Théorème de Sophie Germain

Référence(s) :
– S. Francinou, H. Gianella et S.Nicolas - *Oraux X-ENS, algèbre 1*

Soit p un nombre premier de Sophie Germain ; c'est-à-dire p est impair et $q = 2p + 1$ est premier.

Théorème 1

Il n'existe pas $(x, y, z) \in \mathbb{Z}^3, xyz \not\equiv 0 \mod p$ *et* $x^p + y^p + z^p = 0$

[1]

Par l'absurde, on suppose qu'un tel triplet existe, soit (x, y, z).
Quitte à poser $x' = \frac{x}{d}, y' = \frac{y}{d}$ et $z' = \frac{z}{d}$, où $d = \text{pgcd}(x, y, z)$, on peut supposer que x, y et z sont premiers entre eux.

Étape 1

Les entiers x,y et z sont premiers entre eux deux à deux.

Par l'absurde : Soit p_0 un facteur premier de $\text{pgcd}(x, y)$. Alors :

$$p_0 | x^p + y^p = -z^p$$

Comme p_0 est premier, nécessairement $p_0|z$ et $\text{pgcd}(x, y, z) > 1$, ce qui est impossible d'après ce qui précède.

Étape 2

Lemme : Soient $u, v \in \mathbb{Z}$ tels que $u \wedge v = 1$ et il existe $w \in \mathbb{Z}$ tel que $uv = w^k$, avec $k \geqslant 2$. Alors

$$\exists \alpha, \beta \in \mathbb{Z}, u = \alpha^k \text{ et } v = \beta^k$$

On écrit : $u = \prod_{p \in \mathcal{P}} p^{\alpha_p}$; $v = \prod_{p \in \mathcal{P}} p^{\beta_p}$; $w = \prod_{p \in \mathcal{P}} p^{\gamma_p}$. Pour tout $p \in \mathcal{P}$, on a : $\alpha_p + \beta_p = \gamma_p$ et $\alpha_p \beta_p = 0$, puisque u et v sont premiers entre eux.
Ainsi, pour tout p, $k \mid \alpha_p$ et $k \mid \beta_p$. Ainsi, u et v sont des puissances k-ièmes.

Étape 3

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

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

Par l'absurde, supposons que $(y + z) \wedge \left(\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \right) \neq 1$. Soit p' un co-diviseur premier.

Alors $p'^2 | ('x)^p$ donc $p'|x$. Or, $y \equiv -z \; [p']$ donc $\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \equiv p y^{p-1} \equiv 0 \; [p']$. Ainsi, $p' | p y^{p-1}$.

Cas 1 : $p'|p$ donc $p' = p$ et $p|x$, ce qui est impossible.
Cas 2 : $p'|y^{p-1}$ donc $p'|y$ donc $x \wedge y \neq 1$, ce qui est impossible.

Ainsi, on peut appliquer le lemme et on obtient : Il existe $(a, \alpha) \in \mathbb{Z}^2, y + z = a^p$ et $\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = \alpha^p$.
De même, il existe $b, c \in \mathbb{Z}$ tels que $x + y = c^p$ et $x + z = b^p$

1. C'est une résolution partielle du grand théorème de Fermat

Étape 4

Soit $m \in \mathbb{Z}$, $q \not| m$, alors $m^p \equiv \pm 1$ $[q]$.

Par le petit théorème de Fermat, on a $m^{q-1} \equiv 1$ $[q]$, i.e. $m^{2p} \equiv (m^p)^2 \equiv 1$ $[q]$. Comme q est premier, $\mathbb{F}_q$ est un corps et $m^p \equiv \pm 1$ $[q]$ [2]
Par l'absurde, supposons que $q \not| x, y, z$. Alors $x^p, x^p, z^p \equiv \pm 1 [q]$; donc $x^p + y^p + z^p \equiv \pm 1, \pm 3$ $[q]$ ce qui est impossible car $q > 5$.
Par exemple, on peut donc supposer que $q | x$ (et donc $q \not| y, z$ car x, y, z sont premiers entre eux).

Étape 5

Conclusion

On a : $b^p + c^p - a^p = x + y + x + z - y - z = 2x \equiv 0$ $[q]$.
De plus $y = c^p - x \equiv c^p$ $[q]$ mais $q \not| y$ donc $q \not| c$. De la même façon, on montre que $q \not| z$ et donc $q \not| b$.
Par ailleurs, on a, d'après ce qui précède $y, z \equiv \pm 1$ $[q]$. Ainsi, $a^p \equiv -2, 0$ ou 2 $[q]$. Or, $a^p \equiv -1, 0$ ou 1 $[q]$, donc

$$a^p \equiv 0 \ [q] \text{ et } y + z = 0$$

On a donc : $y \equiv -z$ $[q]$, et $\alpha^p = \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \equiv p y^{p-1} \equiv p(-1)^{p-1} \equiv p$ $[q]$ puisque $y \equiv \pm 1$ $[q]$ et p impair.
Or, $\alpha^p \equiv 0, \pm 1$ $[q]$: on a une **Contradiction**. Ainsi, on a bien montré :
Il n'existe pas $(x, y, z) \in \mathbb{Z}^3, xyz \not\equiv 0 \mod p$ et $x^p + y^p + z^p = 0$

2. Le polynôme $X^2 - 1 \in \mathbb{F}_q[X]$ admet au plus deux racines car il est de degré 2 sur un corps. Or ± 1 sont racines.