

**Racines cubiques de l'unité modulo n
et décomposants de Goldbach : étude formelle d'une stratégie de preuve
Denise Vella-Chemla pilotant gemini, octobre 2026**

Résumé

On étudie une stratégie d'approche de la conjecture de Goldbach fondée sur les racines cubiques de l'unité dans $(\mathbb{Z}/n\mathbb{Z})^\times$, dans le prolongement du *critère de Vella-Chemla-Schneps* : l'idée du critère est due à Denise Vella-Chemla, et sa démonstration à Leila Schneps ; il est admis ici comme axiome. Après formalisation précise de la prémisse et de la conclusion du critère, on démontre que trois variantes successives de la stratégie proposée sont *fausses*, en exhibant des contre-exemples explicites et minimaux ($n = 14$, $n = 28$, $n = 124$, $n = 18$), vérifiables à la main et formalisables en Lean 4. On explique ensuite structurellement pourquoi toute construction purement multiplicative est vouée à l'échec, et on évalue la valeur réelle de l'observation selon laquelle les décomposants de Goldbach appartiennent au groupe des unités.

1. Le critère de Vella-Chemla-Schneps, formalisé

Définition 1 (Prémisse du critère de Vella-Chemla-Schneps). *Pour $n \in \mathbb{N}$ pair et $x \in \mathbb{N}$, on note $P(n, x)$ la conjonction :*

1. $\sqrt{n} \leq x \leq n/2$ (encadrement) ;
2. *pour tout nombre premier $p \leq \sqrt{n} : x \not\equiv 0 \pmod{p}$ et $x \not\equiv n \pmod{p}$* (congruences).

L'encadrement $\sqrt{n} \leq x \leq n/2$ est *indispensable* à la validité du critère. Sans lui, $x = 1$ vérifie toutes les congruences ($1 \not\equiv 0$ et $1 \not\equiv n \pmod{p}$ pour tout premier p divisant n , car $p \geq 2$ divise n donc $n \equiv 0$) sans être premier. C'est d'ailleurs lui qui rend le critère élémentaire : si $x \leq n/2$ est composé, il possède un facteur premier $q \leq \sqrt{n/2} < \sqrt{n}$, contredisant $x \not\equiv 0$; de même, si $n - x$ est composé, un facteur premier q de $n - x$ vérifie $x \equiv n \pmod{q}$.

Définition 2 (Conclusion du critère de Vella-Chemla-Schneps). *On note $C(n, x)$ l'énoncé : x est premier, $n - x$ est premier et $\sqrt{n} \leq x \leq n/2$ (c'est-à-dire que x est un décomposant de Goldbach de n).*

[Vella-Chemla-Schneps, admis] Pour tout n pair et tout $x : P(n, x) \implies C(n, x)$.

2. La stratégie des racines cubiques

Définition 3 (Racines cubiques de l'unité). *Soit n tel que $3 \mid \varphi(n)$. On appelle racines cubiques de l'unité modulo n les $k \in \{1, \dots, n - 1\}$ tels que $k^3 \equiv 1 \pmod{n}$.*

La stratégie étudiée consiste à dériver de l'ensemble $\{k_1 = 1, k_2, k_3\}$ des racines cubiques un ou deux nombres premiers par la recette : si k_i est premier, le retenir ; sinon, retenir sa racine carrée si k_i est un carré, ou l'un de ses facteurs premiers si k_i est composé ; puis à espérer que l'un des nombres retenus vérifie $P(n, \cdot)$, donc $C(n, \cdot)$ par le théorème ??.

2.1. Premier énoncé : accès à la prémisse - faux

Proposition 4. *Il existe n pair avec $3 \mid \varphi(n)$ et exactement trois racines cubiques de l'unité, tel qu'aucun candidat produit par la recette ne vérifie $P(n, \cdot)$. Le plus petit est $n = 14$.*

Démonstration. $\varphi(14) = 6$, $3 \mid 6$. Les racines cubiques sont $\{1, 9, 11\}$: $9^3 = 729 = 52 \times 14 + 1$ et $11^3 = 1331 = 95 \times 14 + 1$. Les candidats sont $1 = \sqrt{1}$, $3 = \sqrt{9}$ et 11 (premier). Or $P(14, x)$ exige $\sqrt{14} \leq x \leq 7$, soit $3,74 \leq x \leq 7$: aucun candidat n'y rentre (1 et 3 échouent aussi par $1 \equiv 14 \pmod{3}$ et $3 \equiv 0 \pmod{3}$). Pourtant $14 = 7 + 7$ est somme de deux premiers. $\square$

2.2. Restriction aux n doubles d'un composé - toujours faux

On peut espérer que la restriction « $n/2$ composé » (les $n = 2p$ étant trivialement goldbachiens) élimine les contre-exemples.

