126

Exemples d'équations diophantiennes

[Con] p. 274 [Con] p. 264 [Con] p. 264

Déf 1 : On appelle équation diophantienne toute équation de la forme $P(X_1, \dots, X_n) = 0$, où P est une fonction polynomiale à n variables à coefficients entiers. On cherche les solutions entières à ce genre d'équations.

Remarque : On autorise parfois les fonctions puissance.

I Equations linéaires

1) Equation de Bézout

On cherche à résoudre l'équation $AX = B$ avec $A \in \mathcal{M}_{m,n}(\mathbb{Z})$ et $B \in \mathcal{M}_{m,1}(\mathbb{Z})$.

Prop 3 : L'équation $ax = b$ admet une solution dans $\mathbb{Z}$ si et seulement si $a \mid b$.

Prop 4 : L'équation $ax + by = c$, d'inconnues x et y, admet une solution dans $\mathbb{Z}$ si et seulement si le PGCD d de a et b divise c.
Si c'est le cas on trouve une relation de Bézout de la forme $\frac{a}{d}u + \frac{b}{d}v = 1$, et le couple $(u\frac{c}{d}, v\frac{c}{d})$ est solution.

Exemple 5 : Résoudre $522x + 2214y = 36$:
$522 \wedge 2214 = 18 \mid 36$
L'équation équivaut donc à $29x + 123y = 2$. On trouve que 17 est l'inverse de 29 modulo 123.
Alors $29x = 2\ [123] \iff x = 34\ [123] \iff \exists k \in \mathbb{Z},\ x = 34 + 123k$.
On trouve que l'ensemble des solutions est $\{(34+123k, -8-29k), k \in \mathbb{Z}\}$.

Th 6 (forme normale de Smith) : Il existe $U \in GL_m(\mathbb{Z}), V \in GL_n(\mathbb{Z})$ et des entiers $d_1, \dots, d_r$ tels que $d_1 \mid d_2 \mid \dots \mid d_r$ et

$$UAV = \left(\begin{array}{ccc|c} d_1 & & (0) & \\ & \ddots & & (0) \\ (0) & & d_r & \\ \hline & (0) & & (0) \end{array}\right).$$

On a alors $AX = B \iff UAVY = UB$ avec $Y = V^{-1}X$, que l'on sait résoudre car chaque équation est de la forme $ax = b$. (2)

II Méthodes algébriques et géométriques

1) Réduction modulo un nombre premier

Déf 7 : Soit p un nombre premier. Pour $a \in \mathbb{Z}/p\mathbb{Z}$, on définit $\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a = 0 \\ 1 \text{ si } a \text{ est un carré non nul dans } \mathbb{Z}/p\mathbb{Z} \\ -1 \text{ sinon} \end{cases}$.

Prop 8 : Soient p un nombre premier et a dans $\mathbb{Z}/p\mathbb{Z}$.
Alors $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

Exemple 9 : Soit p premier. L'équation $x^2 + y^2 = pz^2$ n'admet pas de solutions si $p = 3\ [4]$, et en admet une infinité si $p = 2$ ou si $p = 1\ [4]$.

Prop 10 : Dans $\mathbb{Z}/p\mathbb{Z}$ (avec p premier), il y a exactement $\frac{p+1}{2}$ carrés.

Prop 11 : Pour p premier et, $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$, l'équation $ax^2 + by^2 = 1$ admet toujours une solution dans $\mathbb{Z}/p\mathbb{Z}$.

Th 12 (des quatre carrés) : Pour tout $n \in \mathbb{N}$, l'équation $x^2 + y^2 + z^2 + t^2 = n$ admet une solution, autrement dit tout entier naturel est somme de quatre carrés.

Th 13 (Loi de réciprocité quadratique) : Soient p et q deux nombres premiers impairs. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Exemple 14 : 7 n'est pas un carré modulo 37, donc l'équation $y^2 = 37x + 7$ n'a pas de solutions dans $\mathbb{Z}$.

[H2G2] p. 183 [Con] p. 275 [Ber] p. 74 [FGN1] p. 162 [H2G2] p. 185

[Bos]p.56 [Bos]p.57 [Bos]p.58 [Bos]p.59 [Bos]p.56 [Per]p.56

2) Utilisation de la factorialité

Déf 15 : L'anneau des entiers de Gauss est $\mathbb{Z}[i] = \{a+ib, a,b \in \mathbb{Z}\}$.

