126

Exemples d'équations diophantiennes

DEF 1 : une équation diophantienne est une équation $P(x_1,\dots,x_n)=0$ d'inconnues $(x_1,\dots,x_n)\in\mathbb{Z}^n$ et $P\in\mathbb{Z}[X]$.

I - Équations du premier degré

1. En deux variables 1001 p10

Résolution de $ax+by=c$ (1) avec $a,b,c\in\mathbb{Z}\setminus\{0\}$.

THM 2 : On pose $d=\mathrm{pgcd}(a,b)$

* Si $d\nmid c$ alors (1) n'a pas de solutions entières.
* sinon l'ensemble des solutions est donné par

$$\left\{\left(x_0+\frac{bk}{d}\ ;\ y_0-\frac{ak}{d}\right) : k\in\mathbb{Z}\right\}$$

où (x_0,y_0) est une solution particulière de (1)

EX 3 Solutions de $3x+7y=11$ sont $\{(6+7k,-1-3k)\ k\in\mathbb{Z}\}$

EX 4 L'équation $303x+57y=a^2+1$ pour $a\in\mathbb{Z}$ n'a pas de solutions entières.

2. En n variables BER p248

Résolution de $a_1x_1+\dots+a_nx_n=b$ (2) où $a_1,\dots a_n\in\mathbb{Z}\setminus\{0\}$ et $b\in\mathbb{Z}$.

THM 5 On pose $d=\mathrm{pgcd}(a_1,\dots a_n)$

L'équation (2) a une solution entière $(x_1,\dots x_n)$ ssi $d\mid b$. Dans ce cas, l'ensemble des solutions de (2) est donné par

$$\left\{\frac{b}{d}V_1+x_2V_2+\dots+x_nV_n : (x_2,\dots x_n)\in\mathbb{Z}^{n-1}\right\}$$

où V_i sont les colonnes de $V\in GL_n(\mathbb{Z})$ qui vérifie $(a_1,\dots a_n)V=(d\ 0\ \dots\ 0)$

EX 6 Application à $3x+4y+7z=b$ où $b\in\mathbb{N}$.

On a $d=1$ et par exemple $V=\begin{pmatrix}-1 & 4 & -1\\ 1 & -3 & -1\\ 0 & 0 & 1\end{pmatrix}$

Les solutions sont alors

$$\begin{cases}x=-b+4k-p\\ y=b-3k-p\\ z=p\end{cases}\quad \text{où } k,p\in\mathbb{Z}.$$

3. Problème de la monnaie

On considère R types de pièces de monnaie de valeurs $0<a_1<\dots<a_R$ où $(a_1,\dots a_R)$ sont premiers dans leur ensemble.

Problème de la monnaie

Déterminer N le montant le plus élevé qu'on ne peut pas obtenir en utilisant que des pièces $a_1,\dots a_R$.
Mathématiquement, déterminer le plus grand entier N

* $\forall n>N\ \exists x_1,\dots x_R\in\mathbb{N} : n=a_1x_1+\dots+a_Rx_R$
* N n'est pas combinaison linéaire entière de $a_1,\dots a_R$.

PROP 7 : Un tel N existe. (admis)

DEF 8 : L'entier N est appelé nombre de Frobenius. En général il n'est pas explicite.

PROP 9 Pour $R=2$: $N=a_1a_2-a_1-a_2$

EX 10 Pour $a_1=5$ et $a_2=7$ $(R=2)$. On a $N=23$

* Pour $n>23$, n est représentable par a_1 et a_2
* Pour $n\leq 23$, n est représentable ou non par a_1 et a_2 (ex 22 ne l'est pas mais 24 l'est).

