126

Exemples d'équations diophantiennes

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

I - Equations du premier degré

1. En deux variables — 1001 p40

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

où (x_0, y_0) est une solution particulière de (1) exo 801

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. 847

2. En n variables — BER p248

Résolution de $a_1 x_1 + \dots + a_n x_n = b$ (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 $\{\frac{b}{d} V_1 + x_2 V_2 + \dots + x_n V_n \quad (x_2, \dots x_n) \in \mathbb{Z}^{n-1}\}$

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

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

3 Problème de la monnaie — RB p25

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

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

CORO 7b Un tel N existe.

DEF 8 : L'entier N est appelé nombre de Frobenius

En général il n'est pas explicite.

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

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 18 ne l'est pas mais 24 l'est).

PROP 7 Entiers à parts fixes — FGN

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

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

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 $\sum_{i=1}^{p} M_i U_i = 1$

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

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 q, on étudie $\bar{P}(x_1, \dots x_n) = 0$ dans $\mathbb{F}_q$

- Si $\bar{P}$ n'a pas de zéros dans $\mathbb{F}_q$ alors P n'a pas de zéros dans $\mathbb{Z}$

814

EX 14 : $x^2+y^2=4z+7$ 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.

et 289

EX 15 $x^3+5=117y^3$ n'a pas de solutions entières
réduire modulo 9

844

EX 16 $x^3+y^3+z^3=4$ n'a pas de solutions entières
réduire modulo 9

85

EX 17 $x^2+y^2=8z+7$ n'a pas de solutions entières
réduire modulo 8

EX 18 $x^2+4=p$ 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.

854

EX 19 L'équation $x^3+2y^3=4z^3$ n'a pas d'autres solutions entières que $(0,0,0)$.

D p52-53

DEV

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
· 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 $y^2 = x^3 - 1$ 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
$$\mathbb{Z}(j)^\times = \left\{-1, 1, \frac{1-i\sqrt{3}}{2}, \frac{1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}, \underbrace{\frac{-1+i\sqrt{3}}{2}}_{=j}\right\}$$

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,
$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right), \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

11 α ordre 8 dans $\mathbb{F}_{p^2}^\times$

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

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 $p \equiv 1 \bmod 4$.)

DEV

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 $1 + x^2 + y^2 = 0 \, [p]$

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

EX 42: $15 = 3^2 + 2^2 + 1^2 + 1^2$

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

IV - Représentation par des formes quadratiques

Problème: Étant 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 (Dur)

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 $\psi(x,y) = x^2 + y^2$. 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 $(1,0,5)$
$61 = 4^2 + 5 \cdot 3^2$

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

BER = Modèles, théorie, pratique et un peu d'algorithme Bonthuy

RB = Risler Boyer