Conjecture de Goldbach et descente infinie (Denise Vella-Chemla, 12.04.2021)

1. Descente infinie

On fournit ici une sorte de “démonstration idéale” de la conjecture de Goldbach, dont on souhaiterait qu’elle soit juste, et qui s’inspirerait de la démonstration d’Euclide de l’infinitude de l’ensemble des nombres premiers mais irait “en descendant infiniment” d’un nombre au suivant, plutôt qu’“en montant”, et utiliserait pour ce faire l’idée de descente infinie de Fermat.

Dans la seconde section est fournie une démonstration qui caractérise les nombres premiers compris entre $\sqrt{n}$ et $n/2$ qui sont des décomposants de Goldbach de n, i.e. les nombres premiers dont le complément à n est premier également, n étant un nombre entier pair supérieur ou égal à 6.

On a, par définition, que n un entier pair $\geqslant 6$ vérifie la conjecture de Goldbach si et seulement si $\exists p$ tel que p est un décomposant de Goldbach de n.

Or $p \leqslant n/2$ est un décomposant de Goldbach de n si ~~et seulement si~~ [1] p est premier et $\forall q$, q premier et $q \leqslant \sqrt{n} \implies p \not\equiv n \ (mod\ q)$.

On aimerait démontrer qu’il est impossible, pour tout n pair $\geqslant 6$, que n ne vérifie pas la conjecture de Goldbach. Or *“n ne vérifie pas la conjecture de Goldbach”* est équivalent à

$$\forall p \text{ premier} \leqslant n/2, \exists q \text{ premier} \leqslant \sqrt{n} \text{ tel que } p \equiv n \ (mod\ q).$$

En effet, la condition $\exists q$ premier $\leqslant \sqrt{n}$ tel que $p \equiv n \ (mod\ q)$ rend $n-p$ composé alors que $n-p$ doit être premier pour que $p+(n-p)$ soit une décomposition de Goldbach de n quand p est premier.

La descente infinie va consister à dire que si n ne vérifie pas la conjecture de Goldbach, alors en soustrayant à n le produit de tous les nombres premiers $\leqslant \sqrt{n}$, on obtiendra un nombre strictement plus petit que n, qui appartient aux mêmes classes de congruences de n, et qui donc ne vérifiera pas la conjecture de Goldbach non plus.

En effet, si n ne vérifie pas la conjecture de Goldbach, alors le nombre $n - \prod\limits_{\substack{q_k\ premier \\ 2 \leqslant q_k \leqslant \sqrt{n}}} q_k$ ne vérifie pas la conjecture de Goldbach non plus car $\forall q_k$ compris entre 2 et $\sqrt{n}$, $n - \prod q_k \equiv n \ (mod\ q_k)$: on a soustrait à n un multiple de chaque q_k (puisque $\prod q_k$ est un multiple de chacun des q_k), le nombre obtenu par cette soustraction “conserve” [2] toutes les classes de congruence (mod chacun des q_k) de n et donc, puisqu’on a $\exists q_k$ tel que $p \equiv n \ (mod\ q_k)$ (par non-vérification de la conjecture de Goldbach par n), on a $\exists q_k$ tel que $p \equiv n - \prod q_k \ (mod\ q_k)$ (qui correspond à la non-vérification de la conjecture de Goldbach par le nombre $n - \prod q_k$ qui est un nombre strictement plus petit que n).

C’est un raisonnement en quelque sorte inverse de celui d’Euclide dans lequel on considère une primorielle (un produit de nombres premiers) à laquelle on ajoute 1, pour que le nombre résultant, au contraire de ce qui est présenté ici, ne se voit partager aucune classe de congruence avec chaque module premier considéré isolément.

Il est vraisemblable que le raisonnement proposé ici ne puisse cependant être utilisé car, contrairement à l’argument traditionnel de la descente infinie de Fermat qui est que l’on ne peut avoir de suite infinie décroissante d’entiers parce qu’on “bute sur zéro” (pour le dire rapidement), dans le raisonnement proposé ici, on peut potentiellement “sauter zéro” par les soustractions successives de primorielles car la notion de congruence, définie par Gauss, travaille dans $\mathbb{Z}$ et non dans $\mathbb{N}$.

