25. Théorème de Sophie Germain

[FGN07a, §4.39, p167]

Énoncé

Théorème. [Théorème de Sophie Germain]
Soit p un nombre premier impair tel que $q = 2p+1$ est premier. Alors il n'existe pas de triplet $(x,y,z) \in \mathbb{Z}^3$ tel que $p \nmid xyz$ et $x^p + y^p + z^p = 0$.

Développement

Supposons qu'il existe un triplet (x,y,z) solution.

1. Quitte à diviser par $d = \mathrm{PGCD}(x,y,z)$, on peut supposer $\mathrm{PGCD}(x,y,z) = 1$.
   Si alors $\mathrm{PGCD}(x,y) > 1$, soit p_0 un diviseur premier. Alors $z^p = -(x^p + y^p)$ est divisible par p_0, donc $p_0 \mid z$, et $\mathrm{PGCD}(x,y,z) \geq p_0$, ce qui est contradictoire.
   Ainsi $\mathrm{PGCD}(x,y) = \mathrm{PGCD}(x,z) = \mathrm{PGCD}(y,z) = 1$.

2. On montre le lemme suivant : soit $m \in \mathbb{Z}$ tel que $q \nmid m$, alors $m^p \equiv \pm 1 \mod q$.
   En effet, on sait par le petit théorème de Fermat que
   $$(m^p)^2 = m^{2p} = m^{q-1} \equiv 1 \mod q$$
   et donc $m^p \equiv \pm 1 \mod q$.

3. Ainsi, si q ne divise ni x ni y ni z, alors $x^p, y^p, z^p \mid \pm 1 \mod q$ et donc
   $$0 = x^p + y^p + z^p \equiv \pm 1, \pm 3 \mod q$$
   ce qui est absurde puisque q est impair et supérieur à 5.
   Supposons par exemple que $q \mid x$. Comme $\mathrm{PGCD}(x,y) = \mathrm{PGCD}(x,z) = 1$, on a $q \nmid yz$.

4. Par ailleurs, écrivons
   $$(-x)^p = y^p + z^p = y^p - (-z)^p = (y+z)\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = (y+z)r$$
   Supposons $\mathrm{PGCD}(y+z, r) > 1$ et soit p_0 un diviseur de ce PGCD. Alors $p_0^2 \mid x^p$ donc $p_0 \mid x$, puis comme $y \equiv -z \mod p_0$:
   $$0 \equiv r \equiv py^{p-1} \mod p_0$$
   Donc $p_0 \mid py^{p-1}$. Ainsi :
   - soit $p_0 \mid p$ mais alors $p_0 = p$, ce qui n'est pas possible puisque puisque $p \nmid x$,
   - soit $p_0 \mid y$, ce qui est absurde puisqu'alors $1 = \mathrm{PGCD}(x,y) \geq p_0$.

   Ainsi $\mathrm{PGCD}(y+z, r) = 1$. On en déduit[1] que $y + z = a^p$ et $r = \alpha^p$ pour deux entiers a, α.
   Le même raisonnement donne que $x + z = b^p$ et $x + y = c^p$ pour deux entiers b, c.

5. On remarque que
   $$\begin{cases} b^p + c^p - a^p = 2x \equiv 0 \mod q \\ c^p \equiv y \equiv \pm 1 \mod q \\ b^p \equiv z \equiv \pm 1 \mod q \end{cases}$$
   Si $q \nmid a$, alors $a^p \equiv \pm 1 \mod q$ par le deuxième point donc $b^p + c^p - a^p \equiv \pm 1, \pm 3 \mod q$, ce qui est à nouveau contradictoire.
   Donc $q \mid a$, et alors $y \equiv -z \mod q$. Comme par ailleurs $y \equiv \pm 1 \mod q$, il vient
   $$\alpha^p = r \equiv py^{p-1} \equiv p \mod q$$
   Or $\alpha^p \equiv 0, \pm 1 \mod q$ par le deuxième point, ce qui est absurde.

Ainsi il n'existe pas de triplet satisfaisant.

1. si le produit de deux entiers premiers entre eux est une puissance k-ième, alors ces deux entiers sont des puissances k-ième, ce que l'on vérifie en regardant les décompositions de ces entiers en produit de nombres premiers