NOMBRES PREMIERS. APPLICATIONS.

121

Cadre : On note $\mathcal{P}$ l'ensemble des nombres premiers.

I - Généralités sur les nombres premiers

1 - Définitions et exemples [GOU] p.7-9

Déf 1 : Soit $p \in \mathbb{N}$ tq $p \geq 2$. p est dit premier ssi ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p.

Ex 2 : 2, 3, 5, 7, 11, 13, ...

Thm 3 : (BEZOUT) Soient $a, b \in \mathbb{Z}$. Alors $\text{pgcd}(a,b) = 1$ ssi $\exists (u,v) \in \mathbb{Z}^2$ tq $au + bv = 1$.

Rq : On trouve un tel couple à l'aide de l'algorithme d'Euclide.

Thm 4 : (GAUSS) Soient $a, b, c \in \mathbb{N}^*$. Si $a \mid bc$ et $a \wedge b = 1$ alors $a \mid c$.

Cor 5 : (lemme d'Euclide) Soit p premier. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$

Application 6 : Soit $p \in \mathcal{P}$ et $1 \leq k \leq p-1$. Alors $p \mid \binom{p}{k}$.

2 - Décomposition en facteurs premiers [GOU]

Prop 7 : Tout entier n, $|n| \geq 2$ est divisible par un nombre premier. p.8

Prop 8 : L'ensemble $\mathcal{P}$ des nombres premiers est infini. p.9

Thm 9 : (Théorème fondamental de l'arithmétique)
Soit $n \geq 2$ s'écrit de manière unique à l'ordre près :

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \quad (*) \qquad \text{p.8}$$

où $p_i \in \mathcal{P}$ (distincts) et $\alpha_i \in \mathbb{N}^*$. $(*)$ est la décomposition en facteurs premiers de n.

Ex 10 : $300 = 2^2 \times 3 \times 5^2$

Rq : Cela mène à la définition d'anneau factoriel.

Application 11 : (produit Eulérien) $\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}}$ [R-W] p.279

3 - Deux fonctions arithmétiques

Déf 12 : Soit $n > 1$. On appelle indicatrice d'Euler : [GOU] p.31
$\varphi(n) = \#\{k \in [\![1, n]\!] \mid k \wedge n = 1\}$ ou $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$

Prop 13 : Si $\text{pgcd}(m,n) = 1$, alors $\varphi(mn) = \varphi(m)\varphi(n)$. p.32

Prop 14 : Soit $p \in \mathcal{P}$. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. p.31

Prop 15 : Soit $n \geq 2$, on a $n = \sum_{d \mid n} \varphi(d)$ p.32

Déf 16 : On appelle fonction de Möbius $\mu : \mathbb{N}^* \to \{0, 1, -1\}$ tq $\mu(1) = 1$, $\mu(n) = 0$ si $\exists p \in \mathcal{P}$ tq $p^2 \mid n$ [PER] et $\mu(p_1 \dots p_r) = (-1)^r$ si les p_i sont distincts. p.99

Prop 17 : Si $\text{pgcd}(m,n) = 1$ alors $\mu(mn) = \mu(m)\mu(n)$. p.89

Prop 18 : $\forall n \in \mathbb{N}^*, n \neq 1$, on a $\sum_{d \mid n} \mu(d) = 0$.

Prop 19 : (Formule d'inversion) Soit $n \geq 1$, on a $\varphi(n) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) d$ p.89

Application 20 : Soit Φ_n le n-ième polynôme cyclotomique.

$$\Phi_n(X) = \prod_{d \mid n} (X^{n/d} - 1)^{\mu(d)} \qquad \text{p.92}$$

4 - Répartition des nombres premiers. [R-W] p. 275, 276

Thm 21 : (Dirichlet) [ADMIS] Soit $a, b \in \mathbb{N}$ tq $\text{pgcd}(a,b) = 1$.
Alors $\{an + b \mid n \in \mathbb{N}\}$ contient une infinité de nombres premiers.

Déf 22 : On note $\pi(n) = \text{card}\{p \in \mathcal{P} \mid p \leq n\}$.

