Division euclidienne et conjecture de Goldbach

Denise Chemla

10 août 2013

On n'expliquera pas ici l'argument *"évident pour tout arithméticien"* : étant donné $2n$ un nombre pair, un nombre premier impair p inférieur ou égal à n qui ne partage aucun de ses restes avec $2n$ dans les divisions euclidiennes de diviseurs q inférieurs à $\sqrt{2n}$ est un décomposant de Goldbach de $2n$.

Exemple : on cherche un décomposant de Goldbach du nombre pair 98. 98 a pour reste 0 quand on le divise par 2, 2 quand on le divise par 3, 3 quand on le divise par 5 et 0 quand on le divise par 7.

19, qui est inférieur à $49 = \frac{98}{2}$, et qui a pour reste 1 quand on le divise par 2, 1 quand on le divise par 3, 4 quand on le divise par 5 et 5 quand on le divise par 7, ne partage aucun de ses restes avec 98.

19 est donc un décomposant de Goldbach de 98. En effet, $98 = 19 + 79$ et 79 est un nombre premier, comme l'est 19.

Une manière de démontrer la conjecture de Goldbach consiste donc à comprendre pourquoi un tel nombre premier impair, inférieur ou égal à n, et qui ne partage aucun de ses restes (dans les divisions euclidiennes etc...) avec le nombre pair que l'on cherche à décomposer, existe toujours.

Pour démontrer cela, on cherche à démontrer qu'il n'est pas possible que *tous* les nombres premiers impairs inférieurs ou égaux à n, partagent chacun un reste (dans les divisions euclidiennes etc...) avec $2n$.

Considérons l'exemple du nombre pair 40 pour étudier davantage cela en présentant les données dans un tableau dans lequel la case (a, q) contient le couple (b, r) tel que $a = bq + r$ est le résultat de la division euclidienne de a par q. Les nombres premiers impairs ne partageant aucun de leurs restes avec 40 sont 3, 11 et 17. Effectivement, 40 se décompose en somme de deux nombres premiers impairs en $3 + 37 = 11 + 29 = 17 + 23$.

	3	5	7
3	$(1, 0)$	$(0, 3)$	$(0, 3)$
5	$(1, 2)$	$(1, 0)$	$(0, 5)$
7	$(2, 1)$	$(1, 2)$	$(1, 0)$
11	$(3, 2)$	$(2, 1)$	$(1, 4)$
13	$(4, 1)$	$(2, 3)$	$(1, 6)$
17	$(5, 2)$	$(3, 2)$	$(2, 3)$
19	$(6, 1)$	$(3, 4)$	$(2, 5)$
40	$(13, 1)$	$(8, 0)$	$(5, 5)$

Dans le tableau ci-dessus, on a coloré en bleu les restes que les nombres premiers impairs inférieurs à 20 partagent avec 40. Essayons de comprendre pourquoi il n'est pas possible qu'il y ait un reste coloré dans chaque ligne. Appelons $p_1 = 3, p_2 = 5$ et $p_3 = 7$ les nombres premiers qui interviennent dans ce cas particulier. Supposons par exemple par hypothèse que le reste selon le diviseur p_1 est commun à $2n$ et p_2, que le reste selon le diviseur p_2 est commun à $2n$ et p_3, et enfin que le reste selon le diviseur p_3 est commun à $2n$ et p_1.

Si $2n$ et p_2 ont même reste dans la division euclidienne par p_1, cela équivaut à $p_1 \mid (2n - p_2)$. On déduit des deux autres partages de restes que $p_2 \mid (2n - p_3)$ et que $p_3 \mid (2n - p_1)$.

