

Snurpf ou plongement de Chistyakov : systèmes de restes, p -adiques, et réalisations euclidiennes

Résumé

On formalise ici deux constructions a priori indépendantes : le système de numération par les restes modulaires (*Snurpf*, ou *Residue Number System* au sens de Knuth) utilisé pour étudier la conjecture de Goldbach, et le plongement explicite de $\mathbb{Q}_p$ dans $\mathbb{C}$ construit par Chistyakov (1996)¹. On montre que ces deux constructions sont deux instances particulières d'un même schéma géométrique : coder un reste modulaire par une direction du plan (racine de l'unité) et combiner ces directions niveau après niveau. Ce schéma unifié explique en particulier pourquoi la représentation graphique du Snurpf par cercles imbriqués réalise, sans le savoir, un plongement du même type que celui de Chistyakov.

1. Le système de numération par les restes (Snurpf)

1.1. Définitions

Définition 1 (Moduli et système de restes). Soit $p_1 < p_2 < \dots < p_K$ une suite finie de nombres premiers deux à deux distincts, et $N = \prod_{k=1}^K p_k$. Le Snurpf associé à cette suite est l'application

$$r : \mathbb{Z}/N\mathbb{Z} \longrightarrow \prod_{k=1}^K \mathbb{Z}/p_k\mathbb{Z}, \quad r(x) = (r_1(x), \dots, r_K(x)), \quad r_k(x) = x \bmod p_k.$$

Proposition 2 (Théorème des restes chinois). L'application r est une bijection (c'est même un isomorphisme d'anneaux). En particulier, la connaissance de tous les $r_k(x)$ détermine x de façon unique dans $\mathbb{Z}/N\mathbb{Z}$.

C'est le *Residue Number System* (RNS) décrit par Knuth (*The Art of Computer Programming*, vol. 2). Contrairement à une écriture positionnelle en base p , les coordonnées $r_k(x)$ ne sont pas hiérarchisées : elles vivent chacune dans leur propre groupe $\mathbb{Z}/p_k\mathbb{Z}$, indépendamment les unes des autres, et c'est le théorème des restes chinois - non un algorithme de division successive - qui permet de reconstruire x .

1.2. Caractérisation des nombres premiers par leurs restes

Proposition 3 (Caractérisation des décomposants de Goldbach de Denise Vella-Chemla², démontrée par Leila Schneps). Soit $n \in \mathbb{N}$ et q un nombre premier tel que $q > \sqrt{n}$. Alors q est un décomposant de Goldbach de n (c'est-à-dire que $n - q$ est aussi premier, potentiellement, selon la formulation retenue) si et seulement si q ne partage aucun reste modulaire avec n , au sens où pour tout nombre premier $p_k \leq \sqrt{n}$, $r_k(q) \neq r_k(n)$.

Cette caractérisation des décomposants de Goldbach est ce qui motive l'introduction du Snurpf : elle permet de reformuler un problème additif (Goldbach) en un problème purement modulaire, exprimable uniquement à l'aide des coordonnées $r_k(\cdot)$.

1. Voir <https://denisevellachemla.eu/trad-Chistyakov-p-adique-vers-euclidien.pdf>.

2. Hardy et Mirsky l'avaient aussi découverte.

Remarque : Un nombre premier q se caractérise lui-même, dans ce système, par le fait que $r_k(q) = 0$ pour exactement une valeur de k (celle pour laquelle $p_k = q$, si q figure dans la liste des moduli), et $r_k(q) \neq 0$ pour tous les autres k tels que $p_k < q$. C’est cette propriété qui permet de voir $\mathcal{P}$, l’ensemble des nombres premiers, comme un ensemble obtenu par élimination successive des multiples de chaque p_k .

