Oraux X-ENS Algèbre 1 - FGN (p.153)

120 121 (122) 123 126 142 150

Théorème de Sophie Germain

Théorème : Soit p premier impair tel que $q := 2p+1$ est premier.

Alors : $\nexists (x;y;z) \in \mathbb{Z}^3 \setminus \begin{cases} xyz \not\equiv 0 [p] \\ x^p + y^p + z^p = 0 \end{cases}$

Preuve : oral

L'idée pour montrer ce résultat est de : utiliser l'existence de PGCD dans $\mathbb{Z}$ et la factorialité de $\mathbb{Z}$ pour montrer 6 résultats en raisonnant par l'absurde.

Supposons par l'absurde qu'il existe un tel triplet et soit un tel triplet : $x;y;z$.

① Quitte à diviser par $PGCD(x;y;z)=1$, ops $PGCD(x;y;z)=1$.

② Montrons que $PGCD(x;y) = PGCD(y;z) = PGCD(x;z) = 1$.
Supposons par l'absurde que $PGCD(x;y) \neq 1$.
Soit p' premier tel que $\boxed{p' | x}$ et $\boxed{p' | y}$.
Ainsi, $p' | -z^p$ et puisque p' est premier, par le lemme d'Euclide, $\boxed{p' | z}$
ABSURDE puisque $PGCD(x;y;z)=1$ par ①
En échangeant les rôles de $x;y$ et z, on a le résultat.

③ Montrons : $\forall m \in \mathbb{Z},\ m \not\equiv 0 [q] \Rightarrow m^p \equiv \pm 1 [q]$
Soit $m \in \mathbb{Z}$ tel que $m \not\equiv 0 [q]$.
Par le petit théorème de Fermat,
$$(m^p)^2 \equiv m^{q-1} \equiv 1 [q]$$
Puisque q est premier, $m^p \equiv \pm 1 [q]$

④ Montrons que $q | x$ ou $q | y$ ou $q | z$
Supposons par l'absurde que non.
Ainsi $x \not\equiv 0 [q], y \not\equiv 0 [q], z \not\equiv 0 [q]$.
Alors $x^p + y^p + z^p \equiv \pm 1, \pm 3 [q]$ par ③
ABSURDE car $q \geq 7$
Ops $q | x$ et par ②, $q \nmid y$ et $q \nmid z$.

⑤ Décomposons x^p, y^p et z^p.
$$-x^p = y^p + z^p = y^p - (-z)^p = (y+z) \underbrace{\sum_{k=0}^{p-1} y^k (-z)^{p-k-1}}_{=:r}$$

- Supposons par l'absurde qu'il existe p' premier tel que $p' | y+z$ et $p' | r$. Soit un tel p'.
D'une part, $p'^2 | x^p$ et puisque p' est premier, par le lemme d'Euclide, $\boxed{p' | x}$
D'autre part, $y \equiv -z [p']$ donc : $r \equiv \sum_{k=0}^{p-1} y^{p-1} [p']$
$\equiv p y^{p-1} [p']$
Or : $p \nmid x$ car $p \nmid xyz$ donc $p \neq p'$
Ainsi, $p' | y^{p-1}$ et par lemme d'Euclide, $\boxed{p' | y}$.
ABSURDE car $PGCD(x;y)=1$ par ②.
Il n'existe alors pas de diviseur commun à $y+z$ et r.

- Soit alors $a \wedge \alpha = 1$ tels que $y+z = a^p$ et $r = \alpha^p$.
De même, soit $b, c \in \mathbb{Z}$ tels que $x+y = b^p$ et $x+z = c^p$.

⑥ Trouvons une contradiction.
$$\begin{cases} b^p + c^p - a^p = 2x \equiv 0 [q] \\ y \equiv b^p [q] \equiv \pm 1 [q] \\ z \equiv c^p [q] \equiv \pm 1 [q] \end{cases}$$

- Supposons par l'absurde que $q \nmid a$.
Par ③, $b^p + c^p - a^p \equiv \pm 1, \pm 3 [q]$
ABSURDE car $q \geq 7$. Alors $q | a$.
- En particulier, $q | a^p = y+z$ et alors $y \equiv -z [q]$.
Ainsi, $r = \alpha^p \equiv p y^{p-1} [q] \equiv p (-1)^{p-1} [q]$
d'où : $\boxed{\alpha^p \equiv p [q]}$
- Par ailleurs, $a \wedge \alpha = 1$ donc $q \nmid \alpha$.
Par ③, $\boxed{\alpha^p \equiv \pm 1 [q]}$
Ainsi, $p \equiv \pm 1 [q]$
ABSURDE car $2p \equiv -1 [q]$

Il n'existe alors pas de tel triple $x;y;z$.

Temps
12' 22" Speechless
11' 54" Speechless