Théorème de Sophie Germain

S. Francinou, H. Gianella, S. Nicolas, *Exercices de mathématiques, Oraux X-ENS, Algèbre 1*, 3e édition, Cassini. Exercice 4.39 page 167.

Recasage : 120, 121, 126.

Théorème 1

Soit p un nombre premier de Sophie Germain ie. $q = 2p+1$ est aussi premier. Il n'existe pas de triplet $(x,y,z) \in \mathbb{Z}^3$ tel que $xyz \equiv 0$ mod q et $x^p + y^p + z^p = 0$.

▷ Soit, par l'absurde, $(x,y,z) \in \mathbb{Z}^3$ tel que $xyz \equiv 0 \bmod q$ et $x^p + y^p + z^p = 0$. Quitte à considérer $x' = \dfrac{x}{x \wedge y \wedge z}, y' = \dfrac{y}{x \wedge y \wedge z}, z' = \dfrac{z}{x \wedge y \wedge z}$ on peut considérer $x \wedge y \wedge z = 1$.

– *Étape 1 : q divise l'un des trois entiers.* Supposons par l'absurde que q ne divise pas x, y et z. Alors, par le petit théorème de Fermat, $x^{q-1} \equiv 1 \bmod q$ donc $(x^p)^2 \equiv 1 \bmod q$ d'où, comme $\mathbb{Z}/q\mathbb{Z}$ est un corps, $x^p \equiv \pm 1 \bmod q$. De même, $y, z \equiv \pm 1 \bmod q$. Alors, $0 = x^p + y^p + z^p \bmod q \in \{\pm 1, \pm 3\}$: absurde. On peut donc supposer que q divise x. On a également montré que toute puissance p-ième est congrue à 0, 1, ou -1 modulo q.

– *Étape 2 : x, y, z sont premiers entre eux deux à deux.* Si, par l'absurde, $x \wedge y \neq 1$, soit p' un diviseur premier commun à x et y. Alors, $p' | x^p + y^p = -z^p$ donc $p' | z^p$ donc $p' | z$, ce qui contredit $x \wedge y \wedge z = 1$. Ainsi, $x \wedge y = 1$ et de même pour les autres couples. On en déduit que $q \not| y, z$.

– *Étape 3 : Factorisation de x^p, y^p, z^p en produit de puissance p-ièmes.* On a :

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

Supposons par l'absurde que $y+z$ et $\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$ ne sont pas premiers entre eux et soit p' un diviseur premier commun. Alors $p'^2 | -x^p$ donc $p' | x$. De plus, $y \equiv -z \bmod p'$ donc

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

donc $p' | p y^{p-1}$. Comme p' est premier :

⋆ soit $p' | p$ *ie.* $p' = p$ et alors $p | x$ et $p | xyz$: absurde.

⋆ soit $p' | y^{p-1}$ donc $p' | y$ et $x \wedge y \geq p'$: absurde.

Ainsi, $y+z$ et $\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$ sont premiers entre eux et leur produit est une puissance p-ième. Alors il existe $(a, \alpha) \in \mathbb{Z}^2$ tel que

$$y + z = a^p \qquad \text{et} \qquad \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = \alpha^p.$$

De même, il existe $b, c \in \mathbb{Z}$ tels que $x + y = c^p$ et $x + z = b^p$.

– *Conclusion.* Comme $y \equiv c^p \bmod q$ et $q \not| y$, on a $y \equiv \pm 1 \bmod q$. De même, $z \equiv \pm 1 \bmod q$. Supposons par l'absurde que $q \not| a$. Alors $a^p \equiv \pm 1 \bmod q$ et donc

$$0 \equiv 2x = b^p + c^p - a^p \bmod q \in \{\pm 1, \pm 3\} \qquad \text{absurde.}$$

Donc $q | a$. Ainsi, $y + z = a^p \equiv 0 \bmod q$, donc

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

ce qui contredit $\alpha^p \bmod q \in \{0, \pm 1\}$. □

Lemme 2

Soient a, b deux entiers naturels non nuls premiers entre eux et $k \geq 2$. S'il existe $c \in \mathbb{N}$ tel que $ab = c^k$ alors a et b sont aussi puissance k-ièmes d'entiers.

▷ Écrivons la décomposition de a, b et c en produits de facteurs premiers :

$$a = \prod_{p \in \mathcal{P}} p^{\alpha_p} \qquad b = \prod_{p \in \mathcal{P}} p^{\beta_p} \qquad c = \prod_{p \in \mathcal{P}} p^{\gamma_p}$$

où $(\alpha_p), (\beta_p), (\gamma_p) \in \mathbb{N}^{(\mathcal{P})}$. Comme $ab = c^k$, l'unicité de la décomposition de ab donne

$$\forall p \in \mathcal{P}, \qquad \alpha_p + \beta_p = k\gamma_p.$$

Or comme $a \wedge b = 1$, $\forall p \in \mathcal{P}$, $\alpha_p \beta_p = 0$, donc $\forall p \in \mathcal{P}$, $k | \alpha_p, \beta_p$. □