126

Exemples d'équations en arithmétique

I) Équations diophantiennes de degré 1

Définition 1 : Une équation diophantienne est une équation polynomiale à coefficients dans $\mathbb{Z}$ dont on cherche des solutions dans $\mathbb{Z}$

1) Équations du type $ax+by=c$ (E_1) $a,b,c\in\mathbb{Z}$

Théorème 2 (de Bézout) : Soit $d=\text{pgcd}(a,b)$, avec $a,b\in\mathbb{Z}$ alors $a\mathbb{Z}+b\mathbb{Z}=d\mathbb{Z}$

Proposition 3 (Lemme de Gauss) : Si $a\wedge b=1$, alors
$$a|bc \Rightarrow a|c$$

Théorème 4 : Soit $d=\text{pgcd}(a,b)$. Alors (E_1) admet des solutions ssi $d|c$. De plus si (x_0,y_0) est une solution particulière alors l'ensemble des solutions est
$$\left\{\left(x_0+k\frac{b}{d},\, y_0-k\frac{a}{d}\right),\ k\in\mathbb{Z}\right\}$$

Théorème 5 : Algorithme d'Euclide étendu (voir annexe)
On trouve $u_N, v_N\in\mathbb{Z}$ tq
$$au_N+bv_N=d$$
Ainsi $\left(\frac{c}{d}u_N,\ \frac{c}{d}v_N\right)$ est une solution particulière

Exemple 6 : $7x+11y=20$ a pour ensemble de solutions
$$\{(-60+11k,\,40-7k),\ k\in\mathbb{Z}\}$$

2) Système d'équations

On considère le système suivant
$$\begin{cases} a_{11}x_1+\dots+a_{1m}x_m=b_1 \\ \vdots \\ a_{n1}x_1+\dots+a_{nm}x_m=b_n \end{cases} \quad (E_2)$$
qu'on peut réécrire $AX=B$ avec $A=[a_{ij}]_{\substack{1\le i\le n\\1\le j\le m}}$ et $B=(b_i)_{1\le i\le n}$ d'inconnue $X=(x_j)_{1\le j\le m}$

Théorème 7 (des diviseurs élémentaires) :
Soit $A\in\mathcal{M}_{n,m}(\mathbb{Z})$. Il existe $(U,V)\in Gl_n(\mathbb{Z})\times Gl_m(\mathbb{Z})$, $r\geq 0$, $d_1,\dots,d_r\in\mathbb{Z}$ tels que $UAV=D$ avec $D=\begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & 0 \end{pmatrix}$ et $d_1|\dots|d_r$.

De plus, r est unique, et les d_i sont uniques à association près

Corollaire 8 : Le système (E_2) est équivalent à
$$\begin{cases} DX'=B'=UB \\ X=VX' \end{cases} \leftarrow \text{système diagonal}$$

Exemple 9 : $A=\begin{pmatrix}2&3\\4&5\end{pmatrix}$ donne $U=\begin{pmatrix}1&0\\-1&1\end{pmatrix}$, $V=\begin{pmatrix}-1&3\\1&-2\end{pmatrix}$ $D=\begin{pmatrix}1&0\\0&2\end{pmatrix}$
et le système $\begin{cases}2x+3y=8\\4x+5y=10\end{cases}$ se réécrit $\begin{cases}\begin{pmatrix}1&0\\0&2\end{pmatrix}X'=\begin{pmatrix}8\\2\end{pmatrix}\\ X=VX'\end{cases}$

et on trouve $x=-5$, $y=-6$

II) Équation diophantiennes de degré >1 : Quelques méthodes

1) Une méthode géométrique

L'équation $a^2+b^2=c^2$ (avec $a,b,c\in\mathbb{Z}$) est l'équation de Fermat pour $n=2$ (F_2). Trouver une solution revient à trouver un point à coordonnées rationnelles sur le cercle unité

Proposition 10 : On peut paramétrer le cercle unité dans $\mathbb{Q}^2$ par
$$\{(x,y)\in\mathbb{Q}^2,\ x^2+y^2=1\}=\left\{\left(\frac{1-t^2}{1+t^2},\frac{2t}{1+t^2}\right),\ t\in\mathbb{Q}\right\}\cup\{(-1,0)\}$$

Corollaire 11 : Les triplets solution de F_2, dits triplets pythagoriciens, sont de la forme $(d(u^2-v^2),\ 2duv,\ d(u^2+v^2))$ avec $u,v\in\mathbb{N}$, $d\in\mathbb{Z}$, $u\wedge v=1$, à permutation entre x et y près

Exemples 12 : $u=2$, $v=1$, $d=1$ donne $(3,4,5)$
$u=3$, $v=2$, $d=1$ donne $(5,12,13)$

