126

EXEMPLES D'ÉQUATIONS DIOPHANTIENNES

I. GÉNÉRALITÉS ET ÉQUATIONS DIOPHANTIENNES DU PREMIER DEGRÉ.

1. Définition. Théorème fondamental.

Déf 1 : On appelle équation diophantienne une équation à coefficients entiers dont les solutions recherchées sont entières.

Ex 2 : $3x^2+7y^2+1=0$
$2x^3+xy-7=0$ sont des équations diophantiennes
$n^x+n^y+n^z=n^t$

Thm 3 (Matiyasevich) Il n'existe aucun algorithme général décidant l'existence de solutions pour les équations diophantiennes. (ADMIS)

[HUN] 2. L'équation $ax+by=c$

Prop 4 : $d=a\wedge b$. L'équation $ax+by=c$ admet des solutions entières si et seulement si $d \mid c$ et pour (x_0,y_0) une solution de cette équation, $\{(x_0+\frac{b}{d}t,\ y_0-\frac{a}{d}t),\ t\in\mathbb{Z}\}$ constitue l'ensemble des solution de $ax+by=c$.

Remarque 5 : En pratique on utilise l'algorithme d'Euclide étendu pour déterminer une solution particulière (x_0,y_0)

Exemple 6 :
- $x+3y=5$ a pour solutions $\{(-10+3t,\ 5-t),\ t\in\mathbb{Z}\}$
- $4x+18y=6$ a pour solutions $\{(-12+9t,\ 3-2t),\ t\in\mathbb{Z}\}$
- $7x+28y=5$ n'admet pas de solutions

[HUN] 3. Equation du premier degré à n variables.

Prop 7 : L'équation $a_1x_1+\dots+a_nx_n=b$ admet des solutions entières ssi $d=\mathrm{pgcd}(a_1,\dots,a_n)\mid b$.

Exemple 8 : L'équation $13x+8y+16z=53$ admet des solutions entières.

Déf 9 (Forme normale de Hermite) On dit que la matrice $H=(h_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}}$, $m\geq n$, est sous forme normale de Hermite ssi il existe une fonction f strictement croissante de $[1,n]$ dans $[1,m]$ telle que : [COH]

$$\begin{cases} h_{f(j)j}\geq 1 & \forall j\le n\\ h_{ij}=0 & \text{pour } i>j\end{cases} \quad \text{et } 0\le h_{f(j)k}<h_{f(j)j},\ k>j$$

Prop 10 : Soit $A\in\mathcal{M}_{m,n}(\mathbb{Z})$, $B\in\mathcal{M}_{m,1}(\mathbb{Z})$. Alors $\exists U\in Gl_n(\mathbb{Z})$ et H sous forme normale de Hermite telles que $AU=(\underbrace{0}_{k\text{ colonnes}}\mid H)$. [COH]

De plus, si on écrit $U=(U_1\mid U_2)$, $U_1\in\mathcal{M}_{n,k}(\mathbb{Z})$, $U_2\in\mathcal{M}_{n,n-k}(\mathbb{Z})$ on a que le système d'équations diophantiennes $AX=B$ admet une solution ssi $\exists Z_2 \,/\, HZ_2=B$ et dans ce cas les solutions sont les $U_2Z_2+U_1Y$ avec $Y\in\mathcal{M}_{k,1}(\mathbb{Z})$.

Exemple 11 Les solutions de $13x+8y+16z=53$ sont les
$$\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}-159\\265\\0\end{pmatrix}+\begin{pmatrix}8u\\-2t-13u\\t\end{pmatrix},\ (t,u)\in\mathbb{Z}^2$$
ie
$$\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}-159+8u\\265-2t-13u\\t\end{pmatrix}$$

Application : Partitions d'un entier en parts fixées — DEV 1

II. ÉQUATIONS DIOPHANTIENNES POLYNOMIALES DE DEGRÉ SUPÉRIEUR.

[HEL] 1. Quelques méthodes de résolution.

ⓐ Méthode de la descente infinie.

Déf 12 (Principe de la méthode) : c'est une forme de démonstration par l'absurde où l'on considère un ensemble de $\mathbb{N}$ (supposé non vide) formé d'éléments vérifiant la même propriété dont on choisit le plus petit puis on en exhibe un autre plus petit encore pour obtenir la contradiction.

