Polytopes et décomposants de Goldbach

Denise Vella-Chemla

mars 2023

Dans [1], on a caractérisé les décomposants de Goldbach de n (un nombre pair ≥ 6) supérieurs à $\sqrt{n}$[1] et $\leq n/2$.

Ils ne sont[2] :

1) pas $\equiv 0 \pmod{p_k}$ $\quad \forall p_k$ un nombre premier $\leq \sqrt{n}$ (cette première propriété en fait des nombres premiers) ;

2) pas $\equiv n \pmod{p_k}$ $\quad \forall p_k$ un nombre premier $\leq \sqrt{n}$ (cette seconde propriété en fait des nombres (appelons-les x) dont le complémentaire à n (i.e. $n-x$) est premier) ;

Pour avoir une appréhension géométrique de l'existence de décompositions de Goldbach pour n un nombre pair ≥ 6, on a l'idée de les placer dans un polytope entier de $\mathbb{R}_+^d$ avec $d = \lfloor\sqrt{n}\rfloor$. Un polytope est un polyèdre convexe borné, i.e. un sous-ensemble de $\mathbb{R}_+^d$ qui est l'intersection d'un nombre fini de demi-espaces fermés.

Ce polytope est de taille

$$\prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \lfloor\sqrt{n}\rfloor}} p_k.$$

On gradue ce polytope par un réseau de Minkowski de points entiers. Chaque direction du polytope correspond à un certain nombre premier $p_k \leq \sqrt{n}$. Les coordonnées possibles selon le nombre premier p_k (selon la direction correspondant à ce nombre premier) sont comprises entre 0 et $p_k - 1$. Un nombre est positionné à l'intersection de différentes droites en fonction de son appartenance aux différentes classes modulaires selon les nombres premiers inférieurs à sa racine. Sur un réseau à 3 dimensions[3], le nombre 40 sera positionné sur le point (0,1,0) (il a pour reste 0 quand on le divise par 2, il a pour reste 1 quand on le divise par 3, et il a pour reste 0 quand on le divise par 5). C'est le théorème des restes chinois qui permet de retrouver les nombres associés à un point du réseau de Minkowski graduant le polytope.

Ci-dessous, le réseau des nombres entiers ≤ 40, positionnés aux différents croisements du réseau de Minkowski dans un polytope de dimension 2, les dimensions correspondant aux nombres premiers

[1] dans toute la suite de cette note, l'expression "décomposant de Goldbach de n" sera à lire "décomposant de Goldbach de n supérieur à $\sqrt{n}$".

[2] Donnons un exemple simple pour illustrer la deuxième condition, selon le nombre premier 3 : si n est de la forme $3k+1$, un décomposant de Goldbach x de n (supérieur à $\sqrt{n}$) sera obligatoirement de la forme $3k+2$ (car si et x et n sont de la forme $3k+1$ tous les deux, leur différence est un $3k$ et donc $n-x$ est composé ; et inversement ; tandis que si n est de la forme $3k$, un décomposant de Goldbach de n peut être de l'une ou l'autre des deux formes $3k+1$ ou $3k+2$. En généralisant, si n est de la forme mp_k avec p_k un nombre premier, un décomposant de Goldbach de n peut être de toutes les formes possibles $np_k + i$ avec $1 \leq i \leq p_k - 1$ tandis que si n est de la forme $np_k + i$, un décomposant de Goldbach de n supérieur à $\sqrt{n}$ ne peut être que d'une des formes $mp_k + j$ avec $j \neq i$.

[3] Dans l'illustration ci-après, bien qu'il y ait 3 nombres premiers 2,3 et 5 qui soient $\leq \sqrt{40}$, on a "mélangé" dans le réseau plan les nombres pairs et les nombres impairs, même si, idéalement, ils devraient appartenir à deux sous-espaces différents.

