

Décomposants de Goldbach comme unités modulaires

d'après les notes de Denise Vella-Chemla (février–mars 2022)

Résumé

On formalise ici le contenu de deux notes [1] et [2] consacrées à une caractérisation des décomposants de Goldbach via la théorie de Gauss des résidus de puissances (section 92 des *Recherches arithmétiques*). L'observation de départ est correcte : tout décomposant p de Goldbach de n , étant premier au produit Prod des nombres premiers $\leq \sqrt{n}$, vérifie une équation modulaire d'ordre $\lambda(\text{Prod})$ (l'exposant de Carmichael, plus fin que l'indicatrice d'Euler, comme l'explique précisément Gauss). On montre que cette condition, bien que vraie, est strictement nécessaire et non suffisante : elle est satisfaite par *tout* entier premier à Prod, qu'il soit lui-même premier ou non, et qu'il soit ou non un décomposant de Goldbach. La tentative de resserrement *ad hoc* proposée en fin de première note (une condition de divisibilité par 6 d'un pgcd) est infirmée par un contre-exemple numérique simple. On explique enfin pourquoi l'espoir, formulé dans la seconde note, que le théorème de Chebotarev puisse garantir l'existence d'une solution *petite* ($\leq n/2$) à l'équation modulaire ne peut être satisfait : l'équation en question n'isole pas un petit nombre fini de racines liées par un groupe de Galois commun, mais l'ensemble entier des $\varphi(\text{Prod})$ unités modulo Prod — et décider laquelle de ces unités est premier est, reformulé, le problème de Goldbach lui-même.

1 Le cadre : décomposants de Goldbach comme unités

Définition 1 Soit n pair, $n \geq 6$. On note

$$\text{Prod} = \text{Prod}(n) := \prod_{\substack{p_k \text{ premier} \\ p_k \leq \sqrt{n}}} p_k.$$

Constat 1 (Constat de départ, correct) Si p est un décomposant de Goldbach de n (donc p et $n - p$ premiers, $3 \leq p \leq n/2$), alors p et $n - p$ sont tous deux premiers à $\text{Prod}(n)$: aucun facteur premier $\leq \sqrt{n}$ ne peut diviser p ou $n - p$, ces deux nombres étant eux-mêmes premiers et $> \sqrt{n}$ dès que n est assez grand. Par le théorème d'Euler,

$$p^{\varphi(\text{Prod})} \equiv 1 \pmod{\text{Prod}}, \quad (n - p)^{\varphi(\text{Prod})} \equiv 1 \pmod{\text{Prod}}.$$

1.1 Le raffinement de Gauss : l'exposant de Carmichael

La section 92 des *Recherches arithmétiques* précise cet exposant. Pour $m = A^\alpha B^\beta C^\gamma \dots$ (factorisation en nombres premiers distincts A, B, C, \dots), Gauss pose $\alpha' = A^{\alpha-1}(A - 1)$, etc., et montre que pour tout z premier à m ,

$$z^{\alpha'} \equiv 1 \pmod{A^\alpha}, \quad z^{\beta'} \equiv 1 \pmod{B^\beta}, \quad \dots$$

de sorte que, en posant $\mu = \text{ppcm}\{\alpha', \beta', \gamma', \dots\}$, on obtient $z^\mu \equiv 1 \pmod{m}$ pour tout z premier à m — et Gauss observe que μ (l'exposant que l'on nomme aujourd'hui $\lambda(m)$, exposant de Carmichael) est en général *strictement inférieur* à $\varphi(m) = \alpha'\beta'\gamma'\dots$, sauf lorsque m est un nombre premier, une puissance de nombre premier, ou le double de l'un de ceux-ci.

