réf : FGN, alg 1

Développement : Théorème de Sophie Germain

Leçons : 121, 126, 120, 142

Thm : Soit p un nombre premier impair tq $q = 2p+1$ premier. p est un nombre premier de Sophie Germain. Alors il n'existe pas de solutions $(x,y,z) \in \mathbb{Z}^3$, avec $x,y,z \not\equiv 0\ [p]$ de l'équation $x^p + y^p + z^p = 0$

Preuve :

On raisonne par l'absurde : Supposons $\exists$ une telle solution $(x,y,z) \in \mathbb{Z}^3$.
Soit $d = \text{pgcd}(x,y,z)$. Quitte à considérer $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$ encore solution, on peut supposer x,y,z mutuellement premiers entre eux. Ils sont alors 2 à 2 premiers entre eux :

En effet : soit $d \in \mathbb{P}$ tq $d \mid x$ et $d \mid y$. Alors $d \mid x^p$ et $d \mid y^p$ donc $d \mid x^p + y^p = -z^p$. D'après le lemme d'Euclide, $d \mid z$.
Or $\text{pgcd}(x,y,z) = 1$. Donc $d = 1$.

▶ Mq $\forall m \in \frac{\mathbb{Z}}{q\mathbb{Z}}$, $m^p \equiv \pm 1\ [q]$

Comme $q \in \mathbb{P}$, par le petit théorème de Fermat, $m^{q-1} \equiv 1\ [q]$
Autrement dit, $(m^p)^2 \equiv 1\ [q]$.
Or $\frac{\mathbb{Z}}{q\mathbb{Z}}$ corps et $q \neq 2$ donc on a nécessairement $m^p = \pm 1\ [q]$.
Remarquons que si $m \in q\mathbb{Z}$, on a $m^p \equiv 0\ [q]$.

▶ Mq un et un seul des x,y,z est multiple de q :

D'une part, comme ils sont 2 à 2 premiers entre eux, il y a au plus un multiple de q. S'il n'y en a aucun, d'après le point 1, dans $\frac{\mathbb{Z}}{q\mathbb{Z}}$, $x^p + y^p + z^p \in \{-\bar{3}, -\bar{1}, \bar{1}, \bar{3}\}$
Or $x^p + y^p + z^p = \bar{0}$ et $\bar{0} \notin \{-\bar{3}, -\bar{1}, \bar{1}, \bar{3}\}$ car $q \geqslant 7$

Ainsi un seul des entiers est multiple de q. Quitte à renommer les solutions, on peut supposer $x \in q\mathbb{Z}$. Alors $y,z \notin q\mathbb{Z}$.

▶ Mq $\exists\, a, b, c, \alpha \in \mathbb{Z}$ tq $\begin{cases} y+z = a^p \ ; \ x+z = b^p \ ; \ x+y = c^p \\ \sum_{k=0}^{p-1} y^k \cdot (-z)^{p-1-k} = \alpha^p \end{cases}$

Par l'identité de Bernoulli, et comme p est impair (utiliser $\sum_k q^k$)

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

Montrons par l'absurde qu'ils n'ont aucun diviseur premier commun.

Soit $d \in \mathbb{P}$ tq $d \mid y+z$ et $d \mid \sum_{k=0}^{p-1} y^k \cdot (-z)^{p-1-k}$

Alors $d^2 \mid (-x)^p$ donc par le lemme d'Euclide, $d \mid x$.

De plus, on a $y \equiv -z\,[d]$.

Donc $0 \equiv \sum_{k=0}^{p-1} y^k \cdot (-z)^{p-1-k} \equiv \sum_{k=0}^{p-1} y^{p-1} = p \cdot y^{p-1}\,[d]$.

Ainsi $d \mid p \cdot y^{p-1}$.

Par euclide,

- soit $d \mid p$, alors $d = p$. Ainsi $p \mid x$, et on a fait l'hypothèse que ce n'était pas le cas.
- soit $d \mid y$. On on a déjà $d \mid x$: contradiction car x et y premiers entre eux.

Ainsi, $(y+z) \wedge \sum_{k=0}^{p-1} y^k \cdot (-z)^{p-1-k} = 1$ et la relation initiale nous donne que ce sont tout deux des puissances de p. Par symétrie, $x+z$ et $x+y$ le sont aussi.

▶ Raisonnons modulo q : Dans $\mathbb{Z}/q\mathbb{Z}$

On a $c^p = x+y = y \neq 0$. Donc $c \notin q\mathbb{Z}$. D'où $c^p \equiv \pm 1\,[q]$. (point 1)

De même, $b^p \equiv \pm 1\,[q]$ d'après le premier point.

Supposons que q ne divise pas a. Alors également $a^p \equiv \pm 1\,[q]$. Par suite, $b^p + c^p - a^p \in \{-\bar{3}, -\bar{1}, \bar{1}, \bar{3}\}$. Par ailleurs $b^p + c^p - a^p = 2x = \bar{0}$.

Contradiction, donc $q \mid a$.

En particulier, $y+z \equiv a^p \equiv 0\,[q]$. Par conséquent $\alpha^p \equiv \sum_{k=0}^{p-1} y^k (-z)^{p-1-k} \equiv p \cdot y^{p-1}\,[q]$.

Or $y \equiv \pm 1\,[q]$, et $p-1$ pair d'où $\alpha^p \equiv p\,[q]$. Or d'après le lemme $\alpha^p \equiv -1, 0, 1\,[q]$: contradiction.

Questions :

1) Prouver le théorème de Fermat :

Théorème : soit p premier. $x \in \mathbb{N}$. Alors $x^p \equiv x \ [p]$

preuve

cas $p=2$ | $\forall x \in \mathbb{Z}$, $x^2 - x = x(x-1)$. Ainsi $x^2 - x$ produit de deux nbrs consécutifs, et est donc pair. Autrement dit $x^2 \equiv x \ [2]$, $\forall x \in \mathbb{Z}$.

Supposons p impair. Mq par récurrence sur $x \in \mathbb{N}$ que $x^p \equiv x \ [p]$. Vrai pour $x=0$.

$(x+1)^p = x^p + C_p^1 x^{p-1} + \cdots + C_p^k x^{p-k} + \cdots + C_p^1 * 1$

et $p \mid C_p^k$ $\forall k \in]0, p[$. Ainsi : $(x+1)^p \equiv x^p + 1$

$\overset{HR}{\equiv} x+1 \ [p]$

Pour les entiers négatifs, on multiplie par $(-1)^p$.

Corollaire : p premier, $p \nmid x$. $x^{p-1} \equiv 1 \ [p]$.

preuve

| soit x tq. $p \nmid x$. $p \mid x^p - x = x(x^{p-1} - 1)$, or $p \nmid x$ donc $p \mid x^{p-1} - 1$. (Euclide). Ainsi $x^{p-1} \equiv 1 \ [p]$.