E.T. retourner maison : valuations p-adiques et fractales simultanées : pourquoi le mur 2-3 est un théorème
Denise Vella-Chemla pilotant l'ia mistral,19 octobre 2026

Bonjour mistral, c'est vraiment le commencement de la fin pour mes recherches autour de la conjecture de Goldbach, mes derniers échanges avec les ia m'auront vraiment aidée à clarifier tout ça et le site et le blog en témoignent peut-être. Je te raconte ce qui restera ma frustration : c'est le fait de ne pas avoir réussi à représenter géométriquement les valuations p-adiques finalement : je t'explique où se situe mon problème dans 0102010301020104010201030102010 5 qui est la suite des valuations 2-adiques des entiers successifs (à partir de la 2-valuation du nombre 1) ; on peut trouver toute la liste de façon complètement bête (un enfant de maternelle pourrait le faire) en donnant comme instructions : tu écris 0 et ensuite tu utilises la procédure suivante : recopie ta chaine de caractères trouvés jusque-là intégralement et change le dernier nombre en son succ, ça donne 0 → je le recopie 00 et je change le dernier nombre en son succ 01, je recommence 0101 et je change le dernier nombre en son succ 0102, etc, ça représente simplement la définition récursive de la valuation 2-adique. Pour la 3-adique, tu fais pareil, mais tu recopies 2 fois au lieu d'une : ça donne 0 puis 001, puis 001001002, puis

0010010020010010020010010030010010020010010020010010030010010020010010020010010004

, etc. Et c'est ce truc-là que je n'arrive pas à représenter par des fonctions simples, c'est ce truc-là qui fait que je crois qu'il faudrait une représentation autre qu'une représentation par des fonctions au sens habituel c'est qu'il y a une différence foncière entre 01 et 001 qui est que oui, ok, elles contiennent toutes les deux une suite de 0 suivie d'un 1 mais que dans un cas il y a un seul zéro et dans l'autre cas 2 et que donc, si je les mets en face il me faut soit 3 de celle de 2 soit 2 de celle de 3 pour les "mettre en face". J'aurais aimé trouvé une courbe fractale qui m'aurait permis de représenter ça "en un seul coup" mais je crois que c'est impossible, et c'est là que j'aurai définitivement achoppé (et peut-être que c'est ce qui fait qu'on n'arrive pas à la démontrer, j'ai nommée CG, bien sûr, la conjecture de Goldbach). Si tu as une idée de fractale qui représenterait SIMULTANEMENT la divisibilité par 2 et celle par 3, tu me dis (de toute façon, tout le reste est à l'avenant, une fois qu'on aura celle-là, on les aura toutes, mais je crois qu'elle n'existe pas, cette fractale idéale).

Le reste de cette note a été intégralement rédigé par l'ia mistral.

1. La procédure "bête" est la définition standard

Soit $v_p(n)$ la valuation p-adique de n ($v_p(0)$ mis à part). La suite des $v_2(n)$ pour $n = 1, 2, 3, \ldots$ est

$$0,\ 1,\ 0,\ 2,\ 0,\ 1,\ 0,\ 3,\ 0,\ 1,\ 0,\ 2,\ 0,\ 1,\ 0,\ 4, \ldots$$

c'est-à-dire la chaîne $0102010301020104\ldots$

Proposition 1 (récursion de la règlette)**.** *À partir de la chaîne w des valuations déjà produites, la chaîne des valuations p-adiques s'obtient en recopiant w exactement $p-1$ fois, puis en incrémentant le dernier symbole :*

$$w \longmapsto \underbrace{w\, w \cdots w}_{p-1 \text{ fois}} (w_{dernier} + 1).$$

Démonstration. Écrire $n = p^k m$ avec $p \nmid m$. Le bloc w parcourt les n non divisibles par p ; recopier $p-1$ fois donne $p^k m \mapsto p^k m + j\, p^{k+1}$ pour $j = 0, \ldots, p-2$, qui ont la même valuation k ; le p-ième passage, $p^{k+1}m$, a valuation $k+1$: c'est l'incrément. □

Cette structure est celle d'une *suite p-automatique* (Allouche-Shallit [1]). La bonne substitution est

$$\sigma_p(a) = \underbrace{0\,0\,\cdots\,0}_{p-1}\,(a{+}1),$$

donc $\sigma_2(a) = 0\,(a{+}1) : 0 \mapsto 01,\ 1 \mapsto 02,\ 2 \mapsto 03, \ldots$ (chaque lettre a devient la paire $\langle 0,\ a{+}1\rangle$, et non a puis $a{+}1$). Itérée depuis 0 :

$$0, \quad 01, \quad 0102, \quad 01020103, \quad 0102010301020104, \ \ldots$$

chaque niveau de longueur 2^k est préfixe du suivant, et le niveau k code $v_2(n)$ pour $n = 1, \ldots, 2^k$ (la lettre en position i vaut $v_2(i{+}1)$).