3 et 5, et de taille 3×5 (on a projeté les pairs et les impairs d'un réseau de dimension 3 "au même étage") :

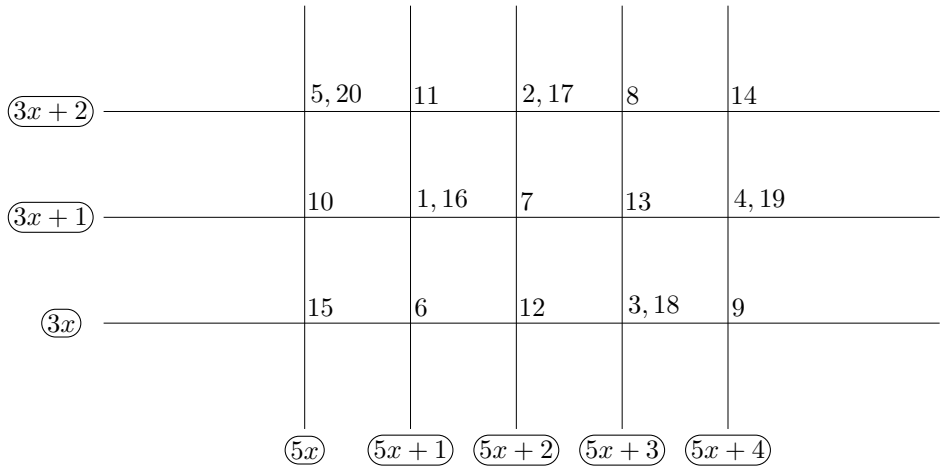


Figure 1 : positionnement des nombres dans le réseau de Minkowski
inclus dans le polytope de taille 3×5
pour illustrer la recherche des décomposants de Goldbach de 40

Les opérations 1) et 2) ci-dessus de criblage des nombres pour trouver de potentiels décomposants de Goldbach de n vont correspondre aux opérations géométriques ci-dessous, à effectuer dans le polytope :

1) les "divisibles" par un nombre premier quelconque sont sur les hyperplans bords[4] du polytope (cela correspond à la nullité de l'une de leur coordonnée) ;

2) les "congrus à n" selon un nombre premier quelconque sont éliminés en supprimant tout un hyperplan de l'espace ; par exemple l'hyperplan $x_3 = 2$ éliminera tous les nombres de reste 2 lorsqu'on les divise par $p_3 = 5$, si on appelle x_3 la coordonnée selon le nombre premier 5 ;

On symbolise sur le réseau l'élimination des hyperplans "nuls" (opération 1) par deux droites "au bord" et l'élimination des "congrus à 40" (opération 2) par une droite correspondant à un plan vertical, éliminant les $x_2 = 1$ (correspondant à $x \equiv 1 \pmod{p_2 = 3}$). Pour le nombre premier 5 qui divise 40, l'hyperplan bord et l'hyperplan $\equiv n \pmod 5$ sont confondus. On prend une même couleur pour des hyperplans parallèles (ici rouge pour le module 3 et bleu pour le module 5).

[4]En fait, il n'y a pas de bords, l'espace est un tore multi-dimensionnel (produit de cercles complexes sur lesquels sont positionnées les unités de la forme $e^{2i\pi m/p_k}$ avec m variant de 0 à $p_k - 1$) ; on peut aussi voir cet espace comme le produit cartésien des corps premiers $\mathbb{Z}/p_k\mathbb{Z}$, mais on se place dans $\mathbb{R}_+^d$ pour rendre l'exposé plus simple.

