Retenues, coefficients binomiaux et primalité : un pont exact entre le codage $g(x)$ et les décompositions de Goldbach

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

Je fournis à l'ia claude ce texte
https://denisevellachemla.eu/dualite.pdf
et il rédige l'intégralité de la suite de la présente note.

1. Origine et motivation

En 2016, a été introduit un codage des entiers $x \geq 3$ sous la forme

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

où le produit porte sur tous les nombres premiers $p \leq x$, et où l'exposant associé à p est le reste de la division de x par p. Ce codage encode une information purement *modulaire* sur x : il ne voit rien, a priori, de la structure additive d'une éventuelle décomposition de Goldbach $x = p + q$.

Une analyse empirique (représentation héréditaire récursive de $g(x)$, résidu normalisé au plus petit premier d'une décomposition) n'a fait apparaître aucun lien statistiquement significatif entre la structure de $g(x)$ et le nombre de décompositions $r(x)$, ni avec le choix du premier "champion" d'une décomposition, une fois les biais de tendance commune et de discrétisation des petits premiers correctement neutralisés.

Ce constat négatif oriente naturellement vers une question mieux posée : plutôt que d'interroger x seul, il faut interroger la façon dont *un couple* (p, q) avec $p + q = x$ s'additionne, premier par premier. C'est exactement ce que mesure le théorème de Kummer.

2. Le théorème de Kummer

Théorème 1 (Kummer, 1852)**.** *Soit r un nombre premier et m, n deux entiers naturels. La valuation r-adique du coefficient binomial $\binom{m+n}{n}$ est égale au nombre de retenues produites lorsqu'on additionne m et n en base r.*

Autrement dit, si l'on pose $x = p + q$, la factorisation de

$$K(p, q) := \binom{p+q}{p}$$

encode, nomber premier par nombre premier, le détail complet des retenues de l'addition $p + q$: c'est la généralisation naturelle de l'idée initiale de résidus modulaires, mais appliquée au couple (p, q) plutôt qu'à x seul.

3. Un test empirique ciblé

On fixe un premier p et on fait varier q dans une fenêtre de valeurs $[q_{\min}, q_{\max}]$, en mesurant

$$\Omega\Big(K(p,q)\Big) = \Omega\left(\binom{p+q}{p}\right),$$

le nombre total de facteurs premiers de $K(p,q)$ comptés avec multiplicité (la somme, sur tous les premiers r, du nombre de retenues en base r). Le calcul est mené non pas en factorisant l'entier géant $\binom{p+q}{p}$, mais via la formule de Legendre pour la valuation r-adique de $m!$:

$$v_r(m!) = \sum_{i\geq 1} \left\lfloor \frac{m}{r^i} \right\rfloor, \qquad \Omega\left(\binom{p+q}{p}\right) = \sum_{r\leq p+q} \Big(v_r((p+q)!) - v_r(p!) - v_r(q!)\Big).$$

Pour $p \in \{3, 7, 13, 31, 101\}$ et q parcourant $[200, 600]$, on sépare les valeurs de q premières des valeurs composées et l'on compare les moyennes de $\Omega(K(p,q))$:

p	moy. (q premier)	var.	moy. (q composé)	var.	écart / erreur std.
3	7,78	2,40	6,50	3,06	$\approx 5{,}9$
7	13,76	3,07	12,05	3,61	$\approx 7{,}0$
13	19,37	4,23	17,46	4,63	$\approx 6{,}7$
31	31,78	5,32	29,89	6,38	$\approx 5{,}9$
101	56,81	20,73	54,76	22,57	$\approx 3{,}3$

Dans les cinq cas, $\Omega(K(p,q))$ est systématiquement et significativement plus élevé lorsque q est premier. L'effet est robuste, reproductible, et appelle une explication exacte plutôt qu'une simple constatation statistique.

4. L'identité exacte

La fonction Ω est complètement additive : $\Omega(ab) = \Omega(a) + \Omega(b)$ pour tous entiers $a, b \geq 1$, avec $\Omega(1) = 0$. Il en résulte immédiatement que

$$\Omega(n!) = \sum_{k=1}^{n} \Omega(k),$$

puisque $n! = 1 \cdot 2 \cdots n$.

