Théorème de Sophie Germain

Laura Gay d'après M. Varvenne et C. Robet

Référence : FGNAL1 : p.168 (Théorème) et p.140 (Lemme)

Lemme

Si le produit de deux entiers a et b premiers entre eux est une puissance k-ième (avec $k \geqslant 2$), alors a et b sont tous les deux des puissances k-ièmes.

Preuve du Lemme :

Soient a et b deux entiers premiers entre eux tels que $ab = c^k$ avec $c \in \mathbb{Z}$ et $k \geqslant 2$. Écrivons la décomposition en facteurs premiers de a, b et c :

$$a = \prod_{p \text{ premier}} p^{\alpha_p},\ b = \prod_{p \text{ premier}} p^{\beta_p} \text{ et } c = \prod_{p \text{ premier}} p^{\gamma_p}$$

où α_p, β_p et γ_p sont des familles d'entiers à support fini.
Comme $ab = c^k$, on obtient par unicité de la décomposition $\alpha_p + \beta_p = k\gamma_p$ pour tout p premier. De plus, comme $\text{pgcd}(a, b) = 1$ on a $\alpha_p \beta_p = 0$ [1] pour tout p premier. Il en résulte que pour tout p premier, α_p et β_p sont divisibles par k.
Finalement, a et b sont bien des puissances k-ièmes. ■

Théorème (*de Sophie Germain - 1823*)

Soit p un nombre premier de Sophie Germain, c'est-à-dire un nombre premier impair tel que $q = 2p + 1$ soit premier. Alors

$$\nexists\ (x, y, z) \in \mathbb{Z}^3 \text{ tel que } \ xyz \not\equiv 0\ [p] \ \text{ et } \ x^p + y^p + z^p = 0$$

Preuve du théorème :

On raisonne par l'absurde.
On suppose donné dans la suite un triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0\ [p]$ et $x^p + y^p + z^p = 0$.
Soit $d = \text{pgcd}(x, y, z)$. Quitte à poser $x' = \dfrac{x}{d}$, $y' = \dfrac{y}{d}$ et $z' = \dfrac{z}{d}$, on peut supposer [2] $d = 1$.

Etape 1 Montrons que x, y, z sont premiers entre eux deux à deux.
Supposons par l'absurde que $\text{pgcd}(x, y) > 1$ et soit p_0 un facteur premier qui divise x et y. Alors $p_0 | x^p + y^p$ donc $p_0 | z^p$ et donc $p_0 | z$ (Lemme d'Euclide) ce qui contredit le fait que $\text{pgcd}(x, y, z) = 1$.
Ainsi $\text{pgcd}(x, y) = 1$. De même, on en déduit que $\text{pgcd}(x, z) = 1$ et $\text{pgcd}(y, z) = 1$.

Etape 2 Montrons l'existence de $(a, \alpha) \in \mathbb{Z}^2$ tels que $y + z = a^p$ et $\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = \alpha^p$:

On remarque que :

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

D'après le **Lemme**, il suffit donc de montrer que $(y + z)$ et $\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$ sont premiers entre eux.

Supposons par l'absurde qu'il existe p' premier qui divise $(y + z)$ et $\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$.

Alors d'après $(\star)$, p'^2 divise x^p donc p' divise x.

1. car α_p ou β_p doit être nul
2. On aura toujours $x'y'z' \not\equiv 0\ [p]$ et $x'^p + y'^p + z'^p = 0$.

Comme $y \equiv -z\ [p']$, on en déduit une nouvelle "égalité" [3]

$$\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k \begin{cases} \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv py^{p-1}\ [p'] \\ \equiv 0\ [p']\ (\text{car } p' \Big| \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k) \end{cases}$$

Donc $p' \mid py^{p-1}$. D'après le lemme d'Euclide [4], $p'|p$ ou $p'|y^{p-1}$ dont $p'|y$.
$\hookrightarrow$ Si $p'|p$ (ie $p' = p$), cela signifie que $p|x$ (absurde par hypothèse).
$\hookrightarrow$ Si $p'|y$, cela contredit le fait que $\text{pgcd}(x, y) = 1$
D'où $(y + z)$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont premiers entre eux.

D'après le **Lemme**, comme leurs produits est une puissant p-ième $(-x^p)$ il existe $(a, \alpha) \in \mathbb{Z}^2$ tel que $y + z = a^p$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p$.

Par symétrie, il existe $(b, c) \in \mathbb{Z}^2$ tel que $\underline{x + y = c^p \text{ et } x + z = b^p}$.