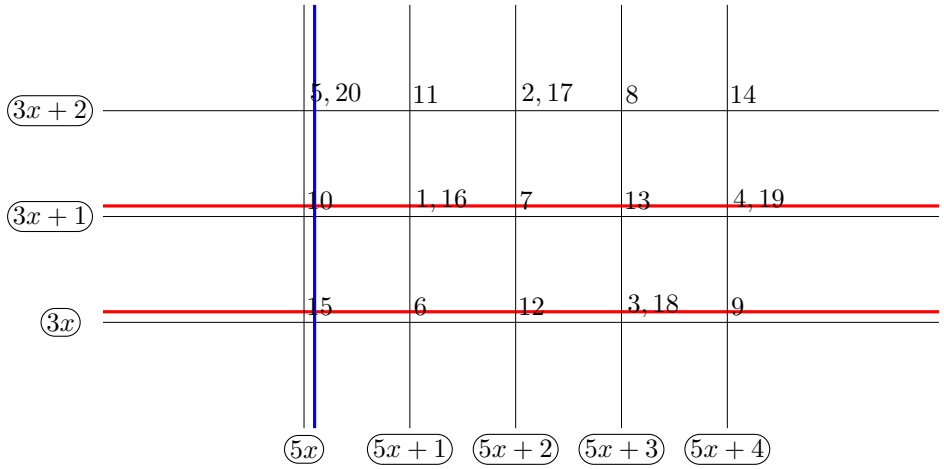


Figure 2 : positionnement des nombres dans le réseau de Minkowski
inclus dans le polytope de taille 3×5
pour illustrer la recherche des décomposants de Goldbach de 40

Cette modélisation étant choisie, quel problème géométrique se pose à nous qui pourrait empêcher l'existence d'un décomposant de Goldbach ?

D'abord, on voit qu'on se situe dans un espace bien plus grand que l'espace souhaité : on a dans le polytope tous les nombres de 1 à $\prod_{\substack{p_k \text{ premier} \\ 3 \leq p_k \leq \lfloor \sqrt{n} \rfloor}} p_k$. Or notre caractérisation d'un décomposant de Goldbach par [1] nécessite que ce nombre soit compris entre $\sqrt{n}$ et $n/2$.

Pour essayer de comprendre un peu mieux ce qui se passe, la première question à laquelle on doit répondre est : combien de croisements du réseau reste-t-il qui n'ont pas été éliminés une fois qu'on a éliminé les hyperplans contenant l'origine ainsi que les hyperplans contenant n ?

Il en reste :

(1)
$$\prod_{\substack{p_k \text{ premier} \\ 3 \leq p_k \leq \lfloor \sqrt{n} \rfloor \\ p \nmid n}} (p_k - 2) \times \prod_{\substack{p_k \text{ premier} \\ 3 \leq p_k \leq \lfloor \sqrt{n} \rfloor \\ p \mid n}} (p_k - 1)$$

Pour s'en convaincre, on peut analyser la grille de recherche des décomposants de Goldbach de 98 ci-après, ou relire la note de bas de page n° 2 de la page 1 :

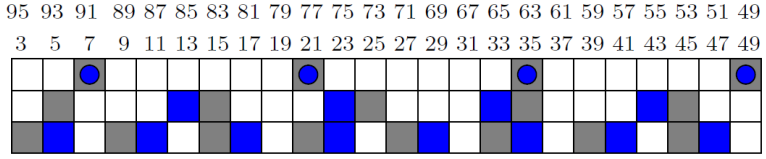


Figure 3 : visualisation des décomposants de Goldbach de $n = 98$. Les nombres ont été notés au-dessus de la grille. Seules les colonnes des nombres 19, 31 et 37 ne contiennent aucune case colorée. La ligne en bas de la grille montre la divisibilité par 3 (en gris, celle des nombres $\leq n/2$, en bleu, celle des nombres $\geq n/2$) ; la ligne médiane correspond à la divisibilité par 5 et la ligne en haut de la grille correspond à la divisibilité par 7.

Remarquons bien dans la visualisation par grille ci-dessus que comme le nombre premier 7 divise 98, les cases bleues et grises coïncident dans la ligne du haut : on élimine **un** nombre tous les $p_k = 7$ nombres dans la ligne du haut. Dans les deux autres lignes, on élimine **deux** nombres sur $p_k = 3$ ou bien 2 nombres sur $p_k = 5$ respectivement. On résumera cette idée par la phrase "Parmi les nombres premiers inférieurs ou égaux à $\sqrt{n}$, les nombres premiers intervenant dans la décomposition en facteurs premiers de n font éliminer moins de nombres que les autres nombres premiers.".

