(126*)

NOM : UMBER Prénom : Pierre Jury :

(Algèbre) — Entourez l'épreuve → Analyse

Sujet choisi : Exemples d'équations diophantiennes

Autre sujet : /

I. Définitions et premières remarques

1) Définitions

Déf 1 : on appelle équation diophantienne la donnée de $P \in \mathbb{Z}[X_1, \dots, X_n]$. Résoudre cette équation revient à trouver les zéros de P

Déf 2 : Si $P \in \mathbb{Z}[X_1, \dots, X_n]$ est homogène, on appelle solution triviale la solution $(0, \dots, 0)$

Rem 3 : Matiyasevich a montré que le problème de savoir si une équation a une solution est indécidable (1970)

2) Le lien $\mathbb{Z}$ - $\mathbb{Q}$

Prop 4 : Soit $P = \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}[X]$ et $\frac{p}{q} \in \mathbb{Q}$ racine de P, avec $p \wedge q = 1$. Alors $q \mid a_m$ et $p \mid a_0$

Ex 5 : Les solutions de $x^4 + 3x^3 - x^2 - 5x + 2 = 0$ dans $\mathbb{Q}$ sont $x = 1$ et $x = -2$

Rem 6 : quitte à ajouter des variables, on peut ramener la résolution d'équations sur $\mathbb{Q}$ à la résolution d'une équation diophantienne

3) Méthode de la descente infinie

Prop 7 : Soit $A \subset \mathbb{N}$, $A \neq \emptyset$. Alors A admet un plus petit élément

Ex 8 : $x^2 = 2y^2$ n'a pas de solution non triviale

$\Leftrightarrow$ $P \in \mathcal{P}$ (ensemble des nombres premiers)

alors $x^3 + py^3 + p^2 z^3 = 0$ n'a pas de solution non triviale

II. Equations diophantiennes de degré 1

Th 9 (Bezout) : Soit $a_1, \dots, a_n \in \mathbb{Z}$, alors :

$a_1, \dots, a_n$ sont premiers entre eux $\Leftrightarrow \exists u_1, \dots, u_n \in \mathbb{Z}$ tq $\sum_{i=1}^{n} a_i u_i = 1$

dans un anneau

Lemme 10 (Gauss) : Soit $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et $a \wedge b = 1$ alors $a \mid c$

1) Résolution dans $\mathbb{Z}$ d'équations linéaires

Déf 11 : si $P \in \mathbb{Z}[X_1, \dots, X_n]$, on parle d'équation diophantienne linéaire lorsque $\deg P \leq 1$. Elle revient à résoudre $MX = B$, $M \in \mathcal{M}_{p,m}(\mathbb{Z})$, $B \in \mathbb{Z}^p$, lorsque l'on considère un système à p équations.

Prop 12 : L'équation $a_1 x_1 + \dots + a_n x_n = b$ admet une solution ssi $\text{pgcd}(a_1, \dots, a_n) \mid b$.

Rem 13 : pour trouver une telle combinaison, on utilise l'algorithme d'Euclide étendu

Prop 14 : Soit $a, b, c \in \mathbb{Z}$, avec $a \wedge b$. Alors, si (x_0, y_0) est une solution particulière de $ax + by = c$, alors l'ensemble des solutions de cette équation est $S = \{(x_0 + k\frac{b}{b \wedge a}, y_0 - k\frac{a}{b \wedge a}), k \in \mathbb{Z}\}$

DEV 1

2) Exemple de résolution dans $\mathbb{N}$

DEV 1 : Soit $a_1, \dots, a_p \in \mathbb{N}^*$ nombres premiers entre eux dans leur ensemble. On pose $S_m := |\{(x_1, \dots, x_p) \in \mathbb{N}^p, \sum_{i=1}^{p} a_i x_i = m\}|$

alors $S_m \sim \frac{1}{\prod_{i=1}^{p} a_i} \frac{m^{p-1}}{(p-1)!}$

III. Utilisation de la congruence

1) Equation de congruence

Déf 15 : On appelle équation de congruence une équation polynomiale dans $\mathbb{Z}/n\mathbb{Z}$

Prop 16 : L'équation $ax = b \ [n]$ a une solution ssi $d := a \wedge n$ divise b. Dans ce cas, l'équation admet d solutions, dont x_0 est une solution particulière, alors les solutions sont les $x_0 + k\frac{n}{d}$, $0 \leq k \leq d-1$

