Développement : Théorème de Sophie-Germain.

RM

2022-2023

Référence :

1. Oraux X-ENS tome 1 (algèbre ou nouvelle édition)

Énoncé :

Soit p un nombre premier de Sophie Germain, c'est-à-dire 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 $xyz \not\equiv 0[p]$ et $x^p + y^p + z^p = 0$.

Résolution :

On va procéder en plusieurs étape avec une démonstration par l'absurde. Supposons qu'il existe un tel triplet.

• 1er étape : On peut supposer $\text{pgcd}(x, y, z) = 1$ et alors x, y, z sont premiers entre eux deux à deux.
Soit $d = \text{pgcd}(x, y, z)$. On pose $x' = x/d$,$y' = y/d$et $z' = z/d$. On a alors $x'^p + y'^p + z'^p = 0$ avec $\text{pgcd}(x', y', z') = 1$ et $x'y'z' \not\equiv 0[p]$. On peut donc supposer que $\text{pgcd}(x, y, z) = 1$. Supposons alors que $\text{pgcd}(x, y) > 1$ et notons p_0 un diviseur premier de $\text{pgcd}(x, y)$. Comme $p_0 | -(x^p + y^p) = z^p$, alors $p_0 | z$ avec le lemme d'Euclide. Absurde car $\text{pgcd}(x, y, z) = 1$. Donc x et y sont premiers entre eux, et on applique le même raisonnement aux autres couples.

• 2ème étape : On montre qu'il existe deux entiers a et α tels que

$$y + z = a^p \text{ et } \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = \alpha^p.$$

Puis qu'il existe deux entiers b et c tels que $x + y = c^p$ et $x + z = b^p$.
Montrons en raisonnant par l'absurde que $y + z$ et $\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$ sont premiers entre eux. Supposons qu'ils ont un codiviseur p' premier. Comme $(-1)^p = -1$, on a

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

On en déduit que p' divise $-x^p$ et donc divise x. De plus, $y \equiv -z[p']$, donc

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

c'est-à-dire que p' divise py^{p-1}. Par le lemme d'Euclide, soit p' divise p, ie $p' = p$, et donc $p|x$, or impossible car $xyz \not\equiv 0[P]$. Soit p' divise y^{p-1} et donc divise y. Mais alors x et y ne sont pas premiers entre eux, impossible.

Ainsi, $y+z$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont premiers entre eux et de l'égalité (1) ci-dessus, on déduit l'existence de deux entiers a et α tels que

$$y+z=a^p \text{ et } \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k=\alpha^p.$$

> En effet , si $ab=c^k$ avec a et b premiers entre eux, si on considère leurs décomposition en produits de facteurs premiers $a=\prod_{p\in\mathcal{P}}p^{\alpha_p}$,$b=\prod_{p\in\mathcal{P}}p^{\beta_p}$ et $c=\prod_{p\in\mathcal{P}}p^{\gamma_p}$, alors par unicité de la décomposition, on a $\forall p\in\mathcal{P}$, $\alpha_p+\beta_p=k\gamma_p$ et $\alpha_p\beta_p=0$ car premiers entre eux. Donc soit β_p ou α_p est nul et donc $\alpha_p=k\gamma_p$ ou $\beta_p=k\gamma_p$. Donc k divise β_p et α_p, et donc on a bien que a et b sont des puissances k-ièmes.

Par symétrie, on prouve qu'il existe b et c tel que $x+y=c^p$ et $x+z=b^p$.

• 3ème étape : Si $m\in\mathbb{Z}$ n'est pas divisible par q, on montre que $m^p\equiv\pm1[q]$. On en déduit qu'un et un seul des trois entiers x,y,z est divisible par q. On supposera que c'est x.
Soit m un entier non divisible par q. Comme q est premier, par le petit théorème de Fermat, on sait que $m^{q-1}\equiv1[q]$, ce qui donne $(m^p)^2\equiv1[q]$. Donc m^p est racine du polynôme X^2-1 dans $\mathbb{Z}/q\mathbb{Z}$ qui est un corps, donc ce polynôme à deux racines qui sont 1 et -1 et donc $m^p\equiv1[q]$ ou $m^p\equiv-1[q]$.
Supposons par l'absurde qu'aucun des trois entiers x,y,z ne soit divisible par q. Alors on a $x^p\equiv\pm1[q]$,$y^p\equiv\pm1[q]$ et $z^p\equiv\pm1[q]$ et en sommant, on obtient que $x^p+y^p+z^p$ est congru à $3,1,-1,-3$ modulo q (selon chaque entier si il est congrus à 1 ou -1). C'est absurde car $q>5$. Donc l'un des trois entiers est divisible par q. On peut évidemment supposer sans perte de généralité que c'est x.
Alors on a $yz\not\equiv0[q]$ car x,y,z sont premiers entre eux deux à deux, et donc il y a bien un et un seul entier divisible par q.

• 4ème étape : On établie que $b^p+c^p-a^p\equiv0[q]$,$a\equiv0[q]$,$y\equiv c^p[q]$ et $\alpha^p\equiv py^{p-1}$. On obtient alors une contradiction qui permet de conclure.
On sait d'après la question 2 que $y+z=a^p$,$x+y=c^p$ et $x+z=b^p$. Il en résulte que $b^p+c^p-a^p\equiv2x\equiv0[q]$. On a évidemment $y\equiv c^p[q]$ puisque $x\equiv0[q]$. Par ailleurs , q ne divise pas y, donc ne divise pas c. D'après le travail précédent, on a que $c^p\equiv y\equiv\pm1[q]$. De la même manière, on obtient $z\equiv\pm1[q]$. Si maintenant q ne divise pas a, on a alors $a^p\equiv\pm1[q]$. On en déduit que $c^p+b^p-a^p$ est congrus de la même manière à $3,1,-1,-3$ modulo q, absurde car q divise ce nombre. On conclut que $q|a$.
Regardons maintenant α^p. Sachant que $y+z\equiv\alpha^p\equiv0$ ie $y\equiv-z[q]$, on en déduit que

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

Nous avons montré que $y\equiv\pm1[q]$. Il s'ensuit que $\alpha^p\equiv p[q]$ (car $p-1$ paire donc $(-1)^{p-1}=1$).
Or comme a et α sont premiers entre eux et que q divise a, alors q ne divise pas α et donc $\alpha^p\equiv\pm1[q]$.
Donc $p\equiv\pm1[q]$ ce qui est absurde car $2p\equiv-1[q]$ et $q>5$.
On aboutit dans tous les cas à une contradiction, donc un tel triplet n'existe pas.