

Plaquette 5 – Équations diophantiennes et problèmes

Arithmétique dans $\mathbb{Z}$ — Licence 1 (L1)

Exercices

Méthode

Une **équation diophantienne** se résout en entiers. Trois stratégies couvrent l'essentiel : la méthode **Bézout-Gauss** pour $ax + by = c$ (solution particulière puis solution générale), la **factorisation** ($x^2 - y^2 = n$, $xy = 2x + 3y$, $\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$) qui ramène à une liste finie de diviseurs, et l'**obstruction modulaire** ou la **descente infinie** qui prouvent l'absence de solution. Les problèmes en contexte (monnaie, volailles, noix de coco) se traduisent d'abord en équation, puis on garde les solutions **positives**.

Exercice 1 – Solution générale d'une équation linéaire

- L'équation $15x + 21y = 40$ a-t-elle des solutions entières ?
- Résoudre dans $\mathbb{Z}^2$ l'équation $15x + 21y = 39$.
- Existe-t-il des solutions avec $x > 0$ et $y > 0$? Avec $x \geq 0$ et $y \geq 0$?
- Parmi les solutions, laquelle minimise $|x| + |y|$?

Exercice 2 – Les cent volailles

Problème de Zhang Qiu Jian (V^e siècle) : un coq coûte 5 pièces, une poule 3 pièces, et l'on a 3 poussins pour 1 pièce. Avec 100 pièces, on achète exactement 100 volailles. Combien de coqs x , de poules y et de poussins z ?

- Traduire l'énoncé par un système de deux équations en entiers naturels.
- Éliminer z et montrer que $7x + 4y = 100$.
- Résoudre cette équation en entiers naturels.
- Donner toutes les solutions du problème et les vérifier.

Exercice 3 – Pièces de 5 et de 7

On ne dispose que de pièces de 5 € et de 7 €. Un montant n est **payable** s'il existe $u, v \in \mathbb{N}$ avec $5u + 7v = n$.

- Montrer que 23 n'est pas payable.
- Montrer que 24, 25, 26, 27 et 28 sont payables. En déduire que tout $n \geq 24$ l'est.
- Lister tous les montants non payables.
- Démontrer en général que si $a \wedge b = 1$, alors $ab - a - b$ n'est pas payable avec des pièces de a et b .

Exercice 4 – Différence de deux carrés

- Résoudre dans $\mathbb{N}^2$ l'équation $x^2 - y^2 = 45$.
- Montrer qu'un entier $n \equiv 2 \pmod{4}$ n'est jamais différence de deux carrés.
- Montrer que tout entier impair et tout multiple de 4 est une différence de deux

carrés.

d) De combien de façons 2 026 et 2 027 s'écrivent-ils comme différence de deux carrés d'entiers naturels ? (2 027 est premier.)

Exercice 5 - Triplets pythagoriciens

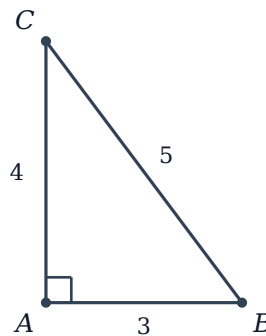
On cherche les triplets (a, b, c) d'entiers naturels non nuls tels que $a^2 + b^2 = c^2$ et $\text{pgcd}(a, b, c) = 1$ (**primitifs**).

a) Montrer que a et b ne sont pas tous deux impairs (raisonner modulo 4). On suppose désormais b pair.

b) Montrer que $\frac{c+a}{2}$ et $\frac{c-a}{2}$ sont des entiers premiers entre eux dont le produit est $\left(\frac{b}{2}\right)^2$. En déduire qu'ils sont des carrés m^2 et n^2 .

c) En déduire $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$.

d) Lister les triplets primitifs avec $c \leq 30$ et vérifier le premier sur la figure.



Exercice 6 - Somme de deux fractions égyptiennes

On cherche les couples (x, y) d'entiers naturels non nuls tels que $\frac{1}{x} + \frac{1}{y} = \frac{1}{6}$.

a) Montrer que $x > 6$ et $y > 6$.

b) Montrer que l'équation équivaut à $(x - 6)(y - 6) = 36$.

c) En déduire toutes les solutions. Combien y en a-t-il ?

d) Généraliser : combien de couples ordonnés vérifient $\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$? Application à $n = 12$.

Exercice 7 - Équation de Pell-Fermat

On étudie $(E) : x^2 - 2y^2 = 1$ en entiers naturels.

a) Vérifier que $(3, 2)$ est solution. Montrer que si (x, y) est solution, alors $(3x + 4y, 2x + 3y)$ aussi.

b) En déduire trois autres solutions.

c) Montrer que $(x + y\sqrt{2})(3 + 2\sqrt{2}) = (3x + 4y) + (2x + 3y)\sqrt{2}$ et interpréter a).

d) Montrer que si (x, y) est solution avec $y \geq 1$, alors $\left|\frac{x}{y} - \sqrt{2}\right| < \frac{1}{2y^2}$. Que donnent les

solutions trouvées ?

Exercice 8 - Factoriser une équation produit

- Résoudre dans $\mathbb{Z}^2$ l'équation $xy = 2x + 3y$.
- Parmi les solutions, lesquelles ont x et y strictement positifs ?
- Résoudre dans $\mathbb{N}^2$: $xy - 5x - 5y = 0$.
- Un rectangle à côtés entiers a une aire égale à son périmètre. Quelles sont ses dimensions ?