1.3. L’ensemble de la castafiore : une réalisation réelle

Définition 4 (Construction par élimination). *On part de l’intervalle $[0, 1]$ ³. Au niveau k , on élimine de chaque intervalle survivant le sous-intervalle central correspondant au reste nul modulo p_k (les multiples de p_k), et on conserve les deux sous-intervalles de part et d’autre, de longueur $t_k = \frac{\prod_{2 \leq p_j \leq p_{k-2}} p_j}{\prod_{2 \leq p_j \leq p_k} p_j}$.*

Cette construction (“l’ensemble de la castafiore”, Vella-Chemla, juin 2025) réalise, sur la droite réelle, une version *binnaire* de l’information portée par $r_k(x)$: à chaque niveau, on ne retient que l’alternative “ $r_k(x) = 0$ ” / “ $r_k(x) \neq 0$ ”, projetée sur un axe unique. L’ensemble limite a la puissance du continu (c’est un ensemble de Cantor au sens topologique), bien qu’il code une information arithmétique (la primalité) plutôt qu’un simple développement en base fixe. On verra en partie 3 que cette construction est l’ombre à une dimension d’un plongement plus riche, à valeurs complexes, qui retient l’intégralité de chaque reste $r_k(x) \in \{0, \dots, p_k - 1\}$ et non sa seule nullité.

2. Le plongement p -adique de Chistyakov

2.1. Nombres p -adiques

Soit p un nombre premier fixé. Tout $x \in \mathbb{Q}_p$ s’écrit de façon unique

$$x = \sum_{n=v}^{\infty} x_n p^n, \quad x_n \in \{0, \dots, p-1\}, \quad v \in \mathbb{Z},$$

la série convergeant pour la norme p -adique $\|x\| = p^{-v(x)}$. On note $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : \|x\| \leq 1\}$ l’anneau des entiers p -adiques, c’est-à-dire les x pour lesquels $v \geq 0$.

Contrairement au Snurpf, les coefficients x_n sont *hiérarchisés* : x_n n’est défini qu’après réduction de x modulo p^{n+1} et soustraction des termes de rang inférieur. C’est une écriture positionnelle en base p , non un système de restes indépendants.

2.2. Les applications de Chistyakov

Définition 5 (Caractères tronqués). *Pour $n \in \mathbb{Z}$ et $m \in \mathbb{N} \cup \{\infty\}$, on pose*

$$\chi_n^{(m)}(x) = \exp\left(2i\pi \sum_{k=0}^m x_{n-k} p^{-k-1}\right), \quad x \in \mathbb{Q}_p.$$

3. voir <https://denisevella chemla.eu/castafiore.pdf>.

Définition 6 (Plongement $\Upsilon_s^{(m)}$). Pour $s \in U_1 = \{z \in \mathbb{C} : |z| < 1\}$ et $m \in \mathbb{N} \cup \{\infty\}$, on définit $\Upsilon_s^{(m)} : \mathbb{Q}_p \rightarrow \mathbb{C}$ par

$$\Upsilon_s^{(m)}(x) = \sum_{n=0}^{\infty} s^n \chi_n^{(m)}(x).$$

2.3. Cas $m = 0$: structure d'IFS

Dans le cas le plus simple $m = 0$, en posant $\zeta_p = e^{2i\pi/p}$,

$$\Upsilon_s^{(0)}(x) = \sum_{n=0}^{\infty} s^n \zeta_p^{x_n}.$$

Proposition 7 (Relation d'échelle). Pour $x = x_0 + px' \in \mathbb{Z}_p$ (avec $x_0 \in \{0, \dots, p-1\}$, $x' \in \mathbb{Z}_p$),

$$\Upsilon_s^{(0)}(x_0 + px') = \zeta_p^{x_0} + s \Upsilon_s^{(0)}(x').$$

Autrement dit, $\Upsilon_s^{(0)}(\mathbb{Z}_p)$ est l'attracteur du système de fonctions itérées (IFS) à p branches

$$f_a(z) = \zeta_p^a + s z, \quad a = 0, \dots, p-1.$$

Théorème 8 (Chistyakov, injectivité). Il existe $s_0 = s_0(p) = \frac{\sin(\pi/p)}{1 + \sin(\pi/p)}$ tel que, pour $|s| < s_0$, l'application $\Upsilon_s^{(m)}$ est un plongement (une L -isométrie de $(\mathbb{Q}_p, |\cdot|_p^{D_s})$ dans $(\mathbb{C}, |\cdot|)$, où $D_s = -\log_p^{-1} |s|$), pour tout m .