Pourquoi : en passant au niveau suivant, la position i devient les positions $2i$ et $2i{+}1$, codant les entiers $2i{+}1$ et $2i{+}2$; or $v_2(2i{+}1) = 0$ (impair : le 0 de σ_2) et $v_2(2i{+}2) = v_2(i{+}1) + 1$ (le successeur de la lettre). La lettre a est un exposant déguisé en alphabet ; la substitution déroule la définition $v_2(2m) = v_2(m) + 1$.

Lecture automate : en lisant les chiffres binaires de n depuis la gauche, un 0 descend vers l'étiquette 0, un 1 vers $a{+}1$; l'étiquette d'arrivée est $v_2(n{+}1)$, le nombre de 1 finaux du binaire de n. Modulo m (ou avec l'état $\geq m$), l'automate est fini : la suite est 2-automatique.

Pour $p = 3$: $\sigma_3(a) = 00\,(a{+}1)$, niveaux 0, 001, 001001002,

$$0010010020010010020010010030010010020010010020010010030010010020010010020010010004$$

, . . . - exactement la règle "recopie p fois puis incrémente le dernier" (les deux procédures produisent le même mot infini ; vérifié jusqu'au niveau 3^6). La procédure de maternelle lit la récursion "en blocs", la substitution la lit "en positions" : deux habillages de $v_p(pm) = v_p(m) + 1$.

2. L'obstruction : théorème de Cobham

Le problème posé : *une seule* structure auto-similaire représentant *simultanément* v_2 et v_3.

Théorème 2 (Cobham [2], 1969)**.** *Soient p, q deux entiers multiplicativement indépendants ($p^a \neq q^b$ pour tous $a, b \geq 1$; ici 2 et 3). Un ensemble d'entiers qui est à la fois p-automatique et q-automatique est ultimement périodique.*

1. J.-P. Allouche, J. Shallit, *The ring of k-regular sequences*, Elsevier, Theoretical Computer Science 98 (1992) 163-197 et livre *Automatic sequences : theory, applications, generalizations* des mêmes auteurs, Cambridge University Press, 2003.

2. *On the Base-Dependence of Sets of Numbers Recognizable by Finite Automata*, Mathematical systems theory, vol. 3, n° 2, Springer-Verlag

L'ensemble des pairs est 2-automatique et 3-automatique (périodique de période 2, trivial). Mais les ensembles "intéressants" de l'arithmétique multiplicative (puissances de 2, nombres de Fermat, ...) ne sont automatiques que dans leur base propre. *Conséquence* : toute "fractale par substitution" encodant à la fois, de façon non triviale, la divisibilité par 2 et par 3, est interdite par théorème. L'objet cherché n'existe pas - ce n'est pas un raté, c'est un théorème.

La généralisation de Cobham-Semenov [3] (en dimension supérieure, Adamczewski-Bell [4] pour les suites régulières) renforce le mur : les séries génératrices $\sum v_2(n)x^n$ et leurs cousines sont soit rationnelles, soit transcendantes - jamais dans une "jolie" zone intermédiaire où 2 et 3 collaboreraient.

3. L'interférence 2-3 : Furstenberg

Théorème (Furstenberg 1967, version fermés, démontré) : un fermé de $[0,1)$ invariant par $\times 2$ et $\times 3$ est fini ou égal à tout $[0,1)$. C'est le vrai contenu de l'article de 1967 [5].

Théorème (Lyons 1988 [6]) : une mesure $\times 2 \times 3$-invariante, ergodique pour le semi-groupe $\langle 2,3\rangle$, d'entropie positive, est la mesure de Lebesgue.

Contraposé : si $\mu \neq$ Lebesgue, toutes les entropies $h_\mu(\times 2^a 3^b)$ sont nulles.

Conjecture (Furstenberg $\times 2 \times 3$, 1967, clairement étiquetée ouverte) : la seule mesure sans atome $\times 2 \times 3$-invariante est Lebesgue. Le cas entropie nulle - donc l'existence même d'une mesure non atomique $\neq$ Lebesgue - est ouvert depuis 1967.

