I/ Équations diophantiennes de degré 1

1) Équation à une ou deux variables

Prop 1 : L'équation $ax=b$, pour $(a,b)\neq(0,0)$ possède une unique solution entière ssi $a|b$. La solution est alors $\frac{b}{a}$.

Théorème 2 (Bézout) : Soient $a,b\in\mathbb{Z}$ et $d=\text{pgcd}(a,b)$. Alors il existe $(u,v)\in\mathbb{Z}^2$ tel que $au+bv=d$.
Réciproquement, si $au'+bv'=c$, alors $d|c$.

Corollaire 3 : L'équation $ax+by=c$ admet des solutions ssi $d=\text{pgcd}(a,b)\,|\,c$. Dans ce cas, pour (u_0,v_0) une solution particulière, les solutions sont de la forme $\left(u_0+k\frac{b}{d}, v_0-k\frac{a}{d}\right)$, pour $k\in\mathbb{Z}$.

Remarque 4 : On peut trouver une solution particulière par l'algorithme d'Euclide.

Exemple 5 : $42x+66y=10$ n'admet aucune solution.

Exemple 6 : $112x+70y=14$ admet des solutions, par exemple $(2,-3)$.
Les solutions sont donc les $(2+5k,-3-8k)$, pour $k\in\mathbb{Z}$.

2) Système d'équations de degré 1

On considère le système : (E) $\begin{cases} a_{11}x_1+\dots+a_{1m}x_m=b_1 \\ \vdots \qquad\qquad \vdots \qquad\quad \vdots \\ a_{n1}x_1+\dots+a_{nm}x_m=b_n \end{cases}$

que l'on peut réécrire $AX=B$; avec $A\in\mathcal{M}_{n,m}(\mathbb{Z})$, $X\in\mathbb{Z}^m$, $B\in\mathbb{Z}^n$

Théorème 7 (Forme normale de Schmidt) : Soit $A\in\mathcal{M}_{n,m}(\mathbb{Z})$.
Il existe $(U,V)\in GL_n(\mathbb{Z})\times GL_m(\mathbb{Z})$; $r\geq 0$ et $d_1,\dots,d_r\in\mathbb{Z}$ tels que : $UAV=D:=\begin{pmatrix} d_1 & & & (0) \\ & \ddots & & \\ & & d_r & \\ (0) & & & \ddots \ 0 \end{pmatrix}$; $d_1|\dots|d_r$.

Prop 8 : Le système (E) est équivalent à : $\begin{cases} DX'=B':=UB \\ X=VX' \end{cases}$

Exemple 9 : On veut résoudre $\begin{cases} 2x+3y=8 \\ 4x+5y=14 \end{cases}$
qui se réécrit $\underbrace{\begin{pmatrix}2&3\\4&5\end{pmatrix}}_{A}\underbrace{\begin{pmatrix}x\\y\end{pmatrix}}_{X}=\underbrace{\begin{pmatrix}8\\14\end{pmatrix}}_{B}$. On trouve $U=\begin{pmatrix}-5&3\\2&-1\end{pmatrix}$, $V=\begin{pmatrix}0&1\\1&0\end{pmatrix}$.
On a $D=\begin{pmatrix}1&0\\0&2\end{pmatrix}$, $B'=\begin{pmatrix}2\\2\end{pmatrix}$ donc le système équivaut à : $\begin{cases} DX'=B' \\ X=VX' \end{cases}$
d'où $X'=\begin{pmatrix}2\\1\end{pmatrix}$ et $X=\begin{pmatrix}1\\2\end{pmatrix}$.
Donc le système a une unique solution $(x,y)=(1,2)$.

Exemple 10 : On veut résoudre $\underbrace{\begin{pmatrix}2&4\\3&8\end{pmatrix}}_{A}\underbrace{\begin{pmatrix}x\\y\end{pmatrix}}_{X}=\underbrace{\begin{pmatrix}-2\\1\end{pmatrix}}_{B}$.
Il a une unique solution $(x,y)=(-5,2)$

3) Équations modulaires

Théorème 11 (chinois) : Soient $m,n\in\mathbb{N}$ tels que $\text{pgcd}(m,n)=1$.
Alors l'application $\mathbb{Z}/mn\mathbb{Z}\xrightarrow{\sim}\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$
$[x]^{mn}\longmapsto([x]^n,[x]^m)$
est un isomorphisme de groupes, où $[x]^p$ est la classe de $x\in\mathbb{Z}$ modulo p dans $\mathbb{Z}/p\mathbb{Z}$.

Corollaire 12 (système de congruences) : Soient $m_1, \dots, m_n \in \mathbb{N}^*$ des entiers deux à deux premiers entre eux. Soient $a_1, \dots, a_n \in \mathbb{N}$.
Alors le système de congruences : $\begin{cases} x \equiv a_1 [m_1] \\ \vdots \\ x \equiv a_n [m_n] \end{cases}$ d'inconnue $x \in \mathbb{Z}$

admet pour solutions l'ensemble $\{x_0 + m_1 \dots m_n r, r \in \mathbb{Z}\}$, où x_0 est une solution particulière.

