FGN, Alg 1	Théorème de Sophie-Germain	L 120 L 121 L 126 L 142

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

Démonstration : On raisonne par l'absurde en supposant qu'il existe une telle solution $(x, y, z) \in \mathbb{Z}^3$.
Soit $d = \text{pgcd}(x, y, z)$. Quitte à considérer $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ encore solution, on peut supposer x, y, z mutuellement 1ers entre eux.
Ils sont alors 2 à 2 premiers entre eux. En effet,
Soit $d \in \mathbb{P}$ tq $d | x$ et $d | y$, alors $d | x^p + y^p = -z^p$.
D'après le lemme d'Euclide, $d | z$. Or $\text{pgcd}(x, y, z) = 1$ ↯.

① Mq $\forall m \in \mathbb{Z} \setminus q\mathbb{Z}$, on a : $m^p \equiv \pm 1 \ [q]$.
Comme $q \in \mathbb{P}$, d'après le petit th de Fermat, $m^{q-1} \equiv 1 \ [q]$
autrement dit, $(m^p)^2 \equiv 1 \ [q]$.
Or $\mathbb{Z}/q\mathbb{Z}$ est un corps, et $q \neq 2$, donc on a nécessairement $m^p \equiv \pm 1 \ [q]$.
Remarquons que si $m \in q\mathbb{Z}$, on a : $m^p \equiv 0 \ [q]$

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

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

③ Mq $\exists\, a, b, c, \alpha \in \mathbb{Z}$ tels que :

$y+z = a^p$; $x+z = b^p$; $x+y = c^p$; $\sum_{k=0}^{p-1} y^k (-z)^{p-1-k} = \alpha^p$.

Par l'identité de Bernoulli, et comme p est impair,

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

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

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

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

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

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

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

D'après Euclide, ou bien $d \mid p$ alors $d = p$, auquel cas $p \mid x$,

or on a fait l'hypothèse que ce n'était pas le cas;

ou bien : $d \mid y$. Or on a déjà $d \mid x$ $\lightning$ car x et y st 1^{ers} entre eux.

Ainsi, $y+z \wedge \sum_{k=0}^{p-1} y^k (-z)^{p-1-k} = 1$, et la relation initiale nous donne

que ce sont tous deux des puissances de p.

Par symétrie, $x+z$ et $x+y$ le sont aussi.

④ 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 $c^p \equiv \pm 1\ [q]$

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

Supposons que q ne divise pas a, alors on a 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, $b^p + c^p - a^p = 2x = \bar{0}$: $\lightning$ Donc $q \mid a$

En particulier, $y+z \equiv a^p \equiv 0\ [q]$.

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

Or $y \equiv \pm 1\ [q]$ et $p-1$ est pair, d'où $\alpha^p \equiv p\ [q]$.

Or d'après le lemme $\alpha^p \equiv -1, 0, 1\ [q]$.

Contradiction finale.