X-ENS Al 1
4.39
$p \in \mathbb{P}$, $2p+1 \in \mathbb{P}$, $p \neq 2$.

Théorème de Sophie Germain

126, 142,

Théorème : Il n'existe pas de triplet $(x,y,z) \in \mathbb{Z}^3$, $x^p + y^p + z^p = 0$ et $xyz \not\equiv 0 [p]$.

Raisonnons par l'absurde : soit $(x,y,z) \in \mathbb{Z}^3$ tq $x^p + y^p + z^p = 0$ et $xyz \not\equiv 0 [p]$.

Résultat 1 : On peut supposer $\text{pgcd}(x,y,z) = 1$ et $x \wedge y = y \wedge z = z \wedge x = 1$.

Soit $d = \text{pgcd}(x,y,z)$. Si $x' = \frac{x}{d}$, $y' = \frac{y}{d}$, $z' = \frac{z}{d}$, alors $\begin{cases} x'^p + y'^p + z'^p = 0 \text{ et } x' \wedge y' \wedge z' = 1 \\ x'y'z' \not\equiv 0 [p] \end{cases}$.

Donc on peut supposer $\text{pgcd}(x,y,z) = 1$.

Si p_0 divise x et y, alors p_0 divise $x^p + y^p = -z^p$ puis par lemme d'Euclide, p_0 divise z. Mais $\text{pgcd}(x,y,z) = 1$ donc $p_0 = 1$. Ainsi $x \wedge y = 1$

De même pour les autres couples.

Résultat 2 : Il existe a, α entiers tels que $y+z = a^p$, $\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = \alpha^p$
b, c $x+z = b^p$, $x+y = c^p$.

On a $(y+z)\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = y^p + z^p = -x^p$. (*)

Si $p_0^{\neq 1}$ divise $y+z$ et $\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$, alors $p_0^2 \mid x^p$ donc $p_0 \mid x$ par Euclide

De plus, $p_0 \mid y+z$, donc $-z \equiv y [p_0]$, donc $\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \equiv p\, y^{p-1} [p_0]$.
$\equiv 0 [p_0]$ car p_0 divise

Donc $p_0 \mid p y^{p-1}$. Par lemme de Gauss :

→ soit $p_0 \mid p$, et alors $p_0 = p$ et donc $p \mid x$, absurde. ($xyz \not\equiv 0 [p]$).

→ soit $p_0 \mid y^{p-1}$ et alors $p_0 \mid y$ par lemme d'Euclide, donc $p_0 \mid x \wedge y = 1$ absurde.

De là, $y+z$ et $\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$ sont p.c.e. et (*) donne a et α valués (en observant les valuations des décompositions)

De même pour $x+z$, $x+y$.

Résultat 3 : Si $m \in \mathbb{Z}$ tq $q \nmid m$ alors $m^p \equiv \pm 1 [q]$.

q est premier, donc par petit théorème de Fermat, $m^{q-1} \equiv 1 [q]$.

Autrement dit, $(m^p)^2 - 1 \equiv 0 [q]$. Puisque $X^2 - 1$ a deux racines ± 1 dans $\mathbb{F}_q$, un corps, $m^p \equiv \pm 1 [q]$.

De là, si ni x, ni y, ni z ne sont divisibles par q, $x^p + y^p + z^p \equiv \pm 1$ ou $\pm 3 [q]$ ce qui est impossible car $x^p + y^p + z^p = 0$ et $q > 5$.

On peut donc supposer $\boxed{q \mid x}$ (quitte à permuter) et $q \nmid yz$ car $x \wedge y = x \wedge z = 1$.

Résultat 4 : On a : $b^p + c^p - a^p \equiv 0 [q]$, $a \equiv 0 [q]$, $y \equiv c^p [q]$, $\alpha^p \equiv p y^{p-1} [q]$.

D'après 2, $b^p + c^p - a^p = 2x \equiv 0 [q]$. De plus, $x + y = c^p$ donc $y \equiv c^p [q]$ car $q \mid x$.

Or $q \nmid y$ donc $q \nmid c$ donc d'après 3, $c^p \equiv \pm 1 [q]$, et de même, $b^p \equiv \pm 1 [q]$.

Si $q \nmid a$, alors $a^p \equiv \pm 1 [q]$, donc $b^p + c^p - a^p \equiv \pm 1$ ou $\pm 3 [q]$, absurde (car $q > 5$).

Donc $q \mid a$.

Enfin, $y + z = a^p$ donc $-z \equiv y [q]$ donc $\alpha^p \equiv p y^{p-1} [q]$. Or $y \equiv c^p \equiv \pm 1 [q]$

Donc $y^{p-1} \equiv 1 [q]$, $\alpha^p \equiv p [q]$ absurde par 3.