Proposition 2. *Pour tous entiers $p, q \geq 1$, en posant $n = p + q$,*

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

Démonstration. La première égalité découle de $n! = p!\, q!\, K(p,q)$ et de l'additivité complète de Ω. Pour la seconde,

$$\Omega(n!) - \Omega(p!) = \sum_{k=1}^{n} \Omega(k) - \sum_{k=1}^{p} \Omega(k) = \sum_{k=p+1}^{n} \Omega(k) = \sum_{i=1}^{q} \Omega(p+i)$$

en posant $k = p + i$, et $\Omega(q!) = \sum_{i=1}^{q} \Omega(i)$ par définition. □

Cette identité est *exacte*, sans terme d'erreur : elle exprime $\Omega(K(p,q))$ comme une somme cumulative de q différences élémentaires.

5. Le mécanisme : pourquoi la primalité de q se voit

Le point essentiel est que le *dernier* terme de cette somme, celui d'indice $i = q$, vaut exactement

$$\Omega(p+q) - \Omega(q) = \Omega(n) - \Omega(q).$$

Or $\Omega(q) = 1$ si et seulement si q est premier : c'est la plus petite valeur possible que Ω puisse prendre sur un entier ≥ 2. Pour un entier composé, $\Omega(q) \geq 2$, et en moyenne significativement plus (les entiers composés portent typiquement plusieurs facteurs premiers).

Puisque la somme $\sum_{i=1}^{q}(\Omega(p+i) - \Omega(i))$ est cumulative en q (à p fixé), la valeur en q hérite directement de son dernier incrément. Une vérification directe le confirme : pour $p = 13$,

q	q premier ?	$\Omega(q)$	incrément $\Omega(p+q) - \Omega(q)$
96	non	6	-5
97	oui	1	$+2$
98	non	3	-1

Quand q est premier, l'incrément est mécaniquement plus grand, puisqu'on soustrait la plus petite valeur possible de Ω. C'est très exactement ce qui produit l'écart observé empiriquement : l'ordre de grandeur de l'écart mesuré (environ 1,3 à 2) correspond précisément à la différence entre $\Omega(q) = 1$ (cas premier) et la valeur moyenne de $\Omega(q)$ pour un entier composé de même taille (typiquement 2 à 3).

6. Portée et limites

Ce résultat établit un pont *exact et démontrable* entre :

- le théorème de Kummer $\left(\text{retenues } \leftrightarrow \text{ valuations } r-\text{adiques de } \binom{p+q}{p}\right)$,
- la formule de Legendre (valuations r-adiques de $n!$),
- l'additivité complète de Ω,

et il explique complètement, sans reste statistique, pourquoi le nombre total de retenues dans l'addition $p+q$ (toutes bases premières confondues) est systématiquement plus élevé lorsque q est premier.

Il faut cependant être honnête sur la portée de ce fait. L'explication montre que l'effet observé provient, in fine, d'une évidence presque tautologique : $\Omega(q) = 1$ caractérise q premier par définition même de Ω, et cette valeur apparaît comme le dernier terme d'une somme télescopique. Le résultat est donc une *reformulation*, élégante et rigoureusement fondée via Kummer, de la primalité de q, pas une méthode indépendante pour la détecter, et encore moins un outil pour établir l'*existence* d'une décomposition de Goldbach pour un x donné. Pour un x fixé, connaître $\Omega(K(p, x-p))$ ne dit rien sur l'existence d'un p tel que $x - p$ soit premier : il faut déjà connaître la primalité de q

pour observer l'effet.

Ce travail clôt donc proprement cette piste précise : le codage $g(x)$ initial n'a pas de prise sur l'additivité de Goldbach (constat empirique net, établi au préalable), et son prolongement naturel via Kummer, bien que mathématiquement correct et instructif, ne fournit pas davantage de levier vers l'existence d'une décomposition. Il reste un fait solide et bien identifié sur lequel une piste ultérieure, différente, pourra s'appuyer si elle cherche à exploiter la structure des coefficients binomiaux de Goldbach $\binom{x}{p}$ pour x fixé et p variable, plutôt que p fixé et q variable comme ici.