Thm 23 : (Théorème des nombres premiers)

$$\pi(n) \underset{+\infty}{\sim} \frac{n}{\ln n}$$

II - Corps finis

1 - Anneau $\mathbb{Z}/n\mathbb{Z}$ [GOU] p.9 et p.31

Prop 24 : Soit $n \geq 2$. $\mathbb{Z}/n\mathbb{Z}$ est un corps ssi $n \in \mathcal{P}$.
On note $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Méthode : Soit $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^*$. Par Bezout $ap + bx = 1 \Rightarrow \bar{x}^{-1} = \bar{b}$

Ex 25 : $\bar{36}^{-1} = \bar{17}$ dans $(\mathbb{Z}/47\mathbb{Z})^*$.

Thm 26 : (FERMAT) Soit $p \geq 2$ premier. Alors :

$$\forall a \in \mathbb{Z},\ a^p \equiv a \ [p]$$
$$\forall a \in \mathbb{Z},\ p \nmid a,\ a^{p-1} \equiv 1 \ [p].$$

DVPT 1

Application 27 : (Thm de Sophie Germain) Soit $p \in \mathcal{P}$ impair tq $q = 2p + 1 \in \mathcal{P}$. Alors $\exists (x, y, z) \in \mathbb{Z}^3$ tq $xyz \not\equiv 0 [p]$ et $x^p + y^p + z^p = 0$. [FGN] p.167

Application 28 : (Chiffrement RSA). Soient $p, q \in \mathcal{P}$ distincts et $n = pq$.
Soient $c, d \in \mathbb{Z}$ tq $cd \equiv 1 [\varphi(n)]$. $\forall t \in \mathbb{Z}$, on a $t^{cd} \equiv t [\varphi(n)]$
- fonction de chiffrement : $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\bar{t} \mapsto \bar{t}^c$

• fonction de déchiffrement: $g: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\bar{t} \mapsto \bar{t}^d$ [GOU] p.34-35

On a $f \circ g(\bar{t}) = \bar{t}$.
(n,c) est la clé publique et d est la clé secrète.
Sans la connaissance de d, il est quasiment impossible de déchiffrer le message $\bar{t}$.

2- Théorie élémentaire des corps finis [PER] p.72

Déf 29: Soit k un corps et $\Psi: \mathbb{Z} \to k$, $n \mapsto n.1_k$. Le nombre p générateur de $\ker\Psi$ est la caractéristique de k, $p=0$ ou $p \in \mathcal{P}$.

Rq: Ici k est fini donc $car(k) = p > 0$.

Prop 30: Soit k un corps fini tq $car(k) = p$.
Alors $q = |k| = p^n$. $(n \in \mathbb{N}^*)$.

Prop 31: Soit k un corps fini, $car(k) = p > 0$.
$F: k \to k$, $x \mapsto x^p$ est un automorphisme (appelé morphisme de Frobenius).

Thm 32: Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}^*$, $q = p^n$.
1) $\exists$ un corps k à q éléments, c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.
2) k est unique à isomorphisme près. On le note $\mathbb{F}_q$.

Thm 33: Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique (isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$)

3- Carrés dans $\mathbb{F}_q$ $(q = p^n)$ [R-W] p.129-130, [PER] p.74

$\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q \text{ tq } x = y^2\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$

Rq: Pour $p=2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$.

Prop 34: Pour $p \geq 3$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$.

Déf 35: Soit $p \in \mathcal{P}$, $p \geq 3$. Soit $x \in \mathbb{F}_p^*$. Symbole de Legendre:

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \in \mathbb{F}_p^{*2} \\ -1 & \text{sinon} \end{cases}$$

Si $p \nmid a$, $\left(\frac{a}{p}\right) = \left(\frac{x}{p}\right)$ où x est la classe de a modulo p.

Prop 36: (Formule d'Euler) Soit $x \in \mathbb{F}_p^*$. Alors $\left(\frac{x}{p}\right) = x^{(p-1)/2}$ DVPT 2 [FGN] p.158 ou [PER] p.57

Application 37 (Théorème des 2 carrés)
p est somme de 2 carrés $\iff p \equiv 1 [4]$ ou $p=2$

Thm 38: (Loi de réciprocité quadratique)
Soit $q \in \mathcal{P}$, $q \neq p$. Alors $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)/2 \times (q-1)/2}$

Ex 39: $\left(\frac{3}{17}\right) = -1$.

