥ 4 ,

$$D_n \cap P_x \cap P_y \neq \emptyset \quad (\text{au sens des points entiers}).$$

L'intersection $D_n \cap P_x \cap P_y$ est un sous-schéma de $\mathbb{A}_{\mathbb{Z}}^2$, de dimension 0 attendue (une fois $x + y = n$ imposé, il ne reste qu'un paramètre entier x , et l'on demande que x et $n - x$ soient premiers).

3.2. Crible géométrique

L'idée du *crible géométrique* (Selberg, puis développements modernes) est de remplacer les conditions “ x premier” et “ $n - x$ premier” par des conditions de non-divisibilité modulo chaque petit premier ℓ , puis de passer à la limite. On obtient ainsi une famille de sous-schémas

$$D_n^{(\ell)} \subset \mathbb{A}_{\mathbb{F}_{\ell}}^2,$$

où l'on impose $x \not\equiv 0$ et $x \not\equiv n \pmod{\ell}$, et de même pour $y = n - x$. C'est exactement l'analogue de votre condition initiale, mais *simultanément pour tous les ℓ et dans un cadre géométrique de dimension 1* (la droite $x + y = n$).

Le point clé : au lieu de travailler dans le produit fini $\prod_{k \leq K} \mathbb{Z}/p_k \mathbb{Z}$, on travaille dans la droite projective $\mathbb{P}_{\mathbb{Z}}^1$, et l'on considère les fibres modulo ℓ de la famille D_n .

3.3. Faisceaux ℓ -adiques et caractères de Chern

Pour aller plus loin, on remplace $\mathbb{Z}$ par un corps de nombres K , et l'on considère des variétés sur K . On dispose alors de :

- la *cohomologie ℓ -adique* $H_{\text{ét}}^i(X_{\overline{K}}, \mathbb{Q}_{\ell})$, qui est un module galoisien ;
- les *caractères de Chern ℓ -adiques*

$$\text{ch} : K_0(X) \rightarrow \bigoplus_i H_{\text{ét}}^{2i}(X, \mathbb{Q}_{\ell}(i)),$$

qui relie K -théorie et cohomologie ;

- le *théorème de Riemann-Roch-Grothendieck* pour les variétés propres et lisses, qui donne

$$\text{ch}(f_! \mathcal{F}) \cdot \text{td}(T_f) = f_* \left(\text{ch}(\mathcal{F}) \cdot \text{td}(T_X) \right).$$

Dans le cas de la conjecture de Goldbach, on chercherait à évaluer une fonction L attachée à la variété $D_n \cap P_x \cap P_y$, et à montrer qu'elle ne s'annule pas en un point critique, ce qui forcerait l'existence de points entiers. C'est l'esprit des travaux sur les problèmes de Goldbach *tournés* (twisted) ou sur les *sommes de deux nombres premiers* étudiés via la géométrie arithmétique.

3.4. Pourquoi c’est “infernale”

Les difficultés sont multiples :

1. les sous-schémas P_x et P_y ne sont pas de type fini sur $\mathbb{Z}$ de manière raisonnable : l’ensemble des nombres premiers n’est pas l’ensemble des points d’un schéma de type fini.
2. il faut remplacer “premier” par des conditions de crible, ce qui introduit des poids et des fonctions de comptage.
3. la cohomologie ℓ -adique et les motifs sont des outils de théorie des nombres avancée, dont l’implémentation informatique est très lourde (par exemple via des bibliothèques de calcul de motifs, qui n’existent pas vraiment).
4. aucune preuve de Goldbach par cette voie n’est connue à ce jour ; les résultats partiels (Chen, Tao, etc.) utilisent plutôt l’analyse harmonique et la théorie analytique des nombres.

4. Conclusion

Votre cadre initial (produit de corps finis) est un schéma fini étale de dimension zéro. Les faisceaux naturels sont $\mathcal{O}_X$ et $\mathcal{O}_X^\times$, et les outils de Riemann-Roch-Grothendieck et de caractère de Chern y sont dégénérés. La géométrie algébrique ne transporte donc pas Goldbach dans ce cadre.

La piste la plus judicieuse consiste à considérer la droite $x+y=n$ dans $\mathbb{A}_{\mathbb{Z}}^2$ et à étudier l’intersection avec les conditions de primalité via un crible géométrique, puis à faire intervenir la cohomologie ℓ -adique et les caractères de Chern. Cette voie est puissante mais techniquement redoutable, et reste ouverte.

5. Reformulation en termes de schémas en groupes finis étales et de revêtements étales de $\mathrm{Spec} \mathbb{Z}$

5.1. Le point de vue “revêtement étale”

Un *revêtement étale fini* d’un schéma S est un morphisme

$$\pi : X \rightarrow S$$

qui est fini, plat, non ramifié, et localement de présentation finie. Sur $\mathrm{Spec} \mathbb{Z}$, les revêtements étales finis sont essentiellement classifiés par les algèbres finies étales sur $\mathbb{Z}$, c’est-à-dire les produits de corps de nombres (pour la partie générique) et de corps finis (pour la partie modulaire).

Dans votre cas, le schéma

$$X = \coprod_{k=1}^K \mathrm{Spec}(\mathbb{F}_{p_k})$$

est un revêtement étale fini de $\mathrm{Spec}(\mathbb{Z})$: le morphisme structural envoie chaque point fermé (p_k) sur le point fermé (p_k) de $\mathrm{Spec}(\mathbb{Z})$. C’est un revêtement *constant* de degré K , mais avec des fibres de tailles variables selon le point de base.