PROP 11 : Entiers à parts fixes FGN

Soient $a_1,\dots a_R\in\mathbb{N}\setminus\{0\}$ premiers entre eux dans leur ensemble. On pose $U_n=\mathrm{card}\left\{(x_1,\dots x_R)\in\mathbb{N}^R : \sum_{i=1}^{R}a_ix_i=n\right\}$

Alors $U_n\underset{n\to\infty}{\sim}\dfrac{1}{a_1\dots a_R}\dfrac{n^{R-1}}{(R-1)!}$

4. Systèmes modulo Combes p249

THM 12 (Chinois) Soient $m_1,\dots m_p\in\mathbb{Z}$ premiers entre eux 2 à 2. Pour tout $a_1,\dots a_p\in\mathbb{Z}$, il existe une unique solution (modulo $m_1\dots m_p$) au système
$\forall 1\leq i\leq p\quad x\equiv a_i \bmod m_i$ (3)

Méthode de résolution : Méthode de NEWTON

Avec les notations du THM 12, on pose $M_i=\prod_{k\neq i}m_k$ qui sont premiers dans leur ensemble.
On détermine une relation de Bezout $\sum_{i=1}^{p}M_iU_i=1$

CCL : L'ensemble des solutions est $\left\{\sum_{i=1}^{p}M_iU_ia_i+k(m_1\dots m_p) : k\in\mathbb{Z}\right\}$

EX 13 Résolution de $\begin{cases}x\equiv 2 \bmod 4\\ x\equiv 3 \bmod 5\\ x\equiv 1 \bmod 9.\end{cases}$ — SOLUTIONS $118+180k$, $k\in\mathbb{Z}$

II - Exemples et méthodes

1. Réduction modulaire 1001 + C

Idée Lorsque des coefficients de P sont multiples d'un nombre premier q, on étudie $\overline{P}(x_1,\dots x_n)=0$ dans $\mathbb{F}_q$.

* si $\overline{P}$ n'a pas de zéros dans $\mathbb{F}_q$ alors P n'a pas de zéros dans $\mathbb{Z}$

EX 44 : $x^2+y^2=4z+7$ n'a pas de solutions entières
si (x,y,z) est solution on réduit modulo 4
or $x^2+y^2 \not\equiv 3 \bmod 4$ et $4z+7 \equiv 3 \bmod 4$ Absurde.

EX 45 $x^3+5=117y^3$ n'a pas de solutions entières
réduire modulo 9

EX 46 $x^3+y^3+z^3=4$ n'a pas de solutions entières
réduire modulo

EX 47 $x^2+y^2=8z+7$ n'a pas de solutions entières
réduire modulo 8

ex 48 $x^2+1=p$ avec p nombre premier $p\not\equiv 1 \bmod 4$
n'a pas de solutions entières. (Réduire modulo p).
C p 223

2. Descente infinie

Méthode Montrer qu'une équation n'a que des solutions triviales.
→ Raisonner par l'absurde : supposer qu'il existe une solution non triviale $(x_1 \dots x_n)$ avec des conditions de minimalité sur $x_1, \dots x_n$.
→ construire une autre solution non triviale "plus" petite que la solution minimale précédente.
→ On aboutit à une contradiction.

EX 49 L'équation $x^3+2y^3=4z^3$ n'a pas d'autres solutions entières que $(0,0,0)$.

DEV D p52-53

THM 20 Les solutions de $x^2+y^2=z^2$ avec x,y,z premiers entre eux sont données à permutation de x et y près par $x=u^2-v^2$ $y=2uv$ $z=u^2+v^2$ avec $u,v\in\mathbb{Z}$ tels que $\mathrm{pgcd}(u,v)=1$ et u et v sont de parité différente.

THM 21 L'équation $x^4+y^4=z^4$ n'a pas de solutions entières vérifiant $xyz\neq 0$.

3. Avec les corps quadratiques D p 47

Soit $d\in\mathbb{Z}$ sans facteurs carrés.

DEF-PROP 22 : Soit $\mathbb{Q}(\sqrt{d})=\{\alpha+\beta\sqrt{d}\in\mathbb{C} : \alpha,\beta\in\mathbb{Q}\}$.
$\mathbb{Q}(\sqrt{d})$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$. On dit que $\mathbb{Q}(\sqrt{d})$ est un corps de nombres quadratiques.

