

Analyse critique de l'approche par automorphismes intérieurs pour la conjecture de Goldbach

Denise Vella-Chemla pilotant gemini, juillet 2026

1. Introduction

Ce document analyse une approche originale de la conjecture de Goldbach utilisant des **automorphismes intérieurs** sur des ensembles de décompositions additives. Cette méthode, développée par Denise Vella-Chemla, aurait souhaité s'inspirer de la preuve élégante de Don Zagier pour le théorème des deux carrés.

“On revient à une note de 2018 <https://denisevellachemla.eu/palindromes.pdf>, dans laquelle intervenait un automorphisme intérieur dont on avait vu qu'il permettait de distinguer les nombres impairs des nombres pairs. Il permettait également de distinguer les nombres premiers des nombres composés.”

Notre analyse montre que cette construction est **mathématiquement valide et intéressante**, mais qu'elle **ne prouve pas** la conjecture de Goldbach dans son état actuel. Nous expliquons pourquoi, tout en identifiant les pistes prometteuses.

2. Construction mathématique

2.1. Définitions fondamentales

Définition 1 (Ensemble des décompositions). Soit n un entier pair ≥ 6 . On définit l'ensemble :

$$E_n = \left\{ a + b \mid a \text{ impair}, b \text{ impair}, a \in \mathcal{P}, 3 \leq a \leq \frac{n}{2}, 6 \leq a + b \leq n \right\}$$

où \mathcal{P} désigne l'ensemble des nombres premiers.

Remarque 2. L'ensemble E_n contient toutes les décompositions de n en somme de deux nombres impairs, où le premier terme a est un nombre premier impair compris entre 3 et $n/2$. Le second terme $b = n - a$ est impair (car n est pair et a est impair), mais **pas nécessairement premier**.

Définition 3 (Automorphisme intérieur). On définit l'application $f_n : E_n \rightarrow E_n$ par :

$$f_n(a + b_1) = a + b_2 \quad \text{si et seulement si} \quad b_1 + b_2 = n$$

Remarque 4. Cette définition est bien posée car :

- Si $a + b_1 \in E_n$, alors $b_1 = n - a$ est impair et $6 \leq a + b_1 \leq n$.
- On pose $b_2 = n - b_1 = a$, donc $a + b_2 = a + a = 2a$.
- Comme $3 \leq a \leq n/2$, on a $6 \leq 2a \leq n$, donc $a + b_2 \in E_n$.

2.2. Propriétés de l'automorphisme f_n

Lemme 5 (f_n est une involution). *L'application f_n est une **involution**, c'est-à-dire que $f_n \circ f_n = Id$.*

Démonstration. Soit $x = a + b_1 \in E_n$. Alors $f_n(x) = a + b_2$ où $b_2 = n - b_1$.
Appliquons f_n une seconde fois :

$$\begin{aligned} f_n(f_n(x)) &= f_n(a + b_2) = a + b_3 \quad \text{avec} \quad b_2 + b_3 = n \\ &= a + b_3 \quad \text{où} \quad b_3 = n - b_2 = n - (n - b_1) = b_1 \\ &= a + b_1 = x \end{aligned}$$

Donc $f_n(f_n(x)) = x$ pour tout $x \in E_n$. □

Lemme 6 (Caractérisation des points fixes). *Les points fixes de f_n sont exactement les éléments de la forme $a + \frac{n}{2}$ où :*

- n est de la forme $4k + 2$ (donc $n/2$ est impair),
- a est un nombre premier impair tel que $3 \leq a \leq \frac{n}{2}$.

Démonstration. Un point fixe satisfait $f_n(a + b) = a + b$. Par définition de f_n , cela implique :

$$\begin{aligned} a + b &= a + b_2 \quad \text{avec} \quad b + b_2 = n \\ \Rightarrow b &= b_2 = n - b \\ \Rightarrow 2b &= n \\ \Rightarrow b &= \frac{n}{2} \end{aligned}$$

Donc n doit être pair (ce qui est le cas) et $b = n/2$ doit être impair (car $b \in E_n$ implique b impair).
Donc $n = 2 \times \text{impair} = 4k + 2$.