4- Application à la réduction des polynômes mod p

Prop 40: (Critère d'Eisenstein) $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$. [GOU] p.58
On suppose que $\exists p \in \mathcal{P}$ tq:
(i) $p \mid a_k$ $\forall k \in [\![0, n-1]\!]$ et $p \nmid a_n$
(ii) $p^2 \nmid a_0$
Alors P est irréductible dans $\mathbb{Q}[X]$.

Application 41: Soit $p \in \mathcal{P}$ et $\Phi(X) = X^{p-1} + \dots + X + 1$.

Thm 42: $P = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$ et $\bar{P}$ sa réduction mod p.
On suppose $\bar{a}_n \neq 0$ dans $\mathbb{F}_p$. Alors, si $\bar{P}$ est irréductible sur $\mathbb{F}_p[X]$, P est irréductible sur $\mathbb{Q}[X]$. [PER] p.77

Ex 43: $p=2$, $P = X^3 + 462X^2 + 2433X - 67691$
$\bar{P} = X^3 + X + 1$ irréductible sur $\mathbb{F}_2$.

Rq: La réciproque est fausse: X^4+1 irréductible sur $\mathbb{Q}[X]$ mais réductible sur $\mathbb{F}_p$ $\forall p \in \mathcal{P}$. [PER] p.78.

III - Théorie des groupes

1- p-groupes $(p \in \mathcal{P})$ [GOU] p.27

Déf 44: Un p-groupe est un groupe d'ordre p^α $(\alpha \in \mathbb{N}^*)$.

Ex 45: $(\mathbb{Z}/2\mathbb{Z})^2$, Q_8 sont des 2-groupes.

Prop 46: Tout groupe d'ordre p est cyclique.

Prop 47: Le centre d'un p-groupe non trivial est non trivial.

Cor 48: Tout p-groupe d'ordre p^2 est abélien.

Cor 49: Tout p-groupe est résoluble.

2 - Théorèmes de Sylow [PER] p. 18-20

Déf 50 : Soit G un groupe tq $|G| = n = p^\alpha m$ avec $p \in \mathbb{P}$ et $p \nmid m$. On appelle p-sous-groupe de Sylow de G, un sous-groupe de cardinal p^α.

Ex 51 : $G = GL_n(\mathbb{F}_p)$, $P = \{ A = (a_{ij}) \mid a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1 \}$ est un p-Sylow de G.

Thm 52 (Sylow) Soit G un groupe tq $|G| = p^\alpha m$ avec $p \nmid m$.

1) G contient au moins un p-sous groupe de Sylow.
2) Si $H < G$ est un p-groupe, alors $\exists$ un p-Sylow S tq $H \subset S$.
3) Les p-Sylows sont conjugués.
4) $n_p \equiv 1 \ [p]$ (n_p = nombre de p-Sylow)

Cor 53 : S un p-Sylow de G.

$S \triangleleft G \iff S$ est l'unique p-Sylow de G.

Application 54 : Un groupe d'ordre 63 n'est pas simple.

IV - Primalité en pratique

1 - Algorithmes élémentaires

Algorithme 55 : Soit $n \in \mathbb{N}$, $n \geq 2$. On teste si $i \mid n$ pour $i \in [2, n-1]$

Algorithme 56 : (Critère d'Ératosthène)

On veut trouver $\mathbb{P} \cap \{2, \dots, N\}$ pour un certain N.

On pose $P_1 := \{2, \dots, N\}$, $P_2 := \emptyset$ et on fait :

Tant que $P_1 \neq \emptyset$ | $P_2 \leftarrow P_2 \cup \{\min P_1\}$
| $P_1 \leftarrow P_1 \setminus (\min P_1)\mathbb{N}^*$

Alors $P_2 = \mathbb{P} \cap \{2, \dots, N\}$.

Rq : Cet algorithme a l'avantage de nous donner tous les nombres premiers $\leq N$ contrairement au premier.

