Théorème de Sophie Germain

Réf:
- Algèbre 1 Oraux X-ENS, S. Francinou.

Leçons: 120, 121, 126, 142.

Théorème

Soit p un nombre premier impair tel que $2p+1$ soit premier.
Alors il n'existe pas de triplet (x,y,z) dans $\mathbb{Z}^3$ tel que

$$xyz \neq 0 \mod p \quad \text{et} \quad x^p + y^p + z^p = 0$$

Preuve

Supposons qu'il existe (x,y,z) dans $\mathbb{Z}^3$ tel que

$$[xyz]_p \neq [0]_p \quad \text{et} \quad x^p + y^p + z^p = 0$$

Etape 1: on peut supposer x, y et z deux à deux premiers entre eux.

Notons d le pgcd de x, y et z. On a alors

$$\left(\frac{x}{d}\right)^p + \left(\frac{y}{d}\right)^p + \left(\frac{z}{d}\right)^p = 0 \quad , \quad \left[\frac{xyz}{d^3}\right]_p \neq 0$$

et $\operatorname{pgcd}\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right) = 1$. On peut donc supposer qu'on a

$$\operatorname{pgcd}(x,y,z) = 1.$$

Si on a $\operatorname{pgcd}(x,y) > 1$ alors considérons p_0 un diviseur

premier de $\text{pgcd}(x,y)$. Alors p_0 divise $x^p + y^p$ donc $-z^p$, puis comme p_0 est premier, on obtient qu'il divise z.
Or on a $\text{pgcd}(x,y,z) = 1$. Contradiction $\lightning$ Nécessairement, x, y et z sont premiers entre eux deux à deux.

Etape 2 : l'entier $q = 2p+1$ divise x, y ou z.

Pour montrer cela, on utilise le lemme suivant.

Lemme

Soit $m \in \mathbb{Z} \setminus q\mathbb{Z}$. Alors on a

$$m^p \equiv 1 \mod q \quad \text{ou} \quad m^p \equiv -1 \mod q$$

Preuve : comme q est premier, le petit théorème de Fermat assure qu'on a

$$m^{q-1} \equiv 1 \mod q$$

c-à-d $$(m^p)^2 \equiv 1 \mod q$$

Comme $\mathbb{F}_q$ est un corps, on en déduit le lemme ■

A présent, supposons que q ne divise aucun des entiers x, y et z.

Alors par le lemme, on obtient que la somme $x^p + y^p + z^p$ est congrue, modulo q, à $3, -3, 1$ ou -1, ce qui est contradictoire car on a

$$x^p + y^p + z^p = 0 \quad \text{et} \quad q > 5$$

Nécessairement, q divise un des entiers x, y, z.

Supposons que q divise x, cela ne perd pas en généralité.

Etape 3 : les entiers $x+y$, $y+z$ et $x+z$ sont des puissances de p.

On a

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

Notons m l'entier $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$.

- Montrons que m et $y+z$ sont premiers entre eux.

Supposons que cela ne soit pas le cas. Soit p_0 un diviseur premier commun à m et $y+z$.

Alors p_0^2 divise $-x^p$ et donc p_0 divise x. De plus, on a

$$y \equiv -z \mod p_0$$

et donc $$m \equiv \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv p y^{p-1} \mod p_0$$

Par lemme de Gauss, on en déduit

$$p_0 \mid p \quad \text{ou} \quad p_0 \mid y \qquad (p_0 \mid y^{p-1} \text{ puis } p_0 \mid y)$$

Comme $\text{pgcd}(y,z) = 1$ et $p_0 \mid y+z$, on obtient que p_0 ne divise pas y.

Par ailleurs, on ne peut avoir $p_0 = p$ car p ne divise pas x

Nécessairement, on obtient que $y+z$ et m sont premiers entre eux.

Alors comme $(y+z)m = (-x)^p$, il existe a, α des entiers tels que $y+z = a^p$ et $m = \alpha^p$.

De même, il existe b et c des entiers tels que $y+x = b^p$ et $z+x = c^p$.

Etape 4 : le bouquet final : la contradiction.

On a alors

$$b^p + c^p - a^p = x+y+x+z-(y+z) = 2x \equiv 0 \bmod q$$

Par ailleurs, comme $x \equiv 0 \bmod q$, on a

$$y \equiv b^p \bmod q \quad \text{et} \quad z \equiv c^p \bmod q$$

donc q ne divise ni b ni c car il ne divise ni y ni z (premiers avec x)

Comme b et c sont inversibles dans $\mathbb{F}_{2p+1}$, les éléments b^p et c^p ont pour carré 1.

On en déduit

$$y \equiv \pm 1 \bmod q \quad \text{et} \quad z \equiv \pm 1 \bmod q$$

Comme $y + z - a^p$ est congru à 0 modulo q, on en déduit que nécessairement q divise a^p donc divise a.

Comme q divise alors $y+z$, on en déduit comme précédemment

$$\alpha^p \equiv m \equiv p y^{p-1} \bmod q$$

puis $\alpha^p \equiv p\,(-1)^{p-1} \equiv p \bmod q$ car $\begin{cases} p-1 \text{ est pair} \\ y \equiv \pm 1 \bmod q \end{cases}$

ce qui est absurde par le lemme précédent $\lightning$

(Nécessairement, une puissance p-ième est congrue à -1, 0 ou 1 modulo q)

Cela conclut ∎