II/ Équations diophantiennes de degré 2 ou plus - suite

(E_3) $x^3+y^3 = xyz$

On se ramène au cas $\operatorname{pgcd}(x,y,z) = 1$, $xyz \neq 0$, $z > 0$

Proposition 13 : Le folium de Descarte ($X^3+Y^3 = XY$) intersecté avec $\mathbb{Q}$ est paramétrisable : il s'agit de l'ensemble

$$\left\{ \left(\frac{t}{t^3+1} \right), \left(\frac{t^2}{t^3+1} \right), t \in \mathbb{Q} \right\}$$

Corollaire 14 : L'équation E_3 a pour solution les triplets

$$(duv^2, du^2v, d(u^3+v^3)) \text{ où } d \in \mathbb{N}, (u,v) = 1, u,v \in \mathbb{Z}, \text{ et}$$

ceux de la forme $(x, -x, 0)$, $x \in \mathbb{Z}$.

2) Méthode de descente infini

Principe On considère une solution qui minimise une fonction ω avec la valeur ω_0 et on construit une solution dont l'image ω_1 par ω vérifie $\omega_1 < \omega_0$. Par l'absurde l'équation n'a pas de solution

Applications 15

- $x^4+y^4 = z^2$ n'a pas de solutions dans $\mathbb{Z}$
- $x^2+y^2 = pz^2$ n'a pas de solutions si $p \equiv 3 [4]$
- $x^4+y^4 = z^4$ n'a pas de solutions !

3) Réduction modulaire

Principe : si $P(a_1 \ldots a_m) = 0$ dans $\mathbb{Z}$ alors le réduit modulo m vérifie $\overline{P}(\overline{a_1}, \ldots, \overline{a_m}) = \overline{0}$ dans $\mathbb{Z}/m\mathbb{Z}$ pour tout $m \geq 2$

Applications 16 :

$x^2+3y = 5z$ n'admet aucune solution (prendre $m = 3$)

$x^2+y^2 = 4z+7$ n'admet aucune solution ($m = 4$)

4) L'équation de Pell Fermat $x^2 - dy^2 = \pm 1$ (PF)

On considère que d n'a pas de facteurs carrés. Trouver (x,y) solution de (PF) revient à trouver les inversibles de $\mathbb{Z}[\sqrt{d}]$

Théorème 17 Il existe un nombre $\varepsilon_1 = a + b\sqrt{d}$ ($a, b \in \mathbb{N}$) unique tel que les inversibles de $\mathbb{Z}[\sqrt{d}]$ soient les éléments de l'ensemble $\{ \pm \varepsilon_1^n, n \in \mathbb{Z} \}$. On appelle ε_1 l'unité fondamentale

Exemples 18

$d = 2 \quad \varepsilon_1 = 1+\sqrt{2}$

$d = 5 \quad \varepsilon_1 = 2+\sqrt{5}$

5) Somme de deux carrés

Théorème 19 L'équation $n = a^2+b^2$ admet une solution ssi pour tout $p \equiv 3 [4]$, $v_p(n)$ est pair.

On étudie pour prouver ce théorème l'anneau des entiers de Gauss $\mathbb{Z}[i]$

Proposition 20 $\mathbb{Z}[i]$ a pour inversible ± 1, $\pm i$

Proposition 21 $\mathbb{Z}[i]$ est euclidien donc factoriel

Proposition 22 La norme sur $\mathbb{Z}[i]$ définit par $N(a+ib) = a^2+b^2$ est multiplicative

6) Somme de quatre carrés

Théorème 23 Pour tout $n \in \mathbb{N}$, l'équation $n = a^2+b^2+c^2+d^2$ admet au moins une solution

On pose $A = \mathbb{Z}[1, I, J, K] + \mathbb{Z}\left[\frac{1+I+J+K}{2}\right]$ où $(1, I, J, K)$ est la base canonique de l'anneau des quaternions

Proposition 24 : les inversibles de A sont $\pm 1, \pm I, \pm J, \pm K$

Proposition 25 : A est euclidien donc factoriel

Proposition 26 : la norme $N(a+bI+cJ+dK) = a^2+b^2+c^2+d^2$ est multiplicative

7) L'équation de Fermat pour $n = 3$

Théorème 27 : L'équation $x^3+y^3 = z^3$ n'admet pas de solution non triviale dans $\mathbb{Z}^3$

III) Équations dans d'autres anneaux

1) Systèmes de congruences

Théorème 28 (des restes chinois) : Si $a,b \in \mathbb{Z}$ tq $a \wedge b = 1$, alors

$$\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \simeq \mathbb{Z}/ab\mathbb{Z}$$

