VH
2/05/15

Théorème de Sophie-Germain

120, 121, 126.

Réf : FGN alg 1.

Théorème (Sophie-Germain)

Soit p un nombre premier impair tel que $q = 2p+1$ soit premier. Alors il n'existe pas de triplet $(x,y,z) \in \mathbb{Z}^3$ tel que $x^p + y^p + z^p = 0$ et $xyz \not\equiv 0 \pmod p$.

dém : Raisonnons par l'absurde. Soit $(x,y,z) \in \mathbb{Z}^3$ tel que

$$x^p + y^p + z^p = 0 \quad (*) \quad \text{et} \quad xyz \not\equiv 0 \pmod p.$$

- Quitte à diviser x, y, z par leur pgcd, on peut supposer $\text{pgcd}(x,y,z) = 1$.

Montrons que $\text{pgcd}(x,y) = 1$. Supposons $\text{pgcd}(x,y) > 1$.

Soit p_0 premier divisant x et y. Alors p_0 divise $x^p + y^p = -z^p$

Donc p_0 divise z donc p_0 divise $\text{pgcd}(x,y,z) = 1$: exclu.

On a donc $\text{pgcd}(x,y) = 1$. De même, $y \wedge z = 1$, $x \wedge z = 1$.

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

$$= (y+z)\, u.$$

Supposons par l'absurde que $\text{pgcd}(y+z, u) > 1$. Soit p_0 premier divisant $y+z$ et u.

Alors $y \equiv -z \pmod{p_0}$

Donc $0 \equiv u \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv p\, y^{p-1} \pmod{p_0}$

On p_0 divise $(y+z)u = -x^p$ donc p_0 divise x. Comme $x \wedge y = 1$, p_0 ne divise pas y. D'après le théorème de Gauss, p_0 divise p.

Ainsi $p_0 = p$. Donc p divise x donc xyz, ce qui est exclu par hypothèse.

Donc $\text{pgcd}(y+z, u) = 1$.

On a $(y+z)u = (-x)^\uparrow$, $\operatorname{pgcd}(y+z, u) = 1$.

Par factorialité de $\mathbb{Z}$, $\exists a, \alpha \in \mathbb{Z}$ tels que

$$y+z = a^\uparrow \quad \text{et} \quad u = \alpha^\uparrow.$$

De même, il existe $b, c \in \mathbb{Z}$ tels que $x+z = b^\uparrow$, $x+y = c^\uparrow$.

Lemme : Si $m \in \mathbb{Z}$ n'est pas divisible par q, alors $m^\uparrow \equiv \pm 1 \ [q]$

dém : Par le petit théorème de Fermat, $m^{q-1} \equiv 1 \ [q]$,
donc $m^{\uparrow 2} \equiv 1 \ [q]$. $X^2 - 1$ a deux racines (1 et -1)
dans $\mathbb{F}_q$: $m^\uparrow \equiv \pm 1 \ [q]$. □

- Montrons que q divise xyz.
  Si $q \nmid xyz$, alors $x^\uparrow \equiv \pm 1 [q]$, $y^\uparrow \equiv \pm 1 [q]$, $z^\uparrow \equiv \pm 1 [q]$
  donc $x^\uparrow + y^\uparrow + z^\uparrow \equiv \pm 3, \pm 1 \ [q]$.
  On $q \geq 5$, donc $x^\uparrow + y^\uparrow + z^\uparrow \neq 0$: exclu.

  ↳ Comme q est premier, on peut supposer que q divise x.
  Comme $\operatorname{pgcd}(x, y) = 1$, $\operatorname{pgcd}(x, z) = 1$, q ne divise ni y ni z.

- Montrons que q divise a :

  q divise x donc $2x = x+z+x+y-(y+z)$
  $= b^\uparrow + c^\uparrow - a^\uparrow \equiv 0 \ [q]$

  q ne divise pas y donc q ne divise pas x : $y \equiv c^\uparrow \equiv \pm 1 \ [q]$
  ——— z ——— q ne divise pas b : $y \equiv b^\uparrow \equiv \pm 1 \ [q]$.

  Ainsi on ne peut avoir $a^\uparrow \equiv \pm 1 \ [q]$ donc q divise a.

- Comme q divise a, $y+z \equiv 0 \ [q]$

$$\alpha^\uparrow \equiv u \equiv \sum_{k=0}^{\uparrow -1} (-z)^{\uparrow -1-k} y^k \equiv \uparrow y^{\uparrow -1} \ [q]$$
$$\equiv \uparrow \ [q]$$

car $\uparrow -1$ est pair et $y \equiv \pm 1 \ [q]$.

Ceci est absurde car $\alpha^\uparrow \equiv 0, \pm 1 \ [q]$.

——— D.