Etape 3 Un et un seul des 3 entiers x, y, z est divisible par q :
Soit $m \in \mathbb{Z}$ tel que $m \not\equiv 0\ [q]$, d'après le petit théorème de Fermat

$$m^{q-1} \equiv 1\ [q] \Rightarrow m^{2p} \equiv 1\ [q] \Rightarrow m^p \equiv \pm 1\ [q]\ \ (\text{car } \mathbb{Z}/q\mathbb{Z} \text{ est un corps})\ [5]$$

Supposons par l'absurde qu'aucun des trois entiers x, y, x n'est divisible par q.
Alors $x^p \equiv \pm 1\ [q]$, $y^p \equiv \pm 1\ [q]$ et $z^p \equiv \pm 1\ [q]$.
Donc $(0 =)x^p + y^p + z^p$ est congru à $3, 1, -1$ ou -3 ce qui est absurde car $q > 5$ donc on ne peut pas avoir $3, -1, 1, -3 \equiv\ 0[q]$.

On peut donc supposer sans perte de généralité que $\underline{x \text{ est divisible par } q}$ (et c'est le seul car x, y, z sont premiers entre eux deux à deux).

Etape 4 Contradiction et conclusion :
On a $y + z = a^p$, $x + z = b^p$ et $x + y = c^p$ donc $b^p + c^p - a^p = 2x \equiv 0\ [q]$ $(\star\star)$.
D'autre part, $y \equiv c^p\ [q]$ car $x \equiv 0\ [q]$.
De plus, q ne divise pas y donc ne divise pas c^p et donc ne divise pas c. D'où $\underline{y \equiv c^p \equiv \pm 1\ [q]}$ (c'est le début de l'étape 3).
De même, $\underline{z \equiv \pm 1\ [q]}$.

Supposons q ne divise pas a, alors $a^p \equiv \pm 1\ [q] \Rightarrow c^p + b^p - a^p \equiv \pm 1$ ou $\pm 3\ [q]$ (absurde d'après $(\star\star)$).
Donc q divise a ie $y + z \equiv 0\ [q]$.
Avec cette dernière congruence, on peut écrire d'autre part

$$\begin{aligned} \alpha^p = \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k &\equiv py^{p-1}\ [q] \\ &\equiv p(\pm 1)^{p-1}\ [q] \\ &\equiv\ ^{[6]}\ p\ [q] \end{aligned}$$

Or une puissance p-ième $\equiv 0, \pm 1\ [q]$ (c'est le Fermat du début de l'étape 3 qui nous dit ça).
Dans tous les cas, on aboutit à une contradiction (si c'est congru à 0 ça nous donne $p \equiv 0\ [q]$ absurde, si c'est ± 1 ça nous donne $p \equiv \pm 1\ [q]$ ie $2p + 1 = q \equiv \pm 2 + 1 = 3$ ou $-1\ [q]$ absurde).
On en déduit finalement que

$$\underline{\nexists\ (x, y, z) \in \mathbb{Z}^3 \text{ tel que } xyz \not\equiv 0\ [p] \text{ et } x^p + y^p + z^p = 0.}$$

■

3. ça ne découle pas d'$(\star)$
4. et non Gauss comme écrit dans le livre
5. En fait on dit que dans $\mathbb{Z}/q\mathbb{Z}$ on a $(m^p)^2 - 1 = 0$ donc $(m^p - 1)(m^p + 1) = 0$ et par intégrité -car c'est un corps- on a le truc voulu
6. car $p - 1$ est pair

Réponses à de possibles questions

1. Pourquoi on suppose p impair ?
   $\hookrightarrow$ L'égalité $x^p + y^p = (x+y)\sum_{k=0}^{p-1} x^k(-y)^{p-1-k}$ n'est vraie que pour p impair (faux je crois ? ?).
   Si $p = 2$, il n'y a pas de solutions.

Notes :

✓ **A l'oral**, bla
✓ Lemme d'Euclide : Si un nombre premier p divise bc, alors p divise b ou c. Une généralisation est :
Lemme de Gauss : Si un nombre entier a divise bc, et si $a \wedge b = 1$, alors a divise c.
✓ Le plus grand nombre premier de Sophie Germain actuellement connu est $39051 \times 2^{6001} - 1$ trouvé en 1986. On conjecture qu'il en existe un infinité.
♣ Marie-Sophie Germain (1776 - 1831), est une mathématicienne et philosophe française. Elle est connue pour le théorème d'arithmétique qui porte son nom, pour ses échanges avec le mathématicien Gauss et pour ses travaux sur l'élasticité des corps. Elle avait pour nom d'emprunt Antoine Auguste Le Blanc. Lorsqu'elle se voit obligée de réveler son identité, Gauss devient encore plus fan d'elle et lui envoie une lettre de "déclaration" d'admiration.