Pourquoi tout nombre pair sauf 2 est-il la somme de deux nombres premiers ?

Denise Vella-Chemla

22/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. On rappelle qu'un nombre premier impair p est un décomposant de Goldbach de n un nombre pair supérieur ou égal à 6 si p est incongru* à n selon tout module premier impair p' inférieur à $\sqrt{n}$. En effet, dans le cas contraire, le complémentaire à n de p est composé.

Exemple : 19 est un décomposant de Goldbach de 98 car 19 est incongru à 98 selon 3, 5 et 7. Par contre, 3 n'est pas un décomposant de Goldbach de 98 car $3 \equiv 98$ (*mod* 5) (ce qui correspond au fait que 5 divise $98-3$). 5 n'est pas un décomposant de Goldbach de 98 car $5 \equiv 98$ (*mod* 3). 7 n'est pas un décomposant de Goldbach de 98 car $7 \equiv 98$ (*mod* 7) (ce qui correspond au fait que 7 divise $98-7$, 7 est diviseur de 98). 11 n'est pas un décomposant de Goldbach de 98 car $11 \equiv 98$ (*mod* 3). 13 n'est pas un décomposant de Goldbach de 98 car $13 \equiv 98$ (*mod* 5). 17 n'est pas un décomposant de Goldbach de 98 car $17 \equiv 98$ (*mod* 3).

2 Démonstration

Un décomposant de Goldbach de n, s'il existe, est un élément du groupe des unités $(\mathbb{Z}/n\mathbb{Z})^*$. Son complémentaire à n appartient lui aussi au groupe des unités. Il y a $\frac{\varphi(n)}{2}$ décompositions possibles qui font intervenir deux unités complémentaires.

On considère donc l'ensemble des unités à n, n étant un nombre pair supérieur ou égal à 6. On va démontrer que si tous les nombres premiers (forcément impairs) unités à n sont congrus à n selon un certain module, on aboutit à une contradiction. Cela aura pour conséquence que l'un des nombres premiers impairs inférieurs à n et premiers à n devant être incongru à n selon tout module premier impair inférieur à $\sqrt{n}$, ce nombre premier a son complémentaire à n qui est premier également. Le nombre premier en question est donc un décomposant de Goldbach de n.

Pour cela, on va utiliser trois éléments :

- l'article 78 des Recherches Arithmétiques : Le théorème de *Wilson* peut être rendu plus général en l'énonçant comme il suit : *le produit de tous les nombres premiers avec un nombre donné A et moindres que ce nombre, est congru suivant A, à l'unité prise positivement ou négativement.* L'unité doit être prise négativement quand A est de la forme p^m ou $2p^m$, p étant un nombre premier différent de 2, ou encore quand $A = 4$, et positivement dans tous les autres cas. Le théorème de Wilson est contenu dans le premier cas. *Exemple.* Pour $A = 15$, le produit des nombres $1, 2, 4, 7, 8, 11, 13, 14$ est $\equiv 1$ (*mod* 15). Nous supprimons, pour abréger, la démonstration. Nous observerons seulement qu'on peut y parvenir comme dans l'article précédent, excepté que la congruence $x^2 \equiv 1$ peut avoir plus de deux racines ; ce qui demande certaines considérations particulières. On pourrait aussi la tirer de la considération des indices, comme dans le $n°75$, si l'on y joint ce que nous dirons tout à l'heure des modules composés. ;

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

- un *"artifice technique"* que Gauss présente à la fin de la section 4 des Recherches Arithmétiques : $a \equiv b\ (mod\ m)$ est équivalent à $ca \equiv cb\ (mod\ cm)$[†].
  Par exemple, $5 \equiv 17\ (mod\ 3) \iff 35 \equiv 119\ (mod\ 21)$;
- enfin, l'extrait de l'article 5 de la section 1 des Recherches : *"On doit supposer la même identité de module dans ce qui suit."*, et plus loin, dans l'article 7, *Si* $A \equiv a$ *et* $B \equiv b$, $AB \equiv ab$ (conservation des congruences par le produit).