2 - Un test de primalité [DEM] p. 72

Prop 57 : (Critère de Lehmer) Soit $n > 1$ impair.

n premier $\iff$ ($\exists a \in \mathbb{N}$ tq $a^{n-1} \equiv 1 \ [n]$ et $a^{(n-1)/q} \not\equiv 1 \ [n]$ pour tout facteur premier q de $(n-1)$.)

Ex 58 : $n = 7$ et $a = 3$.

3 - Deux classes de nombres remarquables

• Nombres de Fermat : [DEM] p. 75

Conjecture de Fermat : tous les nombres de la forme $Fer_m = 2^{2^n} + 1$ sont premiers.

En réalité, $Fer_1, Fer_2, Fer_3, Fer_4$ sont premiers mais pas Fer_5 !

Lemme 55 (Critère de Pépin)

Fer_n premier $\iff (3^{2^{2^n}-1} \equiv -1 \ [Fer_n])$

Rq : Ce critère est encore valable avec 5 ou 7 au lieu de 3.

• Nombres de Mersenne : [DEM] p. 77

Ce sont les entiers de la forme $2^s - 1$.

Comme $2^a - 1 \mid 2^{ab} - 1$, $2^s - 1$ est premier $\Rightarrow s$ premier.

$2^s - 1$ est premier pour $s = 2, 3, 5, 7$ mais pas pour $s = 11$!

En effet, $2^{11} - 1 = 2047 = 23 \times 89$

Références :

[GOU] : Gourdon, Algèbre.
[PER] : Daniel Perrin, Cours d'algèbre.
[R-W] : Ramis - Warusfel, Algèbre.
[DEM] : Demazure, Cours d'algèbre, Primalité, divisibilité, codes.
[FGN] : Francinou, Gianella, Nicolas, Oraux X-ENS Algèbre 1.

$\mathbb{Z}[i]$ et le théorème des deux carrés

Maylis Varvenne & Caroline Robet

Soit $\Sigma = \{n \in \mathbb{N} \mid n = a^2 + b^2;\ a, b \in \mathbb{N}\}$.
On veut démontrer le théorème suivant :

Théorème des deux carrés. *Soit p un nombre premier impair.*
On a l'équivalence suivante :

$$p \in \Sigma \Longleftrightarrow p \equiv 1 \pmod 4$$

Pour démontrer ce théorème, l'idée est de penser que si $n \in \Sigma$, alors $n = a^2 + b^2 = (a + ib)(a - ib)$ dans $\mathbb{C}$. On va donc introduire l'anneau des entiers de Gauss $\mathbb{Z}[i]$.

1 L'anneau $\mathbb{Z}[i]$

Définition 1. *On définit l'anneau $\mathbb{Z}[i]$ par :*

$$\mathbb{Z}[i] = \{a + ib \in \mathbb{C} | a, b \in \mathbb{Z}\}$$

Cet anneau est intègre car inclus dans $\mathbb{C}$. De plus, on dispose d'un automorphisme de $\mathbb{Z}[i]$ donné par la conjugaison :

$$\begin{array}{rccc} \sigma & : & \mathbb{Z}[i] & \to & \mathbb{Z}[i] \\ & & a + ib & \mapsto & \bar{z} = a - ib \end{array}$$

Cet automorphisme nous permet de définir une "norme"

$$\begin{array}{rccc} N & : & \mathbb{Z}[i] & \to & \mathbb{N} \\ & & a + ib & \mapsto & z\bar{z} = a^2 + b^2 \end{array}$$

qui est multiplicative, c'est à dire $N(zz') = N(z)N(z')$.
L'introduction de cette norme permet de calculer les inversibles de $\mathbb{Z}[i]$:

Proposition 1. *On a $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.*

Démonstration. Si $z \in \mathbb{Z}[i]^*$, $\exists z' \in \mathbb{Z}[i]^*$ tel que $zz' = 1$, d'où $N(z)N(z') = 1$.
Donc $N(z) = N(z') = 1 \ \Rightarrow\ a^2 + b^2 = 1 \ \Rightarrow\ (a = 0$ et $b = \pm 1)$ ou $(a = \pm 1$ et $b = 0)$.
D'où le résultat. □

Proposition 2. *L'ensemble Σ des sommes de deux carrés est stable par multiplication.*
(Ceci découle simplement du fait que N est multiplicative).