Prop 16 : les inversibles de $\mathbb{Z}[i]$ sont $1, -1, i$ et $-i$.

Prop 17 : L'anneau $\mathbb{Z}[i]$ est euclidien relativement à $N : a+ib \mapsto a^2+b^2$. En particulier $\mathbb{Z}[i]$ est factoriel.

Déf 18 : On définit $\Sigma = \{n \in \mathbb{N}, \exists a,b \in \mathbb{N}, n = a^2+b^2\}$.

On cherche à déterminer Σ, ce que l'on pourra faire grâce à l'étude de $\mathbb{Z}[i]$.

Prop 19 : Σ est stable par multiplication.

Prop 20 : Pour p premier on a $p \in \Sigma \iff p$ n'est pas irréductible dans $\mathbb{Z}[i]$

Prop 21 : les éléments irréductibles de $\mathbb{Z}[i]$ sont, avec éléments inversibles près, les éléments de norme N un nombre premier et les nombres premiers $p = 3[4]$.

Corollaire 22 : Pour p premier on a $p \in \Sigma \iff p = 2$ ou $p = 1[4]$

Th 23 (des deux carrés) : Soit n dans $\mathbb{N} \setminus \{0,1\}$. On décompose n en facteurs premiers : $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$.
Alors $n \in \Sigma \iff \forall p \in \mathbb{P}$ tel que $p = 3[4]$, $v_p(n)$ est pair.
On a trouvé à quelles conditions l'équation $n = x^2+y^2$ a des solutions

[H46-4] p.383 [H464] p.384 [H464] p.388 [H464] p.390

3) (*) Structure de groupe sur les coniques

On va chercher à résoudre l'équation de Pell-Fermat $x^2 - dy^2 = 1$ avec $d \in \mathbb{N}$ sans facteur carré.

Déf 26 : Soit C une conique affine sur $\mathbb{R}^2$. On fixe un point E de C. Pour A et B dans C on définit $A * B$ de la façon suivante :
Si $A = B$, on définit Δ_A comme l'unique droite passant par E et parallèle à la tangente à C en A. Sinon, Δ_{AB} est la droite parallèle à (AB) passant par E.
La droite Δ_{AB} intersecte C en deux points, distincts ou non. L'un est E et l'autre est $A*B$. (Voir annexe)

Prop 27 : Dans le cas où C est l'hyperbole $\mathcal{H}$ d'équation $xy = 1$ et $E = (1,1)$, la loi $*$ définit une structure de groupe abélien sur $\mathcal{H}$, de neutre E.
Si $A = (a, \frac{1}{a})$ et $B = (b, \frac{1}{b})$ sont dans $\mathcal{H}$ alors $A * B = (ab, \frac{1}{ab})$.

DVPT 1

Th 28 : Soient d dans $\mathbb{N}^*$ sans facteur carré et $\mathcal{H}$ l'hyperbole d'équation $X^2 - dY^2 = 1$. On pose $E = (1,0)$ et $\Pi_1 = (X_1, Y_1)$ avec $X_1, Y_1 \in \mathbb{N}^*$ et $X_1^2 + Y_1^2$ aussi petit que possible. Alors l'ensemble des points entiers de la branche de $\mathcal{H}$ contenant Π_0 est $\langle \Pi_1 \rangle$. L'ensemble des points entiers de $\mathcal{H}$ forme un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Corollaire 29 : Soit d comme précédemment.
Alors $\mathbb{Z}[\sqrt{d}]^\times = \mathbb{Z} \times \Gamma$, où $\Gamma \simeq \mathbb{Z}/2\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$.

III Equation de Fermat

Th 30 (Grand théorème de Fermat, Wiles, 1995) : Soit $n \geq 3$. L'équation de Fermat $x^n + y^n = z^n$ n'admet pas de solution $(x,y,z) \in \mathbb{Z}^3$ avec $xyz \neq 0$.

Remarque 31 : Il suffit de le montrer pour $n=4$ et $n=p$ avec p premier.

1) Les cas $n=2$ et $n=4$

Prop 32 : Le cercle unité S^1 est paramétré par
$]0,1[\to \mathbb{R}^2$
$t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$

Th 33 : Pour $x,y,z \in \mathbb{Z}$, on a $x^2+y^2=z^2$ si et seulement si il existe $d \in \mathbb{N}$ et $u,v \in \mathbb{N}^*$ premiers entre eux tels que (x,y,z) ou (y,x,z) soit égal à $(d(u^2-v^2), 2duv, d(u^2+v^2))$

Corollaire 34 : L'équation $x^4+y^4=z^2$ n'a pas de solutions dans $\mathbb{Z}^3$ avec $xyz \neq 0$.