Prop 17: Soit $m_1, \dots, m_k \in \mathbb{N}^*$ premiers entre eux 2 à 2. On veut résoudre $x \equiv a_i [m_i]$. On pose $m := \prod_i m_i$. Alors ce système d'équations a une unique solution modulo m. Si l'on pose $b_i := \prod_{j \neq i} m_j$ et c_i t.q. $c_i b_i = 1 [m_i]$, alors $x := \sum_i b_i c_i a_i$ est une solution

2) Loi de réciprocité quadratique

Def 18: Soit $p \in \mathcal{P}$ impair, $a \wedge p = 1$. On pose $\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{si } a \text{ est un carré mod } p \\ -1 & \text{sinon} \end{cases}$

Prop 19 (Euler): Si $a \wedge p = 1$, on a $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} [p]$

Prop 20 (loi de réciprocité quadratique): Soit $p, q \in \mathcal{P}$ impairs, $p \neq q$ alors $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$

Prop 21: On a : • $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 [4]$

• $\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 [8]$ • si $p \neq 3$, $\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 [12]$ $\left(\frac{-3}{p}\right) = 1 \Leftrightarrow p \equiv 1 [3]$

Exe 22: l'équation $y^2 = 41x + 3$ n'a pas de solutions

Exe 23: Si $p \equiv 3 [4]$, $p \in \mathcal{P}$, l'équation $x^2 + y^2 = pz^2$ n'a pas de solution non triviale

3) Equation de Mordell/Bachet

Def 24: On appelle équation de Mordell/Bachet l'équation $y^2 = x^3 + k$ pour $k \in \mathbb{Z}$

Prop 25: si $M \equiv 3 [4]$, $N \equiv 2 [4]$ et, $\forall p \in \mathcal{P}$, $p \mid \frac{N}{2} \Rightarrow p \equiv 1 [4]$, alors, pour $k = M^3 - N^2$, l'équation n'a pas de solutions

Prop. 26: si $M \equiv 2 [4]$, $N \equiv 1 [2]$ et, $\forall p \in \mathcal{P}$, $p \mid N \Rightarrow p \equiv 1 [4]$, alors, pour $k = M^3 - N^2$, l'équation n'a pas de solutions

Exe 27: $y^2 = x^3 - 5$ n'a pas de solutions

$y^2 = x^3 + 7$ n'a pas de solutions

V. De l'arithmétique dans un autre anneau

Prop 28: Soit A un anneau principal, $p \in A$ non nul non inversible. Alors : p est premier ($\Leftrightarrow p$ est irréductible $\Leftrightarrow A/(p)$ est un corps

1) Autour de l'anneau de Gauss

Def 29: on appelle anneau de Gauss l'anneau $\mathbb{Z}[i]$

Prop 30: On a $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2+1)$

Prop 31: $\mathbb{Z}[i]$ est euclidien pour le stathme $N(a+ib) = a^2 + b^2$

Prop 32: $\mathbb{Z}[i]^\times = \{-1; 1\}$

Lemme 33: On pose $\Sigma := \{a^2 + b^2, a, b \in \mathbb{Z}\}$. Alors Σ est stable par multiplication

Th. 34: Soit $n \in \mathbb{N}$. alors : $n \in \Sigma \Leftrightarrow \forall p \in \mathcal{P}, p \equiv 3 [4], p \mid n \Rightarrow v_p(n)$ est pair

App. 35: Si $a + ib \in \mathbb{Z}[i]$ $\{a+ib$ est irréductible dans $\mathbb{Z}[i]\} \Leftrightarrow \{a^2 + b^2 \in \mathcal{P}$ ou $a^2 + b^2 = p^2, p \in \mathcal{P}$ et $p \equiv 3 [4]\}$

App. 36: Si $p \in \mathcal{P}$, avec $p = 2$ ou $p \equiv 1 [4]$, alors l'équation $x^2 + y^2 = pz^2$ a une infinité de solutions

Def 37: On appelle ~~équation~~ équation de Pythagore l'équation $x^2 + y^2 = z^2$. Une solution (x, y, z) de cette équation est dit triplet pythagoricien

Th. 38: Le triplet (x, y, z) est un triplet pythagoricien, si et seulement si il existe $d > 0$ et $u, v \in \mathbb{N}$, $u \wedge v = 1$, $u > v$ et $\begin{cases} x = d(u^2 - v^2) \\ y = 2duv \\ z = d(u^2 + v^2) \end{cases}$

(x à permutation de x et y près)

((x, y, z) non triviale)