Plus précisément, au-dessus du point générique (0) , la fibre est vide ; au-dessus de (p_k) , la fibre est $\text{Spec}(\mathbb{F}_{p_k})$; au-dessus de tout autre point premier $\ell \neq p_1, \dots, p_K$, la fibre est vide. Ce n'est donc pas un revêtement au sens topologique habituel, mais cela reste un morphisme étale fini.

5.2. Structure de schéma en groupes

L'anneau $A = \prod_{k=1}^K \mathbb{Z}/p_k\mathbb{Z}$ est muni d'une structure naturelle de *schéma en groupes fini étale* sur $\text{Spec}(\mathbb{Z})$:

- la multiplication $A \times A \rightarrow A$ composante par composante,
- l'unité $1_A = (1, \dots, 1)$,
- l'inverse, qui n'est défini que sur le sous-schéma ouvert $A^\times = \prod_k (\mathbb{Z}/p_k\mathbb{Z})^\times$.

En toute rigueur, A est un *schéma en anneaux*, et $A^\times$ est le *schéma en groupes* des unités. Le groupe $A^\times$ est un groupe abélien fini étale, isomorphe à

$$A^\times \cong \prod_{k=1}^K \mathbb{F}_{p_k}^\times \cong \prod_{k=1}^K \mathbb{Z}/(p_k - 1)\mathbb{Z}.$$

C'est un groupe cyclique par composante, donc un produit de groupes cycliques d'ordres $p_k - 1$.

5.3. Votre condition comme section d'un toreur

Soit $n \in A$ fixé. Considérons le *torseur* (espace principal homogène) sous $A^\times$ défini par le translaté

$$T_n = n + A^\times \subset A.$$

Un élément $m \in A$ appartient à T_n si et seulement si $m - n \in A^\times$. Votre condition initiale, à savoir

$$m \in A^\times \quad \text{et} \quad m - n \in A^\times,$$

se réécrit donc :

$$m \in A^\times \cap T_n.$$

C'est l'intersection de deux ouverts de A : le groupe des unités $A^\times$ et le toreur translaté $T_n = n + A^\times$.

Géométriquement, c'est l'intersection de deux revêtements étales de $\text{Spec}(\mathbb{Z})$, ou plus exactement de deux ouverts du schéma en anneaux A .

5.4. Faisceaux associés

Sur le schéma en groupes $A^\times$, on peut considérer :

- le faisceau structural $\mathcal{O}_{A^\times}$;
- le faisceau des caractères $\widehat{A^\times} = \text{Hom}(A^\times, \mathbb{G}_m)$, qui est un faisceau localement constant de groupes finis ;
- le faisceau ℓ -adique $A^\times \otimes \mathbb{Q}_\ell$, qui est une représentation du groupe de Galois $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

La condition $m \in A^\times \cap (n + A^\times)$ se lit alors comme l'existence d'une section globale du faisceau $\mathcal{O}_{A^\times} \cap (n + \mathcal{O}_{A^\times})$.

5.5. Pourquoi cela reste de la “combinatoire déguisée”

Malgré le vocabulaire géométrique, tout se réduit à des calculs sur des groupes finis :

1. $A^\times$ est un produit de groupes cycliques $\prod_k \mathbb{Z}/(p_k - 1)\mathbb{Z}$.
2. Le tore $T_n = n + A^\times$ est un translaté de ce groupe.
3. L'intersection $A^\times \cap T_n$ se calcule composante par composante : en chaque k , il faut que $m_k \neq 0$ et $m_k \neq n_k$ dans $\mathbb{F}_{p_k}^\times$.
4. Le nombre d'éléments de cette intersection est

$$\#(A^\times \cap (n + A^\times)) = \prod_{k=1}^K \#(\mathbb{F}_{p_k}^\times \cap (n_k + \mathbb{F}_{p_k}^\times)),$$

et chaque facteur vaut $p_k - 2$ si $n_k \neq 0$, et $p_k - 1$ si $n_k = 0$.

Autrement dit, la “géométrie” se réduit à un produit de comptages locaux. C'est exactement ce que j'entendais par “combinatoire déguisée” : le langage des schémas en groupes finis étales et des revêtements étales est correct et élégant, mais il ne fournit aucun outil nouveau pour attaquer Goldbach, car la dimension zéro détruit toute cohomologie intéressante.

5.6. Ce que cela apporte malgré tout

Cette reformulation a un intérêt pédagogique et structurel :

- elle montre que votre condition est *intrinsèquement locale* ;
- elle identifie le bon objet : le groupe $A^\times$ et ses toseurs, qui sont les analogues finis des groupes algébriques $\mathbb{G}_m$ et de leurs toseurs ;
- elle prépare le terrain pour une généralisation : remplacer $\prod_k \mathbb{Z}/p_k\mathbb{Z}$ par un schéma en groupes fini étale sur une base plus riche, par exemple un anneau de nombres, où la cohomologie ℓ -adique devient non triviale ;
- elle relie votre question aux *caractères de Dirichlet modulo* Primorielle $= \prod_k p_k$, puisque $A^\times \cong (\mathbb{Z}/\text{Primorielle}\mathbb{Z})^\times$ et le tore T_n correspond à une classe de caractères.

En résumé : la reformulation en schémas en groupes finis étales et revêtements étales de $\text{Spec}(\mathbb{Z})$ est *correcte* et *conceptuellement éclairante*, mais elle reste, dans votre cadre précis, une reformulation combinatoire sans intérêt pour l'objectif qui reste la démonstration de la conjecture de Goldbach .