DEF 23 On définit l'application norme N par
$$N : \begin{array}{ccc} \mathbb{Q}(\sqrt{d}) & \longrightarrow & \mathbb{Q} \\ \alpha+\beta\sqrt{d} & \longmapsto & \alpha^2-d\beta^2 \end{array}$$

DEF 24 (Entiers quadratiques)
• On dit que $x\in\mathbb{Q}(\sqrt{d})$ est un entier quadratique de $\mathbb{Q}(\sqrt{d})$ si x est racine de $X^2+aX+b=0$ où $a,b\in\mathbb{Z}$
• Pour $\mathbb{K}=\mathbb{Q}(\sqrt{d})$ on note $\mathbb{A}_{\mathbb{K}}$ l'ensemble des entiers quadratiques, c'est un sous-anneau de $\mathbb{K}$.

EX 25 : $\frac{1+\sqrt{5}}{2}\in\mathbb{Q}(\sqrt{5})$ est un entier quadratique.

a - Entiers de Gauss $\mathbb{Z}(i)$ $(d=-1)$

THM 26 $(\mathbb{Z}(i),N)$ est euclidien. Et $\mathbb{Z}[i]^\times=\{-i,i,-1,1\}$.

App 27. Equation de Mordell $y^2=x^3-4$ a pour unique solution entière $(x=1, y=0)$. D p 56

b - Entiers $\mathbb{Z}(j)$ $(d=-3)$

THM 28 $(\mathbb{Z}(j),N)$ est euclidien. Et on a D p 50
$$\mathbb{Z}(j)^\times=\left\{-1,1,\frac{1-i\sqrt{3}}{2},\frac{1+i\sqrt{3}}{2},\frac{-1-i\sqrt{3}}{2},-\frac{1+i\sqrt{3}}{2}\right\}$$

App 29 : Equation de Fermat $n=3$
L'équation $x^3+y^3=z^3$ n'a pas de solutions entières vérifiant $xyz\neq 0$. D p 56

III - Carrés

1. Symbole de Legendre D p 64

Soit p un nombre premier.

DEF 30 On définit le symbole de Legendre, pour tout $n\in\mathbb{Z}$ par
$$\left(\frac{n}{p}\right)=\begin{cases} 0 & \text{si } n\equiv 0 \bmod p \\ 1 & \text{si } n\not\equiv 0 \bmod p \text{ et } n \text{ est un carré mod } p \\ -1 & \text{si } n\not\equiv 0 \bmod p \text{ et } n \text{ n'est pas un carré mod } p. \end{cases}$$

EX 31 : $\left(\frac{2}{7}\right)=1$ et $\left(\frac{3}{7}\right)=-1$

PROP 32 (critère d'Euler) Si $p\neq 2$
on a $\left(\frac{n}{p}\right)=n^{\frac{p-1}{2}} \bmod p$.

EX 33 $\left(\frac{7}{11}\right)=7^5 \bmod 11$ donc $\left(\frac{7}{11}\right)=-1$

COR 34 Le symbole de Legendre est multiplicatif, pour tout nombre premier p,
$$\left(\frac{mn}{p}\right)=\left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$$

DEV

THM 36 (Réciprocité quadratique) Soient p et q premiers impairs
on a $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

App 36 : L'équation $x^2+py=q$ pour p premier impair et q non-multiple a une solution ssi $\left(\frac{p}{q}\right)=1$.

2. Somme de carrés

a - De deux carrés Perrin p56

soit $\Sigma = \{a^2+b^2 : a,b \in \mathbb{N}\}$

Thm 37 : Soit p un nombre premier.
On a $p \in \Sigma$ ssi $p=2$ ou $p \equiv 1 \bmod 4$.

THM 38 : (Deux carrés). Soit $n \in \mathbb{N}$ et $n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$ sa décomposition en nombres premiers. Alors,
$n \in \Sigma \Leftrightarrow (\forall p \in \mathbb{P} : p \equiv 3 \bmod 4 \Rightarrow \nu_p(n) \equiv 0 \bmod 2)$

EX 39 : $260 = 8^2 + 14^2$

b - De quatre carrés D p73

LEMME 40 Soit p un nombre premier impair. Alors il existe $(x,y) \in \mathbb{Z}^2$ tels que $1 + x^2 + y^2 = 0$.

THM 41 Tout entier naturel s'écrit comme somme de quatre carrés.

EX 42 $45 = 3^2 + 2^2 + 4^2 + 4^2$

Rmq 43 Ce résultat est optimal car on ne sait pas écrire tout les entiers comme somme de 3 carrés (exemple : 7).

