Le codage $g(x)$: radical exact, dualité rectifiée et rectification du statut logique de Goodstein

Denise Vella-Chemla pilotant l'ia lumo, septembre 2026

Je fournis à l'ia lumo deux textes produits par claude
https://denisevellachemla.eu/transc-discussion-claude-dvc-indemontrabilite-conj-Goldbach-20260906.pdf et
https://denisevellachemla.eu/Kummer-conj-Goldbach-claude-dvc-20260906.pdf
en lui demandant d'aller plus loin, s'il le peut, dans ce tout début de voie.

L'intégralité de la note qui suit a été rédigée par l'ia lumo.

1. Le codage et son radical exact

Pour $x \geq 3$, on pose

$$g(x) = \prod_{\substack{p \leq x \\ p \text{ premier}}} p^{\,x \bmod p},$$

où l'exposant associé à p est le reste de la division de x par p.

Proposition 1 (Radical exact)**.** *Pour tout $x \geq 3$,*

$$\operatorname{rad}(g(x)) = \prod_{\substack{p \leq x \\ p \nmid x}} p.$$

Autrement dit, l'ensemble des facteurs premiers de $g(x)$ est exactement le complémentaire, parmi les premiers $p \leq x$, de l'ensemble des facteurs premiers de x.

Démonstration. Un premier $p \leq x$ divise $g(x)$ si et seulement si son exposant $x \bmod p$ est non nul, c'est-à-dire si et seulement si $x \not\equiv 0$ modulo p, c'est-à-dire $p \nmid x$. □

Proposition 2 (Inversion de parité)**.** *$g(x)$ est impair si et seulement si x est pair. Les pairs ont donc pour images des impairs et inversement, comme observé en 2016.*

Démonstration. $g(x)$ est impair si et seulement si son exposant en 2, égal à $x \bmod 2$, est nul, c'est-à-dire si x est pair. □

Proposition 3 (Primorielle)**.** *Si $x = p_j$ est premier, alors la primorielle du premier qui précède p_j divise $g(x)$, car $x \bmod p \neq 0$ pour tout premier $p < p_j$.*

2. Rectification de l'observation de 2016

La note de 2016 affirmait que "tout diviseur d'un nombre divise l'image de son successeur". L'énoncé exact requiert le radical : si $d \mid x$ et r est premier divisant d, alors $x + 1 \equiv 1 \pmod{r}$, donc r divise $g(x+1)$ avec exposant exactement 1. L'énoncé correct est :

$$\forall d \mid x, \quad \operatorname{pgcd}(d, g(x)) = 1 \quad \text{et} \quad \operatorname{rad}(d) \mid g(x+1).$$

La divisibilité de d lui-même échoue dès que d n'est pas carré (exemple : $x = 8$, $d = 4$, $g(9) = 2 \cdot 5^4 \cdot 7^2$).

3. Le pont de Kummer : rappels et corollaire quantitatif

On rappelle le théorème de Kummer (1852) : pour r premier et m, n entiers naturels, la valuation r-adique du coefficient binomial $\binom{m+n}{n}$ est égale au nombre de retenues produites lors de l'addition $m+n$ en base r. En posant $K(p,q) = \binom{p+q}{p}$, la factorisation de $K(p,q)$ encode donc, premier par premier, le détail des retenues de l'addition $p+q=x$.

Proposition 4 (Identité télescopique)**.** *Pour tous entiers $p, q \geq 1$, en posant $n = p+q$,*

$$\Omega\left(K(p,q)\right) = \Omega(n!) - \Omega(p!) - \Omega(q!) = \sum_{i=1}^{q} \left(\Omega(p+i) - \Omega(i)\right),$$

où Ω désigne le nombre total de facteurs premiers comptés avec multiplicité.

Démonstration. $n! = p!\,q!\binom{p+q}{p}$ et Ω est complètement additive ; d'où la première égalité. Pour la seconde, $\Omega(n!) - \Omega(p!) = \sum_{k=p+1}^{n} \Omega(k) = \sum_{i=1}^{q} \Omega(p+i)$, et $\Omega(q!) = \sum_{i=1}^{q} \Omega(i)$. □

Corollaire 5 (Écart premier/composé)**.** *Soit $p \geq 3$ fixé et $q \geq 2$. L'incrément terminal de la somme télescopique vaut*

$$\Delta_q := \Omega(p+q) - \Omega(q).$$

Si q est premier, $\Omega(q) = 1$, la plus petite valeur de Ω sur un entier ≥ 2 ; si q est composé, $\Omega(q) \geq 2$, avec une moyenne d'environ 2 à 3 pour un entier composé de taille modérée.