Proposition 3. *L'anneau $\mathbb{Z}[i]$ est euclidien (relativement à la fonction N), donc principal.*

Démonstration. Soient $z, t \in \mathbb{Z}[i]\backslash\{0\}$. On a $z/t \in \mathbb{C}$ qui est de la forme $z/t = x + iy$.
On veut approximer z/t par un entier de Gauss $q = a + ib$ où a et b sont tels que $|x - a| \leqslant \frac{1}{2}$ et $|y - b| \leqslant \frac{1}{2}$.
Ainsi,

$$\left|\frac{z}{t} - q\right| \leqslant \frac{\sqrt{2}}{2} < 1$$

On pose alors $r = z - qt$ de telle manière que r est dans $\mathbb{Z}[i]$ et $r = t(z/t - q)$ d'où

$$|r| = |t|\ |z/t - q| < |t| \quad \text{et en élevant au carré,} \quad N(r) < N(t).$$

On a donc bien écrit $z = qt + r$ avec $N(r) < N(t)$ et le résultat est démontré. □

2 Démonstration du théorème des deux carrés

On rapelle le théorème à démontrer :

Théorème des deux carrés. *Soit p un nombre premier impair.*
On a l'équivalence suivante :

$$p \in \Sigma \Longleftrightarrow p \equiv 1 \pmod 4$$

La condition $p \equiv 1 \pmod 4$ est clairement nécessaire car $\forall (a,b) \in \mathbb{N}^2$, $a^2+b^2 \equiv 0,1,2 \pmod 4$ et comme p est premier, $p \not\equiv 0$ ou $2 \pmod 4$.

Lemme 1. *On a l'équivalence suivante :*

$$p \in \Sigma \iff p \text{ n'est pas irréductible dans } \mathbb{Z}[i].$$

Démonstration du lemme.
($\Rightarrow$) : Si $p = a^2+b^2$, on a $p = (a+ib)(a-ib)$ et a, b sont $\neq 0$, donc $a+ib$, $a-ib$ ne sont pas $\mathbb{Z}[i]^*$ d'où p n'est pas irréductible.
($\Leftarrow$) : Si $p = zz'$ avec z, z' non inversibles (donc $N(z), N(z')$ sont $\neq 1$), on a $N(p) = N(z)N(z') = p^2$, donc comme p est premier, nécessairement $p = N(z)$ d'où $p \in \Sigma$ et le lemme est démontré. □

Démonstration du théorème.
$\mathbb{Z}[i]$ est factoriel (car euclidien pour la norme N).
On a donc l'équivalence suivante :

$$\begin{aligned} p \text{ n'est pas irréductible dans } \mathbb{Z}[i] &\iff (p) \text{ n'est pas premier.} \\ &\iff \mathbb{Z}[i]/(p) \text{ non intègre.} \end{aligned}$$

De plus, $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$ donc on a :

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[X]/(X^2+1,p) \simeq (\mathbb{Z}[X]/(p))/(X^2+1) \simeq \mathbb{F}_p[X]/(X^2+1)$$

D'où,

$$\begin{aligned} p \text{ n'est pas irréductible dans } \mathbb{Z}[i] &\iff X^2+1 \text{ n'est pas irréductible dans } \mathbb{F}_p[X] \\ &\iff X^2+1 \text{ admet une racine dans } \mathbb{F}_p \\ &\iff -1 \text{ est un carré dans } \mathbb{F}_p. \end{aligned}$$

D'après le lemme, il nous reste donc juste à démontrer que :

$$-1 \text{ est un carré dans } \mathbb{F}_p \iff p \equiv 1 \pmod 4$$

Or si p impair, on a

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si} \quad p \equiv 1 \pmod 4 \\ -1 & \text{sinon} \end{cases}$$

Et finalement, le théorème est démontré. □

Remarque. *Il est clair que $2 \in \Sigma$ car $2 = 1^2+1^2$.*

Corollaire. *Soit $n \in \mathbb{N}^*$. On décompose n en produit de facteurs premiers : $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$ où $\mathcal{P} = \{\text{nombres premiers}\}$. Alors,*

$$n \in \Sigma \iff \forall p \in \mathcal{P} \text{ tel que } p \equiv 3 \pmod 4, \quad \nu_p(n) \text{ est pair.}$$

Démonstration.

