Équirépartition dans le groupe des unités ? (Denise Vella-Chemla 19.12.2021)

Revenons une fois encore à notre exemple fétiche de la recherche des décomposants de Goldbach de 98 pour voir ce qui se passe "derrière la scène" (cf. [2], [3], [4]).

On a besoin de considérer les seuls nombres premiers inférieurs à la racine carrée de 98, soient 2, 3, 5 et 7.

98 vérifie les congruences suivantes : $98 \equiv 0\ [2], 98 \equiv 2\ [3], 98 \equiv 3\ [5], 98 \equiv 0\ [7]$.

Un décomposant de Goldbach de 98 supérieur à $\sqrt{98}$, s'il existe, devra vérifier les congruences $x \equiv 1\ [2], x \equiv 1\ [3], x \equiv 1 \vee 2 \vee 4\ [5], x \equiv 1 \vee 2 \vee 3 \vee 4 \vee 5 \vee 6\ [7]$. Ci-dessus, les modules sont indiqués entre crochets et la lettre $\vee$ symbolise une disjonction de congruences.

On voit qu'un décomposant de Goldbach de 98 supérieur à $\sqrt{98}$ est la solution potentielle d'un système de congruences parmi $1 \times 1 \times 3 \times 6 = 18$ systèmes de congruences possibles.

Chacun de ces systèmes de congruences se résout en utilisant le théorème des restes chinois.

Chaque solution parmi les 18 possibles est un nombre de la forme suivante (ce nombre est calculé modulo 210, le produit de tous les nombres premiers inférieurs à $\sqrt{98}$, il représente une infinité de nombres possibles) :

$$\Big(\underbrace{[1\ .\ (3.5.7)]}_{\substack{\equiv 1\ [2]\\ \equiv 0\ [3]\\ \equiv 0\ [5]\\ \equiv 0\ [7]}} \times a_1 + \underbrace{[1\ .\ (2.5.7)]}_{\substack{\equiv 0\ [2]\\ \equiv 1\ [3]\\ \equiv 0\ [5]\\ \equiv 0\ [7]}} \times a_2 + \underbrace{[3\ .\ (2.3.7)]}_{\substack{\equiv 0\ [2]\\ \equiv 0\ [3]\\ \equiv 1\ [5]\\ \equiv 0\ [7]}} \times a_3 + \underbrace{[4\ .\ (2.3.5)]}_{\substack{\equiv 0\ [2]\\ \equiv 0\ [3]\\ \equiv 0\ [5]\\ \equiv 1\ [7]}} \times a_4 \Big)\ [2.3.5.7]$$

$$= \Big(105\ a_1 + 70\ a_2 + 126\ a_3 + 120\ a_4 \Big)\ [210]$$

Comme a_1 (resp. a_2) ne peut prendre que la valeur 1, 105 a_1 (resp. 70 a_2) est égal à 105 (resp. 70).

Comme a_3 ne peut prendre que les valeurs 1 ou 2 ou 4, 126 a_3 est égal à $126, 252$ ou 504.

Comme a_4 peut prendre n'importe quelle valeur de 1 à 6, 120 a_4 est égal à 120 ou 240 ou 360 ou 480 ou 600 ou 720.

En combinant toutes ces possibilités (au nombre de 18), voici les valeurs que prend $105\ a_1 + 70\ a_2 + 126\ a_3 + 120\ a_4$ avant réduction modulo 210 (on note les quadruplets (a_1, a_2, a_3, a_4) en regard de chaque valeur). Les décomposants de Goldbach de 98 et leur complémentaire sont notés en bleu.

$$
\begin{array}{lll}
(1,1,1,1) \to 421 & (1,1,2,1) \to 547 & (1,1,3,1) \to 799 \\
(1,1,1,2) \to 541 & (1,1,2,2) \to 667 & (1,1,3,2) \to 919 \\
(1,1,1,3) \to 661 & (1,1,2,3) \to 787 & (1,1,3,3) \to 1039 \\
(1,1,1,4) \to 781 & (1,1,2,4) \to 907 & (1,1,3,4) \to 1159 \\
(1,1,1,5) \to 901 & (1,1,2,5) \to 1027 & (1,1,3,5) \to 1279 \\
(1,1,1,6) \to 1021 & (1,1,2,6) \to 1147 & (1,1,3,6) \to 1399
\end{array}
$$

