Exemples d'équations diophantiennes

Df : Une équation diophantienne est une équation du type $P(x_1,\dots,x_n)=0$ d'inconnues $x_1,\dots,x_n$ où $P\in\mathbb{Z}[X_1,\dots,X_n]$ et dont on cherche les solutions à valeurs dans $\mathbb{Z}$.

Ex : $3x^2+y=5$ d'inconnues x et y.

I Equations diophantiennes d'ordre 1

1) Equations du type $ax+by=c$

On cherche à résoudre l'équation $ax+by=c$ où $(a,b,c)\in\mathbb{Z}^3$ fixés et d'inconnues x et y.

Prop : L'équation $ax+by=c$ admet au moins une solution si et ssi $\mathrm{pgcd}(a,b)\mid c$.

Rq : Découle du théorème de Bézout.
Il y en a en fait une infinité lorsque $\mathrm{pgcd}(a,b)\mid c$.

Supposons $\mathrm{pgcd}(a,b)\mid c$, on peut résoudre l'équation ainsi :

→ on se ramène au cas $a\wedge b=1$ en divisant des deux côtés par $\mathrm{pgcd}(a,b)$.

→ l'algorithme d'Euclide permet par divisions euclidiennes successives de trouver une relation de Bezout entre a et b et donc de trouver une solution particulière $(x_0,y_0)\in\mathbb{Z}^2$.

→ la solution particulière permet de se ramener à l'équation homogène $aX+bY=0$ d'inconnues X et Y. La résolution est possible grâce au lemme de Gauss.

Finalement, on trouve l'ensemble des solutions de l'équation $ax+by=c$ lorsque $a\wedge b=1$:
$[(x_0+kb,\ y_0-ka)$ lorsque $k\in\mathbb{Z}$

Ex : L'ensemble des solutions de $5x-2y=10$ est $\{(4-2k,\ 5+5k)\ /\ k\in\mathbb{Z}\}$

Rq : On peut interpréter géométriquement le résultat : il s'agit des points à coordonnées entières de la droite passant par (x_0,y_0) de coefficient directeur $\frac{-a}{b}$.

Rq : Si on résout $ax+by=n$ sur $\mathbb{N}^2$, il n'y a qu'un nombre fini de solutions.

2) Equations d'ordre 1 avec plus de 2 inconnues

→ On peut résoudre les systèmes d'équations diophantienne à 2 inconnues.

Prop : Une équation diophantienne d'ordre 1 $\sum a_i x_i=1$ peut se ramener à un système d'équations diophantiennes d'ordre 1 à 2 inconnues avec $\mathrm{pgcd}(a_1,\dots,a_n)=1$ (premiers dans leur ensemble)

Rq : Il suffit de traiter le cas à 3 inconnues
Soit $a_1x+a_2y+a_3z=1$ et supposons $a_1\wedge a_2=1$

Alors $a_1x+a_2y+a_3z=1 \iff \begin{cases} a_1x+a_2y=\delta \\ \delta+a_3z=1\end{cases}$

d'où une résolution pratique de $a_1x+a_2y+a_3=1$

DEV 1 — Dénombrement des solutions de $\sum_{i=1}^{k} a_i x_i = n$

Soient $a_1,\dots,a_k$ entiers relatifs premiers dans leur ensemble
Soit $S_n=|\{(x_1,\dots,x_k)\ /\ \sum_{i=1}^{k} a_i x_i=n\}|$
Alors $S_n \underset{+\infty}{\sim} \dfrac{n^{k-1}}{(k-1)!\,a_1\dots a_k}$

Rq : On pourrait trouver un réel explicite mais il n'est pratique.

Rq : Dans cette partie, des méthodes algébriques ont suffi pour résoudre les équations

II Equations diophantiennes d'ordre 2

Pour certaines équations, les méthodes arithmétiques fonctionnent encore.

Ex : L'équation $x^2 = yz$ dans $\mathbb{N}^3$ admet pour solutions $\{(uvw, v^2w, u^2w) / (u,v,w) \in \mathbb{N}^3\}$

Mais d'autres techniques vont permettre de contourner certaines difficultés.

1) L'équation $x^2+y^2=z^2$ et les triplets pythagoriciens

On cherche à résoudre l'équation $x^2+y^2=z^2$ pour $(x,y,z) \in \mathbb{N}^3$ ie les triangles rectangles de côtés entiers.

Propo : $(x,y,z) \in \mathbb{N}^3$ est solution de $x^2+y^2=z^2$ ssi il existe $d \in \mathbb{N}$, $(u,v) \in (\mathbb{N}^*)^2$ tel que $u \wedge v = 1$ et tel que $(x,y,z) = (d(u^2-v^2), 2duv, d(u^2+v^2))$ ou $(y,x,z) = (d(u^2-v^2), 2duv, d(u^2+v^2))$

Idée : On se ramène au cas $\mathrm{pgcd}(x,y,z) = 1$ (d'où $\exists d$) Ensuite, pour $z \neq 0$, les solutions de l'équation correspondent aux points rationnels du cercle unité via la paramétrisation $\frac{x}{z} = \frac{1-t^2}{1+t^2}$ et $\frac{y}{z} = \frac{2t}{1+t^2}$ pour $t \in]0,1[$

Rq : Les solutions (x,y,z) de cette équation sont appelés triplets pythagoriciens.

Rq : La paramétrisation rationnelle de $x^2+y^2=1$ peut s'adapter dans le cas d'équations de coniques ou lorsque l'équation possède un bon paramétrage rationnel (cf suite).