Exercice 9 - Théorème chinois sans coprimauté

- Résoudre le système $x \equiv 3 \pmod{6}$, $x \equiv 5 \pmod{8}$.
- Montrer que le système $x \equiv 1 \pmod{6}$, $x \equiv 2 \pmod{8}$ n'a pas de solution.
- Énoncer la condition générale : le système $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ a des solutions si et seulement si $\text{pgcd}(m, n) \mid a - b$, et elles sont alors uniques modulo $\text{ppcm}(m, n)$.
- Démontrer la condition nécessaire de c).

Exercice 10 - Puissances de 2 et de 3

On cherche les couples (x, y) d'entiers naturels tels que $2^x - 3^y = 1$.

- Trouver les solutions avec $y = 0$.
- On suppose $y \geq 1$. En raisonnant modulo 3, montrer que x est pair.
- On écrit $x = 2m$. Montrer que $(2^m - 1)(2^m + 1) = 3^y$, puis que $2^m - 1$ et $2^m + 1$ sont deux puissances de 3 qui diffèrent de 2.
- Conclure et donner toutes les solutions.

Exercice 11 - Descente infinie

On étudie l'équation $x^2 + y^2 = 3z^2$ en entiers.

- Montrer que si $3 \mid x^2 + y^2$, alors $3 \mid x$ et $3 \mid y$ (carrés modulo 3).
- Soit (x, y, z) une solution. Montrer que $x = 3x'$, $y = 3y'$, puis que $3 \mid z$ et que (x', y', z') avec $z = 3z'$ est encore solution.
- En déduire par **descente infinie** que la seule solution est $(0, 0, 0)$.
- En déduire qu'il n'existe aucun point à coordonnées **rationnelles** sur le cercle d'équation $X^2 + Y^2 = 3$.

Exercice 12 - Compter les décompositions

- De combien de façons peut-on payer 100 € avec des pièces de 2 € et des billets de 5 € ?
- Plus généralement, pour $n \in \mathbb{N}$, montrer que le nombre de couples $(a, b) \in \mathbb{N}^2$ avec $2a + 5b = n$ est le nombre de $b \in \left\{0, \dots, \left\lfloor \frac{n}{5} \right\rfloor\right\}$ de même parité que n .
- Calculer ce nombre pour $n = 101$ et $n = 3$.

d) Un distributeur ne rend que des pièces de 2 et de 5 : quels montants entiers ne peut-il pas rendre ?

Exercice 13 - Les marins et les noix de coco

Trois marins naufragés ramassent N noix de coco. La nuit, le premier se réveille, partage le tas en trois : il reste **une** noix, qu'il donne au singe ; il cache sa part et remet le reste en tas. Le deuxième, puis le troisième font exactement de même. Au matin, ils partagent le tas restant en trois : il reste encore **une** noix pour le singe.

a) Montrer que si le tas contient T noix avec $T \equiv 1 \pmod{3}$, il en reste $\frac{2}{3}(T-1)$ après le passage d'un marin.

b) On pose $M = N + 2$. Montrer qu'après un passage, le nouveau tas T vérifie $T + 2 = \frac{2}{3}(T + 2)$.

c) En déduire que le tas du matin vaut $\left(\frac{2}{3}\right)^3 M - 2$, puis montrer que 3^4 divise M .

d) Trouver le plus petit N et vérifier.

Exercice 14 - Points entiers d'un segment

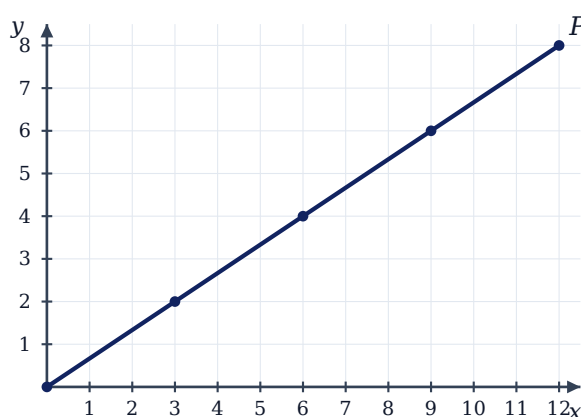
Soient $a, b \geq 1$ des entiers. On compte les points à coordonnées entières (**points du réseau**) sur le segment joignant $O(0; 0)$ à $P(a; b)$.

a) Montrer qu'un point $(x; y)$ du segment a des coordonnées entières si et seulement si $x = \frac{ka}{d}$ et $y = \frac{kb}{d}$ avec $d = \text{pgcd}(a, b)$ et $0 \leq k \leq d$.

b) En déduire que le segment contient $d + 1$ points du réseau.

c) Vérifier sur la figure pour $P(12; 8)$, puis compter pour $P(1\,769; 551)$.

d) Un carreleur trace la diagonale d'un sol de 12×8 carreaux. Combien de carreaux la diagonale traverse-t-elle ? (Admettre la formule $a + b - \text{pgcd}(a, b)$ et la vérifier sur un petit cas.)



Le segment de O à $P(12; 8)$ et ses points à coordonnées entières.

Exercice 15 - Synthèse : racines carrées de 1 modulo 105

On résout $x^2 \equiv 1 \pmod{105}$, avec $105 = 3 \times 5 \times 7$.

a) Montrer que $x^2 \equiv 1 \pmod{105}$ équivaut à $x^2 \equiv 1$ modulo 3, 5 et 7 simultanément.

- b) Résoudre $x^2 \equiv 1$ modulo chacun des trois nombres premiers.
- c) Combien y a-t-il de solutions modulo 105 ? Les déterminer à l'aide des e_i de l'exercice « Le problème de Sunzi » ($e_1 = 70$, $e_2 = 21$, $e_3 = 15$).
- d) Utiliser une solution non triviale pour factoriser 105 à l'aide d'un PGCD, et expliquer l'intérêt de ce phénomène en cryptographie.