De plus, a doit être un nombre premier impair avec $3 \leq a \leq n/2$. □

Corollaire 7. *Le nombre de points fixes de f_n est :*

$$\begin{cases} 0 & \text{si } n = 4k \\ \pi_{\text{impair}}\left(\frac{n}{2}\right) & \text{si } n = 4k + 2 \end{cases}$$

où $\pi_{\text{impair}}(x)$ désigne le nombre de nombres premiers impairs $\leq x$.

Démonstration. Directement issu du Lemme 5.

- Si $n = 4k$, alors $n/2 = 2k$ est pair, donc il n'existe pas de $b = n/2$ impair. Donc 0 point fixe.
- Si $n = 4k + 2$, alors $n/2 = 2k + 1$ est impair. Les points fixes sont les $a + (2k + 1)$ où a est premier impair $\leq 2k + 1$. Le nombre de tels a est exactement $\pi_{\text{impair}}(2k + 1) = \pi_{\text{impair}}(n/2)$. □

Pour $n = 22 = 4 \times 5 + 2$, on a $n/2 = 11$ (impair).

Les points fixes de f_{22} sont les décompositions $a + 11$ où a est premier impair ≤ 11 :

- $3 + 11$ (car 3 est premier impair ≤ 11)
- $5 + 11$ (car 5 est premier impair ≤ 11)
- $7 + 11$ (car 7 est premier impair ≤ 11)
- $11 + 11$ (car 11 est premier impair ≤ 11)

Donc 4 points fixes, ce qui correspond à $\pi_{\text{impair}}(11) = 4$ (les premiers impairs ≤ 11 sont 3, 5, 7, 11).

3. Analyse des résultats numériques

3.1. Observations empiriques

Le programme Python fourni dans le document produit les résultats suivants pour $6 \leq n \leq 102$:

| n | Forme de n | Nombre de points fixes | $\pi_{\text{impair}}(n/2)$ |
|-----|------------------|------------------------|-------------------------------|
| 6 | $4 \times 1 + 2$ | 1 | $\pi_{\text{impair}}(3) = 1$ |
| 8 | 4×2 | 0 | - |
| 10 | $4 \times 2 + 2$ | 2 | $\pi_{\text{impair}}(5) = 2$ |
| 12 | 4×3 | 0 | - |
| 14 | $4 \times 3 + 2$ | 3 | $\pi_{\text{impair}}(7) = 3$ |
| 16 | 4×4 | 0 | - |
| 18 | $4 \times 4 + 2$ | 3 | $\pi_{\text{impair}}(9) = 3$ |
| 20 | 4×5 | 0 | - |
| 22 | $4 \times 5 + 2$ | 4 | $\pi_{\text{impair}}(11) = 4$ |
| 24 | 4×6 | 0 | - |
| 26 | $4 \times 6 + 2$ | 5 | $\pi_{\text{impair}}(13) = 5$ |

Ces résultats **confirment parfaitement** le Corollaire 7.

3.2. Propriétés supplémentaires observées

Le document affirme que :

“le résultat [de la fonction autom] augmente strictement à chaque nombre double d’un nombre premier”.

Cela signifie que pour $n = 2p$ où p est premier, le nombre de points fixes de f_n augmente strictement avec p .

Remarque 8. *Cette propriété est vraie car :*

- Si $n = 2p$ avec p premier, alors $n = 4k + 2$ si et seulement si p est impair (ce qui est toujours vrai pour $p \geq 3$).
- Le nombre de points fixes est $\pi_{\text{impair}}(p)$.
- Comme p est premier impair, $\pi_{\text{impair}}(p)$ augmente strictement avec p (car p est lui-même compté dans $\pi_{\text{impair}}(p)$).

4. Comparaison avec la preuve de Zagier

4.1. La preuve de Zagier (1990)

Don Zagier a démontré en une phrase que tout nombre premier $p \equiv 1 \pmod{4}$ est somme de deux carrés d’entiers [?]. Sa preuve utilise :

Théorème 9 (Zagier, 1990). *Soit $p \equiv 1 \pmod{4}$ un nombre premier. Considérons l’ensemble $S = \{(a, b, c) \in \mathbb{N}^3 \mid a^2 + 4bc = p\}$ et l’involution $(a, b, c) \mapsto (a, b', c')$ définie par :*

- Si $a < b - c$, alors $b' = b - a$, $c' = c$.
- Si $a > b - c$, alors $b' = b + a$, $c' = c$.
- Si $a = b - c$, alors $b' = b$, $c' = c$ (point fixe).