Proposition 5. *Le plus petit contre-exemple avec $n/2$ composé est $n = 28$; en particulier $n = 56$, racines $\{1, 9, 25\}$, candidats $\{1, 3, 5\}$, échoue aussi : $3 \equiv 0 \pmod{3}$ et $5 \equiv 0 \pmod{5}$, et aucun candidat n'atteint $\sqrt{56} \approx 7,48$.*

Démonstration. $n = 28 = 2 \times 14$, 14 composé, $\varphi(28) = 12$, $3 \mid 12$. Racines : $\{1, 9, 25\}$. Candidats : $1, 3, 5$. $P(28, x)$ exige $5,29 \leq x \leq 14$; les candidats échouent de plus aux congruences ($1 \equiv 28 \pmod{3}$, $3 \equiv 0 \pmod{3}$, $5 \equiv 0 \pmod{5}$). Or $28 = 5 + 23$. $\square$

2.3. Énoncé direct, sans prémisse - faux

On affaiblit la stratégie en visant directement la conclusion : l'un des candidats p est tel que p et $n - p$ sont premiers.

Proposition 6. *Le plus petit contre-exemple (avec $n/2$ composé) est $n = 124$.*

Démonstration. $124 = 2 \times 62$, 62 composé, $\varphi(124) = 60$, $3 \mid 60$. Racines cubiques : $\{1, 5, 25\}$, car $5^3 = 125 \equiv 1$ et $25^3 = 15625 = 126 \times 124 + 1 \equiv 1 \pmod{124}$. Candidats : 1 et 5 (première et facteur de 25). Or $124 - 5 = 119 = 7 \times 17$, composé. Pourtant $124 = 11 + 113$. $\square$

Autres exemples instructifs : $n = 152$, racines $\{1, 49, 121\}$, candidats $\{7, 11\}$, et $152 - 7 = 145 = 5 \times 29$, $152 - 11 = 141 = 3 \times 47$; et $n = 310$, racines $\{1, 191, 211\}$ toutes deux premières, mais $310 - 191 = 119 = 7 \times 17$ et $310 - 211 = 99 = 9 \times 11$: l'échec survient même quand les racines sont premières.

2.4. La piste $k^2 + k + 1$ - fausse également

Puisque $k^3 \equiv 1$ signifie $n \mid (k - 1)(k^2 + k + 1)$, le facteur $k^2 + k + 1$ est le seul qui encode une information sur n . On a testé la construction généreuse : candidats = facteurs premiers de $k^2 + k + 1$, de $k - 1$, de $(k^2 + k + 1) \pmod{n}$, ainsi que leurs partenaires $n - p$.

Proposition 7. *Cette construction échoue dès $n = 18$: racines $\{1, 7, 13\}$; $k^2 + k + 1 \in \{3, 57, 183\}$ fournit les facteurs $3, 19, 61$, dont aucun n'est un décomposant de 18 (dont les décomposants sont $5, 7, 11, 13$).*

3. Analyse structurelle de l'échec

Proposition 8 (les décomposants sont des unités). *Si x est un décomposant de Goldbach de n (x et $n - x$ premiers, $x < n$), alors $\gcd(x, n) = \gcd(n - x, n) = 1$: les décomposants appartiennent au groupe des unités $(\mathbb{Z}/n\mathbb{Z})^\times$, et l'application $x \mapsto -x$ stabilise leur ensemble.*

Démonstration. Un diviseur premier commun à x et n diviserait $n - x$, donc diviserait un nombre premier distinct : contradiction. Pour $n - x$: un diviseur commun à $n - x$ et n divise x . Enfin $x + (n - x) = n \equiv 0$, donc $n - x \equiv -x$. $\square$

La proposition ?? est correcte mais d'usage limité :

