Théorème de Sophie Germain

Leçons : ***120, 121, 123, 126***

[X-ENS Al1], exercices 4.39

Théorème

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

Démonstration :

On notera ici $\mathcal{P}$ l'ensemble des nombres premiers.
On raisonne par l'absurde ; soit $(x, y, z) \in \mathbb{Z}^3$, tel que $xyz \not\equiv 0\,[p]$ et $x^p + y^p + z^p = 0$.
Soit $d = \text{pgcd}\,(x, y, z)$, quitte à poser $x' = \dfrac{x}{d}$, $y' = \dfrac{y}{d}$ et $z' = \dfrac{z}{d}$, on peut supposer que $d = 1$.

Étape 1 : Montrons qu'alors x, y et z sont premiers entre eux deux à deux.

Par l'absurde, soit r un facteur premier de x et y.
Alors $r | x^p + y^p$, puis $r | z^p$ et donc, par le lemme d'Euclide : $r | z$.
On contredit alors l'hypothèse selon laquelle x, y et z sont premiers entre eux dans leur ensemble.
Désormais, on a donc : $x \wedge y = x \wedge z = y \wedge z = 1$.

Étape 2 : Montrons que $\exists (a, \alpha) \in \mathbb{Z}^2, y + z = a^p$ et $\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = \alpha^p$.

On va appliquer le lemme suivant.

Lemme

Soit $u, v \in \mathbb{Z}$, avec $u \wedge v = 1$ et $\exists w \in \mathbb{Z}, uv = w^k$, où $k \geqslant 2$.
Alors u et v sont tous les deux des puissances $k^{\text{èmes}}$.

Démonstration :

On écrit $u = \displaystyle\prod_{p \in \mathcal{P}} p^{\alpha_p}$, $v = \prod_{p \in \mathcal{P}} p^{\beta_p}$ et $w = \prod_{p \in \mathcal{P}} p^{\gamma_p}$, où $\alpha, \beta, \gamma \in \mathbb{N}^{(\mathcal{P})}$.
Et comme $uv = w^k$, on a : $\forall p \in \mathcal{P}, \alpha_p + \beta_p = k\gamma_p$.
Mais, α_p et β_p ne peuvent pas être simultanément non-nuls, puisqu'on a $u \wedge v = 1$.
Conséquemment, $\forall p \in \mathcal{P}$, $k | \alpha_p$ et $k | \beta_p$.
Donc u et v sont des puissances $k^{\text{èmes}}$. ■

Ici, on a $(y + z) \left(\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \right) = y^p + z^p = -x^p = (-x)^p$.

Il serait donc intéressant de montrer que $y + z$ et $\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$ sont premiers entre eux.

Par l'absurde, supposons qu'il existe un nombre premier, appelons-le r, qui les divise tous les deux.
Alors, de l'égalité précédente, il vient que $r^2 | x^p$, donc $r | x$.

Comme $y \equiv -z\,[r]$, on a : $\underbrace{\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k}_{\equiv 0\,[r]} \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv p y^{p-1}\,[r]$.

1. Il y a beaucoup de choses intéressantes à dire à propos de ce résultat. Sophie Germain (1776-1831) est quasiment la seule femme mathématicienne de son temps. Elle suivit les cours de l'École polytechnique par correspondance, car les femmes n'y étaient pas admises et c'est sous le pseudonyme masculin de Maurice Leblanc qu'elle écrivait à Gauss pour lui faire part de ses découvertes arithmétiques. En 2001, le plus grand nombre de Sophie Germain qu'on connaissait était $109433307 \times 2^{66452} - 1$, possédant 20013 chiffres. À l'heure actuelle, on conjecture qu'il en existe une infinité. Le théorème de Sophie Germain, démontré en 1823, est une résolution partielle du grand théorème de Fermat — mais si, vous savez : pour $n \geqslant 3$, il n'existe pas de solution non-triviale dans $\mathbb{Z}^3$ à l'équation $x^n + y^n = z^n$ — que Fermat mentionnait dans une annotation marginale, sans la prouver "par manque de place". On est certain aujourd'hui qu'il ne pouvait pas en avoir une démonstration complète (bon, en même temps, quand tu t'appelles Fermat, ton prof de maths va avoir du mal à te reprocher de bluffer dans tes copies, non ?).

Donc $r|py^{p-1}$, et donc, par le lemme de Gauss :
– soit $r|p$, et alors, ces deux nombres étant premiers, on obtient $r = p$ et donc $p|x$, contredisant l'hypothèse $xyz \not\equiv 0\,[p]$;
– soit $r|y$, mais c'est impossible puisque $r|x$ et $x \wedge y = 1$.

On obtient ainsi une contradiction ; et on en déduit $(y+z) \wedge \left(\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k\right) = 1$.

Puis, par le lemme, on obtient :

$$\exists (a,\alpha) \in \mathbb{Z}^2, y+z = a^p \text{ et } \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = \alpha^p.$$

Similairement, on montrerait $x+z = b^p$ et $y+z = c^p$, avec $b, c \in \mathbb{Z}$.

Étape 3 : Un (et un seul, vu qu'ils sont premiers entre eux deux à deux) des trois entiers x, y et z est divisible par q.
Soit $m \in \mathbb{Z}$, tel que $q \nmid m$.
Alors, par le petit théorème de Fermat, on obtient : $(m^p)^2 = m^{q-1} \equiv 1\,[q]$ et donc, comme $\mathbb{Z}/q\mathbb{Z}$ est un corps [2], on a : $m^p \equiv \pm 1\,[q]$.
Par l'absurde, on suppose $q \nmid x$, $q \nmid y$ et $q \nmid z$.
Alors $0 = x^p + y^p + z^p$ est congru à 3, 1, -1 ou -3 modulo q. Ce qui est absurde puisque $q > 5$.
Sans perte de généralité, disons que $q|x$, et qu'incidemment : $q \nmid y$ et $q \nmid z$.

Étape 4 : Tels Jean-Claude Dusse, cherchons à conclure.
On a : $b^p + c^p - a^p = x + z + x + y - y - z = 2x \equiv 0\,[q]$.
Et comme $x \equiv 0\,[q]$, on a : $y \equiv c^p\,[q]$; mais $q \nmid y$ donc $q \nmid c$, d'où $y \equiv \pm 1\,[q]$. Similairement, $z \equiv \pm 1\,[q]$.
Donc $a^p = y + z$ est congru à 2, 0 ou -2 modulo q ; mais une puissance $p^{\text{ème}}$ est congrue à 1, 0 ou -1 modulo q.
Donc $y + z \equiv 0[q]$.
Comme dans l'étape 2, on obtient : $\alpha^p = \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \equiv p y^{p-1}\,[q]$.
Or $p-1$ est pair et $y \equiv \pm 1\,[q]$ et donc $\alpha^p \equiv p\,[q]$; mais aussi α^p est congru à 1, 0 ou -1 modulo q.
Contradiction !
Il n'y a donc pas de triplet $(x,y,z) \in \mathbb{Z}^3$ tel que : $xyz \not\equiv 0\,[q]$ et $x^p + y^p + z^p = 0$. ■

Références

[X-ENS Al1] S. FRANCINOU, H. GIANELLA et S. NICOLAS – *Oraux X-ENS Algèbre 1*, 3ème éd., Cassini, 2014.

2. Le polynôme $X^2 - 1 \in \mathbb{Z}/q\mathbb{Z}[X]$ admet au plus deux racines puisqu'il est de degré 2 sur un corps ; on vérifie facilement qu'il s'agit de 1 et -1.