Exemples 13. • On appelle triplet pythagoricien $(x,y,z)\in\mathbb{N}^3$ tels que $x^2+y^2=z^2$ (ou triangle Pythagorique).
L'aire d'un triangle Pythagorique ne peut pas être un carré

• $\nexists x\equiv 2\,[3]$ tel que $x=y^2+3z^2$

• $\forall p$ premier, $p\equiv 1 \bmod 4$, $\exists x,y \,/\, p=x^2+y^2$

Prop 14 : L'équation de Fermat $x^n+y^n=z^n$ n'a pas de solution pour $n=4$.

ⓑ Réduction modulo n

Exemples 15. • L'équation $x^2+y^2=3z^2$ n'admet aucune solution (réduire modulo 3)

• L'équation $x^3+5=117y^3$ n'admet aucune solution (réduire modulo 9)

• L'équation $x^2-5y^2=2$ n'admet aucune solution (réduire modulo 5)

[COM] ⓒ Méthode géométrique

On considère ici des équations du type $p(X,Y,Z)=0$ où $p\in\mathbb{Z}[X,Y,Z]$ est un polynôme homogène tel que la courbe d'équation $p(x,y,1)=0$ possède un paramétrage rationnel. Ce paramétrage permet de résoudre l'équation $p(x,y,z)=0$ correspondante.

Exemples 16 : • La paramétrisation du cercle $x^2+y^2=1$ par $\left(\frac{1-t^2}{1+t^2},\frac{2t}{1+t^2}\right)$, permet d'obtenir l'ensemble des triplets pythagoriciens $(x,y,z)\,/\,x^2+y^2=z^2$: ce sont les (x,y,z) ou $(y,x,z)=(d(u^2-v^2),2duv,d(u^2+v^2))$ où $d\in\mathbb{N}$, $u\wedge v=1$.

• De même, les ellipses $\left(\frac{x}{a}\right)^2+\left(\frac{y}{b}\right)^2=1$ ont pour paramétrage $\left(a\frac{1-u^2}{1+u^2},2b\frac{u}{1+u^2}\right)$ et les hyperboles $\left(\frac{x}{a}\right)^2-\left(\frac{y}{b}\right)^2=1$ ont pour paramétrage $\left(a\frac{1+u^2}{1-u^2},2b\frac{u}{1-u^2}\right)$

2. Utilisation des corps quadratiques. [DUV]

Dans ce paragraphe on considère $d\in\mathbb{Z}$ sans facteur carré, $\mathbb{K}:=\mathbb{Q}(\sqrt{d})$ un corps quadratique et $\mathbb{A}_\mathbb{K}$ l'anneau des entiers de ce corps.

Déf 17 : La norme de $x=\alpha+\beta\sqrt{d}\in\mathbb{Q}(\sqrt{d})$ est définie par $N(x)=\alpha^2-d\beta^2=x\bar{x}$ où $\bar{x}=\alpha-\beta\sqrt{d}$ est le conjugué de x.

Thm 18 : $\mathbb{A}_\mathbb{K}=\mathbb{Z}(\sqrt{d})$ si $d\equiv 2$ ou $3 \bmod 4$
$\mathbb{A}_\mathbb{K}=\mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$ si $d\equiv 1 \bmod 4$

Déf 19 : $\mathbb{A}_\mathbb{K}^*:=\{x\in\mathbb{A}_\mathbb{K} \,/\, N(x)=1\}$ est l'ensemble des unités de $\mathbb{A}_\mathbb{K}$. C'est un groupe pour la multiplication.

Lemme 20 : Soit $d>0$. Alors $\exists\,\varepsilon\in\mathbb{A}_K^*$, $\varepsilon>1$ et $\forall\varepsilon\in\mathbb{A}_K^*$, $\varepsilon>1$ on a $\varepsilon\geqslant(1+\sqrt{d})/2$.