DEV 2

2) Autour de l'anneau $\mathbb{Z}[i\sqrt{2}]$

Prop 39 : on a $\mathbb{Z}[i\sqrt{2}] = \mathbb{Z}[X]/(X^2+2)$

Prop 40 : $\mathbb{Z}[i\sqrt{2}]$ est euclidien pour le stathme $N(a+bi\sqrt{2}) = a^2+2b^2$

Prop 41 : on a $\mathbb{Z}[i\sqrt{2}]^\times = \{1, -1\}$

Prop 42 : Soit $p \in \mathcal{P}$. Alors $p = a^2+2b^2 \Leftrightarrow -2$ est un carré mod p

Ex 43 : Les solutions de l'équation de Mordell $y^2 = x^3 - 2$ sont $(3,5)$ et $(3,-5)$

3) Autour de l'anneau d'Eisenstein

Def 44 : on pose $j := \frac{-1+\sqrt{3}}{2}$

Def 45 : on appelle anneau d'Eisenstein l'anneau $\mathbb{Z}[j]$

Prop 46 : on a $\mathbb{Z}[j] \simeq \mathbb{Z}[X]/(X^2+X+1)$

Prop 47 : $\mathbb{Z}[j]$ est euclidien pour le stathme

$$N(a+jb) = a^2 - ab + b^2 = \frac{(2a-b)^2}{4} + \frac{3b^2}{4}$$

Prop 48 : $\mathbb{Z}[j]^\times = \{1; -1; j; -j; j^2; -j^2\}$

Th 49 : Soit $p \in \mathcal{P}$. $p = a^2 - ab + b^2 \Leftrightarrow \begin{cases} p \neq 2 \\ -3 \text{ est un carré mod } p \end{cases}$

Ex 50 : $7 = 3^2 - 2\times 3 + 2^2$ $(7 \equiv 1 [3])$

V. Autres équations

1) L'équation de Pell

Def 51 : on appelle équation de Pell l'équation $x^2 - dy^2 = m$ où $m \in \mathbb{Z}$ et $d \geq 2$ est sans facteur carré

Rem 52 : pour étudier cette équation, on se place dans $\mathbb{Z}[\sqrt{d}]$

Th 53 (Lagrange) : ① Il existe une infinité de solutions de l'équation $x^2 - dy^2 = 1$. Il existe une solution minimale (x_1, y_1), $x_1, y_1 > 0$, dit solution fondamentale, t.q. les autres solutions dans $(\mathbb{N}^*)^2$ sont les (x_m, y_m) où $x_m + \sqrt{d}\, y_m = (x_1 + \sqrt{d}\, y_1)^m$

② Si $x^2 - dy^2 = -1$ a une solution, alors il existe une solution minimale (x_1, y_1), $x_1, y_1 > 0$, dite solution fondamentale, t.q. les autres solutions dans $\mathbb{N}^2$ sont les (x_m, y_m) où $x_m + \sqrt{d}\, y_m = (x_1 + \sqrt{d}\, y_1)^m$ et m impair. Le couple (x_2, y_2) est alors solution fondamentale de $x^2 - dy^2 = 1$

Rem. 54 : si (x,y), $x, y > 0$, est une solution de $x^2 - dy^2 = \pm 1$, alors $\frac{x}{y}$ est une réduite du développement en fraction continue de $\sqrt{d}$

Ex. 55 : $\sqrt{7} = [2,1,1,1,4,\ldots]$, ce qui donne $8^2 - 7\times 3^2 = 1$

$\sqrt{37} = [6,\overline{1,2}]$, ce qui donne $6^2 - 37\times 1 = -1$

2) L'équation de Fermat

Def 56 : on appelle équation de Fermat l'équation $x^m + y^m = z^m$

Prop 57 : si $x, y, z \geq 1$, l'équation $x^4 + y^4 = z^2$ n'a pas de solutions

Cr. 58 : si $m = 4$, l'équation de Fermat n'a pas de solution.

