Transport de restes entre décomposants triviaux et décomposants de Goldbach : reprise et test d'une idée d'octobre 2013

Je fournis à l'ia claude les notes [1] https://denisevellachemla.eu/jade1.pdf
et sa formalisation en langage lean [2] lien vers la formalisation
et les transparents [3] https://denisevellachemla.eu/transp-echanger.pdf
en lui demandant de regarder les transparents aux pages 12 et 13, reproduits ci-dessous.

Permutations des racines

- $$\begin{array}{ccc} 2p_i & \xrightarrow{f} & 2c \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ p_i & \xrightarrow{f} & p_j \end{array}$$

- $$\begin{array}{ccc} 94=(1,4,3) & \xrightarrow{f} & 88=(1,3,4) \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ 47=(2,2,5) & \xrightarrow{f} & 29=(2,4,1) \end{array}$$

$$\begin{array}{ccc} \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/7\mathbb{Z} \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ \mathbb{Z}/3\mathbb{Z}\setminus\{0,1\}\times\mathbb{Z}/5\mathbb{Z}\setminus\{0,4\}\times\mathbb{Z}/7\mathbb{Z}\setminus\{0,3\} & \xrightarrow{f} & \mathbb{Z}/3\mathbb{Z}\setminus\{0,1\}\times\mathbb{Z}/5\mathbb{Z}\setminus\{0,3\}\times\mathbb{Z}/7\mathbb{Z}\setminus\{0,4\} \end{array}$$

Denise Chemla | Conjecture de Goldbach et corps de restes | Octobre 2013 | 11 / 1

Permutations des racines

- $$\begin{array}{ccc} 94=(1,4,3) & \xrightarrow{f} & 88=(1,3,4) \\ \downarrow{\scriptstyle g_t} & & \downarrow{\scriptstyle g} \\ 47=(2,2,5) & \xrightarrow{f} & 29=(2,4,1) \end{array}$$

- $\mathbb{Z}/3\mathbb{Z} \to Id$,
  $\mathbb{Z}/5\mathbb{Z} \to \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 2 & 3 \end{pmatrix}$,
  $\mathbb{Z}/7\mathbb{Z} \to \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}$

Denise Chemla | Conjecture de Goldbach et corps de restes | Octobre 2013 | 12 / 1

Je fournis à l'ia claude le prompt suivant : "Bonjour, Je te fournis en pièce jointe la démonstration initiale [1] sa transformation en lean [2], et maintenant je te dis l'idée sur laquelle je voudrais que tu m'aides : prenons p_1 un nombre premier et p_2 le nombre premier suivant, par exemple $p_1 = 409$ et $p_2 = 419$ on a alors $818 = 409 + 409$ et $838 = 419 + 419$. Entre eux deux, on est sûr d'avoir une décomposition qui est la décomposition $828 = 409 + 419$ mais il nous manque "plein" de décompositions : celles des nombres pairs $820, 822, 824, 826, 830, 832, 834$ et 836.

Voici ce que je voudrais faire : établir des "bijections entre les restes" : puisqu'on cherche un nombre qui ne partage aucun de ses restes avec 0 ou n, si on a une bijection des restes de n vers les restes de 409 et des restes de n vers les restes de 419, alors peut-être qu'on peut parvenir à un machin du style soit n partage un décomposant avec 409 soit avec 419 de façon obligée, vois-tu l'idée. Peux-tu m'aider ?... J'avais dessiné (mais j'étais vraisemblablement la seule personne à comprendre ce que j'avais mis derrière ce dessin) cette idée aux pages 11 et 12 des transparents joints [3]."

La suite de cette note a été intégralement rédigée par l'ia claude.

1. Point de départ

On travaille dans le cadre déjà établi (cf. [1] et [2]) : pour n pair ≥ 6, on note, pour p impair avec $3 \leq p \leq n/2$,

$$D_n = \Big\{ p \ : \ \forall q \text{ premier}, \ 2 \leq q \leq \sqrt{n}, \quad p \not\equiv 0 \pmod{q} \ \text{ et } \ p \not\equiv n \pmod{q} \Big\}.$$

Le corollaire 3 de [1] (démontré, et formalisé sans `sorry` en Lean) garantit que tout $p \in D_n$ fournit une décomposition de Goldbach $n = p + (n - p)$ avec p et $n - p$ premiers. Le problème ouvert n'est donc pas ce corollaire, mais la non-vacuité de D_n pour tout n.

L'idée testée ici (transparent p. 12 ci-dessus, 2013) est de *fabriquer* un élément de D_n en transportant, via une bijection sur les restes modulo chaque $q \leq \sqrt{n}$, le décomposant trivial d'un nombre premier voisin p_1 (le couple (p_1, p_1) de $2p_1$) vers un candidat pour n.