Th 35 : L'équation de Fermat n'a pas de solutions non triviales pour $n=4$.

2) Le théorème de Sophie Germain

Th 36 (de Sophie Germain) : Soit p un nombre premier impair tel que $2p+1$ soit premier. Il n'existe pas d'entiers x,y,z tels que $x^p+y^p=z^p$ et $xyz \neq 0$ [p].

3) Le cas $n=3$

Th 37 : L'équation de Fermat n'a pas de solutions non triviales pour $n=3$.

(*) Errata :

Déf 24 : L'anneau des entiers d'Eisenstein est $\mathbb{Z}[j] = \{a+jb, a,b \in \mathbb{Z}\}$.

Prop 25 : L'équation de Mordell $y^2 = x^3 - 1$ n'admet pour solution dans $\mathbb{Z}$ que $(1,0)$.

Références :

[Con] "Algèbre et géométrie", F. Combes

[Duv] "Théorie des nombres", D. Duverney

[FGN1] "Oraux X-ENS : Algèbre 1", Francinou / Gianella / Nicolas

[H2G2] "Histoires hédonistes de groupes et de géométrie - Tome 1", P. Caldero

[H4G4] _____ Tome 2 G. Cermoni

[Per] "Cours d'algèbre", D. Perrin

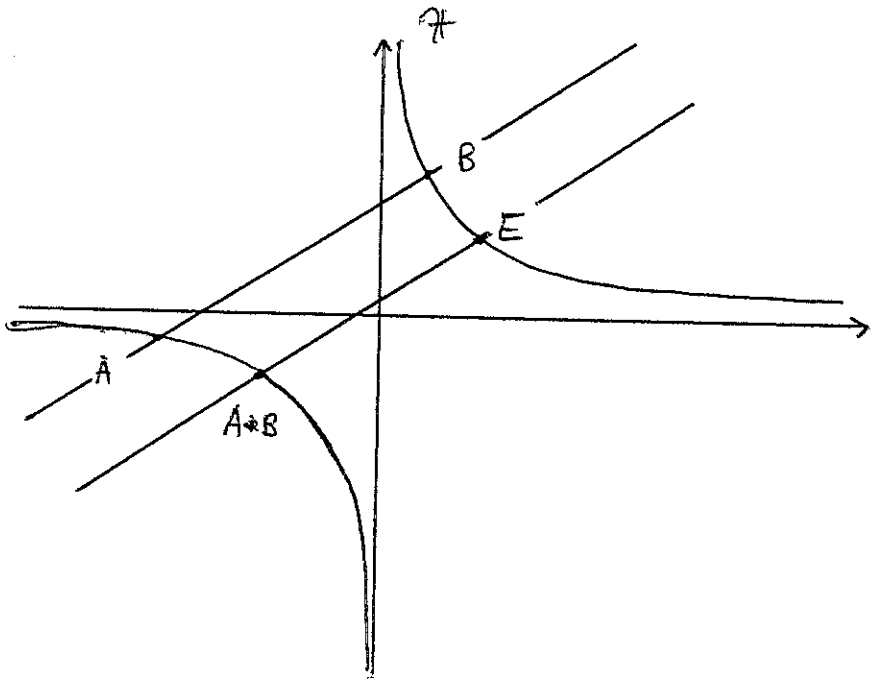
[Con] p. 275 [Con] p. 273 [Con] p. 274

[FGN1] p. 167

[Duv] p. 56

[Duv] p. 56

Détermination de A * B sur une hyperbole :



Equation de Pell-Fermat

Leçons : 126, 180, 183.

Référence :

Philippe Caldero - Jérôme Germoni,
Histoires hédonistes de groupes et de géométrie, Tome second - p.388,
Calvage et Mounet - 2015.

Le développement

L'objectif est de résoudre l'équation de Pell-Fermat, i.e chercher les couples d'entiers (x, y) vérifiant $x^2 - dy^2 = 1$ avec d une entier sans facteur carré.