($\Leftarrow$) : On décompose n de la façon suivante :

$$n = \left(\prod_{p \equiv 3 \ [4]} p^{\frac{\nu_p(n)}{2}} \right)^2 \left(\prod_{p \not\equiv 3 \ [4]} p^{\nu_p(n)} \right)$$

Le produit de gauche est un carré parfait donc il appartient à Σ.
Dans le produit de droite, chaque p est congru à 1 modulo 4 ou égal à 2 donc dans Σ.
La stabilité par multiplication de Σ permet alors de conclure.

($\Rightarrow$) : On a $n = a^2 + b^2$. Soit $d = \text{pgcd}(a, b)$.
Quitte à considérer $\frac{n}{d^2} = \left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2$, on peut supposer $d = 1$.
Remarque : La parité des $\nu_p(n/d^2)$ et $\nu_p(n)$ sont les mêmes quelque soit p.
Soit $p \in \mathcal{P}$ tel que p divise n. Alors $a^2 + b^2 \equiv 0 \pmod{p}$.
p ne divise pas a. En effet, si p divisait a, alors p diviserait $n - a^2 = b^2$ donc p diviserait b ce qui est exclu car $d = 1$.
Ainsi b appartient à $\mathbb{F}_p^*$ et $(ab^{-1}) \equiv -1 \pmod{p}$, c'est-à-dire -1 est un carré modulo p.
D'après le théorème des deux carrés, cela entraîne que $p = 2$ ou $p \equiv 1 \pmod{4}$.
Ainsi, tous les $\nu_p(n)$ sont nuls pour $p \equiv 3 \pmod{4}$.
Remarque : Dans le cas général où $d \neq 1$, on obtient le fait que $\nu_p(n)$ est pair dès que $p \equiv 3 \pmod{4}$.

□

Référence : Daniel Perrin, *Cours d'Algèbre*, p.56,57,58.

Théorème de Sophie Germain

Maylis Varvenne & Caroline Robet

Théorème. *Soit p un nombre premier de Sophie Germain, c'est-à-dire un nombre premier impair tel que $q = 2p + 1$ soit premier. Alors*

$$\nexists\ (x, y, z) \in \mathbb{Z}^3 \text{ tel que } xyz \not\equiv 0\ [p] \text{ et } x^p + y^p + z^p = 0$$

Lemme. *Si le produit de deux entiers u et v premiers entre eux est une puissance k-ième (avec $k \geqslant 2$), alors u et v sont tous les deux des puissances k-ièmes.*

Démonstration du théorème. On raisonne par l'absurde.
On suppose donné $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0\ [p]$ et $x^p + y^p + z^p = 0$.
Soit $d = pgcd(x, y, z)$. Quitte à poser $x' = \frac{x}{d}$, $y' = \frac{y}{d}$ et $z' = \frac{z}{d}$, on peut supposer $d = 1$.
Montrons qu'alors x, y, z sont premiers entre eux deux à deux. Supposons par l'absurde que $pgcd(x, y) > 1$ et soit p_0 un facteur premier qui divise x et y. Alors $p_0 | x^p + y^p$ donc $p_0 | z^p$ et donc $p_0 | z$ ce qui contredit le fait que $pgcd(x, y, z) = 1$.
Ainsi $\underline{pgcd(x, y) = 1}$. De même, on en déduit que $\underline{pgcd(x, z) = 1}$ et $\underline{pgcd(y, z) = 1}$.

