Théorème de Sophie Germain

Dorian Cacitti-Holland

2020-2021

Références.

1. Oraux X-ENS Algèbre 1

Leçons.

1. 121 Nombres premiers, applications
2. 126 Exemples d'équations en arithmétique
3. 142 PGCD et PPCM, algorithmes de calcul, applications

Théorême. Soit $p \in \mathcal{P}$ impair tel que $q = 2p + 1 \in \mathcal{P}$, alors il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que p ne divise pas xyz et

$$x^p + y^p + z^p = 0$$

Démonstration. On suppose par l'absurde qu'il existe $(x, y, z) \in \mathbb{Z}^3$ tel que

$$x^p + y^p + z^p = 0$$

Etape préliminaire : Se x, y, z premiers entre eux deux à deux(expliquer rapidement)
Sous-étape a : Premiers entre eux dans leur ensemble
Soit $d = PGCD(x, y, z)$, alors

$$\left(\frac{x}{d}\right)^p + \left(\frac{y}{d}\right)^p + \left(\frac{z}{d}\right)^p = \frac{1}{d^p}\left(x^p + y^p + z^p\right) = 0$$

avec $PGCD\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right) = 1$.
On peut donc supposer, quitte à diviser par d, que $PGCD(x, y, z) = 1$.
Sous-étape b : Premiers entre eux deux à deux
Si $PGCD(x, y) > 1$ alors il existe $p' \in \mathcal{P}$ divisant x et y.
Donc

$$p' \mid -(x^p + y^p) = z^p$$

Or $p' \in \mathcal{P}$, donc $p' \mid z$, d'où

$$1 = PGCD(x, y, z) \geq p'$$

Ce qui est absurde, d'où x et y sont permiers entre eux et par symétrie des rôles de x, y, z, on en déduit que

$$PGCD(x, y) = PGCD(y, z) = PGCD(x, z) = 1$$

Lemme. Soit $m \in \mathbb{Z}$ non divisible par q, alors

$$m^p \equiv \pm 1[q]$$

Démonstration. D'après le théorème de Fermat

$$(m^p)^2 = m^{q-1} \equiv 1[q]$$

D'où m^p est racine de $X^2 - 1 = (X-1)(X+1)$ dans $\mathbb{F}_q[X]$, ie $m^p \equiv \pm 1[q]$. □

Etape 1 : q divise au moins x, y ou z
On suppose par l'absurde que q ne divise ni x ni y ni z, alors d'après ce qui précède

$$x^p, y^p, z^p \equiv \pm 1[q]$$

D'où

$$0 = x^p + y^p + z^p \equiv \pm 1, \pm 3[q]$$

Ce qui est absurde car $q = 2p + 1 \geq 7$.
On peut donc supposer, quitter à inverser les rôles de x, y et z, que

$$q \mid x$$

De plus, comme x est premier avec y et z, q ne divise pas y et z.
Etape 2 : Calcul de $x + y, y + z$ et $x + z$
On a

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

Soit $p' \in \mathcal{P}$ divisant $y + z$ et r, alors, d'après le calcul précédent, $p'^2 \mid x^p$, d'où, comme p' premier,

$$p' \mid x$$

De plus

$$\sum_{k=0}^{p-1} y^k (-z)^{p-1-k} = r \equiv 0[p'], y \equiv -z[p']$$

Donc $py^{p-1} \equiv 0[p']$ ie $p' \mid py^{p-1}$.
Or p ne divise pas x car p ne divise pas xyz, donc $p \neq p'$, d'où $p' \mid y^{p-1}$.
Ainsi, comme p' premier,

$$p' \mid y$$

Ce qui est absurde car $PGCD(x, y) = 1$.
Par conséquent, en écrivant la décomposition en produits d'irréductibles de $-x$ et $1^p = 1, (-1)^p = -1$ car p impair, on en déduit qu'il existe $(a, \alpha) \in \mathbb{Z}^2$ premiers entre eux tel que

$$y + z = a^p, r = \alpha^p$$

Et par symétrie des rôles, de même, il existe $(b, c) \in \mathbb{Z}^2$ tel que

$$x + z = b^p, x + y = c^p$$

Etape 3 : Contradiction
Or $q \mid x$, donc q ne divise pas y et z, ainsi, d'après le lemme,

$$\begin{cases} y \equiv c^p[q] \equiv \pm 1[q] \\ z \equiv b^p[q] \equiv \pm 1[q] \end{cases}$$

De plus on a

$$b^p + c^p - a^p = 2x \equiv 0[q]$$

Si q ne divise pas a, alors, d'après le lemme, $a^p \equiv \pm 1[q]$ ce qui donne

$$\pm 1, \pm 3 \equiv 0[q]$$

ce qui est absurde car $q \geq 7$, donc

$$q \mid a$$

D'où $q \mid a^p = y + z$ ie $y \equiv -z[q]$.
Ainsi, par définition de r et imparité de p,

$$\alpha^p = r \equiv py^{p-1}[q] \equiv p(\pm 1)^{p-1}[q] \equiv p[q]$$

Or a et α sont premiers entre eux, donc q ne divise pas α, d'où, d'après le lemme,

$$\alpha^p \equiv \pm 1[q]$$

Par conséquent

$$p \equiv \pm 1[q]$$

Ce qui est absurde car $2p \equiv -1[q]$ et $q \geq 7$.
On aboutit finalement à une contradiction ce qui permet de conclure. □