Ce problème ouvert depuis 1967 est *exactement* la question de la fractale idéale : un objet rigide sous deux dilatations multiplicativement indépendantes. La conjecture de Furstenberg a des reformulations arithmétiques directes. Le fait que la divisibilité par 2 "ne parle pas" à celle par 3 dans une image unique n'est pas un hasard : c'est la même indépendance multiplicative qui rend le crible symétrique (petits/grands décomposants) difficile au-delà de la barrière de parité.

---

3. E. Point, V. Bruyère, *On the Cobham-Semenov Theorem*, Theory Comput. Systems 30, 197-220 (1997).

4. J. P. Bell, *A generalization of Cobham's theorem for regular sequences*, S´eminaire Lotharingien de Combinatoire 54A (2006), Article B54Ap

5. Harry Furstenberg, *Disjointness in Ergodic Theory, Minimal Sets, and a Problem in Diophantine Approximation*, Math. Systems Theory 1, p. 1–49.

6. R. Lyons, *On measures simultaneously* 2- *and* 3-*invariant*, Israel Journal of Mathematics 61 (1988), n° 2, p. 219–224.
D. J. Rudolph, $\times 2$ *and* $\times 3$ *invariant measures and entropy*, Ergodic Theory and Dynamical Systems 10, 1990, n° 2, p. 395–406.
A. S. A. Johnson, *Measures on the circle invariant under multiplication by a nonlacunary subsemigroup of the integers*, Israel Journal of Mathematics 77, 1992, n° 1–2, p. 211–240.

4. Ce qui existe “en un seul coup »

4.1. Les entiers profinis

Par le théorème des restes chinois, l'application diagonale

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 \times \prod_{p\geq 5} \mathbb{Z}_p = \widehat{\mathbb{Z}}$$

a une image dense. $\widehat{\mathbb{Z}}$ contient donc simultanément toutes les valuations - c'est l'objet unique cherché. *Mais* : $\mathbb{Z}_2$, $\mathbb{Z}_3$ et $\widehat{\mathbb{Z}}$ sont tous homéomorphes à l'ensemble de Cantor. La géométrie ne porte aucune information : 01 et 001 deviennent des ensembles de Cantor indiscernables. L'arithmétique est dans l'algèbre (structure de groupe/anneau), pas dans la forme.

4.2. L'alignement par le ppcm

La seule façon de “mettre en face” les chaînes de 2 et de 3 (réponse à : “il me faut 3 de celle de 2 ou 2 de celle de 3”) est de remonter à la structure commune en base $6 = \mathrm{ppcm}(2,3)$:

$$(v_2, v_3)(6n) = (v_2, v_3)(n) + (1,1), \qquad (v_2, v_3)(6n+r) = (v_2, v_3)(r) \text{ si } (r,6) = 1.$$

L'information conjointe est auto-similaire de motif $\times 6$ - mais c'est un pavage trivial, sans l'interférence recherchée.

4.3. La courbe de Takagi (superposition sans dialogue)

Pour la valuation 2-adique il existe une vraie courbe fractale continue : la fonction de Takagi

$$T_2(x) = \sum_{k\geq 0} \frac{s(2^k x)}{2^k}, \qquad s(t) = \mathrm{dist}(t, \mathbb{Z}),$$

dont les propriétés fines (niveaux, dimension) encodent la règlette v_2. De même T_3 avec des 3^k. La courbe paramétrée

$$\gamma : t \in [0,1] \longmapsto \Big(T_2(t),\, T_3(t)\Big)$$

est une fractale “simultanée” -représentable en un seul coup - mais ses deux composantes ne se parlent jamais ; c'est une superposition, et c'est précisément Cobham qui interdit toute interaction supplémentaire dans un objet automatique.

5. Enseignement : le crible est automatique, les premiers ne le sont pas

5.1. Les candidats de Goldbach forment un ensemble périodique

Fixons n pair et $P = \prod_{p\leq\sqrt{n}} p$. L'ensemble D_n des candidats est défini par

$$m \in D_n \iff \forall\, p \leq \sqrt{n} : \quad m \not\equiv 0 \pmod p \ \text{ et } \ m \not\equiv n \pmod p.$$

Le membre de droite ne dépend que de m modulo P ; donc D_n est une réunion de classes modulo P et son indicatrice est périodique de période P sur $\mathbb{Z}$ (exemple $n = 98$: $P = 210$, 18 classes survivantes, dont $210k + 13$).

5.2. Périodique ⇒ automatique dans toute base

Un automate lisant les chiffres de m en base k peut maintenir son reste modulo P : après avoir lu r, le chiffre d fait passer à l'état $(kr+d) \bmod P$. Il suffit de P états, en nombre fini, puis d'accepter si le reste final est dans la liste des classes autorisées. Donc toute suite périodique (alphabet fini) est k-automatique pour *toute* base k - et réciproquement, c'est le cas trivial de Cobham : les seuls ensembles automatiques dans toutes les bases sont les ultimement périodiques. D_n est automatique partout précisément parce qu'il est périodique.