Théorème.
Soit d un entier naturel sans facteur carré et soit $\mathcal{H}$ l'hyperbole d'équation $X^2 - dY^2 = 1$ dans le plan $\mathbb{R}^2$. Soit $E = M_0 = (1, 0)$. Soit $M_1 = (X_1, Y_1)$ un point de $\mathcal{H}$ où X_1 et Y_1 sont des entiers naturels avec $X_1^2 + Y_1^2$ aussi petit que possible. Alors l'ensemble des points entiers de la branche de $\mathcal{H}$ qui contient M_0 est le groupe engendré par M_1. L'ensemble des points entiers de $\mathcal{H}$ forme un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Démonstration.
On calcule, en coordonnées, l'application $M \in \mathcal{H} \mapsto M_1 \star M \in \mathcal{H}$. Pour cela, on passe au repère OXY où M_0 a pour coordonnées $(1, 1)$, en posant

$$\begin{cases} x = X + \sqrt{d}Y \\ y = X - \sqrt{d}Y \end{cases}$$

Notons (x_1, y_1) les coordonnées de M_1 dans ce repère. Si un point M a pour coordonnées (X, Y) dans le premier repère et (x, y) dans le deuxième, alors $M_1 \star M$ a pour coordonnées $(x_1 x, y_1 y)$ dans le deuxième repère et

$$(X', Y') = (X_1 X + dY_1 Y_1 X + XY_1)$$

dans le premier.

L'hyperbole $\mathcal{H}$ est la réunion de deux branches. Dans le repère Oxy, l'opération de groupe est le produit coordonnée par coordonnée donc $\mathcal{H}$ est un groupe topologique. Ainsi $\mathcal{H}_0$, la branche contenue dans le demi-plan $\{X > 0\}$, en tant que composante neutre de $\mathcal{H}$, est un sous-groupe de $\mathcal{H}$. La projection sur l'axe des abscisses x permet d'identifier $\mathcal{H}_0$ à $\mathbb{R}_+^*$, ce qui donne un ordre sur $\mathcal{H}_0$. Si les coordonnées d'un point $M = (X, Y)$ de $\mathcal{H}_0$ sont (x, y), alors $x = \sqrt{1 - dY^2} + \sqrt{d}Y$. Cette fonction de Y est strictement croissante donc l'ordre se lit indifféremment sur la coordonnée x ou sur la coordonnée Y. Par exemple, pour cet ordre, la fonction

$$\varphi : \begin{array}{ccc} \mathcal{H}_0 & \to & \mathcal{H}_0 \\ M & \mapsto & M_1 \star M \end{array}$$

est strictement croissante car les coordonnées de $\varphi(M)$ sont $(x_1 x, y_1 y)$ et $x \mapsto x_1 x$ est strictement croissante.

Pour tout n entier, posons $M_n = M_1^n = (X_n, Y_n)$. Il est immédiat que $M_{-1} = (X_1, -Y_1)$ d'où on tire par récurrence que $Y_{-n} = -Y_n$ pour tout n entier. Comme φ est strictement croissante et que $M_{n+1} = \varphi(M_n)$, la suite (M_n) est strictement croissante. De plus, comme $X_1 \geq 1$, $Y_1 > 0$ et $X_n \geq 1$ pour tout n, $Y_{n+1} > Y_n$ pour tout $n \in \mathbb{Z}$. Comme les Y_n sont entiers, (Y_n) diverge vers $+\infty$.

Soit $M = (X, Y)$ un point entier de $\mathcal{H}_0$. D'après ce qui précède, il existe un entier n tel que $Y_n \leq Y < Y_{n+1}$. Notons $M' = (X', Y') = M_{-n} \star M$. Grâce à la croissance stricte de φ, donc de

φ^{-n}, on a $M_0 \leq M' < M_1$. Mais, par hypothèse, M_1 est la solution entière minimale de l'équation de Pell-Fermat, donc $M' = M_0$ puis $M = M_n$.

On remarque pour terminer que la reflexion $\sigma : (X, Y) \mapsto (-X, Y)$ échange les deux branches de $\mathcal{H}$ et preserve $\mathbb{Z}^2$, et on peut affirmer que les points entiers de $\mathcal{H}$ sont les $(\pm X_n, Y_n)$ pour $n \in \mathbb{Z}$. □

Corollaire.
$\mathbb{Z}[\sqrt{d}]^* \simeq \mathbb{Z} \times \Gamma$ *avec* $\Gamma \simeq \mathbb{Z}/2\mathbb{Z}$ *ou* $\Gamma \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

