Dev : Thm de Sophie Germain.

Leçons: 120, 142
Réf : Oraux X-ENS Al 1 p 167.

Thm : Soit p un nombre premier de Sophie Germain. (p impair, $q=2p+1$ 1er)
Il n'existe pas de triplet $(x,y,z)\in\mathbb{Z}^3$ tq $\begin{cases} xyz\not\equiv 0 \ [p] \\ x^p+y^p+z^p=0 \end{cases}$

Dem : Soit p un nombre de Sophie Germain.
Supposons, PAR L'ABSURDE : $\exists (x,y,z)\in\mathbb{Z}^3$, $\begin{cases} xyz\not\equiv 0 \ [p] \\ x^p+y^p+z^p=0 \end{cases}$

admettre.

① Se ramener aux pgcd $=1$.

$d := \text{pgcd}(x,y,z)$. et $x'=\frac{x}{d}$, $y'=\frac{y}{d}$, $z'=\frac{z}{d}$. ($\text{pgcd}(x',y',z')=1$)

* $x'^p+y'^p+z'^p = \frac{x^p+y^p+z^p}{d^p} = 0$

* $x'y'z' = \frac{xyz}{d^3} \not\equiv 0 \ [p]$.

② x, y, z 2à2 premiers entre eux.
Par absurde, Supp $x\wedge y \neq 1$. Soit p_0 un diviseur premier.
$p_0 \mid x^p+y^p \Rightarrow p_0 \mid z^p \Rightarrow p \mid z$ (car p 1er + lemme d'Euclide).
$p_0 \mid \text{pgcd}(x,y,z)=1$ ABSURDE.
x, y sont premiers entre eux et on conclu par symétrie des rôles.

③ $y+z=a^p$; $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p$ ($x+z=b^p$, $x+y=c^p$)

$\underbrace{(y+z)}_{:=X}\underbrace{\left(\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k\right)}_{:=Y} = y^p+z^p = -x^p = (-x)^p$ car p impair
par somme télescopique. car nbre S G.

Supposons par l'absurde que $X\wedge Y\neq 1$. Soit p' diviseur premier.
* $p' \mid (-x)^p \Rightarrow p' \mid x$ (car p' 1er) (*)
* $y\equiv -z \ [p'] \Rightarrow Y \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv p y^{p-1} \ [p']$

* $p' \mid Y \Rightarrow Y\equiv 0 \ [p']$ d'où $p' \mid p y^{p-1}$
  i) $p' \mid p \Rightarrow p'=p \Rightarrow p \mid x \Rightarrow xyz\equiv 0 \ [p]$: ABS. (†)
  (car tous 2 1er)
  ii) $p' \mid y^{p-1} \Rightarrow p' \mid y \Rightarrow p' \mid x\wedge y = 1$: ABS.

Ainsi $X\wedge Y = 1$: $\exists a, \alpha\in\mathbb{Z}$; $X=a^p$ $Y=\alpha^p$.

De même ; $\exists b, c$ $x+z=b^p$, $x+y=c^p$. (par symétrie des rôles)

④ x ou y ou z est divisible par q.
Supp, par l'absurde, qu'aucun de x, y, z ne soit divisible par q.

Soit $m\in\mathbb{Z}$ tq $q\nmid m$. q 1er de $q\wedge m=1$ et par le petit Thm de Fermat :

$m^{q-1}\equiv 1 \ [q] \Leftrightarrow (m^p)^2 \equiv 1 \ [q] \Leftrightarrow (m^p-1)(m^p+1)\equiv 0 \ [q]$
(id remarquable)
$q=2p+1$
$\Leftrightarrow m^p\equiv 1 \ [q]$ ou $m^p\equiv -1 \ [q]$ car $\mathbb{Z}/q\mathbb{Z}$ corps

Ainsi, $x^p+y^p+z^p \equiv 3, 1, -1$ ou $-3 \ [q]$.

Or $q>5$. ABSURDE !
On suppose $q \mid x$.

⑤ $a^p \equiv 0 \ [q]$.

$y \equiv c^p$ et $z \equiv b^p$ (car $x \equiv 0 \ [q]$)
Or $x \wedge y = 1$ donc $q \nmid y \Rightarrow q \nmid c \Rightarrow y \equiv \pm 1 \ [q]$ par ③.
De même $z \equiv \pm 1 \ [q]$.
Supposons $q \nmid a$: $a^p \equiv \pm 1 \ [q] \Rightarrow c^p + b^p - a^p \equiv 3, 1, -1, -3 \ [q]$.
Or $c^p + b^p - a^p \equiv x + z + x + y - y - z = 2x \equiv 0 \ [q]$ ABSURDE. $(q > 5)$
Donc $q \mid a$ et $a^p \equiv 0 \ [q]$.

⑥ Etude de α^p + Conclusion :
$y + z \equiv a^p \equiv 0 \Rightarrow \alpha^p = Y \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv p\, y^{p-1} \ [q]$ (car $-z \equiv y \ [q]$)

Or $y \equiv \pm 1$ donc $\alpha^p \equiv p \ [q]$ ($p-1$ est pair) $(\pm 1)^{p-1} = 1$.

ABSURDE car $\rightarrow q \mid \alpha \rightsquigarrow \alpha^p \equiv 0 \ [q]$
$\rightarrow q \nmid \alpha \rightsquigarrow \alpha^p \equiv \pm 1 \ [q]$ par ③. $p \neq 0, 1, -1$

On en conclut qu'il n'existe pas de tel triplet.