IV - Représentation par des formes quadratiques

Problème : Etant donné une forme quadratique $q(x,y) = ax^2 + bxy + cy^2$ avec $a,b,c \in \mathbb{Z}$ qu'on note (a,b,c).
Quels entiers n s'écrivent $n = q(x,y)$ avec $x,y \in \mathbb{Z}$?

Rmq 44 : c'est une généralisation du théorème des 2 carrés.

DEF 45 : Le discriminant Δ de la forme quadratique $q(x,y) = ax^2+bxy+cy^2$ est $\Delta = b^2 - 4ac$.
La matrice de (a,b,c) est $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$.

DEF 46 : * on dit que n est représentable par la forme (a,b,c) s'il existe $x,y \in \mathbb{Z}$ tel que $n = ax^2+bxy+cy^2$.
* on dit que n est représentable proprement par la forme (a,b,c) s'il existe $x,y \in \mathbb{Z}$ $x \wedge y = 1$ tels que $n = ax^2+bxy+cy^2$.

1. Formes équivalentes Duv.

DEF 47 On dit que deux formes q notée (a,b,c) et q' notée (a',b',c') sont équivalentes s'il existe $M \in SL_2(\mathbb{Z})$ tel que $q' \circ M = q$ et on notera $(a,b,c) \sim (a',b',c')$.

Rmq 48 : Matriciellement si $Q = \mathrm{Mat}\, q$ et $Q' = \mathrm{Mat}\, q'$
on a $q' = q \circ M$ ssi $Q' = {}^tMQM$.

PROP 49 : La relation $\sim$ est une relation d'équivalence.

PROP 50 : Si deux formes sont équivalentes alors elles ont même discriminant.

PROP 51 : Deux formes équivalentes représentent (proprement) les mêmes entiers.

2. Réduction des formes définies positives D p70

DEF 52 La forme (a,b,c) est définie positive si $a>0, c>0$ et si le discriminant $\Delta < 0$.

EX 53 $\varphi(x,y) = x^2+y^2$. φ est définie positive

DEF 54 : La forme (a,b,c) est réduite si
$-a < b \leq a < c$ ou $0 \leq b \leq a = c$ (*)

THM 54 Toute forme définie positive est équivalente à une unique forme quadratique réduite

Algorithme de réduction (annexe)

EX 55 La forme $\varphi(x,y) = 10x^2 + 34xy + 29y^2$ est équivalente à $\varphi(x,y) = x^2+y^2$. n est représentable par φ ssi n est la somme de 2 carrés.

THM 57 Il n'existe qu'un nombre fini de classes d'équivalence de formes quadratiques de discriminant $\Delta<0$ donné.
Ce nombre $h(\Delta)$ est appelé nombre de classes et vaut le nombre de solutions de $\Delta = b^2 - 4ac$ avec $a \leq \sqrt{|\Delta|/3}$ et (a,b,c) vérifiant (*).

3. Résolution du problème D p72

THM 58 : L'entier n est représenté proprement par une forme de discriminant Δ ssi $\Delta = k^2 \bmod 4n$ a une solution

Rmq 59 : C'est une nouvelle preuve du théorème des deux carrés.

EX 60 : $h(-7) = 1$. Les nombres 7 ou p premier avec $p \equiv 1, 2$ ou $4 \bmod 7$ sont représentés par $x^2+xy+2y^2$.
POUR $P = 211$. $211 = 1^2 + 1 \times 10 + 2 \times 100$

EX 61 : 61 est représentable par la forme $(1,0,5)$
$61 = 4^2 + 5 \cdot 3^2$

Théorème des deux carrés

Soit $\Sigma = \{ n = a^2+b^2 : a, b \in \mathbb{N} \}$.

Soit $\mathbb{Z}[i] = \{ a+ib : a, b \in \mathbb{Z} \}$. anneau des entiers de Gauss.

Soit $N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$
$z = a+ib \longmapsto z\bar{z} = a^2+b^2$ application "norme" qui est multiplicative.

<u>Rmq</u> $n \in \Sigma \iff \exists z \in \mathbb{Z}[i] : n = N(z)$.

