Sandrine CARUSO

Théorème de Sophie Germain

Référence : Oraux X-ENS, Francinou-Ginanella-Nicolas, algèbre 1, p 167

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

On raisonne par l'absurde en supposant qu'il existe une telle solution (x, y, z). Soit d le PGCD de x, y et z. Alors $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$ est encore une telle solution, et de plus, ces trois nombres sont premiers entre eux dans leur ensemble.

On suppose dorénavant que x, y et z sont premiers entre eux. Alors, ils sont premiers entre eux deux à deux : en effet, si un nombre premier p_0 divise x et y, il divise $-z^p = x^p + y^p$ et donc divise z, ce qui contredit le fait que x, y et z sont premiers entre eux.

Lemme 1. *Il existe des entiers a, b, c et α tels que $y + z = a^p$, $x + z = b^p$, $x + y = c^p$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p$.*

Démonstration. On a

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

Montrons que $y + z$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont premiers entre eux. Supposons par l'absurde qu'ils ont un diviseur premier commun p'. Alors p'^2 divise $(-x)^p$, donc p' divise x. De plus, $y \equiv -z \pmod{p'}$ donc

$$0 \equiv \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv py^{p-1} \pmod{p'}$$

et par conséquent, p' divise py^{p-1}. De deux choses l'une : soit p' divise p, auquel cas p divise x. Mais on a fait l'hypothèse que ce n'était pas le cas. Alors p' divise y^{p-1}, donc y, et on a une contradiction puisque x et y sont premiers entre eux.

Ainsi, $y + z$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont premiers entre eux, et de (1), on déduit que $y + z$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont tous deux des puissances de p.

Par symétrie de x, y et z, $x + y$ et $x + z$ sont aussi des puissances de p. □

Lemme 2. *Soit m un entier non multiple de $q = 2p + 1$. Alors $m^p \equiv \pm 1 \pmod{q}$.*

Démonstration. D'après le petit théorème de Fermat, $m^{q-1} \equiv 1 \pmod{q}$, autrement dit, $m^{2p} \equiv 1 \pmod{q}$. Comme $\mathbb{Z}/q\mathbb{Z}$ est un corps, on a nécessairement $m^p \equiv \pm 1 \pmod{q}$. □

Lemme 3. *Un et un seul des trois entiers x, y et z est multiple de q.*

Démonstration. Supposons que ce ne soit pas le cas. D'après le lemme 2, $x^p + y^p + z^p$ est congru soit à 3, soit à 1, soit à -1, soit à -3 modulo q. En tout cas, pas à 0 car $q > 3$. Ce n'est pas possible.

Un des trois nombres est donc multiple de q, et comme ils sont premiers entre eux deux à deux, c'est le seul. □

On suppose, sans perte de généralité, que c'est x. On utilise dans la suite les notations du lemme 1. On a $c^p = y+x \equiv y \pmod q$; comme y n'est pas multiple de q, c non plus et d'après le lemme 2, $c^p \equiv \pm 1 \pmod q$. De même, $b^p \equiv \pm 1 \pmod q$. Supposons que q ne divise pas a. Alors on a également $a^p \equiv \pm 1 \pmod q$ et ainsi, $b^p + c^p - a^p$ est congru à -3, -1, 1 ou 3 modulo q. Mais par ailleurs, $b^p + c^p - a^p = 2x \equiv 0 \pmod q$, d'où une contradiction. Donc q divise a. En particulier, $y + z = a^p \equiv 0 \pmod q$.

Par conséquent,

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

Rappelons que $y \equiv \pm 1 \pmod q$. Comme $p-1$ est pair, $y^{p-1} \equiv 1 \pmod q$. On a donc $\alpha^p \equiv p \pmod q$. Mais d'après le lemme 2, une puissance p-ième est congrue à 0, 1 ou -1 modulo q, donc pas à p. C'est la contradiction finale désirée.