Thm 21 : Soit $d>0$. $\exists\,\omega>1\in\mathbb{A}_\mathbb{K}^*$ appelé unité fondamentale telle que $\mathbb{A}_\mathbb{K}^*=\{\pm\omega^n, n\in\mathbb{Z}\}$

Thm 22 Soient x_1, y_1 tels que $x_1+\sqrt{d}y_1$ unité fondamentale de A_K^*. Alors les solutions de l'équation de Pell $x^2-dy^2=1$, rangées par ordre croissant, vérifient :

- $x_n+y_n\sqrt{d}=(x_1+y_1\sqrt{d})^n$, $\forall n\in\mathbb{N}$
- $x_{n+2}=2x_1x_{n+1}-x_n$ et $y_{n+2}=2x_1y_{n+1}-y_n$, $\forall n\in\mathbb{N}$

Exemple 23 : L'équation de Pell $x^2-19y^2=1$ admet pour solution fondamentale $(x_1=170, y_1=39)$ et la relation de récurrence fournit : $(x_2=57799, y_2=13260)$...

Rmq 24 : La solution fondamentale s'obtient à l'aide de fractions continues.

Rmq 25 : L'équation de Pell $x^2+dy^2=1$, $d>0$ n'admet pas d'autres solutions que les solutions triviales $(1,0)$ et $(-1,0)$ pour $d>1$ et $(1,0),(-1,0),(0,1),(0,-1)$ pour $d=1$.

Thm 26 : L'anneau A_K est euclidien pour les valeurs de d suivantes : $-11,-7,-3,-2,-1,2,3,5$ et 13.

DEV 2

Application 27 : Etude de l'équation de Pell $x^2+2y^2=n$, $n\in\mathbb{N}$

App 28 : L'équation de Mordell $y^2=x^3-1$ admet pour unique solution $(1,0)$.

App 29 : L'équation de Fermat $x^3+y^3=z^3$ n'a pas de solution telle que $xyz\neq 0$.

Rmq : Grand thm de Fermat : $x^n+y^n=z^n$ sans solutions pour $n\geq 3$.

[STE]

3. Utilisation des réseaux

Thm 30 (Minkowski) Soit L un réseau de dimension n de $\mathbb{R}^n$ de domaine fondamental T et soit X un convexe symétrique borné. Si $vol(X)>2^n vol(T)$, alors X contient un point de L non nul.

App 31 : Théorème des deux carrés : l'équation $x^2+y^2=p$ avec p premier admet des solutions ssi $p\equiv 1 \mod 4$

App 32 : Théorème des quatres carrés : l'équation $x^2+y^2+z^2+t^2=n$ admet des solutions pour tout $n\in\mathbb{N}$.

III - AUTRES TYPES D'ÉQUATIONS DIOPHANTIENNES.

1. Equations modulaires

Exemple 33 : L'équation $ax\equiv b \mod n$ a des solutions ssi $pgcd(a,n)\mid b$ et dans ce cas les solutions sont de la forme $\frac{1}{pgcd(a,n)}(bx_0+kn)$, $k\in\mathbb{Z}$ avec x_0 une solution de $\frac{a}{pgcd(a,n)}x\equiv 1 \mod \left(\frac{n}{pgcd(a,n)}\right)$

Exemple 34 pour $n\wedge m=1$, le lemme chinois permet d'obtenir que $\begin{cases} x\equiv a \mod n \\ x\equiv b \mod m\end{cases}$ possède une infinité de solutions dans $\mathbb{Z}$

Exemple 35 : $x^2\equiv x \mod p$, p premier possède une infinité de solutions dans $\mathbb{Z}$.

2. Equations non polynomiales [STE]

Exemple 36 L'équation $n^x+n^y+n^z=n^t$ a pour solutions : pour $x\leq y\leq z$,
- $n=2$; $y=x$; $z=x+1$; $t=x+2$
- $n=3$; $y=x$; $z=x$; $t=x+1$

Bibliographie :

DUVERNEY Daniel, Théorie des nombres : cours et exercices corrigés, DUNOD, 1998 [DUV]

COHEN Henri, Number Theory, Vol 1 : tools and diophantine equations, Springer, 2007 [COH]

HELLEGOUARCH Yves, Invitation aux mathématiques de Fermat-Wiles, Masson, 1997 [HEL]

COMBES François, Algèbre et géométrie, Bréal, 1998 [COM]

STEWART Ian, Algebraic number theory and Fermat's last theorem, A.K. Peters, 2002 [STE]

SIERPINSKI Waclaw, 250 problems in elementary number theory, Elsevier, 1970 [SIE]

HUNTER John, Number theory, Oliver & Boyd, 1964 [HUN]