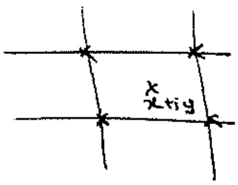
<u>PROP</u> : [$\mathbb{Z}[i]^\times = \{ \pm 1, \pm i \}$.

<u>dem</u> : • soit $z = a+ib \in \mathbb{Z}[i]^\times$. Alors il existe $\tilde{z} \in \mathbb{Z}[i] : z\tilde{z} = 1$.
donc $N(z\tilde{z}) = \underbrace{N(z)}_{\in \mathbb{N}}\underbrace{N(\tilde{z})}_{\in \mathbb{N}} = 1$ donc $N(z) = 1 = a^2+b^2$
or $a, b \in \mathbb{Z}$ donc $(a = 0$ et $b = \pm 1)$ ou $(a = \pm 1$ et $b = 0)$
donc $z = \pm i$ ou $z = \pm 1$.
• Réciproquement, $-1, 1, -i, i$ sont dans $\mathbb{Z}[i]^\times$. ☒

<u>PROP</u> : [Σ stable par multiplication.

<u>PROP</u> [$(\mathbb{Z}[i], N)$ est euclidien donc principal

<u>dem</u> : soient $z \in \mathbb{Z}[i]$ et $t \in \mathbb{Z}[i] \setminus \{0\}$.
on a $\frac{z}{t} = x+iy \in \mathbb{C}$.

or 

soit $a, b \in \mathbb{Z}$ tel que $|x-a| \leq \frac{1}{2}$ et $|y-b| \leq \frac{1}{2}$.

on pose $q = a+ib \in \mathbb{Z}[i]$ et $r = z - qt \in \mathbb{Z}[i]$.
$\left|\frac{z}{t} - q\right|^2 = |x-a|^2 + |y-b|^2 \leq \frac{1}{2}$ donc $\left|\frac{z}{t} - q\right| \leq \frac{\sqrt{2}}{2} < 1$.

soit $r = 0$ soit $|r| = |t| . \left|\frac{z}{t} - q\right| < |t|$
ie $N(r) < N(t)$ ☒

<u>LEMME</u> :
[soit p un nombre premier. On a $p \in \Sigma \iff p$ réductible dans $\mathbb{Z}[i]$

<u>dem</u> :
$(\Rightarrow)$ On a $p = a^2+b^2$ avec $a, b \in \mathbb{Z}$.
donc $p = (a-ib)(a+ib)$ comme $p \in \mathbb{P}$ p est non-nul, non-inversible
ainsi $a \neq 0$ et $b \neq 0$

$\Rightarrow$) Il existe $z, \tilde{z} \notin \mathbb{Z}[i]$: $p = z\tilde{z}$

donc $p^2 = N(p) = N(z)N(\tilde{z})$

or $z, \tilde{z} \in \mathbb{Z}[i]$ $\quad N(z) \neq 1$ et $N(\tilde{z}) \neq 1$

et donc $N(z) = p$ ie $p \in \Sigma$ $\boxtimes$.

THM [Soit p un nombre premier. $\quad p \in \Sigma \Longleftrightarrow p = 2$ ou $p \equiv 1 \bmod 4$

__dem :__ on a $p \in \Sigma \Longleftrightarrow p$ réductible dans $\mathbb{Z}[i]$

$\Longleftrightarrow p$ non premier dans $\mathbb{Z}[i]$ } $\mathbb{Z}[i]$ principal

$\Longleftrightarrow \mathbb{Z}[i]/(p)$ non intègre.

| or $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2+1)$

| or $\mathbb{Z}[X]/(X^2+1)/(\bar{p}) \cong \mathbb{Z}[X]/(X^2+1, p) \cong \mathbb{Z}[X]/(p) / (\overline{X^2+1})$

$\cong \mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$.

donc $p \in \Sigma \Longleftrightarrow \mathbb{Z}/p\mathbb{Z}[X]/(X^2+1)$ non intègre

$\Longleftrightarrow X^2+1$ non premier dans $\mathbb{Z}/p\mathbb{Z}[X]$ } $\mathbb{Z}/p\mathbb{Z}[X]$ principal.