[Triangle de Sierpiński] Pour $p = 3$, $s = 1/2$, $\zeta_3 = e^{2i\pi/3}$: les trois applications $f_0(z) = z/2$, $f_1(z) = \zeta_3 + z/2$, $f_2(z) = \zeta_3^2 + z/2$ forment l'IFS canonique du triangle de Sierpiński. (Ici $s = 1/2$ est le cas limite $|s| = s_0$ à un facteur près ; les copies se touchent en des points isolés, sans se chevaucher.)

3. Le pont : du Snurpf vers l'euclidien

3.1. Deux structures de groupe pour un même geste

Les parties 1 et 2 codent chacune un même geste géométrique élémentaire : associer à un reste modulaire une direction du plan, via une racine de l'unité ζ_p^r . Elles diffèrent uniquement par la façon dont les restes s'articulent entre eux :

Chistyakov (p -adique)	Snurpf (RNS)
un seul p , une tour de restes emboîtés $x_n =$ reste au rang n de l'écriture positionnelle	plusieurs p_k distincts, restes indépendants $r_k(x) = x \bmod p_k$
groupe ambiant $\mathbb{Z}_p$	groupe ambiant $\mathbb{Z}/N\mathbb{Z} \cong \varprojlim \mathbb{Z}/p_k\mathbb{Z}$ (restes chinois)

Le cadre commun aux deux est le groupe des entiers profinis $\widehat{\mathbb{Z}} = \varprojlim_N \mathbb{Z}/N\mathbb{Z} \cong \prod_{p \text{ premier}} \mathbb{Z}_p$: le p -adique de Chistyakov en est la projection sur un seul facteur, le Snurpf en est une troncature finie (produit sur $p_1, \dots, p_K$ seulement, et réduction de chaque facteur à $\mathbb{Z}/p_k\mathbb{Z}$ plutôt qu'à $\mathbb{Z}_p$ tout entier).

3.2. Un IFS non autonome commun

Définition 9 (Plongement mélangé). Soit $(p_k)_{k \geq 1}$ une suite de nombres premiers (pas nécessairement tous distincts, ni ordonnée par taille) et $(s_k)_{k \geq 1}$ une suite de paramètres complexes, $|s_k| < 1$. On pose $S_1 = 1$, $S_k = \prod_{j < k} s_j$, et pour x dont on note $r_k(x) = x \bmod p_k$:

$$\Phi\left((r_k(x))_{k \geq 1}\right) = \sum_{k=1}^{\infty} S_k \zeta_{p_k}^{r_k(x)}, \quad \zeta_{p_k} = e^{2i\pi/p_k}.$$

Ce plongement contient les deux cas précédents comme cas particuliers :

- si tous les p_k sont égaux à un même p et tous les $s_k = s$ constants, on retrouve $\Phi = \Upsilon_s^{(0)}$;
- si $(p_1, \dots, p_K)$ sont K nombres premiers distincts et que la somme est tronquée à $k = K$, on obtient un plongement de $\mathbb{Z}/N\mathbb{Z} \cong \prod_{k \leq K} \mathbb{Z}/p_k\mathbb{Z}$ (donc du Snurpf) dans $\mathbb{C}$.

Proposition 10 (Relation d'échelle généralisée). En notant $x = r_1(x)$ modulo p_1 et x' “ce qui reste” après le premier niveau,

$$\Phi_K(x) = \zeta_{p_1}^{r_1(x)} + s_1 \Phi_{K-1}(x').$$

C'est encore la construction d'un cercle de rayon S_k centré en chaque point du cercle de rayon S_{k-1} obtenu au niveau précédent : la même récursivité géométrique que dans la partie 2, désormais avec un nombre de branches et un rayon de contraction qui changent à chaque niveau.

