Oraux X-ENS
Algèbre 1 - FGN (p153)

120 Développement : Théorème de Sophie Germain.
121
122 Théorème : Soit p premier impair tel que $q = 2p+1$ est premier.
123 Alors $\nexists (x,y,z) \in \mathbb{Z}^3 \setminus \; p \nmid xyz$ et $x^p + y^p + z^p = 0$.
126
142 Preuve : ORAL
150 L'idée est d'utiliser l'existence de PGCD dans $\mathbb{Z}$ et la factorialité de $\mathbb{Z}$ pour montrer 6 résultats en raisonnant par l'absurde.

On suppose par l'absurde qu'il existe un tel triplet et soit un tel triplet (x,y,z).

① Quitte à diviser par $x \wedge y \wedge z$, on peut supposer $x \wedge y \wedge z = 1$

② Montrons que $x \wedge y = x \wedge z = y \wedge z = 1$.
Supposons par l'absurde que $x \wedge y \neq 1$. Soit k premier tel que $k \mid x$ et $k \mid y$ (par le lemme d'Euclide). Ainsi $k \mid -z^p$ et puisque k est premier, par le lemme d'Euclide, $k \mid z$. ABS car $x \wedge y \wedge z = 1$ par ①
En échangeant les rôles de x, y et z, on obtient le résultat.

③ Soit $m \in \mathbb{Z}$ tel que $q \nmid m$. Par le petit théorème de Fermat
$m^{q-1} = m^{2p} = (m^p)^2 \equiv 1 \; [q]$
Alors $(m^p)^2 - 1^2 = (m^p - 1)(m^p + 1) \equiv 0 \; [q]$ or $\mathbb{Z}/q$ int car q l'est.
donc $m^p \equiv \pm 1 \; [q]$ (car $q \neq 1$).

④ Montrons que $q \mid x$, ou $q \mid y$, ou $q \mid z$. Si c'était pas le cas :
$q \nmid x$, $q \nmid y$ et $q \nmid z$ et d'après ③ $x^p + y^p + z^p = 0 \equiv \pm 1, \pm 3 \; [q]$
ABS car $q \geq 7$ ne peut pas diviser $\pm 1, \pm 3$.
On peut supposer $q \mid x$ et par ②, $q \nmid y$ et $q \nmid z$.

⑤ On décompose x^p, y^p, z^p.
$-x^p = y^p + z^p = y^p - (-z)^p = (y+z) \underbrace{\sum_{k=0}^{p-1} y^k (-z)^{p-k-1}}_{n} = (y+z)\,n.$
(p impair)

• Mq $y+z \wedge n = 1$. Si ce n'est pas le cas, il existe k premier tel que :

i) d'une part $k^2 \mid x^p$ et puisque k est premier, $k \mid x$ (lemme d'Euclide)

ii) d'autre part $y \equiv -z \ [k]$ et $n \equiv \sum_{0}^{p-1} y^{p-1} \equiv p y^{p-1} \ [k]$

Or $p \nmid x$ car $p \nmid x y z$ donc $k \neq p$ et $k \wedge p = 1$

Par Gauss, $k \mid y^{p-1}$ et par euclide $k \mid y$. ABS car $x \wedge y = 1$ par ②

Ainsi $n \wedge y+z = 1$.

Astuce ⚠ $\begin{cases} -x^p = (y+z)n = -(x_1^{\alpha_1} \dots x_n^{\alpha_n})^p \text{ où } x_i \mid y+z \text{ ou (exclusif)} \\ x_i \mid n \text{ car } n \wedge (y+z). \text{ Dans ce cas } x_i^{\alpha_i \cdot p} \mid y+z \text{ ou } n \text{ et il} \end{cases}$

existe $\alpha \wedge a = 1$ tels que $a^p = y+z$ et $\alpha^p = n$

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

Pour b et c, ce raisonnement, il faut juste l'écrire

⑥ On cherche une contradiction.

$$\begin{cases} b^p + c^p - a^p \equiv 2x \equiv 0 \ [q] \\ y \equiv b^p \equiv \pm 1 \ [q] \\ z \equiv c^p \equiv \pm 1 \ [q] \end{cases}$$

• Si $q \nmid a$ alors par ③ $b^p + c^p - a^p \equiv \pm 1, \pm 3 \ [q]$ donc $q \mid \pm 1, \pm 3$

ABS car $q \geq 7$. Alors $q \mid a$

• En particulier, $q \mid a^p = y+z$ et $y \equiv -z \ [q]$

Ainsi $n = \alpha^p \equiv p y^{p-1} \ [q] \equiv p(-1)^{p-1} \ [q] \equiv p \ [q]$.

• Par ailleurs $a \wedge \alpha = 1$ donc $q \nmid \alpha$ et par ③ $\alpha^p \equiv \pm 1 \ [q]$.

Ainsi $p \equiv \pm 1 \ [q]$ ABS car $2p+1 = q > p+1$.

Conclusion : il n'existe pas de tel triplet (x, y, z).