Démonstration.
Soit $A = \mathbb{Z}[\sqrt{d}]$. L'ensemble des solutions de l'équation de Pell-Fermat est en bijection avec les éléments de A de norme 1. De plus, les inversibles de A sont les éléments de norme inversible, i.e $M = (X, Y)$ est inversible si et seulement si M est un point entier de l'une des hyperboles $X^2 - dY^2 = \pm 1$. Notons, avec les notations de la démonstration précédente, que

$$X' + \sqrt{d}Y' = (X_1 + \sqrt{d}Y_1)(X + \sqrt{d}Y).$$

Alors $(X, Y) \mapsto X + \sqrt{d}Y$ qui, à un point entier de $\mathcal{H}$, associe un inversible de norme 1, est un isomorphisme de groupes. D'après le théorème précédent, le noyau de la norme est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

L'hyperbole $X^2 - dY^2 = -1$ peut ne pas avoir de point entier ($d = 7$ par exemple car -1 n'est pas un carré modulo 7). Supposons néanmoins qu'elle en ait un, i.e qu'il y ait un élément $\tilde{a} = \tilde{X} + \sqrt{d}\tilde{Y}$ de A de norme -1. Alors tout élément de norme -1 est le produit de $\tilde{a}$ par un élément de norme 1, i.e

$$A^* = \ker(N) \cup \tilde{a} \ker(N) \simeq \mathbb{Z}/2\mathbb{Z} \times \ker(N)$$

où N est la norme de A. □

Théorème de Sophie Germain

Leçons : *120, 121, 123, 126*

[X-ENS Al1], exercices 4.39

Théorème

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

Démonstration :

On notera ici $\mathcal{P}$ l'ensemble des nombres premiers.
On raisonne par l'absurde ; soit $(x, y, z) \in \mathbb{Z}^3$, tel que $xyz \not\equiv 0\,[p]$ et $x^p + y^p + z^p = 0$.
Soit $d = \text{pgcd}\,(x, y, z)$, quitte à poser $x' = \dfrac{x}{d}$, $y' = \dfrac{y}{d}$ et $z' = \dfrac{z}{d}$, on peut supposer que $d = 1$.

Étape 1 : Montrons qu'alors x, y et z sont premiers entre eux deux à deux.

Par l'absurde, soit r un facteur premier de x et y.
Alors $r | x^p + y^p$, puis $r | z^p$ et donc, par le lemme d'Euclide : $r | z$.
On contredit alors l'hypothèse selon laquelle x, y et z sont premiers entre eux dans leur ensemble.
Désormais, on a donc : $x \wedge y = x \wedge z = y \wedge z = 1$.

Étape 2 : Montrons que $\exists (a, \alpha) \in \mathbb{Z}^2, y + z = a^p$ et $\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = \alpha^p$.

On va appliquer le lemme suivant.

Lemme

Soit $u, v \in \mathbb{Z}$, avec $u \wedge v = 1$ et $\exists w \in \mathbb{Z}, uv = w^k$, où $k \geqslant 2$.
Alors u et v sont tous les deux des puissances $k^{\text{èmes}}$.

Démonstration :

On écrit $u = \displaystyle\prod_{p \in \mathcal{P}} p^{\alpha_p}$, $v = \prod_{p \in \mathcal{P}} p^{\beta_p}$ et $w = \prod_{p \in \mathcal{P}} p^{\gamma_p}$, où $\alpha, \beta, \gamma \in \mathbb{N}^{(\mathcal{P})}$.
Et comme $uv = w^k$, on a : $\forall p \in \mathcal{P}, \alpha_p + \beta_p = k\gamma_p$.
Mais, α_p et β_p ne peuvent pas être simultanément non-nuls, puisqu'on a $u \wedge v = 1$.
Conséquemment, $\forall p \in \mathcal{P}$, $k | \alpha_p$ et $k | \beta_p$.
Donc u et v sont des puissances $k^{\text{èmes}}$. ∎

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

Il serait donc intéressant de montrer que $y + z$ et $\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$ sont premiers entre eux.
Par l'absurde, supposons qu'il existe un nombre premier, appelons-le r, qui les divise tous les deux.
Alors, de l'égalité précédente, il vient que $r^2 | x^p$, donc $r | x$.
Comme $y \equiv -z\,[r]$, on a : $\underbrace{\displaystyle\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k}_{\equiv 0\,[r]} \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv p y^{p-1}\,[r]$.