On peut donc déduire du fait qu'un reste soit partagé par $2n$ et *tout* nombre premier impair inférieur ou égal à n le critère de divisibilité suivant :

$$p_1 p_2 p_3 \mid (2n - p_1)(2n - p_2)(2n - p_3)$$

Développons le produit à droite du signe “divise”.

$$\begin{aligned}(2n-p_1)(2n-p_2)(2n-p_3) &= (4n^2-2np_1-2np_2+p_1p_2)(2n-p_3)\\ &= 8n^3-4n^2p_1-4n^2p_2+2np_1p_2-4n^2p_3+2np_1p_3+2np_2p_3-p_1p_2p_3\\ &= 8n^3-4n^2(p_1+p_2+p_3)+2n(p_1p_2+p_1p_3+p_2p_3)-p_1p_2p_3\end{aligned}$$

Mais puisque $p_1p_2p_3$ se divise trivialement lui-même et puisqu'on peut mettre $2n$ en facteur dans le début de la somme obtenue $8n^3-4n^2(p_1+p_2+p_3)+2n(p_1p_2+p_1p_3+p_2p_3)$, alors il faudrait pour que $p_1p_2p_3 \mid (2n-p_1)(2n-p_2)(2n-p_3)$ que $p_1p_2p_3$ divise $2n$, ce qui est impossible (non, problème, pour conclure ça, il faudrait que $p_1p_2p_3$ soit premier avec $4n^2-2n(p_1+p_2+p_3)+(p_1p_2+p_1p_3+p_2p_3)$). On a ainsi abouti à une contradiction.

L'hypothèse qu'on a choisie au départ était très particulière, qui consistait à fixer que

$$p_1 \mid (2n-p_2) \quad \text{et} \quad p_2 \mid (2n-p_3) \quad \text{et} \quad p_3 \mid (2n-p_1)$$

On aboutirait à la même conclusion impossible en permutant de toutes les façons possibles la manière dont les p_i peuvent diviser les $2n-p_j$, si on prend comme hypothèse que *tous* les nombres premiers impairs inférieurs à n partagent un reste avec $2n$.

Appelons

$$p_k \;=\; max\{p_u \;/\; p_u \; premier \; et \; 3 \leqslant p_u \leqslant \sqrt{2n}\}$$

et

$$p_l \;=\; max\{p_v \;/\; p_v \; premier \; et \; 3 \leqslant p_v \leqslant n\}$$

Ce qui est nécessaire pour pouvoir mener un tel raisonnement, c'est de prendre un partage de reste au moins dans chaque colonne, de manière à obtenir le produit complet des nombres premiers impairs inférieurs à $\sqrt{2n}$, i.e. $\prod_{p_i=3}^{p_i=p_k} p_i$ comme diviseur du produit des $2n-p_j$, i.e. $\prod_{p_j=3}^{p_j=p_l}(2n-p_j)$

Puisqu'il n'est pas possible que tous les nombres premiers impairs inférieurs à n partagent un reste avec $2n$ dans les divisions euclidiennes par les nombres premiers impairs inférieurs à $\sqrt{2n}$, il existe pour tout nombre pair un nombre premier inférieur à sa racine qui ne partage aucun de ses restes avec $2n$. Ce nombre premier est un décomposant de Goldbach de $2n$.

Essayons une autre piste :
on peut penser que pour qu'il y ait un nombre coloré par ligne au moins, il faudrait que le produit $\prod_{p_i \leqslant n}(2n-p_i)$ soit divisible par un nombre de la forme $\prod_{p_i \leqslant \sqrt{2n}} p_i^{\alpha_i}$ avec $\sum \alpha_i \geqslant \pi(n)-1$. Mais un petit test montre que ce raisonnement ne convient pas non plus : à la recherche des décompositions de Goldbach de 80, écrivons les factorisations des nombres de la forme $2n-p_i$ pour p_i compris entre 3 et 37.

p_i	$2n-p_i$	$factorisation(2n-p_i)$
3	77	7.11
5	75	3.5^2
7	73	*premier*
11	69	3.23
13	67	*premier*
17	63	$3^2.7$
19	61	*premier*
23	57	3.19
29	51	3.17
31	49	7^2
37	43	*premier*

$3^6.5^2.7^4$ divise le produit des $(2n-p_i)$ avec $6+2+4$ supérieur au nombre de lignes et pourtant, il se trouve des premiers dans le produit, du fait de la grandeur des puissances dans les factorisations d'autres.

Le seul argument valable serait finalement de réussir à prouver que le $\prod_{p_i \leqslant n}(2n-p_i)$ contient au moins un diviseur premier plus grand que n.