Ecrivons comme hypothèse initiale que chaque nombre premier impair inversible est congru à n selon un module :

$$\begin{cases} p_1 \equiv n\ (mod\ p'_1) \\ p_2 \equiv n\ (mod\ p'_2) \\ \vdots \\ p_i \equiv n\ (mod\ p'_i) \end{cases}$$

Cela nous permet d'ajouter les congruences suivantes.

$$\begin{cases} n - p_1 \equiv 0\ (mod\ p'_1) \\ n - p_2 \equiv 0\ (mod\ p'_2) \\ \vdots \\ n - p_i \equiv 0\ (mod\ p'_i) \end{cases}$$

Utilisons l'*artifice technique* pour ramener toutes les congruences selon le même module, de manière à pouvoir ensuite les multiplier entre elles. Pour cela, appelons G le plus petit commun multiple des modules p'_i[‡]. On note car cela servira ensuite que le nombre G étant un produit d'éléments inversibles ne peut être nul.

$$\begin{cases} p_1.\frac{G}{p'_1} \equiv n.\frac{G}{p'_1}\ (mod\ G) \\ p_2.\frac{G}{p'_2} \equiv n.\frac{G}{p'_2}\ (mod\ G) \\ \vdots \\ p_i.\frac{G}{p'_i} \equiv n.\frac{G}{p'_i}\ (mod\ G) \\ (n - p_1).\frac{G}{p'_1} \equiv 0.\frac{G}{p'_1}\ (mod\ G) \\ (n - p_2).\frac{G}{p'_2} \equiv 0.\frac{G}{p'_2}\ (mod\ G) \\ \vdots \\ (n - p_i).\frac{G}{p'_i} \equiv 0.\frac{G}{p'_i}\ (mod\ G) \end{cases}$$

Pour avoir une congruence portant sur chacune des unités, il nous faut cependant ajouter également les congruences suivantes, qui portent sur les c_j, les c_j étant les nombres composés premiers à n dont le complémentaire à n est lui-aussi composé. Le nombre particulier $n - 1$ fait partie des p_i s'il est premier et des c_i s'il est composé même si son complémentaire, le nombre 1, n'est pas un nombre composé. Ces congruences supplémentaires vont nous permettre d'obtenir notre *"produit des unités"* de l'article 78.

$$\begin{cases} c_1 \equiv \alpha_1\ (mod\ G) \\ \vdots \\ c_j \equiv \alpha_j\ (mod\ G) \end{cases}$$

[†]L'extrait de l'article 152, page 117 est *Soit la congruence* $ax^2 + bx + c \equiv 0\ (mod\ m)$ *; elle sera équivalente à celle-ci :* $4a^2x^2 + 4abx + 4ac \equiv 0\ (mod\ 4am)$.

[‡]Il faut noter que les p'_i ne sont pas une substitution des p_i, il peut y avoir des redondances (un p'_i égal à un p'_j) et des "disparitions" (un p_i n'intervenant jamais comme module).

On obtient alors le système de congruences suivant :

$$\begin{cases} p_1.\frac{G}{p'_1} \equiv n.\frac{G}{p'_1}\ (mod\ G) \\ p_2.\frac{G}{p'_2} \equiv n.\frac{G}{p'_2}\ (mod\ G) \\ \vdots \\ p_i.\frac{G}{p'_i} \equiv n.\frac{G}{p'_i}\ (mod\ G) \\ (n-p_1).\frac{G}{p'_1} \equiv 0.\frac{G}{p'_1}\ (mod\ G) \\ (n-p_2).\frac{G}{p'_2} \equiv 0.\frac{G}{p'_2}\ (mod\ G) \\ \vdots \\ (n-p_i).\frac{G}{p'_i} \equiv 0.\frac{G}{p'_i}\ (mod\ G) \\ c_1 \equiv \alpha_1\ (mod\ G) \\ \vdots \\ c_j \equiv \alpha_j\ (mod\ G) \end{cases}$$

Du fait de la conservation des congruences par le produit lorsque le module est le même dans les différentes congruences, on peut réécrire cela en :

$$\underbrace{p_1.p_2.\ldots.p_i.(n-p_1).(n-p_2).\ldots.(n-p_i).c_1.\ldots.c_j}_{\prod_{i=1}^{\varphi(n)} u_i}.\frac{G^{2\pi(n)}}{\prod p'^2_i} \equiv 0.\frac{G^{2\pi(n)}}{\prod p'^2_i}.\prod \alpha_i\ (mod\ G)$$

On reconnaît dans le produit des éléments de gauche le produit des unités auquel Gauss fait référence dans l'article 78, qui vaut $+1$ ou -1 selon les cas.
Les produits sont nul quant à celui de gauche et nul quant à celui de droite. On a abouti à une tautologie.

Snif !

Donc on ne peut toujours pas dire qu'il existe un nombre premier incongru à n selon tout nombre premier inférieur à $\sqrt{n}$. Dommage, ce nombre premier aurait eu son complémentaire à n qui aurait été premier également et aurait ainsi fourni une décomposition de Goldbach de n...