Revenons à la modélisation géométrique. On se pose le problème de l'existence d'un point "non éliminé" par tous les plans de coupe. La formule (1) bien comprise nous indique qu'il y a deux plans de coupe (le plan bord, contenant 0, et le plan contenant n) selon tout nombre premier ne divisant pas n, tandis qu'il n'y a qu'un seul plan de coupe pour les diviseurs de n (les deux plans de coupe de 0 et de n sont alors confondus).

Pour garantir l'existence d'un point au moins, on va montrer qu'on peut toujours trouver un petit carré composé de 4 mailles du réseau, qui ne sont touchées par aucun plan de coupe, ce qui garantit l'existence d'un point au croisement central de ces 4 carrés qui n'appartient à aucun plan de coupe, i.e. qui n'est pas éliminé par les hyperplans de coupe.

On cherche le carré de 4 mailles en question dans une projection plane de l'ensemble des points non éliminés :

- si n est de la forme $6p_mk$, seuls les hyperplans aux 2 bords sont éliminés sur le plan de taille $3 \times p_m$ avec $p_m > 3$, et on dispose donc d'un carré assez grand pour contenir un petit carré de 2×2 mailles du réseau, qui contient en son centre un point non éliminé par les coupes ;

- si n est de la forme $2p_mp_nk$, seuls les hyperplans aux 2 bords sont éliminés sur le plan de taille $p_m \times p_n$ avec $p_m \geq 3$ et $p_n \geq 3$, et on dispose donc d'un carré assez grand de 2×2 mailles du réseau, qui contient en son centre un point non éliminé par les coupes ;

- si n est de la forme $2p_m$, n vérifie trivialement la conjecture de Goldbach, on n'a pas besoin de se préoccuper de ce cas ;

- si n est de la forme $2p_m^k$, on ne sait pas quoi faire...

En admettant que l'existence d'un point au moins puisse être assurée selon le raisonnement présenté ci-dessus, on est confronté à un autre problème : le point dont on a pu prouver l'existence pourrait ne pas être compris entre $\sqrt{n}$ et $n/2$. Il nous faudrait être capable de garantir, plutôt que l'existence d'un seul point, l'existence d'une chaîne complète non coupée de points successifs en progression arithmétique, cette chaîne devant être assez longue pour contenir un point au moins qui soit compris entre $\sqrt{n}$ et $n/2$.

Dit autrement, on comprend bien que les "hyperplans de coupe" font perdre la propriété de convexité de l'ensemble des points intérieurs du réseau de Minkowski, alors que cette propriété de convexité des parties "entre" les plans de coupe, en apportant l'existence de chaînes de nombres successifs en progression arithmétique suffisamment longues, pourrait nous garantir de trouver un nombre aussi petit que désiré (i.e. $\leq n/2$).

Étudions deux directions de coupe et combinons-les pour comprendre plus précisément encore le processus de criblage par élimination d'hyperplans : dans la direction correspondant au nombre premier 5, on a 5 droites possibles, correspondant aux $5k$, aux $5k+1$, aux $5k+2$, aux $5k+3$, aux $5k+4$.

Si 5 divise n, on n'aura que l'hyperplan bord (contenant l'origine) à éliminer. On aura alors 4 points du réseau successifs qui seront restés contigus (non séparés par un plan de coupe) selon la direction 5.

Si 5 ne divise pas n, on aura l'hyperplan bord à éliminer ainsi que l'un des autres hyperplans. On se retrouvera alors soit avec 3 points non séparés par le plan de coupe, le plan de coupe étant collé au plan bord (nombres $5k+1$) ou opposé au plan bord (nombres $5k+4$) , soit avec 1 point tout seul et 2 points contigus de part et d'autre du plan de coupe (plan de coupe $5k+2$), soit l'inverse (plan de coupe $5k+3$). Modulo 7, un raisonnement similaire amène aux contiguités possibles de points non séparés par des plans de coupe suivantes 6, 5, 4+1 ou 1+4 et 2+3 ou 3+2.

