Racines de certaines équations modulaires (Denise Vella-Chemla, 1.3.2022)

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 rappelle que x un entier naturel est "premier à" y un autre entier naturel si leur plus grand commun diviseur est 1 (leurs factorisations ne partagent aucun facteur premier).

$$x \text{ premier à } y \iff (x,y) = 1.$$

Un nombre premier est "premier à" tout autre nombre qu'il ne divise pas.

On a précisé dans *p-et-n-sont-toujours-de-classes-differentes* les caractéristiques permettant à p un nombre premier inférieur ou égal à $n/2$ d'être un décomposant de Goldbach de n (un nombre pair supérieur ou égal à 6).

Considérons n un nombre pair supérieur ou égal à 6, compris entre p_k^2 et p_{k+1}^2, p_k et p_{k+1} étant deux nombres premiers consécutifs. Notons p un nombre premier inférieur ou égal à $n/2$ et appelons $Prod$ le produit des nombres premiers inférieurs ou égaux à $\sqrt{n}$.

$$Prod = \prod_{\substack{p_k \text{ premier} \\ p_k \leq \sqrt{n}}} p_k$$

$n = p + q$ est une décomposition de Goldbach de n si on peut trouver une solution à l'équation modulaire :

$$(n-p)^{\varphi(Prod)} \equiv 1 \pmod{Prod}.$$

Gauss fournit dans la section 92 des Recherches arithmétiques la condition de résolubilité d'une telle équation (voir Annexe 1) : il faut que le plus petit commun multiple des différents nombres premiers que l'on a multipliés pour obtenir $Prod$ auxquels on soustrait 1 (i.e. ppcm$\{p_k - 1\}$) divise $\varphi(Prod)$ (voir en Annexe 2 les premiers exemples numériques).

Cela découle du fait que $\varphi(\prod_{\substack{p_k \text{ premier} \\ p_k \leq \sqrt{n}}} p_k) = \prod_{\substack{p_k \text{ premier} \\ p_k \leq \sqrt{n}}} (p_k - 1)$.

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 ppcm$\{p_k - 1\}$ ne contient qu'un sous-ensemble de l'ensemble des facteurs en question. Le ppcm considéré divise l'indicatrice d'Euler considérée par simple inclusion ensembliste. Cette vision ensembliste de la notion de factorisation était celle de Laisant dans *Une vision ensembliste de la factorisation* .

On est donc garanti d'avoir une solution à cette équation inférieure à $Prod$.

Mais ce que l'on souhaite, c'est que cette solution soit inférieure à $n/2$. Le fait qu'il soit garanti qu'existe une solution "assez petite" de l'équation modulaire (i.e. une solution telle que p est inférieur à $n/2$) pourrait peut-être découler du théorème de Chebotarev.

Annexe 1 : Section 92 des Recherches arithmétiques de C.F. Gauss

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.

Annexe 2 : plus petits communs multiples et indicatrices d'Euler

Prod	ens. des p_k1	leur ppcm	$\varphi(Prod)$	$col.4/col.3$
2.3	$\{1, 2\}$	2	2	1
2.3.5	$\{1, 2, 4\}$	4	8	2
2.3.5.7	$\{1, 2, 4, 6\}$	12	48	4
2.3.5.7.11	$\{1, 2, 4, 6, 10\}$	60	480	8
2.3.5.7.11.13	$\{1, 2, 4, 6, 10, 12\}$	60	5760	96
2.3.....17	$\{1, 2, 4, 6, 10, 12, 16\}$	240	92160	384
2.3.....19	$\{1, 2, 4, 6, 10, 12, 16, 18\}$	720	1 658 880	2304
2.3.....23	$\{1, 2, 4, 6, 10, 12, 16, 18, 22\}$	7920	36 495 360	4608