Voici les mêmes nombres réduits modulo 210.

$$
\begin{array}{rrr}
1 & 127 & 169 \\
121 & 37 & 79 \\
31 & 157 & 199 \\
151 & 67 & 109 \\
61 & 187 & 19 \\
181 & 97 & 139
\end{array}
$$

Comme attendu, ces nombres sont tous des unités du groupe $\mathbb{Z}/210\mathbb{Z}$ car leur expression montrent qu'ils ne sont divisibles ni par 2, ni par 3, ni par 5, ni par 7.

$\varphi(210) = 48$ ($\varphi(n)$ compte les unités de $\mathbb{Z}/210\mathbb{Z}$, le nombre de nombres inférieurs à n et premiers à n).

Les unités trouvées comme solutions potentielles par le théorème des restes chinois, au nombre de 18 sur 48 unités, sont équiréparties dans l'intervalle $[3, 210]$.

Cette équirépartition a pour conséquence que 3 systèmes de congruences parmi les 18 systèmes envisageables ont pour solution respective les nombres $19, 31$ et 37, qui sont tous les trois compris entre 3 et 49 la moitié de 98 et sont donc des décomposants de Goldbach de 98.

Si l'on cherche maintenant les décomposants de Goldbach de 120 ($\equiv 0\,[2], \equiv 0\,[3]$, $\equiv 0\,[5], \equiv 1\,[7]$), lui aussi compris entre 7^2 et 11^2, une solution potentielle a davantage de latitude ($\equiv 1\,[2], \equiv 1 \vee 2\,[3], \equiv 1 \vee 2 \vee 3 \vee 4\,[5], \equiv 2 \vee 3 \vee 4 \vee 5 \vee 6\,[7]$). Les solutions potentielles à calculer modulo 210 sont au nombre de 40 et l'intervalle à couvrir est plus grand $[3, 60]$. Le nombre ramené dans $\mathbb{Z}/210\mathbb{Z}$ est noté à côté de chaque $105a_1 + 70a_2 + 126a_3 + 120a_4$, après une virgule. On a coloré en bleu les décomposants de Goldbach et leur complémentaire pour 120 et 104 dans les tableaux ci-après.

$(1,1,1,2) \to 541, 121$	$(1,2,1,2) \to 611, 191$
$(1,1,1,3) \to 661, 31$	$(1,2,1,3) \to 731, 101$
$(1,1,1,4) \to 781, 151$	$(1,2,1,4) \to 851, 11$
$(1,1,1,5) \to 901, 61$	$(1,2,1,5) \to 971, 131$
$(1,1,1,6) \to 1021, 181$	$(1,2,1,6) \to 1091, 41$
$(1,1,2,2) \to 667, 37$	$(1,2,2,2) \to 737, 107$
$(1,1,2,3) \to 787, 157$	$(1,2,2,3) \to 857, 17$
$(1,1,2,4) \to 907, 67$	$(1,2,2,4) \to 977, 137$
$(1,1,2,5) \to 1027, 187$	$(1,2,2,5) \to 1097, 47$
$(1,1,2,6) \to 1147, 97$	$(1,2,2,6) \to 1217, 167$
$(1,1,3,2) \to 793, 163$	$(1,2,3,2) \to 863, 23$
$(1,1,3,3) \to 913, 73$	$(1,2,3,3) \to 983, 143$
$(1,1,3,4) \to 1033, 193$	$(1,2,3,4) \to 1103, 53$
$(1,1,3,5) \to 1153, 103$	$(1,2,3,5) \to 1223, 173$
$(1,1,3,6) \to 1273, 13$	$(1,2,3,6) \to 1343, 83$
$(1,1,4,2) \to 919, 79$	$(1,2,4,2) \to 989, 149$
$(1,1,4,3) \to 1039, 199$	$(1,2,4,3) \to 1109, 59$
$(1,1,4,4) \to 1159, 109$	$(1,2,4,4) \to 1229, 179$
$(1,1,4,5) \to 1279, 19$	$(1,2,4,5) \to 1349, 89$
$(1,1,4,6) \to 1399, 139$	$(1,2,4,6) \to 1469, 209$

On peut constater en étudiant le cas $n = 104 = 8 \times 13$ que les solutions, bien qu'étant des nombres premiers qui donc sont premiers à n, ne sont cependant pas à chercher dans le groupe des unités de $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/104\mathbb{Z}$ mais dans le groupe des unités de $\mathbb{Z}/(2.3.5.7)\mathbb{Z} = \mathbb{Z}/210\mathbb{Z}$.