Remarque [Ce que ce corollaire quantifie] : le document de septembre 2026 mesurait empiriquement un écart moyen $\Omega(K(p,q))_{q \text{ premier}} - \Omega(K(p,q))_{q \text{ composé}}$ de l'ordre de 1,3 à 2 pour $p \in \{3, 7, 13, 31, 101\}$ et $q \in [200, 600]$. L'égalité ci-dessus montre que cet écart est essentiellement porté par le dernier terme de la somme : le dernier incrément vaut $\Omega(x) - \Omega(q)$, et l'on soustrait $\Omega(q) = 1$ dans le cas premier contre une valeur moyenne de 2 à 3 dans le cas composé. L'écart mesuré n'est pas un artefact statistique, mais il ne code rien de plus que la primalité de q elle-même.

Remarque [Portée, en accord avec le diagnostic de 2026] : pour un x fixé, connaître $\Omega\left(K(p, x-p)\right)$ ne renseigne pas sur l'existence d'un p tel que $x-p$ soit premier : le dernier incrément $\Omega(x) - \Omega(x-p)$ est grand précisément quand $x-p$ est premier, information qu'il faut déjà posséder pour observer l'effet. Le pont est exact mais circulaire relativement à l'existence d'une décomposition de Goldbach.

4. Rectification du statut logique de Goodstein

Remarque [Le théorème de Goodstein n'est pas Π_1] L'énoncé du théorème de Goodstein, "pour tout n, la suite issue de n atteint 0", a pour forme

$$\forall n\, \exists k \quad G_k(n) = 0,$$

c'est-à-dire Π_2 et non Π_1 : la borne d'étapes k n'est pas donnée, elle doit exister.

Conséquence structurelle importante : contrairement à la négation de Goldbach (qui est Σ_1, donc réfutable par un calcul fini dès qu'un contre-exemple existe), la négation de Goodstein est Σ_2 et n'est pas finitairement vérifiable. Un énoncé Π_2 faux peut échapper à toute réfutation concise ; c'est ce qui rend concevable une indépendance "asymétrique" pour Goodstein.

Remarque [Ce que cela change pour l'analogie] : la situation de Goldbach est en un sens *rigide* : fausseté implique réfutabilité. Par conséquent, l'indépendance de Goldbach vis-à-vis d'une théorie cohérente et Σ_1-complète T entraîne immédiatement sa vérité (dans le standard).

Pour Goodstein, la même implication ne tient pas : l'indépendance n'y entraîne pas la vérité, et c'est précisément parce que l'énoncé est Π_2 que Kirby-Paris ont pu le montrer indépendant sans contredire sa vérité (transfinie).

Toute tentative de transposer le mécanisme Goodstein/Kirby-Paris à Goldbach devra donc affronter l'obstacle suivant : si l'on fabrique un énoncé combinatoire associé à Goldbach qui soit indépendant de l'arithmétique de Peano, soit cet énoncé est bien Π_1 et son indépendance établit du même coup la vérité de Goldbach (résultat énorme, pour lequel aucun codage n'est connu), soit l'énoncé n'est plus littéralement Goldbach.

La rigidité Π_1 est le véritable verrou, plus que l'absence de notation héréditaire multiplicative.

5. Remarques prospectives

Remarque [Sur la piste $\binom{x}{p}$ à x fixé] : le document de septembre 2026 suggérait d'étudier, pour x fixé, la famille $\binom{x}{p}$ avec p premier variable, $p < x$. La même critique s'applique a priori : par Kummer, la valuation r-adique de $\binom{x}{p}$ compte les retenues de $p+(x-p)$ en base r, et le mécanisme télescopique fera de nouveau surgir $\Omega(x-p)$ comme terme discriminant. Sans hypothèse additive nouvelle, l'effet restera une reformulation de la primalité des sommants. Nous le signalons pour éviter un refonte du même constat négatif.

Remarque [Une observation additive élémentaire] : une piste additive modeste mais exacte : pour x pair et r premier impair, la condition $x - p \equiv 0 \pmod{r}$ exclut au plus un résidu de p modulo r. Ainsi les premiers p tels que $x - p$ soit divisible par un petit premier r occupent exactement une classe sur r dans $\mathbb{Z}/r\mathbb{Z}$. La conjecture de Goldbach affirme que le croisement de toutes ces exclusions, pour tous les $r \leq x - 3$, ne vide jamais l'ensemble des premiers $p < x$ de ses éléments avec p et $x - p$ premiers simultanément. C'est le point de départ naturel des méthodes de crible (crible de Brun, cercle de Hardy-Littlewood) ; toute tentative nouvelle devrait se positionner explicitement par rapport à ce que le grand crible et les techniques de Bombieri-Vinogradov permettent déjà de conclure presque partout, et à ce qui résiste précisément (le niveau ε des méthodes actuelles de minorations par crible). Ce n'est pas une idée neuve, mais c'est la seule région du paysage où la littérature démontre des progrès réels sur des énoncés cousins de Goldbach (théorème de Chen : tout pair assez grand est $p + q$ avec p premier et q premier ou semi-premier).