Alors $|S|$ est impair, donc il existe au moins un point fixe, qui correspond à une solution de $p = a^2 + b^2$.

Remarque 10. La clé de la preuve de Zagier est :

- Construire un ensemble fini S dont les éléments correspondent aux solutions potentielles.
- Définir une involution sur S .
- Montrer que le nombre de points fixes est congru à $|S|$ modulo 2.
- Calculer $|S|$ et montrer qu'il est impair, donc il existe au moins un point fixe.

4.2. Analogie très lointaine avec l'approche de Denise Vella-Chemla

| Preuve de Zagier | Approche de Denise Vella-Chemla |
|---|---|
| $S = \{(a, b, c) \mid a^2 + 4bc = p\}$ | $E_n = \{a+b \mid a \text{ premier impair}, b \text{ impair}, a+b \leq n\}$ |
| Involution sur S | Automorphisme intérieur f_n sur E_n |
| Points fixes \leftrightarrow solutions de $p = a^2 + b^2$ | Points fixes \leftrightarrow décompositions $a + n/2$ avec a premier impair |
| $ S $ est impair | $ E_n $ est... ? |
| Preuve complète du théorème des deux carrés | Approche partielle pour Goldbach |

TABLE 1 – Comparaison entre les deux approches

4.3. Pourquoi l'approche de Denise Vella-Chemla ne prouve pas la conjecture de Goldbach

Théorème 11 (Obstacle fondamental). *L'automorphisme f_n ne peut pas permettre de prouver la conjecture de Goldbach dans son état actuel.*

Démonstration. La conjecture de Goldbach affirme que pour tout entier pair $n \geq 4$, il existe deux nombres premiers p et q tels que $n = p + q$.

L'ensemble E_n défini par Vella-Chemla contient des décompositions $a + b$ où :

- a est un nombre premier impair,
- $b = n - a$ est impair,
- mais b n'est pas nécessairement premier.

Donc même si E_n est non vide (ce qui est toujours vrai pour $n \geq 6$), cela ne garantit pas l'existence d'une décomposition avec b premier.

Exemple

Pour $n = 8$, on a $E_8 = \{3 + 5\}$ (car 3 est premier impair, 5 est impair, et $3 + 5 = 8$). Ici, 5 est premier, donc $8 = 3 + 5$ est une décomposition de Goldbach.

Pour $n = 10$, on a $E_{10} = \{3 + 7, 5 + 5, 7 + 3\}$. Toutes les décompositions ont b premier, donc Goldbach est vérifié.

Mais pour $n = 14$, on a $E_{14} = \{3 + 11, 5 + 9, 7 + 7, 9 + 5, 11 + 3\}$. Ici, 9 est impair mais pas premier. Cependant, il existe d'autres décompositions ($3 + 11, 7 + 7$) où b est premier.

Le problème est que l'automorphisme f_n ne permet pas de **filtrer** les décompositions où b est premier. Il agit sur toutes les décompositions $a + b$ avec b impair, sans distinction de primalité. \square

5. Pistes pour une preuve complète

5.1. Modification de l'ensemble E_n

Pour que l'approche fonctionne, il faudrait définir un ensemble plus restrictif :

Définition 12 (Ensemble des décompositions de Goldbach). Soit $G_n = \{p + q \mid p, q \in \mathcal{P}, p \leq q, p + q = n\}$.

Remarque 13. G_n est exactement l'ensemble des décompositions de Goldbach de n .

Peut-on définir une involution sur G_n dont les points fixes permettraient de prouver que $|G_n| \geq 1$?

5.2. Utilisation de la symétrie

Une idée serait de définir une involution qui "échange" les décompositions. Par exemple :

Définition 14. Pour n pair, définissons $\sigma_n : G_n \rightarrow G_n$ par $\sigma_n(p + q) = (n - q) + (n - p)$. Comme $n - q = p$ et $n - p = q$, on a $\sigma_n(p + q) = p + q$, donc σ_n est l'identité. Cela ne fonctionne pas.