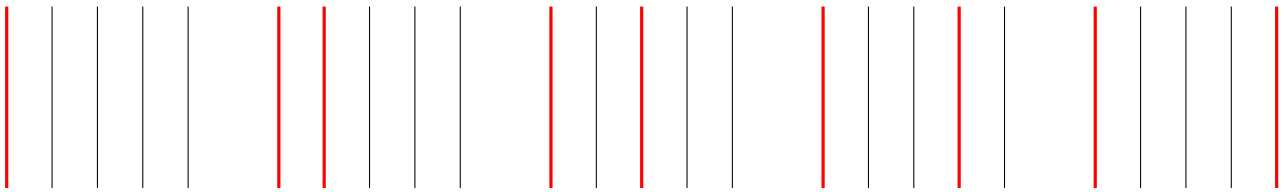


Figure 4 : les 5 positions possibles pour les 2 hyperplans (éventuellement confondus) $x \equiv 0 \pmod 5$ et $x \equiv n \pmod 5$; ils sont colorés en rouge.

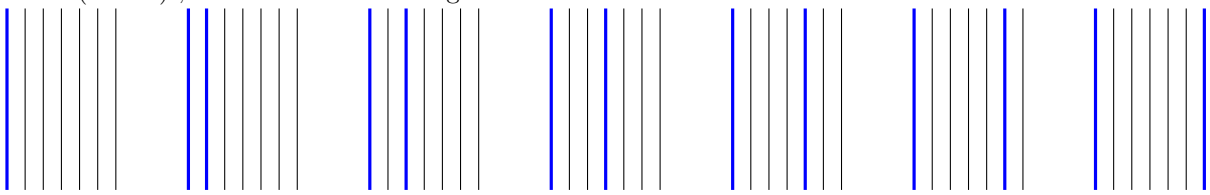
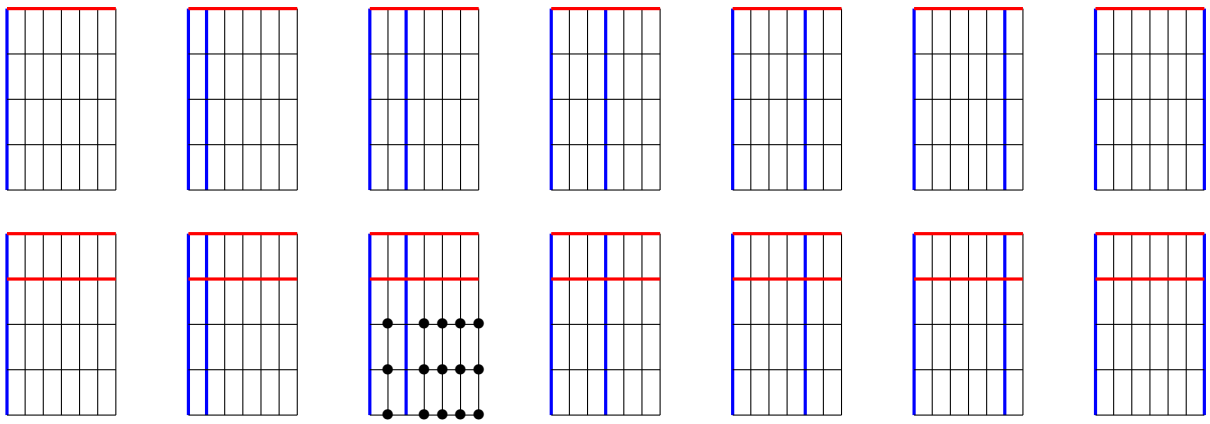


Figure 5 : les 7 positions possibles pour les 2 hyperplans (éventuellement confondus) $x \equiv 0 \pmod 7$ et $x \equiv n \pmod 7$; ils sont colorés en bleu.

En combinant les possibilités pour les plans de coupe selon 5 et 7 ci-dessus, on obtient 35 possibilités de "rectangles" modulo 5 et 7 dont les contiguités sont notées ci-dessous. Pour ne pas surcharger les dessins, pour deux grilles seulement, on a noté par des symboles • les points qui ne sont pas éliminés par les plans de coupe.