$\Longleftrightarrow X^2+1$ réductible dans $\mathbb{Z}/p\mathbb{Z}[X]$

$\Longleftrightarrow -1$ carré dans $\mathbb{Z}/p\mathbb{Z}$

$\Longleftrightarrow \begin{cases} p = 2 & -1 = 1 = (1)^2 \\ p > 3 & (-1)^{\frac{p-1}{2}} = 1 \end{cases}$ $\leftarrow$ critère d'Euler

$\Longleftrightarrow p = 2$ ou $\frac{p-1}{2} \equiv 0 \bmod 2$.

$\Longleftrightarrow p = 2$ ou $p \equiv 1 \bmod 4$.

$\boxtimes$.

__THM DES DEUX CARRES__

| Soit $n \in \mathbb{N}$ et $n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$ décomposition en facteurs premiers.

| on a $n \in \Sigma \Longleftrightarrow (\forall p \in \mathbb{P}$ $\quad p \equiv 3 \bmod 4 \Rightarrow \nu_p(n) \equiv 0 \bmod 2)$

__dem :__

$\Leftarrow$) on a $n = \underbrace{\left(\prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \bmod 4}} p^{\frac{\nu_p(n)}{2}}\right)^2}_{\in \Sigma} \cdot \underbrace{\left(\prod_{p \not\equiv 3 \bmod 4} p^{\nu_p(n)}\right)}_{\substack{p = 2 \text{ ou } p \equiv 1 \bmod 4 \\ (p \text{ premier})}}$ $\in \Sigma$ (Σ stable par multiplication

donc dans Σ (THM précédent)

$\Rightarrow$) si $n = a^2+b^2$ avec $a, b \in \mathbb{Z}$.

on pose $d = \text{pgcd}(a,b)$: $\exists A, B \in \mathbb{Z}$ $\text{pgcd}(A,B) = 1$: $\begin{cases} a = dA \\ b = dB \end{cases}$

donc $n = d^2(A^2+B^2)$.

Soit p premier impair tel que $p/(A^2+B^2)$

- Par l'absurde, on suppose que p irréductible dans $\mathbb{Z}[i]$.

on a $p/(A-iB)(A+iB)$ dans $\mathbb{Z}[i]$

→ comme p irréductible donc p premier

donc $\begin{pmatrix} p/A-iB \\ p/A+iB \end{pmatrix}$ ou $\begin{pmatrix} p/A+iB \\ p/A-iB \end{pmatrix}$ ↲ passage au conjugué

ie $(p/A-iB)$ et $(p/A+iB)$

→ Ainsi $p/2A$ et $p/2B$ dans $\mathbb{Z}[i]$

en passant à la norme $p^2/4A^2$ et $p^2/4B^2$ dans $\mathbb{Z}$.

or p premier impair p/A et p/B donc $p/\text{pgcd}(A,B) = 1$

absurde donc p réductible dans $\mathbb{Z}[i]$.

- $\exists x, y \notin \mathbb{Z}[i]^\times$: $p = xy$ donc $p^2 = N(p) = N(x)N(y)$

comme avant $N(x) = p$ ie $p \in \Sigma \underset{\text{THM précédent}}{\Rightarrow} p \equiv 1 \bmod 4$

- Ainsi les p premier tel que p/n avec $p \equiv 3 \bmod 4$ sont dans le "d^2" qui a un exposant pair

donc $\nu_p(n) \equiv 0 \bmod 2$

$\boxtimes$.

Développement équations de Fermat

Commençons par remarquer que si (x,y,z) est solution de $x^n + y^n = z^n$, pour $n \in \mathbb{N}$ alors, en posant $d = pgcd(x,y,z)$, on a $x'^n + y'^n = z'^n$ où $x' = \frac{x}{d}$, $y' = \frac{y}{d}$ et $z' = \frac{z}{d}$. Ainsi, on se restreint à l'étude de solutions primitives des équations de Fermat.

On étudie l'équation de Fermat dans le cas $n = 2$ et $n = 4$.