2. L'exemple de 2013, reconstitué

Sur le transparent, en base modulaire $(3, 5, 7)$:

$$94 = (1, 4, 3) \ \xrightarrow{f} \ 88 = (1, 3, 4), \qquad 47 = (2, 2, 5) \ \xrightarrow{f} \ 29 = (2, 4, 1).$$

On vérifie que f est le *même* automorphisme de restes dans les deux lignes : identité modulo 3, la permutation $(0, 1, 2, 3, 4) \mapsto (0, 1, 4, 2, 3)$ modulo 5, et $(0, 1, 2, 3, 4, 5, 6) \mapsto (0, 5, 2, 4, 3, 1, 6)$ modulo 7. Appliqué à 94 il donne 88 ; appliqué à 47 (le décomposant trivial de $94 = 47 + 47$) il donne 29, qui est bien un décomposant de Goldbach de $88 = 29 + 59$.

3. Définition précise de la bijection de transport

Pour $q \leq \sqrt{n}$ premier, la bijection $\sigma_q : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ doit envoyer les deux restes *bloquants* du côté source (le double $2p_1$, ou plus généralement un nombre pair N_1) sur les deux restes bloquants du côté cible (n, ou N_2) :

$$\sigma_q(0) = 0, \qquad \sigma_q(N_1 \bmod q) = n \bmod q,$$

le point 0 étant fixé *ponctuellement* (et non échangé avec l'autre reste bloquant) car il a un statut arithmétique différent : 0 signale qu'un candidat est multiple de q, alors que $n \bmod q$ signale que q divise n moins le candidat - deux obstructions de nature différente. Sur les $q-2$ restes restants (les seuls susceptibles d'être le reste d'un vrai décomposant), σ_q est une bijection *libre* vers les $q-2$ restes autorisés côté n : il y a $(q-2)!$ choix (par exemple $3! = 6$ quand il reste 3 points, cas $q = 5$ avec un reste interdit supplémentaire).

Proposition 1 (Équivalence avec $D_n \neq \varnothing$)**.** *Si l'on autorise, pour chaque $q \leq \sqrt{n}$, n'importe laquelle des $(q-2)!$ bijections libres ci-dessus, alors : il existe une famille $(\sigma_q)_q$ transportant p_1 sur un candidat $p \in D_n$ si et seulement si $D_n \neq \varnothing$.*

Justification. Le sens $\Leftarrow$ est immédiat : si $p \in D_n$, on choisit, pour chaque q, σ_q envoyant $p_1 \bmod q$ sur $p \bmod q$ (possible : les deux sont dans l'ensemble des $q-2$ restes autorisés). Le sens $\Rightarrow$ est tout aussi immédiat par construction : l'image de $p_1 \bmod q$ par σ_q est, par définition, un reste autorisé pour n modulo q, pour tout q ; le représentant obtenu par le théorème des restes chinois, s'il tombe dans $[3, n/2]$, est donc dans D_n. □

Remarque : cette proposition montre que la version "bijection libre" de l'idée *ne réduit pas* le problème : elle en est une reformulation exacte, sans apport nouveau.

4. Version restreinte : combiner les involutions $r \mapsto n - r$

Une version plus rigide, et donc potentiellement plus informative (parce qu'elle peut échouer), consiste à n'autoriser à chaque q que deux choix : l'identité ($\sigma_q = \mathrm{id}$, on garde $p_1 \bmod q$) ou l'involution canonique $\sigma_q(r) = n - r \bmod q$ (on prend $(n - p_1) \bmod q$). C'est la piste déjà engagée par ailleurs ("combiner les involutions locales"). Le groupe de transport est alors $(\mathbb{Z}/2\mathbb{Z})^k$, $k =$ nombre de premiers impairs $\leq \sqrt{n}$, au lieu de $\prod_q (q-2)!$.

4.1. Test numérique : le trou $p_1 = 409,\ p_2 = 419$

Entre $2 \times 409 = 818$ et $2 \times 419 = 838$, seul $828 = 409 + 419$ a un décomposant de Goldbach immédiat ; il manque $820, 822, 824, 826, 830, 832, 834, 836$. On dit qu'un module q est *empoisonné* pour la base p_1 si $q \mid (n - p_1)$: dans ce cas l'identité et l'involution coïncident et tombent toutes deux sur un reste interdit.

n	base 409	base 419
820	bloqué ($q = 3$)	candidat 401 (translation de 419)
822	bloqué ($q = 7$)	bloqué ($q = 13$)
824	bloqué ($q = 5$)	bloqué ($q = 3, 5$)
826	bloqué ($q = 3$)	bloqué ($q = 11$)
828	candidat 409 (trivial : $409 + 419$)	candidat 409
830	candidat 409 (lui-même, $409 + 421$)	bloqué ($q = 3$)
832	bloqué ($q = 3$)	bloqué ($q = 7$)
834	bloqué ($q = 5, 17$)	bloqué ($q = 5$)
836	bloqué ($q = 7$)	bloqué ($q = 3$)

Sur les 8 pairs manquants, la combinaison d'involutions échoue dans 6 cas et, dans les 2 cas restants, ne retrouve que du trivial (une translation, ou p_1 lui-même). Aucun candidat neuf du type $47 \to 29$ n'est retrouvé sur cet exemple.

