Partage de restes euclidiens et conjecture de Goldbach

Denise Chemla

25 août 2013

1 Introduction

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 $49 = \dfrac{98}{2}$, 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 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 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	$(13,1)$	$(8,0)$	$(5,5)$

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 partagé (coloré) dans chaque ligne.

Inventons un tableau factice qui contiendrait un partage de reste par ligne (on représente le partage de reste avec $2n$ par une croix et on omet la ligne de $2n$ qui était fournie pour l'exemple $2n = 40$ ci-dessus) et voyons si un tel tableau obligerait à aboutir à une contradiction.

	p_1	p_2	p_3
p_1	$\times$		
p_2		$\times$	
p_3		$\times$	
p_4	$\times$		
p_5			$\times$

A ce tableau pourraient être associées les équations de la forme $a = bq + r$ suivantes :

$$\begin{cases} p_1 = 2n - k_1 p_1 \\ p_2 = 2n - k_2 p_2 \\ p_3 = 2n - k_3 p_2 \\ p_4 = 2n - k_4 p_1 \\ p_5 = 2n - k_5 p_3 \end{cases}$$

Note : dans le cas présenté ici, p_1 et p_2 sont des diviseurs de $2n$.

On transforme ce système en :

$$\begin{aligned} 2n \quad &= p_1 + k_1 p_1 \\ &= p_2 + k_2 p_2 \\ &= p_3 + k_3 p_2 \\ &= p_4 + k_4 p_1 \\ &= p_5 + k_5 p_3 \end{aligned}$$

Mais puisque par ailleurs, on doit avoir :

$$\begin{cases} p_2 = k'_2 p_1 + r_2 \\ p_3 = k'_3 p_1 + r_3 \\ p_4 = k'_4 p_1 + r_4 \\ p_5 = k'_5 p_1 + r_5 \end{cases}$$

On en déduit que :

$$
\begin{array}{lllll}
2n & = p_1 + k_1 p_1 & = (1+k_1) & p_1 & \\
 & = (k'_2 p_1 + r_2) + k_2(k'_2 p_1 + r_2) & = (1+k_2)k'_2 & p_1 & +r_2(1+k_2) \\
 & = (k'_3 p_1 + r_3) + k_3(k'_2 p_1 + r_2) & = (k'_3 + k_3 k'_2) & p_1 & +(r_3 + k_3 r_2) \\
 & = (k'_4 p_1 + r_4) + k_4 p_1 & = (k'_4 + k_4) & p_1 & +r_4 \\
 & = (k'_5 p_1 + r_5) + k_5(k'_3 p_1 + r_3) & = (k'_5 + k_5 k'_3) & p_1 & +(r_5 + k_5 r_3)
\end{array}
$$

Cela doit vraisemblablement engendrer une contradiction qu'il reste à déterminer.

J'envisagerais bien une contradiction comme celle intervenant dans la démonstration de l'infinité de l'ensemble des nombres premiers d'Euclide. Il dit : "admettons qu'on ait recensé tous les nombres premiers dans un ensemble fini. Fabriquons un nouveau nombre produit de tous les premiers recensés auquel on ajoute 1. Ce nombre a pour reste 1 dans une division par n'importe quel premier déjà recensé. S'il a un diviseur, ce diviseur est forcément un premier qui n'a pas été recensé. Contradiction. L'ensemble des premiers est donc infini."

Peut-être qu'ici la contradiction pourrait provenir du fait qu'on est censé avoir recensé[1] tous les premiers inférieurs à n dans le tableau et les calculs pourraient nous en faire découvrir un nouveau.

Il faudrait généraliser un tel raisonnement, en montrant que toutes les combinaisons possibles de partages de restes engendrent une contradiction. Il faudrait également envisager la façon dont la théorie de Galois, qui entraîne la résolubilité de certaines équations, selon certaines permutations des variables (en l'occurrence les différents nombres premiers inférieurs à n), intervient ici.

[1] Tous ces "censés", c'est insensé !