Théorème 2.1. *Les solutions de l'équation $x^2 + y^2 = z^2$, avec x, y et z premiers entre eux, sont données, à une permutation de x et y près, par :*

$$\begin{cases} x = u^2 - v^2, \\ y = 2uv, \\ z = u^2 + v^2, \end{cases} \tag{1}$$

avec $u, v \in \mathbb{Z}$, premiers entre eux, de parité différente.

Démonstration.

- Soit (x,y,z) une solution.
  - ◇ Commençons par remarquer que si un nombre premier p divise deux des trois nombres, alors il divise le dernier. Ainsi x, y, z sont premiers entre deux à deux.
  - ◇ Si x et y sont impairs, alors $x \equiv 1, 3[4]$ et $y \equiv 1, 3[4]$, donc $x^2 \equiv 1[4]$ et $y^2 \equiv 1[4]$, ainsi $z^2 \equiv 2[4]$. Ceci est impossible car les carrés modulo 4 sont 0 et 1. Donc l'un des deux nombres est pair. Disons y est pair.
  - ◇ Si x est pair, cela contredit le fait que $pgcd(x,y) = 1$, ainsi x est impair. Comme x est impair et y est pair, z ne peut pas être pair car $pgcd(y,z) = 1$ donc z est impair.
  - ◇ L'équation de Fermat se réécrit $z^2 - x^2 = y^2$ ou encore $(z-x)(z+x) = y^2$. L'idée, maintenant, est de chercher les facteurs premiers communs à $z + x$ et $z - x$.
    On a montré que x et z sont impairs, ainsi, $2 \mid (x+z)$ et $2 \mid (z-x)$
    Soit, maintenant, $p \neq 2$ premier tel que $p \mid (z+x)$ et $p \mid (z-x)$. Alors $p \mid (x+z) + (z-x) = 2z$ et $p \mid (x+z) - (z-x) = 2x$. Comme p est premier impair, d'après le lemme de Gauss, on a $p \mid z$ et $p \mid x$. C'est impossible puisque x et z sont premiers entre eux.
    On en déduit donc que $pgcd(z+x, z-x) = 2$, et ainsi, il existe $a, b \in \mathbb{Z}$ premiers entre eux tels que $z + x = 2a$ et $z - x = 2b$. Donc $y^2 = 4ab$, ce qui se réécrit, (rappelons que y est pair), $(\frac{y}{2})^2 = ab$.
  - ◇ La décomposition de $(\frac{y}{2})^2$ en facteurs premiers ne présente que des exposants pairs. Comme, de plus, $pgcd(a,b) = 1$, les mêmes facteurs se retrouvent soit dans a soit dans b, ainsi la décomposition en facteurs premiers de a et de b n'a que des exposants pairs. Il existe donc $u, v \in \mathbb{N}$ premiers entre eux (puisque a et b le sont) vérifiant $a = u^2$ et $b = v^2$. Ainsi, $z + x = 2a = 2u^2$, $z - x = 2b = 2v^2$ et donc $z = u^2 + v^2$, $x = u^2 - v^2$ et $y = 2uv$. Comme z est impair, u et v sont de parité différente.
- Réciproquement, si on a $x = u^2 - v^2$, $y = 2uv$ et $z = u^2 + v^2$, avec $u,\ v \in \mathbb{Z}$, premiers entre eux et de parité différente, alors $x^2 + y^2 = z^2$. En outre, si 2 divise x, y et z, alors en particulier $u^2 \equiv v^2[2]$, ce qui contredit le fait que u et v sont de parité différente. Si $p \neq 2$ premier divise x, y et z, alors $p \mid (u^2 - v^2)$ et $p \mid (u^2 + v^2)$ d'où $p \mid 2u^2$ et $p \mid 2v^2$, ce qui implique par lemme de Gauss que $p \mid u^2$ et $p \mid v^2$. Comme p est premier, on obtient $p \mid u$ et $p \mid v$, ce qui est impossible puisque u et v sont premiers entre eux.