Th. 59 (Sophie-Germain, 1823) : si $p \in \mathcal{P}$ est impair tel que $2p+1 \in \mathcal{P}$, alors $x^p + y^p = z^p$ n'a pas de solution non triviale

Th. 60 (Fermat-Wiles, 1994) : Si $m \geq 3$, l'équation $x^m + y^m = z^m$ n'a pas de solution non triviale

Annexe :

algorithme d'euclide étendu :

Soit $a, b \in \mathbb{Z}$, $a, b \neq 0$

On pose $\begin{cases} x_0 = a \\ x_1 = b \end{cases}$ $\begin{cases} u_0 = 1 \\ u_1 = 0 \end{cases}$ $\begin{cases} v_0 = 0 \\ v_1 = 1 \end{cases}$

- Si $x_m \neq 0$, on note $x_{m-1} = q x_m + r$, division euclidienne de x_{m-1} par x_m

on pose alors $\begin{cases} x_{m+1} := r \\ u_{m+1} := u_{m-1} - q u_m \\ v_{m+1} := v_{m-1} - q v_m \end{cases}$

- $\forall m$, $a u_m + b v_m = x_m$
- $\text{pgcd}(x_m, x_{m+1}) = \text{pgcd}(x_m, x_{m-1})$
- $(|x_m|)$ décroit strictement
- Si $x_m = 0$ et $x_{m-1} \neq 0$, alors x_{m-1} est un pgcd de a et b

Réf : Combes, algèbre et géométrie (Ex. 23, V)
Alaca ; Williams, Introductory algebraic Number Theory (III 3), Ex. 43)
Ireland ; Rosen, A classical introduction to Modern Number Theory (Ch 38, V)
Laurent Berger, Théorie algébrique des nombres (pdf) (Rem. 54)

4/4

Somme de deux carrés

▫ **proposition :** $\mathbb{Z}[i]$ est euclidien

démonstration : On pose $\nu : \mathbb{Z}[i] - \{0\} \to \mathbb{N}^*$
$a + ib \mapsto a^2 + b^2$

Soit $\alpha = a + ib \in \mathbb{Z}[i]$, $\beta = c + id \in \mathbb{Z}[i]$, $\beta \neq 0$
alors $\frac{\alpha}{\beta} = r + is \in \mathbb{Q}(i)$.

Soit $m, n \in \mathbb{Z}$, $|r - m| \leqslant \frac{1}{2}$ et $|s - n| \leqslant \frac{1}{2}$

On pose $\gamma := m + ni \in \mathbb{Z}[i]$
alors $\nu\left(\left(\frac{\alpha}{\beta}\right) - \gamma\right) = (r - m)^2 + (s - n)^2 \leqslant \frac{1}{2}$

On pose alors $\rho := \alpha - \beta\gamma$, on a $\nu(\rho) = \nu(\beta)\nu\left(\frac{\alpha}{\beta} - \gamma\right)$

$\leqslant \frac{\nu(\beta)}{2}$

$< \nu(\beta)$

Ainsi, ν est bien un stathme, donc $\mathbb{Z}[i]$ est euclidien.

▫ **proposition :** Soit $p \in \mathcal{P}$. Alors $\left(p = a^2 + b^2 \Leftrightarrow p \equiv 1 [4] \text{ ou } p = 2\right)$

démonstration : On a $\mathbb{Z}[i]^\times = \{x \in \mathbb{Z}[i], \nu(x) = 1\}$
$= \{1, -1, i, -i\}$.

Montrons que $p = a^2 + b^2 \Leftrightarrow p$ est réductible dans $\mathbb{Z}[i]$:
. Si $p = \alpha\beta$, α, β non inversibles, alors $p^2 = N(p) = N(\alpha) N(\beta)$
donc $N(\alpha) = N(\beta) = p$
. Si $p = a^2 + b^2$, on pose $\alpha := a + ib$. Comme $p \neq 1$,
α est non inversible dans $\mathbb{Z}[i]$, il en est de même
pour $\bar{\alpha}$, et $p = N(\alpha) = \alpha\bar{\alpha}$ est réductible dans $\mathbb{Z}[i]$
Par ailleurs, $\mathbb{Z}[i]$ est euclidien, donc :
$p = a^2 + b^2 \Leftrightarrow (p)$ n'est pas premier.
On a : $\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[X]/(p, X^2 + 1) = \mathbb{F}_p[X]/(X^2 + 1)$

ainsi : $p = a^2 + b^2 \Leftrightarrow -1$ est un carré mod p

. si $p = 2$: ok

. si p est impair, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, donc $p = a^2+b^2 \Leftrightarrow p \equiv 1 [4]$

□ proposition : On pose $\Sigma := \{a^2 + b^2,\ a, b \in \mathbb{Z}\}$, $m \in \mathbb{N}^*$

alors : $m \in \Sigma \Leftrightarrow \forall p \in \mathcal{P}$, $p | m$ et $p \equiv 3 [4] \Rightarrow v_p(m)$ pair.

démonstration : $\Leftarrow$ ok car Σ est stable par multiplication

$\Rightarrow$ par récurrence : Soit $p \in \mathcal{P}$, $p \equiv 3 [4]$, fixé, et $m \in \Sigma$

(H_d) : si $v_p(m) \leq d$, alors $v_p(m)$ est pair.

