Calcule et ... (Denise Vella-Chemla, juillet 2022)

On reprend notre exemple fétiche de la recherche des décomposants de Goldbach de l'entier pair $n = 98$.

$$S_{98} = \begin{cases} 98 \equiv 0 \pmod 2 \\ 98 \equiv 2 \pmod 3 \\ 98 \equiv 3 \pmod 5 \\ 98 \equiv 0 \pmod 7 \end{cases}$$

Appelons d_{98} un décomposant de Goldbach potentiel de $n = 98$. d_{98} peut être congru, hormis 0, à tout ce à quoi $n = 98$ n'est pas congru. Le signe $\vee$ dans le système ci-dessous est à lire comme un ou exclusif, son emploi étendu est à comprendre comme le fait de vérifier autant de systèmes de congruences que la combinatoire le permet.

$$S_{d_{98}} = \begin{cases} d_{98} \equiv 1 \pmod 2 \\ d_{98} \equiv 1 \pmod 3 \\ d_{98} \equiv 1 \vee 2 \vee 4 \pmod 5 \\ d_{98} \equiv 1 \vee 2 \vee 3 \vee 4 \vee 5 \vee 6 \pmod 7 \end{cases}$$

Remarque 1 : on note que la congruence à 1 mod 2 garantit que la solution est un nombre impair.

Remarque 2 : on notera que le fait de respecter le système de systèmes de congruences ci-dessus est une condition suffisante mais non nécessaire pour être un décomposant de Goldbach de n. On trouvera la preuve de cette caractérisation des décomposants de Goldbach d'un nombre pair n qui sont supérieurs à la racine carrée de n en [1].

Comme on peut le comprendre, les modules qui ne divisent pas n "éliminent davantage de classes de congruences" (au nombre de 2) que les modules qui divisent n. Plaçons-nous dans le pire des cas, où l'on élimine deux classes de congruences par module premier inférieur à $\sqrt{n}$, on trouve tout de même

$$\frac{1}{2} \prod_{\substack{p \text{ premier} \\ 5 \leq p \leq \sqrt{n}}} (p-2)$$

classes de congruences différentes par l'application du théorème des restes chinois à chacun des systèmes de congruences combinatoirement trouvé (voir $S_{d_{98}}$ ci-dessus). La division par 2 est justifiée par les symétries autour des moitiés (par exemple, pour 40, les classes de congruences trouvées par l'application du théorème des restes chinois à chaque système[1] sont les classes $30k+11, 30k+17, 30k+23$ et $30k+29$ dont on ne conserve que la moitié par symétrie autour de 20, la moitié de 40.

Mais d'autre part, les solutions étant toutes des unités du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, la moitié d'entre elles sont inférieures à $D = \frac{1}{2} \prod_{\substack{p \text{ premier} \\ 3 \leq p \leq \sqrt{n}}} p$ (pour illustrer cela sur l'exemple $n = 98$, la moitié des solutions

[1] Systèmes de congruences pour $n = 40$:

$$\begin{cases} 40 \equiv 0 \pmod 2 \\ 40 \equiv 1 \pmod 3 \\ 40 \equiv 0 \pmod 5 \end{cases} \qquad S_{d_{40}} = \begin{cases} d_{40} \equiv 1 \pmod 2 \\ d_{40} \equiv 2 \pmod 3 \\ d_{40} \equiv 1 \vee 2 \vee 3 \vee 4 \pmod 5 \end{cases}$$

(s'il en existe) sont forcément inférieures à 105=3×5 × 7).

Serait-il possible de "rater l'intervalle visé", i.e. que toutes les solutions soient supérieures à n, comprises entre n et D ?

Oui, ce serait tout à fait possible : le nombre de solutions trouvées combinatoirement étant très vite inférieur au nombre d'impairs compris entre n et D qui est égal à $\dfrac{D-n+1}{2}$, cette approche est nulle et non avenue.

Référence

[1] D. Chemla, *Réécrire*, http://denise.vella.chemla.free.fr/jade1.pdf