Remarque 15. La difficulté est que G_n est symétrique par nature : si $p + q \in G_n$, alors $q + p \in G_n$ aussi. Une involution non triviale devrait "casser" cette symétrie.

5.3. Approche par comptage modulo 2

Comme dans la preuve de Zagier, on pourrait essayer de montrer que $|G_n|$ est impair, donc non nul. Cependant :

Théorème 16. Pour $n \geq 4$ pair, $|G_n|$ peut être pair ou impair.

Démonstration. Exemples :

- $n = 4 : G_4 = \{2 + 2\}$, donc $|G_4| = 1$ (impair).
- $n = 6 : G_6 = \{3 + 3\}$, donc $|G_6| = 1$ (impair).

- $n = 8 : G_8 = \{3 + 5\}$, donc $|G_8| = 1$ (impair).
- $n = 10 : G_{10} = \{3 + 7, 5 + 5, 7 + 3\}$, donc $|G_{10}| = 3$ (impair).
- $n = 12 : G_{12} = \{5 + 7, 7 + 5\}$, donc $|G_{12}| = 2$ (pair).

Donc $|G_n|$ peut être pair (ex. $n = 12$) ou impair (ex. $n = 10$). □

Remarque 17. *Cette approche ne fonctionne donc pas directement, car $|G_n|$ peut être pair.*

6. Conclusion

6.1. Bilan de l'approche

L'approche par automorphismes intérieurs développée par Denise Vella-Chemla présente plusieurs **qualités remarquables** : **Non, puisqu'elle introduit une circularité : un test sur la primalité est effectué en entrée du processus et ne peut en aucun cas permettre d'aboutir.**

- ✓ **Construction mathématique rigoureuse** : L'ensemble E_n et l'automorphisme f_n sont bien définis et ont des propriétés intéressantes.
- ✓ **Caractérisation des points fixes** : Le Lemme 6 et le Corollaire 7 sont corrects et élégants.
- ✓ **Validation empirique** : Les résultats numériques confirment parfaitement les propriétés théoriques.
- ✓ **Inspiration féconde** : L'analogie avec la preuve de Zagier est pertinente et ouvre des pistes de recherche.

Cependant, **elle ne prouve pas la conjecture de Goldbach** car :

- ✗ L'ensemble E_n contient des décompositions où le second terme n'est pas premier.
- ✗ L'automorphisme f_n ne permet pas de filtrer les décompositions de Goldbach.
- ✗ Le comptage des points fixes ne donne pas d'information directe sur l'existence de décompositions avec deux nombres premiers.

6.2. Perspectives

Pour transformer cette approche en une preuve complète, il faudrait :

1. **Restreindre l'ensemble** : Définir un ensemble G_n contenant uniquement les décompositions de Goldbach.
2. **Trouver une involution adaptée** : Définir une involution sur G_n dont les points fixes permettraient de prouver $|G_n| \geq 1$.
3. **Utiliser des propriétés supplémentaires** : Intégrer des résultats de théorie analytique des nombres (ex. théorème des nombres premiers, théorème de Chen).

4. **Combiner avec d'autres méthodes** : Utiliser cette approche en complément d'autres techniques (cribles, méthodes analytiques).

L'approche de Vella-Chemla reste **une piste très prometteuse** ([voir l'objection sur la circularité de l'argument ci-dessus](#)), car elle apporte une **structure algébrique** à un problème traditionnellement abordé par des méthodes analytiques ou combinatoires.

Références

- [1] Don Zagier. A One-Sentence Proof That Every Prime $p \equiv 1 \pmod{4}$ Is a Sum of Two Squares. *The American Mathematical Monthly*, Vol. 97, n° 2, pp. 144, février 1990.
- [2] Denise Vella-Chemla. Palindromes, 2018.
<https://denisevellachemla.eu/palindromes.pdf>, 2018.
- [3] Denise Vella-Chemla. Qui utilise des automorphismes intérieurs sans en avoir conscience, novembre 2024.
<https://denisevellachemla.eu/automorphismes-interieurs.pdf>