Corollaire 29 : Si $m_1, \dots, m_n \in \mathbb{Z}$ premiers deux à deux et $c_1, \dots, c_n \in \mathbb{Z}$, le système de congruences

$$\begin{cases} x \equiv c_1 \mod m_1 \\ \vdots \\ x \equiv c_n \mod m_n \end{cases}$$

admet une unique solution mod m, où $m = m_1 \cdots m_n$

Exemple 30 : le système

$$\begin{cases} x \equiv 1 \mod 2, \quad x \equiv 2 \mod 3, \quad x \equiv 3 \mod 4 \\ x \equiv 4 \mod 1, \quad x \equiv 5 \mod 6 \\ x \equiv 6 \mod 5, \quad x \equiv 0 \mod 7 \end{cases}$$

est équivalent à

$x \equiv -1 \mod 12$, $x \equiv 1 \mod 5$, $x \equiv 0 \mod 7$

de solution $x \equiv 371 \mod 420$

2) $X^m - 1$ dans $\mathbb{F}_q$ et $\mathbb{Z}/n\mathbb{Z}$, n impair

Prop 31 : Si p premier $\neq 2$, $\alpha \geq 1$, et si q est une puissance d'un nombre premier, alors $\mathbb{F}_q^*$ est cyclique d'ordre $q-1$
$(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est cyclique d'ordre $p^\alpha - p^{\alpha-1}$

Théorème 32 : - $\mathrm{Card}\,\{x \in \mathbb{F}_q^* \,/\, x^m = 1\} = m \wedge (q-1)$
- $\mathrm{Card}\,\{x \in (\mathbb{Z}/p^\alpha\mathbb{Z})^* \,/\, x^m = 1\} = m \wedge (p^\alpha - p^{\alpha-1})$

Si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ impair, alors
- $\mathrm{Card}\,\{x \in (\mathbb{Z}/n\mathbb{Z})^* \,/\, x^m = 1\} = \prod_{i=1}^{r} m \wedge (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$

3) Résidus quadratiques

Définition 33 : on dit que a un entier est un résidu quadratique modulo p s'il existe $b \in \mathbb{N}$, $b^2 \equiv a\,[p]$ et $a \not\equiv 0\,[p]$

Théorème 34 : Soit p premier et $a \in \mathbb{N}$. On appelle symbole de Legendre de a le nombre $\left(\frac{a}{p}\right) := a^{\frac{p-1}{2}} \mod p$. Alors a est un ~~carré~~ résidu quadratique ssi $\left(\frac{a}{p}\right) = 1$

Théorème 35 : i) Pour tout $a,b \in \mathbb{Z}$ on a $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

ii) -1 est un résidu quadratique modulo p ssi $p \equiv 1\,[4]$ et 2 est un résidu quadratique modulo p ssi $p \equiv \pm 1\,[8]$

iii) Loi de réciprocité quadratique : $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$ pour tous p,q premiers impairs distincts.

Applications 36 :
- L'équation $p = x^2 - 6y^2$ avec $p \equiv 7, 11, 13, 17\,[24]$ n'admet pas de solution
- L'équation $x^2 + 8x + 16 \equiv -1\,[17]$ admet des solutions
- L'équation $x^2 - py^2 = q$ avec q premier n'a pas de solutions si $\left(\frac{p}{q}\right) = -1$.

4) Théorème de Chevalley - Warning

Théorème 37 (de Chevalley - Warning)
Soit $K = \mathbb{F}_q$, soient $P_1, \dots, P_k \in K[X_1, \dots, X_n]$ tels que $\sum_{i=1}^{k} \deg(P_i) < n$, et soit Z l'ensemble de leurs zéros communs.

Alors $\# Z \equiv 0 \mod p$

Corollaire 38 :
Si les P_i sont de plus sans coefficient constant, alors ils ont un zéro commun non trivial

Annexe :

Algorithme d'Euclide étendu . $(a \geq 0, b \geq 0)$

r	u	v
$r_0 = a$	$u_0 = 1$	$v_0 = 0$
$r_1 = b$	$u_1 = 0$	$v_1 = 1$
$r_2 = a - \lfloor \frac{a}{b} \rfloor \times b$	$u_2 = 1 - \lfloor \frac{a}{b} \rfloor \times 0 = 1$	$v_2 = -\lfloor \frac{a}{b} \rfloor$
$\vdots$ $r_{i+1} = r_{i-1} - \lfloor \frac{r_{i-1}}{r_i} \rfloor r_i$	$\vdots$ $u_{i+1} = u_{i-1} - \lfloor \frac{r_{i-1}}{r_i} \rfloor u_i$	$\vdots$ $v_{i-1} = v_{i-1} - \lfloor \frac{r_{i-1}}{r_i} \rfloor v_i$

À chaque étape, $r_i = au_i + bv_i$.

Lorsque $r_{N+1} = 0$ on retourne r_N, u_N, v_N