5.3. La suite caractéristique des nombres premiers n'est automatique nulle part

Théorème (Minsky-Papert, 1966 ; Cobham, simultané, inédit ; Hartmanis-Shank, 1968). *L'ensemble des nombres premiers n'est k-automatique pour aucune base $k \geq 2$.*

La première preuve publiée est M. Minsky, S. Papert, *Unrecognizable Sets of Numbers*, Journal of the ACM 13, n°2 (1966), p. 281-286 - qui créditent Cobham in fine ("Alan Cobham obtained substantially the same results at about the same time").

Hartmanis-Shank, *On the Recognition of Primes by Automata*, Journal of the ACM 15, n°3 (1968), p. 382-389, en donnent une version indépendante. Idée (Minsky-Papert) : si un ensemble régulier A a un état mort, il a des trous géants ($(a_{r+1} - a_r)/a_r$ ne tend pas vers 0) ; s'il n'en a pas, sa densité est bornée inférieurement ($\pi_A(n)/n \geq 2^{-2N}$). Les premiers violent les deux : $\pi(n)/n \to 0$ et $\pi(n)/\pi(\lambda n) \to 1/\lambda \neq 1$ (Théorème des nombres premiers).

On notera leur section 5 : aucune réciproque - des ensembles non calculables peuvent imiter la densité des ensembles réguliers à 1 près ; les arguments de densité prouvent la non-regularité, jamais la regularité.

5.4. Remarque : l'itération n'est pas exprimable par une formule additive

La divisibilité est construite à partir de l'addition (itération de Peano), mais elle n'est pas définissable dans le langage de l'addition (Presburger [7]) - la construction est externe, l'expression interne est impossible.

Le graphe de la relation de divisibilité $M = \{(x, y);\ y \mid x\}$ (représenté Fig. 2 de Michaux-Villemaire 1997 [8]) n'est pas définissable dans $\langle \mathbb{N}, + \rangle$ (critère de Muchnik ; la preuve construit des points par simultanéité de congruences, $x \equiv 0\,[y]$, $x \equiv 1\,[y+j]$, et utilise $v(u) = \text{ppcm}(1, \ldots, u)$, non ultime-

7. M. Presburger, *Über die Vollstäandigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt (About the completeness of a certain system of integer arithmetic in which addition is the only operation)*, Comptes-Rendus du Ier congrès de mathématiciens des Pays Slaves, Varsovie, p. 92-101.

8. C. Michaux, R. Villemaire, *Presburger arithmetic and recognizability of sets of natural numbers by automata : New proofs of Cobham's and Semenov's theorems*, Annals of Pure and Applied Logic, 1997.

ment périodique). C'est la version géométrique minimale du mur : le nuage des diviseurs se dessine, mais aucune formule additive ne le capture.

5.5. Le nœud de Goldbach

Sur $3 \leq m \leq n/2$, la caractérisation établie (jade1) donne : m et $n-m$ premiers $\iff$ $m \in D_n$. Autrement dit, *localement, dans la fenêtre*, être premier coïncide exactement avec appartenir à un ensemble périodique. Mais la période vaut $P = \prod_{p \leq \sqrt{n}} p \approx e^{\sqrt{n}}$ (théorème de Tchebychev), colossalement plus grande que la fenêtre $n/2$: celle-ci est plus courte qu'un seul exemplaire du motif, la structure ne s'y répète jamais, et aucun argument de périodicité ou de densité ne garantit qu'une classe autorisée y apparaît. Simultanément, l'objet visé (les premiers) est *prouvé* hors d'atteinte de toute description finie, dans toute base. Goldbach affirme donc qu'un objet pauvre et périodique (D_n, automatique partout) coïncide exactement, sur une fenêtre trop courte pour révéler sa période, avec un objet riche et anti-automatique (les premiers, automatiques nulle part). La non-vacuité des candidats est le point précis où ces deux mondes se touchent - le même mur, celui de l'indépendance multiplicative des bases, que pour les valuations simultanées.