Constat 2 (Exemple de Gauss) *Pour $m = 1001 = 7 \cdot 11 \cdot 13$: $\varphi(7) = 6$, $\varphi(11) = 10$, $\varphi(13) = 12$, et $\lambda(1001) = \text{ppcm}(6, 10, 12) = 60 < \varphi(1001) = 720$.*

Lorsque $\text{Prod}(n)$ est un produit de nombres premiers *simples* (chacun à la puissance 1), on a $\alpha' = p_k - 1$ pour chaque facteur p_k , d'où

$$\lambda(\text{Prod}) = \text{ppcm}\{p_k - 1 : p_k \text{ premier} \leq \sqrt{n}\} \quad \Bigg| \quad \varphi(\text{Prod}) = \prod_{p_k \leq \sqrt{n}} (p_k - 1),$$

la divisibilité provenant de l'inclusion des facteurs premiers de chaque $p_k - 1$ dans l'union de tous les facteurs premiers de tous les $p_k - 1$ — observation déjà formulée par Laisant en termes ensemblistes, et reprise dans la première note.

Proposition 1 (Forme raffinée du Constat 1) *Si p est un décomposant de Goldbach de n , alors*

$$p^{\lambda(\text{Prod})} \equiv 1 \pmod{\text{Prod}}, \quad (n - p)^{\lambda(\text{Prod})} \equiv 1 \pmod{\text{Prod}}.$$

2 Pourquoi cette condition ne caractérise pas les décomposants

Remarque 1 (La limite, identifiée par l'auteure elle-même) *La première note relève explicitement le problème : la condition ci-dessus, telle qu'énoncée, devrait faire de tout nombre premier à Prod un décomposant de Goldbach — ce qui est manifestement faux (la grande majorité des nombres premiers à 98, par exemple, ne sont pas des décomposants de Goldbach de 98). La raison est immédiate : la congruence $z^{\lambda(\text{Prod})} \equiv 1 \pmod{\text{Prod}}$ est satisfaite par toute unité z modulo Prod , qu'elle soit ou non elle-même premier, et que son complémentaire à n soit ou non premier. C'est une conséquence nécessaire d'être premier à Prod , non une condition suffisante d'être un décomposant de Goldbach, ni même d'être premier tout court.*

2.1 Le patch numérique de la fin de la première note, et son contre-exemple

La première note propose, sur la base des trois décomposants de Goldbach de 98 (19, 31, 37), la condition empirique suivante : pour p décomposant de Goldbach de n ,

$$6 \Bigg| \text{gcd}(\lambda(\text{Prod}), p - 1, (n - p) - 1).$$

Elle est vérifiée pour $n = 98$ ($\lambda(\text{Prod}) = 12$ puisque $\sqrt{98} < \sqrt{100} = 10$, $\text{Prod} = 2 \cdot 3 \cdot 5 \cdot 7$) : les trois pgcd valent 6, 6, 12, tous multiples de 6, tandis que pour 17 (non-décomposant), le pgcd vaut 4.

Contre-exemple 1 Pour $n = 100$ (même $\text{Prod} = 210$, même $\lambda(\text{Prod}) = 12$), les six décomposants de Goldbach sont 3, 11, 17, 29, 41, 47 (avec 97, 89, 83, 71, 59, 53). Pour chacun, $\text{gcd}(12, p-1, n-p-1) = 2$: la condition de divisibilité par 6 **échoue pour tous les décomposants de 100**.

Pour $n = 110$ ($\text{Prod} = 210$, $\lambda(\text{Prod}) = 12$ toujours), le décomposant $p = 3$ donne $\text{gcd}(12, 2, 106) = 2$, non multiple de 6, alors même que les cinq autres décomposants de 110 vérifient la condition.

Remarque 2 Le contre-exemple est instructif au-delà du simple échec numérique : pour $n = 100$, c'est $p = 3$ qui casse systématiquement le motif, car $p-1 = 2$ est de 2-valuation maximale triviale et ne peut contribuer le facteur 3 nécessaire à la divisibilité par 6. Le motif observé sur 98 tenait à un accident arithmétique propre à cet exemple (l'absence, parmi ses décomposants, d'un cas comme $p = 3$), non à une régularité générale. C'est un avertissement classique en théorie des nombres expérimentale : un motif vérifié sur un seul n , même « joli », requiert systématiquement un test sur une famille de n avant d'être retenu comme piste sérieuse.