□

A partir de ce théorème, on peut maintenant démontrer le résultat suivant :

Théorème 2.2. *L'équation diophantienne $x^4 + y^4 = z^4$ n'admet pas de solution vérifiant $xyz \neq 0$.*

Démonstration. D'après la remarque du début, on se restreint à la recherche de solutions primitives.
On va utiliser l'idée de Fermat, lui-même. Remarquons que si (x,y,z) est solution de $x^4 + y^4 = z^4$ avec x, y, z premiers entre eux, alors (x, y, z^2) est solution de $x^4 + y^4 = w^2$ avec $x,\ y,\ w = z^2$ premiers entre eux. Il suffit donc de montrer que $x^4 + y^4 = z^2$ n'a pas de solution vérifiant $xyz \neq 0$.
Pour cela, nous allons utiliser la méthode de la descente infinie. Supposons qu'il y ait une telle solution. Soit (x,y,z) un couple solution avec $z > 0$ et z minimal. D'après les remarques du début, x, y, z sont premiers entre eux dans leur ensemble, et même, premiers entre eux deux à deux.

- ◇ On peut refaire les deux premières étapes de la démonstration précédente, ce qui montre que x et z sont impairs et y est pair.
- ◇ Remarquons ensuite que l'équation $x^4 + y^4 = z^2$ se réécrit $(x^2)^2 + (y^2)^2 = z^2$ avec x^2, y^2, z premiers entre eux. Donc, par Théorème 2.1, il existe $u, v \in \mathbb{Z}$ premiers entre eux, de parité différente, tels que $x^2 = u^2 - v^2$, $y^2 = 2uv$ et $z = u^2 + v^2$ (car c'est y^2 qui est pair). Ainsi, on obtient $x^2 + v^2 = u^2$.
- ◇ Comme u et v sont premiers entre eux, x, u et v sont premiers entre eux. De plus, par la même méthode que précédemment, on montre que x et v ne peuvent être tous les deux impairs. Or x est impair, ainsi v est pair et u est impair.
- ◇ On peut donc à nouveau appliquer le Théorème 2.1 : il existe $a, b \in \mathbb{Z}$ premiers entre eux, de parité différente tels que $x = a^2 - b^2$, $v = 2ab$ et $u = a^2 + b^2$ (car c'est v qui est pair). Donc $y^2 = 2uv = 4ab(a^2 + b^2)$.
- ◇ La décomposition de $(\frac{y}{2})^2$ en facteurs premiers ne présente que des exposants pairs. Comme a, b et $a^2 + b^2$ sont premiers entre eux, les mêmes facteurs se retrouvent soit dans a, soit dans b, soit dans $a^2 + b^2$, ainsi la décomposition en facteurs premiers de a, b et $a^2 + b^2$ n'a que des exposants pairs. Ainsi, il existe $\alpha,\ \beta,\ \gamma \in \mathbb{N}$

premiers entre eux tels que $a = \alpha^2$, $b = \beta^2$ et $a^2 + b^2 = \gamma^2$.
Donc $\gamma^2 = a^2 + b^2 = \alpha^4 + \beta^4$, ainsi (α, β, γ) est une solution primitive, or $0 < \gamma \leq \gamma^2 = u < z$ (la première inégalité vient du fait que $(a, b) \neq (0, 0)$ puisqu'on a choisi une solution non triviale, la dernière vient du fait que $v \neq 0$ sinon $x^2 = z$ et cela contredit $pgcd(x, z) = 1$). Ceci contredit la minimalité de z et donc conclut la preuve du théorème.

$\square$

Annexe Algorithme de réduction.

* Si $c < a$ $\quad (a,b,c) \to (c,-b,a)$ avec $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

* si $|b| > a$ $\quad (a,b,c) \to (a,b',c')$
  où il faut choisir δ tel que $b + 2\delta a \in]-a,a[$
  on pose $b' = b + 2\delta a$
  on prend $M = \begin{pmatrix} 1 & \delta \\ 0 & 1 \end{pmatrix}$ et on déduit c' tel que le discriminant soit conservé

* si $(a, \underbrace{-b}_{\leq 0}, a) \to (a,b,a)$ avec $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

* si $(a, \underbrace{-a}_{\leq 0}, c) \to (a,a,c)$ avec $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

REFERENCES

Duverney, Théorie des nombres
Combes, Algèbre et géométrie
De Koninck et Mercier, 1001 Problèmes en théorie classique des nombres.
FGN Analyse 2.
Perrin, Cours d'algèbre