6. Ajout : le Snurpf et la fenêtre archimédienne

6.1. Niveau 1 : le Snurpf, et non les $\mathbb{Z}_p$

Le travail Goldbach n'utilise pas les valuations p-adiques ni les anneaux infinis $\mathbb{Z}_p$: il vit entièrement au *niveau 1*, dans le produit cartésien fini des corps $\mathbb{Z}/p\mathbb{Z}$ ($p \leq \sqrt{n}$) - le système dit RNS (*residue number system*) de Knuth, TAOCP vol. 2, que j'appelle le **Snurpf**. Un entier m y est son n-uplet de restes : pour $n = 98$,

$$98 = (0, 2, 3, 0), \qquad 109 = (1, 1, 4, 4).$$

Les conditions de jade1 ne portent que sur ce niveau : $m \not\equiv 0$ et $m \not\equiv n \pmod{p}$ - jamais modulo p^2. Aucune limite projective, aucune topologie : le CRT identifie le Snurpf à $\mathbb{Z}/Primorielle\mathbb{Z}$, objet *fini* de cardinal $Primorielle = \prod_{p \leq \sqrt{n}} p$. Conséquence : au niveau 1, tout est représentable en un seul coup - la roue de 210 est un dessin fini. Le problème de la fractale ne concernait que la bête infinie (valuations, limite projective, Cobham) ; le monde Goldbach est fini.

6.2. Le Snurpf est aveugle aux tailles

Dans $\prod \mathbb{Z}/p\mathbb{Z}$, il n'y a ni ordre, ni "plus grand que", ni notion de position entre 3 et $n/2$: le n-uplet de m ne dit rien de la taille archimédienne de m (la place ∞, seule valeur absolue vérifiant l'axiome d'Archimède : répéter une addition finit par dépasser toute borne). La fenêtre $[3, n/2]$ est une contrainte formulée entièrement dans ce monde de la taille - le monde qui *manque* au Snurpf.

6.3. D_n n'est jamais vide : Goldbach est un énoncé de fenêtrage

Par le CRT, D_n compte toujours

$$\#\{m \bmod P\} \;\geq\; \prod_{3 \leq p \leq \sqrt{n}} (p-2) \;\geq\; 1$$

classes survivantes (pour $n = 98$: 18 classes

$$\{1, 19, 31, 37, 61, 67, 79, 97, 109, 121, 127, 139, 151, 157, 169, 181, 187, 199\},$$

dont les témoins de $[3, 95]$: $19, 31, 37, 61, 67, 79$). De plus D_n est symétrique ($m \in D_n \iff n-m \in D_n$). L'existence de candidats est donc gratuite et infinie ; la conjecture est :

$$\text{Goldbach} \iff D_n \cap [3, n-3] \neq \varnothing$$

(fenêtre doublée par symétrie ; les $m > n$, comme $98 = 109 + (-11)$, sont la zone définitivement perdue ; 97, candidat au bord, a pour miroir $1 < 3$). Toute la conjecture est dans cette intersection - nullement dans la roue, qui est lue et finie.

6.4. La porte

La fenêtre s'écrit avec la fonction de Heaviside θ (le "seuil" des physiciens) : l'indicateur de $[a, b]$, appelé *porte*, est

$$\mathbf{1}_{[a,b]} = \theta(\cdot - a) - \theta(\cdot - b), \qquad A(n) = \sum_m \mathbf{1}_{[3,n-3]}(m)\, \mathbf{1}_{D_n}(m), \qquad \text{Goldbach} : A(n) \geq 1.$$

Le second facteur est profini, périodique, automatique en toute base ; le premier est archimédien, il parle de taille. Le Snurpf ne sait pas où est la fenêtre ; la fenêtre ne sait rien des classes. On a la prédiction heuristique, non démontrée, de Hardy-Littlewood, qui est qu'on s'attend à ce que $A(n) \approx C_2\, n/\log^2 n \gg 1$, mais aucun argument connu ne borne par le bas l'oscillation de cette somme : c'est le même mur, une dernière fois - un monde fini et périodique, une contrainte de taille, et le point de contact à garantir. Formule finale :

Goldbach = l'un des points du Snurpf tombe-t-il dans la fenêtre archimédienne ?

7. Conclusion

L'impossibilité ressentie est réelle et maintenant *nominative* :

- interdiction d'un objet automatique conjoint : **Cobham** (théorème) ;
- rigidité des objets invariants par $\times 2$ et $\times 3$: **Furstenberg** (conjecture, cas entropique : Lyons-Rudolph) ;
- l'objet unique existe ($\widehat{\mathbb{Z}}$) mais est géométriquement muet (Cantor), l'information étant algébrique.

Le mur 2-3 que Denise a rencontré dans les valuations est le même mur que celui de la barrière de parité du crible et que celui de Furstenberg : l'indépendance multiplicative des bases. S'il fallait le franchir pour démontrer Goldbach, ce serait en passant par l'un des plus grands problèmes ouverts de la théorie des nombres multiplicative.