[Condition de séparation niveau par niveau] Si, pour chaque k ,

$$|s_k| < s_0(p_k) = \frac{\sin(\pi/p_k)}{1 + \sin(\pi/p_k)},$$

alors Φ_K est injective sur $\mathbb{Z}/N\mathbb{Z}$ (avec $N = \prod_{k \leq K} p_k$) : deux entiers ayant un tuple de restes différent ont des images distinctes dans $\mathbb{C}$.

Esquisse. La preuve reproduit, niveau par niveau, l'inégalité (21) de Chistyakov : au niveau k , la distance entre deux branches distinctes issues du même point est minorée par $S_k \Delta_{s_k}^{(0)}(p_k) > 0$, tandis que la somme de toutes les contributions des niveaux $k+1, k+2, \dots$ est majorée par $S_k \cdot \frac{2|s_k|}{1-|s_k|}$, strictement plus petite dès que $|s_k| < s_0(p_k)$. Deux points de restes différents au niveau k restent donc séparés après addition des niveaux suivants. $\square$

3.3. Identification avec la construction en cercles imbriqués

La proposition précédente donne une lecture géométrique directe : pour construire $\Phi_K(x)$, on place un point sur le grand cercle de rayon 1 à l'angle $2\pi r_1(x)/p_1$, puis on centre en ce point un cercle de rayon s_1 , sur lequel on place un point à l'angle $2\pi r_2(x)/p_2$, et ainsi de suite jusqu'au niveau K .

C'est exactement la construction déjà réalisée (indépendamment, et avant toute référence à Chistyakov) dans la figure à cercles imbriqués pour les moduli 2, 3, 5, 7 ($N = 210$) : le grand cercle rouge code $r_1(x) = x \bmod 2$, les cercles verts $r_2(x) = x \bmod 3$, les cercles cyan $r_3(x) = x \bmod 5$, et la position finale du point code $r_4(x) = x \bmod 7$. La différence avec Chistyakov n'est donc pas de nature - c'est la même récursivité “un cercle par niveau, un rayon qui rétrécit” - mais de degré : un seul p répété à l'infini d'un côté, une suite finie de p_k distincts de l'autre.

3.4. Retour à la castafiore : ce qui relie, et ce qui ne relie pas

Remarque : [Mise en garde] Il est tentant de présenter la castafiore comme une simple projection de Φ_K sur la droite réelle, obtenue en ne gardant qu'une partie de l'information portée par Φ_K . **Ce n'est pas exact, et il faut se garder de le formuler ainsi.** À chaque niveau k , Φ_K dispose de p_k issues possibles : les p_k racines $\zeta_{p_k}^r$, $r = 0, \dots, p_k - 1$. La castafiore, elle, n'en distingue que deux : reste nul ou reste non nul. Passer de Φ_K à la castafiore n'est donc pas une projection géométrique qui conserverait une trace fidèle de l'information de départ : c'est un *appauvrissement de l'alphabet des restes*, de $\{0, \dots, p_k - 1\}$ à $\{0, \text{non-0}\}$, décidé *avant* toute réalisation géométrique. On ne retrouve pas la castafiore comme cas particulier calculable de Φ_K en projetant simplement ses points sur un axe : il faut changer l'information elle-même en amont.

Remarque : [Ce que ce rapprochement apporte réellement] Rien, sur le plan mathématique. Aucun théorème sur les nombres premiers, sur la conjecture de Goldbach ou sur la caractérisation des décomposants de Goldbach ne se déduit de la mise en correspondance de la castafiore avec Φ_K ; le seul contenu mathématique non trivial de tout ce document reste celui des théorèmes de Chistyakov (partie 2), déjà publiés. Le point commun réel entre le Snurpf, la castafiore et le plongement de Chistyakov se limite au geste initial qu'ils partagent : coder un reste modulaire par une position géométrique (une racine de l'unité) et empiler ces positions niveau après niveau. Formuler ce constat clarifie la nature respective des trois constructions - en particulier le fait que les restes du Snurpf sont indépendants (produit $\prod_k \mathbb{Z}/p_k\mathbb{Z}$) alors que les chiffres p -adiques de Chistyakov sont hiérarchisés (tour $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$) - mais ne constitue pas un résultat, seulement une clarification terminologique et pédagogique.