On a $104 \equiv 0\ [2], \equiv 2\ [3], \equiv 4\ [5], \equiv 6\ [7]$.

Une solution potentielle vérifie $x \equiv 1\ [2], \equiv 1\ [3], \equiv 1 \vee 2 \vee 3\ [5], \equiv 1 \vee 2 \vee 3 \vee 4 \vee 5\ [7]$, il y a 15 solutions potentielles à calculer modulo 210, l'intervalle est $[3, 52]$.

$(1,1,1,1) \to 421, 1$	$(1,1,2,1) \to 547, 127$	$(1,1,3,1) \to 673, 43$
$(1,1,1,2) \to 541, 121$	$(1,1,2,2) \to 667, 37$	$(1,1,3,2) \to 793, 163$
$(1,1,1,3) \to 661, 31$	$(1,1,2,3) \to 787, 157$	$(1,1,3,3) \to 913, 73$
$(1,1,1,4) \to 781, 151$	$(1,1,2,4) \to 907, 67$	$(1,1,3,4) \to 1033, 193$
$(1,1,1,5) \to 901, 61$	$(1,1,2,5) \to 1027, 187$	$(1,1,3,5) \to 1153, 103$

Voici les unités de $\mathbb{Z}/104\mathbb{Z}$ au nombre de 48 : $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 93, 95, 97, 99, 101, 103\}$.

L'expression mathématique qui représente le nombre de solutions envisageables S est :

$$S = \frac{\prod\limits_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \sqrt{n} \\ p_k | n}} (p_k - 1) \; . \prod\limits_{\substack{p_{k'} \text{ premier} \\ 3 \leq p_{k'} \leq \sqrt{n} \\ p_{k'} \nmid n}} (p_{k'} - 2)}{\varphi(\prod\limits_{\substack{p_{k''} \text{ premier} \\ 2 \leq p_{k''} \leq \sqrt{n}}} p_{k''})}$$

Puisque

$$\begin{aligned} \varphi(\prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \sqrt{n}}} p_k) &= \prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \sqrt{n}}} p_k \prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \sqrt{n}}} \left(1 - \frac{1}{p_k}\right) \\ &= \prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \sqrt{n}}} p_k \prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \sqrt{n}}} \left(\frac{p_k - 1}{p_k}\right) \\ &= \prod_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \sqrt{n}}} (p_k - 1), \end{aligned}$$

on trouve pour S l'expression

$$S = \prod_{\substack{p_k \text{ premier} \\ 3 \leq p_k \leq \sqrt{n} \\ p_k \nmid n}} \frac{p_k - 2}{p_k - 1}$$

Si les solutions envisageables sont équiréparties (on ne sait pas démontrer que c'est le cas), alors pour trouver celles qui sont comprises entre 3 et $n/2$, multiplier S par le ratio $\dfrac{n/2 - 2}{\prod\limits_{\substack{p_k \text{ premier} \\ 2 \leq p_k \leq \sqrt{n}}} p_k}$ devrait compter les décompositions de Goldbach de n. Malheureusement, pour ce dernier calcul, le dénominateur augmentant beaucoup plus vite que le numérateur, on obtient un nombre de solutions de plus en plus petit. On ne sait pas pourquoi il est toujours possible de trouver une solution suffisamment petite (inférieure à $n/2$).

Références

[1] Donald Knuth, The Art of Computer Programming, vol. 1, Fundamental algorithms, Third edition, 1997 (pages 13 à 18).

[2] Denise Vella-Chemla, http://denise.vella.chemla.free.fr/jade1.pdf .

[3] Denise Vella-Chemla, http://denise.vella.chemla.free.fr/invariante.pdf .

[4] Denise Vella-Chemla, http://denise.vella.chemla.free.fr/DLpourCG.pdf .