Théorème de Sophie Germain

Leçons : 121
Référence : *Oraux X-ENS*, tome 1, p. 204.

Théorème 1 (Sophie Germain, 1823). *Soit p un nombre premier de Sophie Germain (i.e. p impair tel que $q = 2p+1$ est premier). Alors, il n'existe pas de triplet $(x,y,z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0 \mod(p)$ et $x^p + y^p + z^p = 0$.*

Démonstration. Soit p un nombre premier de Sophie Germain. Notons $q = 2p+1$. Supposons par l'absurde avoir trouvé $(x,y,z) \in \mathbb{Z}^3$ tels que

$$\begin{cases} xyz \not\equiv 0 \mod(p) \\ x^p + y^p + z^p = 0. \end{cases}$$

Étape 1 ($\text{pgcd}(x,y,z) = 1$) : Quitte à remplacer x, y, z par $\frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ où $d = \text{pgcd}(x,y,z)$, on peut supposer que $\text{pgcd}(x,y,z) = 1$.

Étape 2 (x, y, z sont deux à deux premiers entre eux) : Par symétrie, il suffit de le montrer pour x et y. Supposons par l'absurde que $\text{pgcd}(x,y) > 1$. Soit p_0 un diviseur premier du pgcd. Alors p_0 divise $x^p + y^p = -z^p$, donc, par le lemme d'Euclide, $p_0 \mid z$, donc $p_0 \mid \text{pgcd}(x,y,z) = 1$. Absurde.

Étape 3 : Construction de a, b et c tels que

$$y + z = a^p, \qquad x + z = b^p, \qquad x + y = c^p.$$

Notons $A = y + z$ et $B = \displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$.

Montrons que $\text{pgcd}(A,B) = 1$. Supposons par l'absurde que $\text{pgcd}(A,B) > 1$, et donnons-nous p_0 un diviseur premier commun. Donc $y + z \equiv 0 \mod(p_0)$, donc $-z \equiv y \mod(p_0)$, donc

$$B = \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \equiv \sum_{k=0}^{p-1} y^{p-1} = p\, y^{p-1} \equiv 0 \mod(p_0).$$

Par le lemme d'Euclide, $p_0 \mid p$ ou $p_0 \mid y^{p-1}$.

Si $p_0 \mid p$, alors $p_0 = p$. On a alors $A \cdot B = y^p + z^p = -x^p \equiv 0 \mod(p_0)$, donc, par Euclide, $p_0 \mid x$, et on a donc $p \mid x$, ce qui est exclu car $xyz \not\equiv 0 \mod(p)$.

Donc $p_0 \mid y^{p-1}$, donc $p_0 \mid y$; combiné à $p_0 \mid A = y + z$, on obtient $p_0 \mid z$, donc $p_0 \mid \text{pgcd}(y,z) = 1$ (étape 2), ce qui est absurde.

Donc $\text{pgcd}(A,B) = 1$, et $A \cdot B = (-x)^p$. Or, si deux entiers premiers entre eux ont un produit égal à une puissance p-ième, chacun d'eux est, au signe près, une puissance p-ième (fait admis, vu en cours). Donc il existe $\alpha, a \in \mathbb{Z}$ tels que

$$B = \alpha^p \qquad \text{et} \qquad y + z = a^p.$$

De même, on trouve $b, c \in \mathbb{Z}$ tels que $z + x = b^p$ et $x + y = c^p$.

Étape 4 (Un et un seul des entiers x, y, z est divisible par q) : Comme x, y, z sont deux à deux premiers entre eux (étape 2), il y en a au plus un divisible par q. Il suffit donc de montrer qu'il y en a au moins un.

Supposons par l'absurde qu'aucun des trois entiers n'est divisible par q.

Rappel (critère d'Euler) : pour q premier et $q \nmid m$, $m^{\frac{q-1}{2}} \equiv \left(\frac{m}{q}\right) \bmod(q)$, où $\left(\frac{m}{q}\right) \in \{-1, 1\}$ est le symbole de Legendre. Comme $q = 2p+1$, on a $\frac{q-1}{2} = p$, donc $m^p \equiv \pm 1 \bmod(q)$ dès que $q \nmid m$.

Par hypothèse, q ne divise aucun de x, y, z, donc $x^p, y^p, z^p \equiv \pm 1 \bmod(q)$, donc

$$x^p + y^p + z^p \equiv \{-3, -1, 1, 3\} \bmod(q).$$

Or, $x^p + y^p + z^p = 0$, et $q \geq 7 > 3$ (car $p \geq 3$), donc 0 n'est pas dans $\{-3, -1, 1, 3\} \bmod(q)$: contradiction.

Donc l'un des trois entiers, disons x sans perte de généralité (par symétrie des rôles de x, y, z), est divisible par q.

Étape 5 ($a \equiv 0 \bmod(q)$) : Rappelons $y + z = a^p$, $x + y = c^p$, $z + x = b^p$.

Comme $x \equiv 0 \bmod(q)$, on a $y \equiv c^p \bmod(q)$. Si q divisait c, alors q diviserait y, ce qui contredit l'étape 4 (seul x est divisible par q). Donc $q \nmid c$, donc, par le critère d'Euler, $c^p \equiv \pm 1 \bmod(q)$, donc $y \equiv \pm 1 \bmod(q)$.

De même, $q \nmid b$, donc $z \equiv b^p \equiv \pm 1 \bmod(q)$.

Supposons par l'absurde que $a \not\equiv 0 \bmod(q)$. Alors $a^p \equiv \pm 1 \bmod(q)$ (critère d'Euler), donc

$$b^p + c^p - a^p \equiv \{-3, -1, 1, 3\} \bmod(q).$$

Or, $b^p + c^p - a^p = (z + x) + (x + y) - (y + z) = 2x \equiv 0 \bmod(q)$ (car $x \equiv 0 \bmod(q)$) : absurde, car $q > 3$.

Donc $a \equiv 0 \bmod(q)$, et en particulier $a^p \equiv 0 \bmod(q)$, i.e. $y + z \equiv 0 \bmod(q)$.

Étape 6 ($\alpha^p \equiv p\, y^{p-1} \bmod(q)$) : D'après l'étape précédente, $y + z \equiv 0 \bmod(q)$, donc $-z \equiv y \bmod(q)$, donc

$$\alpha^p = \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \equiv \sum_{k=0}^{p-1} y^{p-1} = p\, y^{p-1} \bmod(q).$$

Conclusion : p est impair, donc $p - 1$ est pair, et comme $y \equiv \pm 1 \bmod(q)$ (étape 5), on a $y^{p-1} \equiv (\pm 1)^{p-1} = 1 \bmod(q)$. Donc

$$\alpha^p \equiv p \bmod(q).$$

Or, $\alpha^p \equiv 0 \bmod(q)$ si $q \mid \alpha$, et $\alpha^p \equiv \pm 1 \bmod(q)$ sinon (critère d'Euler) : dans tous les cas, $\alpha^p \equiv 0, 1$ ou $-1 \bmod(q)$. Comme $0 < p < q - 1$ et $p \neq 1$ (car p est premier), p n'est congru ni à 0, ni à 1, ni à $-1 \equiv q - 1$ modulo q : contradiction.

Donc il n'existe pas de tel triplet (x, y, z). □