1. Il y a beaucoup de choses intéressantes à dire à propos de ce résultat. Sophie Germain (1776-1831) est quasiment la seule femme mathématicienne de son temps. Elle suivit les cours de l'École polytechnique par correspondance, car les femmes n'y étaient pas admises et c'est sous le pseudonyme masculin de Maurice Leblanc qu'elle écrivait à Gauss pour lui faire part de ses découvertes arithmétiques. En 2001, le plus grand nombre de Sophie Germain qu'on connaissait était $109433307 \times 2^{66452} - 1$, possédant 20013 chiffres. À l'heure actuelle, on conjecture qu'il en existe une infinité. Le théorème de Sophie Germain, démontré en 1823, est une résolution partielle du grand théorème de Fermat — mais si, vous savez : pour $n \geqslant 3$, il n'existe pas de solution non-triviale dans $\mathbb{Z}^3$ à l'équation $x^n + y^n = z^n$ — que Fermat mentionnait dans une annotation marginale, sans la prouver "par manque de place". On est certain aujourd'hui qu'il ne pouvait pas en avoir une démonstration complète (bon, en même temps, quand tu t'appelles Fermat, ton prof de maths va avoir du mal à te reprocher de bluffer dans tes copies, non ?).

Donc $r|py^{p-1}$, et donc, par le lemme de Gauss :
- soit $r|p$, et alors, ces deux nombres étant premiers, on obtient $r = p$ et donc $p|x$, contredisant l'hypothèse $xyz \not\equiv 0\,[p]$;
- soit $r|y$, mais c'est impossible puisque $r|x$ et $x \wedge y = 1$.

On obtient ainsi une contradiction ; et on en déduit $(y+z) \wedge \left(\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k\right) = 1$.

Puis, par le lemme, on obtient :

$$\exists (a,\alpha) \in \mathbb{Z}^2, y+z = a^p \text{ et } \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = \alpha^p.$$

Similairement, on montrerait $x+z = b^p$ et $y+z = c^p$, avec $b, c \in \mathbb{Z}$.

Étape 3 : Un (et un seul, vu qu'ils sont premiers entre eux deux à deux) des trois entiers x, y et z est divisible par q.
Soit $m \in \mathbb{Z}$, tel que $q \nmid m$.
Alors, par le petit théorème de Fermat, on obtient : $(m^p)^2 = m^{q-1} \equiv 1\,[q]$ et donc, comme $\mathbb{Z}/q\mathbb{Z}$ est un corps[2], on a : $m^p \equiv \pm 1\,[q]$.
Par l'absurde, on suppose $q \nmid x$, $q \nmid y$ et $q \nmid z$.
Alors $0 \equiv x^p + y^p + z^p$ est congru à 3, 1, -1 ou -3 modulo q. Ce qui est absurde puisque $q > 5$.
Sans perte de généralité, disons que $q|x$, et qu'incidemment : $q \nmid y$ et $q \nmid z$.

Étape 4 : Tels Jean-Claude Dusse, cherchons à conclure.
On a : $b^p + c^p - a^p = x + z + x + y - y - z = 2x \equiv 0\,[q]$.
Et comme $x \equiv 0\,[q]$, on a : $y \equiv c^p\,[q]$; mais $q \nmid y$ donc $q \nmid c$, d'où $y \equiv \pm 1\,[q]$. Similairement, $z \equiv \pm 1\,[q]$.
Donc $a^p = y + z$ est congru à 2, 0 ou -2 modulo q ; mais une puissance $p^{\text{ème}}$ est congrue à 1, 0 ou -1 modulo q.
Donc $y + z \equiv 0[q]$.
Comme dans l'étape 2, on obtient : $\alpha^p = \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \equiv py^{p-1}\,[q]$.
Or $p-1$ est pair et $y \equiv \pm 1\,[q]$ et donc $\alpha^p \equiv p\,[q]$; mais aussi α^p est congru à 1, 0 ou -1 modulo q.
Contradiction !
Il n'y a donc pas de triplet $(x,y,z) \in \mathbb{Z}^3$ tel que : $xyz \not\equiv 0\,[q]$ et $x^p + y^p + z^p = 0$. ■

Références

[X-ENS Al1] S. FRANCINOU, H. GIANELLA et S. NICOLAS – *Oraux X-ENS Algèbre 1*, 3ème éd., Cassini, 2014.

2. Le polynôme $X^2 - 1 \in \mathbb{Z}/q\mathbb{Z}[X]$ admet au plus deux racines puisqu'il est de degré 2 sur un corps ; on vérifie facilement qu'il s'agit de 1 et -1.