Théorème de Sophie Germain

Leçons concernées : 120 121 126 142

Théorème 1. *Soit p un nombre premier de Sophie Germain, c'est-à-dire un nombre premier impair tel que $q = 2p + 1$ soit premier. Il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0[p]$ et $x^p + y^p + z^p = 0$.*

Démonstration.

Raisonnons par l'absurde. On suppose qu'il existe un triplet $(x, y, z) \in \mathbb{Z}^3$ solution.

Étape 1 : Montrons qu'on peut supposer x, y et z premiers entre eux deux à deux.

Quitte à diviser par $\text{pgcd}(x, y, z)$, on suppose que $\text{pgcd}(x, y, z) = 1$. Si alors $\text{pgcd}(x, y) > 1$, soit p_0 un diviseur premier de x et y. Alors $z^p = -(x^p + y^p)$ est divisible par p_0, et donc $\text{pgcd}(x, y, z) \geqslant p_0$, ce qui est contradictoire. Ainsi, on a $\text{pgcd}(x, y) = \text{pgcd}(x, z) = \text{pgcd}(y, z) = 1$.

Étape 2 : Soit $m \in \mathbb{Z}$ non divisible par $q = 2p + 1$. Montrons que $m^p \equiv \pm 1 \mod q$.

Par le petit théorème de Fermat, on a :

$$(m^p)^2 \equiv m^{2p} \equiv m^{q-1} \equiv 1 \mod q$$

Comme q est premier, $\mathbb{Z}/q\mathbb{Z}$ est un corps, donc il est intègre, et $m^p \equiv \pm 1 \mod q$.

Étape 3 : Montrons qu'un seul des trois entiers x, y, z est divisible par q

Si $q \nmid xyz$, alors $x^p, y^p, z^p \equiv \pm 1 \mod q$ par le point précédent, et $0 = x^p + y^p + z^p \equiv \pm 1$ ou $\pm 3 \mod q$, ce qui est absurde car q est impair et supérieur à 5. Ainsi $q \mid xyz$, et supposons par exemple que $q \mid x$. Comme on a vu que $\text{pgcd}(x, y) = \text{pgcd}(x, z) = 1$, on a donc que $q \nmid yz$.

Étape 4 : Écrivons $y + z$, $x + z$, $x + y$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ comme des puissances de p.

En notant $u = \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p$, on a :

$$-x^p = y^p + z^p = y^p - (-z)^p = (y + z)\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = (y + z)u$$

Montrons par l'absurde que $\text{pgcd}(y + z, u) = 1$. Soit alors p_0 un diviseur premier de $\text{pgcd}(y + z, u)$. Comme $p_0^2 \mid x^p$, on a donc $p_0 \mid x$. Or, comme $y \equiv -z \mod p_0$, on a :

$$0 \equiv u \equiv \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv py^{p-1} \mod p_0$$

Donc $p_0 \mid py^{p-1}$, et ainsi :

(i) soit $p_0 \mid p$, mais alors $p_0 = p$, ce qui n'est pas possible puisque $p \nmid x$.

(ii) soit $p_0 \mid y$, mais alors $1 = \text{pgcd}(x, y) \geqslant p_0$, ce qui est absurde.

Ainsi $\text{pgcd}(y + z, u) = 1$. Comme le produit de u et $y + z$ est une puissance de p, et que ces deux termes sont premiers entre eux, chacun des deux est une puissance de p. On a ainsi l'existence de $a, \alpha \in \mathbb{Z}$ tels que $y + z = a^p$ et $u = \alpha^p$. Le même raisonnement donne l'existence de $b, c \in \mathbb{Z}$ tels que $x + z = b^p$ et $x + y = c^p$.

Étape 5 : Conclusion.

On obtient ainsi le système suivant grâce aux étapes précédentes :

$$\begin{cases} b^p + c^p - a^p = 2x \equiv 0 & \mod q \\ c^p \equiv y \equiv \pm 1 & \mod q \\ b^p \equiv z \equiv \pm 1 & \mod q \end{cases}$$

Si $q \nmid a$, alors $a^p \equiv \pm 1 \mod q$, donc $b^p + c^p - a^p \equiv \pm 1$ ou $\pm 3 \mod q$, ce qui est encore contradictoire. Ainsi $q \mid a$, et alors $y \equiv -z \mod q$. Comme par ailleurs $y \equiv \pm 1 \mod q$, il vient que :

$$\alpha^p = u \equiv py^{p-1} \equiv p \mod q$$

Or, $a^p \equiv 0$ ou $\pm 1 \mod q$, ce qui est contradictoire. Finalement, il n'existe pas de triplet satisfaisant.

□

Références

[FGN] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X-ENS Algèbre 1.* Cassini