Unités racines de certaines équations (Denise Vella-Chemla, 23.2.2022)

La conjecture de Goldbach stipule que tout nombre pair n supérieur ou égal à 4 est la somme $p+q$ de deux nombres premiers p et q.

On a constaté dans Retour aux unités que p et q sont à la fois des unités à n (ce sont des nombres premiers à n, i.e. des nombres x tels que $(x,n)=1$, la notation (x,n) désignant le pgcd de x et n), et des unités au produit, qu'on notera P dans la suite, de tous les nombres premiers inférieurs ou égaux à $\sqrt{n}$, c'est-à-dire qu'on a également que $\text{pgcd}(x, \prod_{\substack{p_k \text{ premier} \\ p_k \leq \sqrt{n}}} p_k) = (x, \prod_{\substack{p_k \text{ premier} \\ p_k \leq \sqrt{n}}} p_k) = 1$.

Gauss explique dans les *Recherches arithmétiques* que x, une unité à n (un nombre premier à n), vérifie l'équation modulaire

$$x^{\varphi(n)} \equiv 1 \pmod{n}$$

On vérifie par exemple, puisque $\varphi(98)=42$ et $\varphi(210)=48$, que 19, décomposant de Goldbach de 98, est tel que le système suivant de trois équations modulaires est vérifié :

$$\begin{cases} 19^{42} \equiv 1 \pmod{98} \\ 19^{48} \equiv 1 \pmod{210} \\ 79^{48} \equiv 1 \pmod{210} \end{cases}$$

tandis que 17 n'est pas un décomposant de Goldbach de 98 parce que $98-17=81$ et $81^{48} \not\equiv 1 \pmod{210}$.

Un décomposant de Goldbach p du nombre pair n doit donc rendre vraies les 3 équations modulaires

$$\begin{cases} p^{\varphi(n)} & \equiv 1 \pmod{n} \\ p^{\varphi(P)} & \equiv 1 \pmod{P} \\ (n-p)^{\varphi(P)} & \equiv 1 \pmod{P} \end{cases}$$

avec

$$\varphi(P) = \prod_{\substack{p_k \text{ premier} \\ 3 \leq p_k \leq \sqrt{n}}} (p_k - 1)$$

Gauss fournit un petit exemple à la toute fin de la section 92 qui clôt la section troisième *"Des résidus des puissances"* des Recherches arithmétiques :

> *"Ainsi, par exemple, pour $m = 1001 = 7.11.13$, la puissance 60 d'un nombre quelconque premier avec m, est congrue à l'unité, puisque 60 est le plus petit nombre divisible à la fois par 6, 10 et 12."*

Voici le texte complet de la section 92 des *Recherches arithmétiques* de Gauss :

> "92. Presque tout ce qui a rapport aux résidus des puissances, suivant un module composé de plusieurs nombres premiers, peut se déduire de la théorie générale des congruences ; mais comme nous exposerons plus bas une manière de ramener des congruences dont le module est composé de plusieurs nombres premiers, à d'autres dont le module est un nombre premier, ou une puissance d'un nombre premier, nous ne nous arrêterons pas beaucoup ici sur cette matière. Nous nous contenterons