2) Equation de Pell-Fermat et théorème des deux carrés

Ces deux problèmes sont à rapprocher car leur résolution passe par l'étude de $\mathbb{Z}[\sqrt{d}]$ avec d bien choisi

Equation de Pell-Fermat : $x^2 - dy^2 = 1$ pour $d \in \mathbb{N}^*$

L'anneau $\mathbb{Z}[\sqrt{d}]$ apparait via la factorisation $(x-\sqrt{d}y)(x+\sqrt{d}y) = 1$ pour (x,y) solutions

En mettant au carré l'égalité, on trouve une nouvelle solution $(x^2+dy^2, 2xy)$.

Propo : On appelle solution fondamentale $(x_1, y_1) \in \mathbb{Z}^2$ de l'équation $x^2-dy^2=1$ la solution correspondant à la plus petite valeur absolue de x avec $x > 1$.

Les solutions de l'équation sont $(\pm x_n, \pm y_n)$ où $n \in \mathbb{N}$ tel que $x_n + \sqrt{d}\, y_n = (x_1 + \sqrt{d}\, y_1)^n$

Mais existe-t-il une solution autre que $(\pm 1, 0)$?

Propo : L'équation $x^2 - dy^2 = 1$ admet une solution autre que $(\pm 1, 0)$ ssi d n'est pas un carré

Rq : Pour trouver la solution fondamentale pour $d \neq c^2$, $c \in \mathbb{Z}$ il faut savoir approcher $\sqrt{d}$ ce qui peut être difficile

Ex : $x^2 - 67y^2 = 1$ admet des solutions et la solution fondamentale est $(48842, 5967)$.

Rq : $(\pm 1, 0)$ est toujours solutions

DEV 2 — Théorème des deux carrés

Soit Z l'ensemble des entiers relatifs qui s'écrivent comme la somme de deux carrés.

1/ • $p \in Z \cap \mathcal{P}$ ssi $p = 2$ ou $p \equiv 1 [4]$

2/ • $n = \prod_{p \in \mathcal{P}} p^{v_p(n)} \in Z$ ssi $v_p(n)$ pair pour $p \equiv 3 [4]$

Lemme (admis) : • $\mathbb{Z}[i]$ est euclidien pour la norme $N(x+iy)=x^2+y^2$

• $\left(\frac{-1}{p}\right)=1$ ssi $p\equiv 1\,[4]$

3) Une autre équation et la descente infinie de Fermat

Soit $a\in\mathbb{N}$ tq $a>n$, n fixé et on veut résoudre

$$x_1^2+\dots+x_n^2-a\,x_1\cdots x_n=0$$

La seule solution est $(0,\dots,0)$

L'idée est d'appliquer la descente infinie de Fermat : à partir d'une solution, on en construit une nouvelle de sorte à obtenir une suite de solutions mais qui vérifient une condition qui apporte la contradiction.

Pour l'exemple, on peut construire une suite de solutions $(x_1^k,\dots,x_n^k)_k$ tel que $(x_1^k+\dots+x_n^k)$ est une suite décroissante strictement ce qui est absurde.

III Équations diophantiennes d'ordre n, $n\geq 3$

1) Le grand théorème de Fermat

Th : Grand théorème de Fermat

L'équation $x^n+y^n=z^n$ pour $n\geq 3$, $n\in\mathbb{N}$ n'admet pas de solutions $(x,y,z)\in\mathbb{Z}^3$ non triviales

Rq : Résultat historique et aussi culte pour le coup de la marge de Fermat.
Problème résolu seulement en 1994 ! Très dur.

Le 1° cas du théorème de Fermat c-à-d l'équation $x^p+y^p+z^p=0$ pour $xyz\not\equiv 0\,(p)$ est accessible pour certains nombres premiers, appelés premiers de Sophie-Germain

Th de Sophie-Germain : Soit $p\in\mathcal{P}$ tel que $q=2p+1\in\mathcal{P}$

L'équation $x^p+y^p+z^p=0$ pour $xyz\not\equiv 0\,(p)$ n'a pas de solutions non triviales.

Rq : Utilise la réduction modulo p, autre technique de calculs. De manière générale, réduire modulo p pour p bien choisi peut permettre la résolution d'équations diophantiennes.

Ex : $x^4+y^4=11z^2$ n'a pas de solution non triviale.

Rq : Certains cas du théorème de Fermat sont accessibles comme $n=4$ via une descente infinie de Fermat pour l'équation $x^4+y^4=z^2$. développer un peu plus.

2) Autres équations

Si leurs formes sont correctes, une résolution est possible

Ex 1 : $xyz=x+y+z+2$ dans $\mathbb{N}^3$ admet 10 solutions

Ex 2 : $x^3+y^3=xyz$ admet un nombre infini de solutions

Découle de la paramétrisation rationnelle du folium de Descartes : $X=\frac{t}{t^3+1}$ et $Y=\frac{t^2}{t^3+1}$

Autres idées :

- équations diophantiennes dans $\mathbb{F}_q$ ou $\mathbb{Z}/n\mathbb{Z}$
- Th de Hasse-Minkowski et $\sum_{i=1}^{n} a_i x_i^2 = x_{n+1}$

3) Transition vers le grand théorème de Fermat

Références

[Com] COMBES

[FGN] FGN Algèbre 1

[Per] PERRIN

[War] WARUSFEL - A. - C. - G. - N.
Mathématiques cours + Exos - Arithmétique

[Hin] Marc HINDRY - Arithmétique