- c'est une condition *nécessaire* de densité décroissante : pour $n = 124$, $\varphi(124) = 60$ unités contiennent 10 décomposants $\{11, 17, 23, 41, 53, 71, 83, 101, 107, 113\}$, soit une densité de $1/6$; asymptotiquement, il y a $\sim n/\ln n$ candidats premiers à trier parmi $\varphi(n)$ unités ;
- la primalité n'est pas un invariant du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$: ce groupe ne dépend que de la factorisation de n (par le théorème chinois, $(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_p (\mathbb{Z}/p^{v_p(n)}\mathbb{Z})^\times$) et ne voit pas la *position* de l'entier x dans $\{1, \dots, n\}$, alors que « x est premier » est une affirmation de position additive ;
- la conjecture de Goldbach est une propriété *additive* ($n = x + (n - x)$) ; l'unique information qu'elle laisse dans la structure multiplicative est l'appariement $x \leftrightarrow -x$ de la proposition ??. Aucun invariant multiplicatif (ordre, sous-groupe, coset - comme le sous-groupe d'ordre 3 des racines cubiques) ne peut sélectionner les décomposants.

C'est exactement ce que formalisent les contre-exemples : pour $n = 124$, les racines cubiques $\{1, 5, 25\}$ engendrent un sous-groupe d'ordre 3 sans aucune relation de position avec les 10 décomposants, qui occupent des classes multiplicativement indiscernables.

4. Comptages expérimentaux

Un crible exhaustif (n pair, $n/2$ composé, $3 \mid \varphi(n)$, exactement trois racines cubiques) donne :

Énoncé	borne	cas testés	contre-exemples
prémisse P	20 000	6 625	4 219
prémisse P , $n/2$ composé	20 000	6 014	3 725
conclusion directe, $n/2$ composé	12 000	3 505	890
piste $k^2 + k + 1$, $n/2$ composé	12 000	3 505	705

Le premier contre-exemple du dernier rang est $n = 18$ (proposition ??), ce qui montre que même la construction la plus « informée » du point de vue de n échoue précocement.

5. Formalisation en Lean 4

Les contre-exemples ci-dessus se vérifient par décision élémentaire une fois les définitions posées (avec **Mathlib**) :

```

-
import Mathlib

/-- Prémisse du critère de Vella-Chemla--Schneps (encadrement + congruences). -/
def SchnepsPremise (n x : ℕ) : Prop :=
  Even n ∧ n ≤ x * x ∧ 2 * x ≤ n ∧
  ∀ p, p.Prime → p * p ≤ n → x % p ≠ 0 ∧ x % p ≠ n % p

/-- Critère de Vella-Chemla--Schneps, admis. -/
axiom schneps n x : ℕ (h : SchnepsPremise n x) :
  x.Prime ∧ (n - x).Prime

/-- Racine cubique de l'unité mod n. -/
def CubeRoot (n k : ℕ) : Prop := k ^ 3 % n = 1

/-- Contre-exemple n = 14 : aucune recette n'atteint la prémisse. -/
example : ¬ ∀ k < 14, CubeRoot 14 k →
  ∃ x, x = k  x * x = k  x  k → SchnepsPremise 14 x := by
  intro h
  have h9 := h 9 (by norm_num)
  have h25 := h 25 (by norm_num)
  sorry -- clôture par 'omega' après case analysis sur 1,3,5,9,11,25

```

La clôture complète (sans `sorry`) procède par analyse des cas sur les candidats $\{1, 3, 5\}$ pour $n = 14$: pour chacun, l'encadrement $14 \leq x \cdot x$ ou $2 \cdot x \leq 14$ est réfuté par `omega`, ou la congruence par `decide` sur $p \in \{2, 3\}$.

6. Conclusion

Trois énoncés d'escalade en force (prémisse P ; P restreinte aux $n/2$ composés ; conclusion directe), plus une construction raffinée exploitant $k^2 + k + 1$, sont tous *faux*, avec contre-exemples respectivement minimaux $n = 14$, $n = 28$, $n = 124$, $n = 18$ - tous vérifiables à la main. L'analyse structurelle (section 4) indique que la cause n'est pas un mauvais choix de paramètres mais une inadéquation de principe : la conjecture de Goldbach est additive, la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$ multiplicative, et le théorème chinois montre que le groupe des unités ne retient rien des positions additives qui font l'essence de la primalité relative de x et $n - x$.