• *1ère étape : Montrons l'existence de $(a, \alpha) \in \mathbb{Z}^2$ tels que $y + z = a^p$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p$:*
On remarque que :

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

D'après le lemme, il suffit donc de montrer que $(y + z)$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont premiers entre eux.
Supposons par l'absurde qu'il existe p' premier qui divise $(y + z)$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$.
Alors d'après $(\star)$, p' divise x^p donc p' divise x.
Comme $y \equiv -z\ [p']$, on en déduit

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

D'après le lemme de Gauss, $p' | p$ ou $p' | y$.
Si $p' | p$ (ie $p' = p$), cela signifie que $p | x$ (absurde par hypothèse) et si $p' | y$, cela contredit le fait que $pgcd(x, y) = 1$
D'où $(y + z)$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont premiers entre eux.
D'après le lemme, il existe $(a, \alpha) \in \mathbb{Z}^2$ tel que $\underline{y + z = a^p}$ et $\underline{\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p}$.
Par symétrie, il existe $(b, c) \in \mathbb{Z}^2$ tel que $\underline{x + y = c^p}$ et $\underline{x + z = b^p}$.

• *2ème étape : Un et un seul des 3 entiers x, y, z est divisible par q :*
Soit $m \in \mathbb{Z}$ tel que $m \not\equiv 0\ [q]$, d'après le petit théorème de Fermat

$$m^{q-1} \equiv 1\ [q] \Rightarrow m^{2p} \equiv 1\ [q] \Rightarrow m^p \equiv \pm 1\ [q] \quad (\text{car } \mathbb{Z}/p\mathbb{Z} \text{ est un corps})$$

Supposons par l'absuide qu'aucun des trois entiers n'est divisible par q.
Alors $x^p \equiv \pm 1\ [q]$, $y^p \equiv \pm 1\ [q]$ et $z^p \equiv \pm 1\ [q]$.
Donc $(0 =) x^p + y^p + z^p$ est congru à $3, 1, -1$ ou -3 ce qui est absurde car $q > 5$.

On peut donc supposer que $\underline{x \text{ est divisible par } q}$ (et c'est le seul car x, y, z sont premiers entre eux deux à deux).

- *3ème étape : Contradiction et conclusion* :

On a $y + z = a^p$, $x + z = b^p$ et $x + y = c^p$ donc $b^p + c^p - a^p = 2x \equiv 0\ [q]$ $(\star\star)$.
D'autre part, $y \equiv c^p\ [q]$ car q divise x. De plus, q ne divise pas y donc ne divise pas c^p et donc ne divise pas c. D'où $\underline{y \equiv c^p \equiv \pm 1\ [q]}$. De même, $\underline{z \equiv \pm 1\ [q]}$.
Si de plus, q ne divise pas a, alors $a^p \equiv \pm 1\ [q] \Rightarrow c^p + b^p - a^p \equiv \pm 1 \text{ ou } \pm 3\ [q]$ (absurde d'après $(\star\star)$).
Donc q divise a ie $y + z \equiv 0\ [q]$.
D'autre part

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

Ceci est absurde car d'après la 2ème étape, $\alpha^p \equiv 0, 1 \text{ ou } -1\ [q]$.
Dans tous les cas, on aboutit à une contradiction.
On en déduit finalement que

$$\underline{\nexists\ (x, y, z) \in \mathbb{Z}^3 \text{ tel que } xyz \not\equiv 0\ [p] \text{ et } x^p + y^p + z^p = 0.}$$

□

Démonstration du Lemme. Soient u et v deux entiers premiers entre eux tels que $uv = w^k$ aves $w \in \mathbb{Z}$ et $k \geqslant 2$. Ecrivons la décomposition en facteurs premiers de u, v et w :

$$u = \prod_{p \text{ premier}} p^{\alpha_p},\ v = \prod_{p \text{ premier}} p^{\beta_p} \text{ et } w = \prod_{p \text{ premier}} p^{\gamma_p}$$

où α_p, β_p et γ_p sont des familles d'entiers à support fini.
Comme $uv = w^k$, on a $\alpha_p + \beta_p = k\gamma_p$ pour tout p premier. De plus, comme $pgcd(u, v) = 1$ on a $\alpha_p \beta_p = 0$ pour tout p premier. Il en résulte que pour tout p premier, α_p et β_p sont divisibles par k.
Finalement, $\underline{u \text{ et } v \text{ sont bien des puissances } k\text{-ièmes}}$. □

Référence : Francinou, Gianella, Nicolas, *Oraux X-ENS Algèbre 1*, p.168 (Théorème) et p.140 (Lemme).