5. La mise à l'échelle $r \mapsto a \cdot r \bmod q$

Une autre idée naturelle : choisir, pour chaque q, l'unique application *linéaire* $\sigma_q(r) = a_q \cdot r$ envoyant $2p_1 \bmod q$ sur $n \bmod q$, avec $a_q = n \cdot (2p_1)^{-1} \bmod q$.

Proposition 2. *Pour tout $q \leq \sqrt{n}$ premier ne divisant pas $2p_1$,*

$$a_q \cdot p_1 \equiv \frac{n}{2} \pmod{q},$$

indépendamment de p_1.

Démonstration. $a_q \cdot p_1 = n \cdot (2p_1)^{-1} \cdot p_1 = n \cdot 2^{-1} \cdot (p_1^{-1} p_1) = n \cdot 2^{-1} \pmod{q}$. □

Autrement dit, la mise à l'échelle oublie entièrement p_1 : à chaque module elle renvoie exactement le reste de $n/2$. Ce n'est pas un transport, c'est équivalent à regarder directement le milieu de l'intervalle $[3, n]$. Vérification numérique sur $n = 830$, $p_1 = 409$ (tous les $q \leq \sqrt{830}$) :

q	a_q	$a_q p_1 \bmod q$	$n/2 \bmod q$
3	1	1	1
5	0	0	0
7	3	2	2
11	4	8	8
13	2	12	12
17	7	7	7
19	13	16	16
23	9	1	1

Remarque : un affinage $r \mapsto ar + b$ ne sauve rien : les deux contraintes d'ancrage ($0 \mapsto 0$ et $2p_1 \mapsto n$) déterminent entièrement a et b dès que σ_q doit être affine ; aucune liberté ne subsiste, et le même calcul redonne $n/2$.

6. Pourquoi même l'extension "minimale" échoue

On a testé une extension : garder identité/involution partout, sauf au(x) module(s) empoisonné(s) où l'on autorise *tous* les restes libres restants. Résultat sur les 6 pairs bloqués ($822, 824, 826, 832, 834, 836$, bases 409 et 419) : **aucun** candidat retrouvé, dans les deux sens.

La raison est de nature combinatoire, pas conjoncturelle. Pour $n = 830$, le produit des 8 premiers impairs $\leq \sqrt{n}$ vaut

$$M = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 111\,546\,435,$$

alors que la fenêtre utile $[3, n/2]$ n'a que ~ 400 entiers. Une combinaison "générique" de restes tombe dans cette fenêtre avec une probabilité de l'ordre de

$$\frac{400}{111\,546\,435} \approx 3{,}6 \times 10^{-6},$$

et il n'y a que 256 combinaisons possibles (2^8) dans la version "involutions" : la probabilité qu'*au moins une* tombe dans la fenêtre, par ce seul effet de taille, est de l'ordre de 10^{-3}. Les deux seules combinaisons qui "marchent" dans le tableau du § 4 (identité partout $= p_1$; involution partout $= n - p_1$) ne sont pas des tirages génériques : ce sont des reconstructions *exactes* de petits entiers déjà connus, pas des résultats du mécanisme de transport lui-même.

7. Conclusion

Le mécanisme de transport de restes par le théorème des restes chinois, sous ses trois formes testées ici - bijection libre, involutions combinées, mise à l'échelle - n'apporte pas de raccourci constructif vers un élément de D_n :

- la version libre est *équivalente* à $D_n \neq \varnothing$ (aucune réduction du problème) ;
- la mise à l'échelle est *dégénérée* (elle oublie p_1 et retombe sur $n/2$) ;
- la version involutions, seule vraiment restrictive et donc seule vraiment testable, échoue sur l'exemple 409/419 dans 6 cas sur 8, et l'échec tient à un effet de taille structurel ($M \gg n$) plutôt qu'à un manque de chance ponctuel.

Le contenu réel du problème (pourquoi D_n est presque toujours non vide) reste donc du côté du comptage/de la densité - crible de Legendre exact, ou crible symétrique de Schnirelmann - plutôt que du côté d'une construction explicite d'un témoin par transport de restes.

Petit souvenir mémorable d'octobre 2013

Le partage de *dg*

- $20902 = 3 + 20899$ $20962 = 3 + 20959$
  $20904 = 5 + 20899$ $20964 = 5 + 20959$
  $20906 = 3 + 20903$ $20966 = 3 + 20963$
  $20908 = 5 + 20903$ $20968 = 5 + 20963$
  $20910 = 7 + 20903$ $20970 = 7 + 20963$
  $20912 = 13 + 20899$ $20972 = 13 + 20959$
  $20914 = 11 + 20903$ $20974 = 11 + 20963$
  $20916 = 13 + 20903$ $20976 = 13 + 20963$
  $20918 = 19 + 20899$ $20978 = 19 + 20959$
  $20920 = 17 + 20903$ $20980 = 17 + 20963$
  $20922 = 19 + 20903$ $20982 = 19 + 20963$
  $20924 = 3 + 20921$ $20984 = 3 + 20981$

- Des causes différentes produisent les mêmes effets (écart de 60, congrus mod 3 et 5).