Combiner les involutions locales des décomposants de Goldbach, ia claude pour Denise Vella-Chemla, 24 septembre 2026

Texte intégralement rédigé par l'ia claude.

1. Cadre

Soit n un entier pair fixé. On cherche un décomposant de Goldbach x appartenant à l'intervalle $\left[\sqrt{n}, \ldots, \frac{n}{2}\right]$, c'est-à-dire tel que x et $n-x$ soient tous deux premiers. Une condition nécessaire (crible de Legendre) est : pour tout premier $p \leq \sqrt{n}$,

$$x \not\equiv 0 \pmod{p} \quad \text{et} \quad x \not\equiv n \pmod{p}.$$

On note $F_p = \{0,\ n \pmod{p}\} \subset \mathbb{Z}/p\mathbb{Z}$ l'ensemble des restes interdits, et $R_p = (\mathbb{Z}/p\mathbb{Z}) \setminus F_p$ l'ensemble des restes admissibles.

2. L'involution locale

Pour chaque premier p, on définit

$$\sigma_p : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, \qquad \sigma_p(r) = n - r \pmod{p}.$$

Proposition 1. *σ_p est une involution : $\sigma_p \circ \sigma_p = \mathrm{id}$.*

Démonstration. $\sigma_p(\sigma_p(r)) = n - (n - r) = r$. □

Pour p impair, 2 est inversible modulo p ; σ_p possède un unique point fixe

$$c_p = n \cdot 2^{-1} \pmod{p},$$

et toutes les autres classes se répartissent en $\dfrac{p-1}{2}$ orbites de taille 2, de la forme $\{r,\ n-r\}$. Pour $p = 2$, $\sigma_2 = \mathrm{id}$ (tout est point fixe).

Remarque : σ_p formalise exactement l'identité $(x \pmod{p}) + ((n-x) \pmod{p}) \equiv n \pmod{p}$: c'est l'application qui envoie le reste de x sur le reste de $n - x$.

Fait : F_p est stable par σ_p, et c'est exactement une orbite de σ_p :

- si $p \mid n$, alors $c_p = 0$ et $F_p = \{0\}$ est l'orbite (le point fixe) ;
- si $p \nmid n$, alors $F_p = \{0, n \pmod{p}\}$ est une orbite de taille 2 (et $c_p \notin F_p$ génériquement).

Démonstration. $\sigma_p(0) = n \pmod{p}$ et $\sigma_p(n \pmod{p} = 0$, donc σ_p échange les deux éléments de F_p ; si $p \mid n$ ils coïncident. □

Comme conséquence immédiate de 2., σ_p préserve aussi le complémentaire R_p.

3. Combiner k involutions

Soient $p_1, \ldots, p_k$ les premiers $\leq \sqrt{n}$, et $M = \prod_i p_i$. Par le théorème des restes chinois,

$$\mathbb{Z}/M\mathbb{Z} \;\cong\; \prod_{i=1}^{k} \mathbb{Z}/p_i\mathbb{Z}.$$

Pour $S \subseteq \{1, \ldots, k\}$, on définit τ_S agissant coordonnée par coordonnée dans ce produit :

$$\tau_S = \prod_{i \in S} \sigma_{p_i} \;\times\; \prod_{i \notin S} \mathrm{id}.$$

Proposition 2. *$G = \{\tau_S : S \subseteq \{1, \ldots, k\}\}$ est un groupe isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$, agissant sur $\mathbb{Z}/M\mathbb{Z}$.*

Démonstration. Chaque σ_{p_i} est d'ordre ≤ 2 et agit sur un facteur distinct du produit ; les τ_S commutent donc entre elles et $\tau_S \circ \tau_{S'} = \tau_{S \triangle S'}$ (différence symétrique). □

Fait [Stabilité globale] : si $x \pmod{p_i} \in R_{p_i}$ pour tout i (i.e. x est un candidat valide modulo M), alors pour tout $S \subseteq \{1, \ldots, k\}$, $\tau_S(x)$ est encore un candidat valide.

Démonstration. Sur la coordonnée $i \notin S$, rien ne change : $x \pmod{p_i} \in R_{p_i}$. Sur la coordonnée $i \in S$, l'image est $\sigma_{p_i}(x \pmod{p_i})$; comme σ_{p_i} préserve R_{p_i} (complémentaire de l'orbite F_{p_i}, Fait 2.), on a encore $\sigma_{p_i}(x \pmod{p_i}) \in R_{p_i}$. □

Corollaire 3. *L'ensemble $R_M \subset \mathbb{Z}/M\mathbb{Z}$ des classes candidates (survivantes du crible) est une réunion d'orbites de $G \cong (\mathbb{Z}/2\mathbb{Z})^k$.*

Taille des orbites

Pour $x \in R_M$, notons $m(x) = \#\{i : x \pmod{p_i} \neq c_{p_i}\}$ le nombre de coordonnées où x n'est pas au point fixe local. L'orbite de x sous G a pour cardinal exactement $2^{m(x)}$. Génériquement (aucune coïncidence $x \equiv c_{p_i} \pmod{p_i}$), $m(x) = k$ et l'orbite est pleine, de taille 2^k.

Remarque [Interprétation] : un élément $\tau_{\{i\}}(x)$ (une seule coordonnée retournée) est un entier y tel que $y \equiv n - x \pmod{p_i}$ et $y \equiv x \pmod{p_j}$ pour $j \neq i$: ni x ni $n - x$, mais un candidat "hybride" dont la validité est garantie automatiquement par la structure de groupe, sans calcul supplémentaire. Combiner k involutions engendre ainsi, à partir d'un seul candidat connu, jusqu'à $2^k - 1$ autres candidats valides.

4. Lien avec le crible et limite de l'argument

Le cardinal total est

$$|R_M| = \prod_{\substack{p \leq \sqrt{n} \\ p \mid n}} (p-1) \;\cdot \prod_{\substack{p \leq \sqrt{n} \\ p \nmid n}} (p-2),$$

retrouvant la constante de crible habituelle (liée à la série singulière de Goldbach). L'argument des orbites ne résout pas la difficulté centrale - montrer que $R_M \neq \varnothing$ malgré les chevauchements

d'inclusion-exclusion quand k croît - mais il fournit une symétrie supplémentaire : R_M n'est jamais un ensemble "quelconque" de classes, c'est toujours une union d'orbites de $(\mathbb{Z}/2\mathbb{Z})^k$, ce qui contraint sa structure et pourrait aider à borner sa taille autrement que par la seule inclusion-exclusion brute.