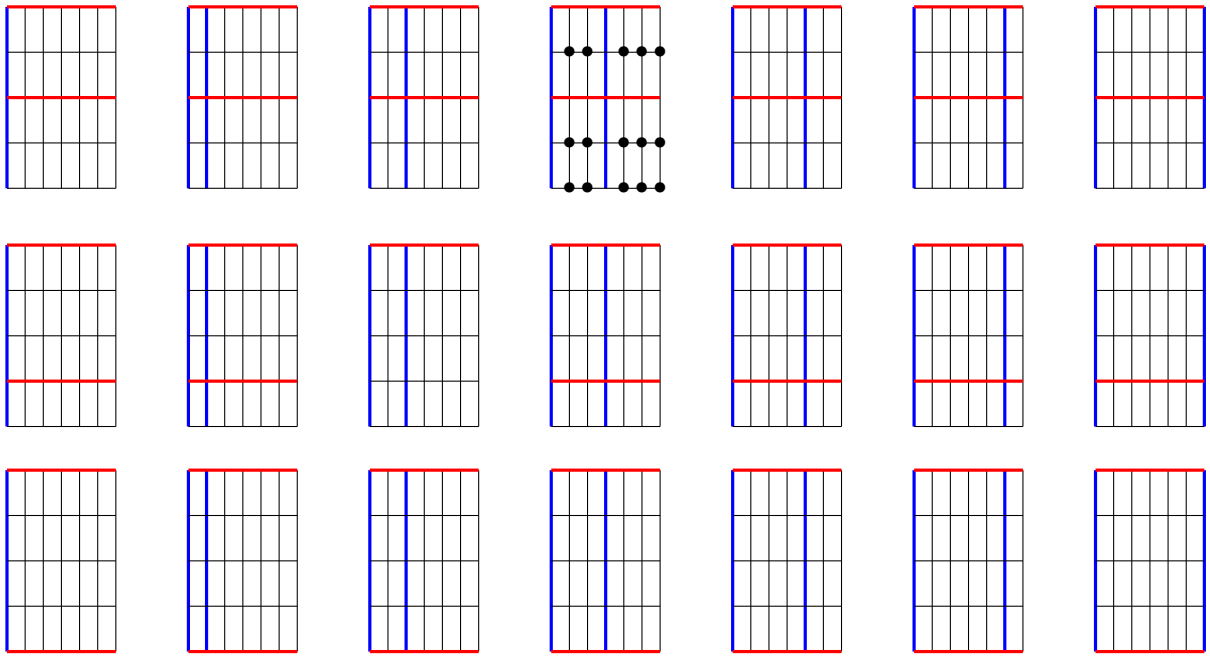


Figure 6 : les 35 positions possibles pour les hyperplans modulo 5 et 7.

On comprend à l'étude de ces cas particulier que les chaînes de longueur les plus grandes possibles, contenant des nombres non séparés par des plans de coupe, vont se trouver sur les rectangles de dimension les 2 plus grands diviseurs de n. En effet, pour les diviseurs en question, le seul hyperplan coupé est celui contenant l'origine et donc une chaîne de nombres "non séparés" d'un tel plan est au moins de longueur $\max\{p_k \text{ tel que } p_k|n\} - 1$.

On comprend également que, selon la direction d'un nombre premier p_k, dans les rectangles dont l'un des côtés est de longueur p_k, quel que soit la position du plan de coupe contenant n (i.e. que ce plan de coupe supprime les nombres de reste modulaire 1, 2, ..., ou $p_k - 1$ modulo p_k), on aura, d'un côté ou de l'autre de ce plan de coupe, des chaînes de longueur $\dfrac{p_k - 1}{2}$ dont la longueur sera maximum sur le rectangle considéré.

On ne sait pas pourquoi une telle longueur pourrait permettre de forcément atteindre un nombre compris entre 3 et $n/2$, qui est l'intervalle que l'on vise pour trouver un décomposant de Goldbach.

Référence

[1] Denise Vella-Chemla, Réécrire, 2019, http://denisevellachemla.eu/jade1.pdf.