1. gloups, erreur corrigée le 19.12.2021, j’ai dû écrire ce $\iff$ plusieurs fois par inadvertance : l’idée de l’incongruence à 0 et au reste de n selon tout module premier inférieur ou égal à $\sqrt{n}$ ne permet pas de trouver les “petits” premiers, congrus à 0 selon eux-mêmes (i.e. divisibles par eux-mêmes).
2. ou bien *partage les mêmes classes de congruences* ou encore *appartient aux mêmes classes de congruence.*

2. Caractérisation des décomposants de Goldbach de n supérieurs à $\sqrt{n}$ [3]

Soit $n \in 2\mathbb{N}+6$ un entier pair supérieur à 6. Pour tout $p \in \mathbb{P}^*$ premier impair inférieur à < $\sqrt{n}$ (*i.e.* $3 \leq p \leq \sqrt{n}$), on définit l'ensemble :

$$F_n(p) = \{m \in 2\mathbb{N}+1 : 3 \leq m \leq n/2,\ m \not\equiv 0\ [p],\ m \not\equiv n\ [p]\}$$

L'intersection des ensembles $F_n(p)$ pour tout p premier compris entre 3 et $\sqrt{n}$ est notée :

$$D_n = \bigcap_{\substack{p \in \mathbb{P} \\ 3 \leq p \leq \sqrt{n}}} F_n(p)$$

Nous allons montrer que D_n et son complémentaire $n - D_n$ ne contiennent que des nombres premiers.
Lemme 1 : Soit $m \in 2\mathbb{N}+1$ un entier impair. Si m n'est divisible par aucun nombre premier compris entre 3 et $\sqrt{m}$, alors il est premier.

Démonstration : Si m est composé, on a $m = pq$, o< p est le plus petit nombre premier intervenant dans la factorisation de m en nombres premiers et où< q est le produit de tous les autres facteurs. Puisque m est impair, $p \geq 3$, et puisque $q \geq p$ (q étant le produit d'entiers $\geq p$), $m = pq \geq pp = p^2$ et donc $\sqrt{m} \geq p$ (la fonction racine carrée étant croissante). On a ainsi montré que si m impair est composé, il est divisible par un premier compris entre 3 et $\sqrt{m}$. Le lemme s'obtient par contraposition. □

Lemme 2 : $D_n \subseteq \mathbb{P}$.

Démonstration : Soit $m \in D_n$. Alors $m \in F_n(p)$ pour tout p premier compris entre 3 et $\sqrt{n}$. Par conséquent, m est impair et m n'est divisible par aucun nombre premier p compris entre 3 et $\sqrt{n}$ (puisque $m \not\equiv 0\ [p]$), et donc *a fortiori* par aucun premier compris entre 3 et $\sqrt{m}$ (car $m \leq n/2 \implies m \leq n \implies \sqrt{m} \leq \sqrt{n}$). D'après le lemme 1, m est donc premier. □

Lemme 3 : $n - D_n \subseteq \mathbb{P}$.

Démonstration : Soit $m \in D_n$. Alors $m \in F_n(p)$ pour tout p premier compris entre 3 et $\sqrt{n}$. Par conséquent, $n - m$ est impair (car m est impair et n pair) et $n - m$ n'est divisible par aucun nombre premier p compris entre 3 et $\sqrt{n}$ (puisque $m \not\equiv n\ [p]$), et donc *a fortiori* par aucun premier compris entre 3 et $\sqrt{n-m}$ (car $n - m \leq n \implies \sqrt{n-m} \leq \sqrt{n}$). D'après le lemme 1, $n - m$ est donc premier. □

Les ensembles D_n ne contiennent que des décomposants de Goldbach de n.

Lemme 4 : Soit $n \in 2\mathbb{N}+6$. Si $D_n \neq \varnothing$, alors n vérifie la conjecture de Goldbach.

Démonstration : Si $D_n \neq \varnothing$, il contient un entier p nécessairement premier (d'après le lemme 1), tel que $q = n - p$ est également premier (d'après le lemme 2), et donc $n = p + q$ vérifie la conjecture de Goldbach.

3. Leila Schneps d'abord, Jacques Chemla ensuite, ont réécrit cette partie.