3 L'espoir d'un recours à Chebotarev, et pourquoi il ne peut suffire

La seconde note reformule la condition comme une équation modulaire unique,

$$(n-p)^{\varphi(\text{Prod})} \equiv 1 \pmod{\text{Prod}},$$

observe — à bon droit — que le théorème de Gauss garantit l'existence d'au moins une solution $< \text{Prod}$ (en fait, l'existence de $\varphi(\text{Prod})$ solutions, toutes les unités modulo Prod), et formule l'espoir que le *théorème de densité de Chebotarev* puisse garantir qu'une de ces solutions est *petite*, au sens $p \leq n/2$.

Constat 3 (Pourquoi Chebotarev ne s'applique pas ici) *Le théorème de Chebotarev répartit, pour une équation algébrique fixe $f(X) = 0$ à coefficients entiers et de groupe de Galois G connu, les nombres premiers ℓ selon le type de cycle de la factorisation de f modulo ℓ — la densité de chaque type étant la proportion d'éléments de G ayant ce type de cycle (cf. la note sur la conférence d'Alain Connes où ce mécanisme est détaillé¹.. Or l'équation $X^{\varphi(\text{Prod})} \equiv 1 \pmod{\text{Prod}}$ n'est pas une équation algébrique fixe dont on chercherait la réduction modulo des nombres premiers variables : c'est, pour un module Prod fixé, l'ensemble de toutes les unités $(\mathbb{Z}/\text{Prod}\mathbb{Z})^\times$ — un groupe entier de cardinal $\varphi(\text{Prod})$, non un ensemble fini de racines indexées par un groupe de Galois. Il n'y a ici ni équation algébrique unique à factoriser, ni paramètre premier ℓ variable : la structure requise par Chebotarev est absente.*

Remarque 3 (Ce que demande réellement la question, une fois reformulée) *Une fois admis que toute unité modulo Prod vérifie l'équation, la question « existe-t-il une solution $p \leq n/2$ » devient triviale au sens brut : il y a $\varphi(\text{Prod}) \sim \text{Prod} \cdot \prod_{p_k \leq \sqrt{n}} (1 - 1/p_k)$ solutions réparties dans $[1, \text{Prod}]$, et $\text{Prod} \gg n/2$ dès que n est modérément grand (le produit des premiers jusqu'à \sqrt{n} croît, par le théorème des nombres premiers, comme $e^{\sqrt{n}}$, bien plus vite que n) — donc une infinité de solutions tombent mécaniquement dans $[1, n/2]$. La vraie question n'est donc jamais « une petite solution existe-t-elle » (oui, banalement), mais « l'une de ces solutions est-elle elle-même un nombre*

1. Voir <https://denisevellachemla.eu/transc-Alain-Connes-Academie-2011-Galois.pdf>, page 15 à 23.

premier p tel que $n - p$ soit également premier » — ce qui est, mot pour mot, sans rien ajouté ni perdu, la conjecture de Goldbach elle-même. Le détour par les unités modulo Prod a reformulé le problème sans le simplifier : aucune information supplémentaire sur la primalité n'a été injectée par le passage aux congruences.

Conclusion

Les deux notes développent, avec une lecture fidèle et soignée de Gauss, une condition nécessaire correcte (et même raffinée via l'exposant de Carmichael) pour qu'un nombre soit premier à $\text{Prod}(n)$. Mais cette condition, par construction, ne distingue pas les nombres premiers des nombres composés premiers à Prod — c'est la même obstruction de fond déjà rencontrée dans les approches précédentes par crible ou par résidus modulaires : une condition portant sur les classes résiduelles modulo de petits nombres ne peut capturer une propriété (la primalité) qui dépend de la valeur entière dans son ensemble. La tentative de resserrement empirique (pgcd multiple de 6) ne résiste pas à un second exemple ; l'espoir d'un recours à Chebotarev se heurte à l'absence, dans cette construction, de la structure (équation algébrique fixe, groupe de Galois associé) que ce théorème requiert pour s'appliquer.

Notes bibliographiques

- D. Vella-Chemla, *Unités racines de certaines équations*, 23 février 2022.
<https://denisevellachemla.eu/rechenarithm.pdf>.
- D. Vella-Chemla, *Racines de certaines équations modulaires*, 1 mars 2022.
<https://denisevellachemla.eu/preciserechenarithm.pdf>.
- C. F. Gauss, *Recherches arithmétiques*, section 92 (trad. française).