$d = 0$: ok

. si $v_p(m) \geq 1$, $p | m = a^2 + b^2 = (a+ib)(a-ib)$

Comme $p \equiv 3 [4]$, p est irréductible dans $\mathbb{Z}[i]$, donc

$p | a+ib$ ou $p | a-ib$, donc $p | a$ et $p | b$ car $p \in \mathbb{Z}$

alors $m = p^2 (a^2 + b^2)$ et $\frac{m}{p^2} \in \Sigma$. On utilise l'hypothèse de récurrence pour conclure.

Leçons : 122 : anneaux principaux

126 : équations diophantiennes

Partition d'un entier en parts fixées

□ **Théorème :** Soient $\alpha_1, \dots, \alpha_p \in \mathbb{N}^*$, premiers entre eux dans leur ensemble.
On pose $S_m := \#\{(x_1, \dots, x_p) \in \mathbb{N}^p, \sum_{i=1}^p \alpha_i x_i = m\}$.
Alors $\boxed{S_m \sim \frac{1}{\prod_{i=1}^p \alpha_i} \frac{m^{p-1}}{(p-1)!}}$

Démonstration : On pose $F := \sum_{m \geq 0} S_m X^m \in \mathbb{C}[[X]]$

On a : $\prod_{i=1}^p \frac{1}{1-X^{\alpha_i}} = \prod_{i=1}^p \left(\sum_{m_i \geq 0} X^{\alpha_i m_i} \right)$

$= \sum_{(m_1, \dots, m_p) \in \mathbb{N}^p} X^{\sum_{i=1}^p \alpha_i m_i}$

$= \sum_{m \geq 0} S_m X^m$

$= F$

Ainsi, F a pour seuls pôles les racines α_i-ièmes de l'unité, $i \in [\![1; p]\!]$. Ainsi, F a un pôle d'ordre exactement p en 1.
Soit ζ un pôle de F d'ordre p, alors : $\forall i, \zeta^{\alpha_i} = 1$, donc $\zeta = 1$ car il existe $m_1, \dots, m_p \in \mathbb{Z}$, $\sum m_i \alpha_i = 1$. Ainsi, les pôles de F autres que 1 sont d'ordre au plus $p-1$. Par décomposition en éléments simples sur $\mathbb{C}$, on a :

$$F = \frac{a}{(1-X)^p} + \sum_{\zeta \in U} \sum_{k=1}^{p-1} \frac{a_{\zeta,k}}{(\zeta - X)^k}$$

où $a, a_{\zeta,k} \in \mathbb{C}$, $U := \{\zeta \in \mathbb{C}^*, \exists i \in [\![1, p]\!], \zeta^{\alpha_i} = 1\}$.
Par ailleurs :

$$\frac{1}{(\zeta - X)^k} = \frac{1}{(k-1)!} \left(\frac{1}{\zeta - X} \right)^{(k-1)} = \frac{1}{(k-1)!} \left(\frac{1}{\zeta} \sum_{m \geq 0} \left(\frac{X}{\zeta} \right)^m \right)^{(k-1)} = \frac{1}{\zeta^k (k-1)!} \sum_{m \geq 0} \frac{(m+1) \cdots (m+k-1)}{\zeta^m} X^m$$

Ainsi, en identifiant terme à terme, on a :

$$S_m = a \frac{(m+1) \cdots (m+p-1)}{(p-1)!} + \sum_{\zeta \in U} \sum_{k=1}^{p-1} a_{\zeta,k} \frac{(m+1) \cdots (m+k-1)}{(k-1)! \, \zeta^{m+k}}$$

Le dernier terme est un $o(m^{p-1})$ car $|\zeta^{m+k}| = 1$, on a donc $S_m \sim a \frac{m^{p-1}}{(p-1)!}$ (si $a \neq 0$)

Il reste à calculer a. On a :

$$a = \left((1-X)^p F(X) \right)\Big|_{X=1}$$

donc $a = \prod_{i=1}^{p} \left(\frac{1}{1+X+\dots+X^{\alpha_i - 1}} \right)\Big|_{X=1}$

$= \prod_{i=1}^{p} \frac{1}{\alpha_i}$.

Leçons : 124 : anneaux des séries formelles. Applications

126 : Exemples d'équations diophantiennes

140 : corps des fractions rationnelles

228 : développement asymptotique