> d'observer que la belle propriété qui a lieu pour les autres modules, savoir : qu'il existe toujours des nombres dont la période renferme tous les nombres premiers avec le module, n'a pas lieu ici, excepté dans le seul cas où le module est le double d'un nombre premier, ou d'une puissance d'un nombre premier. En effet, si l'on ramène le module m à la forme $A^\alpha B^\beta C^\gamma$ etc., A, B, C, etc. étant des nombres premiers différents, qu'on fasse en outre $A^{a-1}(A-1) = \alpha, B^{b-1}(B-1) = \beta, C^{c-1}(C-1) = \gamma$, etc. et que z soit un nombre premier à m, on aura $z^\alpha \equiv 1 \pmod{A^a}$, $z^\beta \equiv 1 \pmod{B^b}$, etc. ; si donc μ est le plus petit nombre divisible par α, β, γ, etc., on aura $x^\mu \equiv 1$ suivant chacun des modules A^a, B^b, etc. et partant, suivant m qui est égal à leur produit ; mais excepté le cas où m est double d'un nombre premier ou d'une puissance d'un nombre premier, on a toujours $\mu < \alpha\beta\gamma$ etc., puisque les nombres α, β, etc. ne peuvent être premiers entre eux, ayant au moins le diviseur commun 2. Ainsi la période d'un nombre ne peut comprendre autant de termes qu'il y a de nombres premiers avec le module, et moindre que lui, puisque leur nombre est égal au produit $\alpha\beta\gamma$ etc. Ainsi, par exemple, pour $m = 1001 = 7.11.13$, la puissance 60 d'un nombre quelconque premier avec m, est congrue à l'unité, puisque 60 est le plus petit nombre divisible à la fois par 6, 10 et 12. Le cas où le module est double d'un nombre premier ou d'une puissance d'un nombre premier est tout à fait semblable à celui où le module est un nombre premier ou une puissance d'un nombre premier.

Considérons un nombre pair n compris entre deux carrés de nombres premiers successifs p_k^2 et p_{k+1}^2. Tous les nombres premiers susceptibles de le décomposer sont à la fois premiers à n et premiers à P le produit des nombres premiers inférieurs ou égaux à $\sqrt{n}$.

Soit p un nombre premier inférieur à $n/2$ dont on a ciblé les caractéristiques dans p-et-n-sont-toujours-de-classes-differentes.

Le complémentaire de p à n qui est égal à $n - p$ est aussi premier à $P = \prod_{\substack{p_k \text{ premier} \\ p_k \leq \sqrt{n}}} p_k$ car le plus petit commun multiple auquel Gauss fait référence, lorsque le module est le produit de nombres premiers simples, et qu'on peut noter $\text{ppcm}\{p_k - 1\}$ divise $\varphi(\prod_{\substack{p_k \text{ premier} \\ p_k \leq \sqrt{n}}} p_k) = \prod_{\substack{p_k \text{ premier} \\ p_k \leq \sqrt{n}}} (p_k - 1)$.

En effet, $\prod_{\substack{p_k \text{ premier} \\ p_k \leq \sqrt{n}}} (p_k - 1)$ contient la totalité des facteurs des factorisations des nombres $p_k - 1$ tandis que $\text{ppcm}\{p_k - 1\}$ ne contient qu'un sous-ensemble de l'ensemble des facteurs en question. Le ppcm divise l'indicateur d'Euler par simple inclusion ensembliste.

Un exemple permettra de fixer les idées : si l'on considère le produit des nombres premiers inférieurs ou égaux à 7, on a $P = 2.3.5.7$, $\varphi(P) = 1.2.4.6 = 48$ tandis que $\text{ppcm}\{1, 2, 4, 6\} = \text{ppcm}\{1, 2, 2.2, 2.3\} = 12$ et $12 \mid 48$.

Ça ne va pas encore tout à fait parce que de la façon dont ça se goupille, cette condition devrait faire de tous les nombres premiers des décomposants de Goldbach d'un nombre pair donné (prenons 98, au hasard), or seuls certains le sont. On dirait que la condition est la suivante : il faut que

le pgcd du ppcm$\{p_k - 1\}$ (égal à 12 pour $2.3.5.7 = 210$) et des 2 nombres $p - 1$ et $q - 1$ soit divisible par 6 mais on ne sait pas encore pourquoi : on a en effet que $\text{pgcd}(12, 18, 78) = 6$ (pour le décomposant de Goldbach 19 de 98) ou que $\text{pgcd}(12, 30, 66) = 6$ pour le décomposant 31 de 98, ou que $\text{pgcd}(12, 36, 60) = 6$ pour le décomposant 37 de 98. Pour 17, qui n'est pas un décomposant de 98, $\text{pgcd}(12, 16, 80) = 4$ que ne divise pas 6.