Exemple 13 : Le système $\begin{cases} x \equiv 2 [4] \\ x \equiv 3 [5] \\ x \equiv 1 [9] \end{cases}$; avec 4, 5, 9 premiers entre eux deux à deux, admet comme solutions l'ensemble $\{118 + 180k, k \in \mathbb{Z}\}$.

II / Méthodes de résolution d'équations diophantiennes de degré supérieur à 2

1) Réduction modulaire

Prop 14 : Soit $P \in \mathbb{Z}[X_1, \dots, X_n]$. Soit l'équation $P(x_1, \dots, x_n) = 0$, d'inconnue $(x_1, \dots, x_n) \in \mathbb{Z}^n$. Alors pour tout $m \in \mathbb{N} \setminus \{0, 1\}$, on a l'équation réduite : $\overline{P}(\overline{x_1}, \dots, \overline{x_n}) \equiv 0 [m]$, d'inconnue $(\overline{x_1}, \dots, \overline{x_n}) \in (\mathbb{Z}/m\mathbb{Z})^n$.

Prop 15 : Si il existe $m \in \mathbb{N} \setminus \{0, 1\}$ tel que l'équation réduite : $\overline{P}(\overline{x_1}, \dots, \overline{x_n}) \equiv 0 [m]$ n'a pas de solutions dans $\mathbb{Z}/m\mathbb{Z}$, alors l'équation : $P(x_1, \dots, x_n) = 0$ n'a pas de solutions dans $\mathbb{Z}$.

Exemple 16 : $x^2 + 1 = p$ n'a pas de solutions si $p \equiv 3 [4]$.

Exemple 17 : $x^2 + y^2 = 4z + 7$ n'a pas de solutions.

Théorème 18 (Sophie Germain) : Soit p un nombre premier impair tel que $q = 2p + 1$ est premier. Alors il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $x^p + y^p = z^p$ et $xyz \not\equiv 0 [p]$.

DEV 1

Déf 19 : On dit que un entier a est un résidu quadratique modulo p s'il existe $b \in \mathbb{N}$ tel que $b^2 \equiv a [p]$ et $a \not\equiv 0 [p]$.

Théorème 20 : Soit p premier et $a \in \mathbb{N}$. On appelle symbole de Legendre de a le nombre $\left(\frac{a}{p}\right) := a^{\frac{p-1}{2}} [p]$.
Alors a est un résidu quadratique ssi $\left(\frac{a}{p}\right) = 1$.

Théorème 21 : Soit p un nombre premier impair.

i) $\forall a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

ii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

iii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{4}}$

iv) Soit q un nombre premier impair, $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}$

Exemple 22 : $x^2 + 8x + 16 \equiv -1 [17]$ admet des solutions car $\left(\frac{-1}{17}\right) = 1$.

Exemple 23 : $x^2 - py = q$ avec q premier n'a pas de solution si $\left(\frac{p}{q}\right) = -1$.

Exemple 24 : $ax^2 + bx + c = 0$, avec a, b, c non-divisibles par p admet des solutions dans $\mathbb{F}_p$ ssi $\left(\frac{b^2 - 4ac}{p}\right) = 1$.

2) Méthode de descente de Fermat

Principe 25 : On veut montrer qu'une propriété (P) n'est pas vérifiée sur les entiers strictement positifs. Par l'absurde, on suppose qu'un entier $a_0 > 0$ vérifie (P). On construit un entier $a_1 < a_0$ strictement positif vérifiant aussi (P). Par récurrence, on construit une suite $(a_n)_{n \in \mathbb{N}}$ infinie strictement décroissante d'entiers strictement positifs vérifiant (P). Cette suite ne pouvant exister. On en déduit que (P) n'est pas vérifiée pour les entiers strictement positifs.

Exemple 26 : $x^2+y^2=pz^2$, p premier et $p\equiv 3[4]$ n'a pas de solutions non-triviales.

3) Paramétrisation rationnelle de courbes :

Prop 27 : Une paramétrisation rationnelle du cercle C d'équation $x^2+y^2=1$ est $C=\left\{\left(\frac{1-t^2}{1+t^2},\frac{2t}{1+t^2}\right), t\in\mathbb{R}\right\}\cup\{(-1,0)\}$.

Théorème 28 : Les solutions de $x^2+y^2=z^2$ telles que $pgcd(x,y,z)=1$ sont les triplets (pythagoriciens) $\{(u^2-v^2, 2uv, u^2+v^2); u,v\in\mathbb{Z}, pgcd(u,v)=1\}$.

L'ensemble des solutions est donc $\{(d(u^2-v^2), 2duv, d(u^2+v^2)); u,v,d\in\mathbb{Z}, pgcd(u,v)=1\}$

Exemple 29 : $u=2, v=1, d=1$ donne $(3,4,5)$ comme solution.
$u=3, v=2, d=1$ donne $(5,12,13)$ comme solution.

Prop 30 : On définit le folium de Descartes F comme la courbe d'équation : $x^3+y^3=xy$. On a une paramétrisation rationnelle :
$F=\left\{\left(\frac{t}{1+t^3},\frac{t^2}{1+t^3}\right), t\in\mathbb{R}\right\}$

Théorème 31 : Les triplets (uv^2, u^2v, u^3+v^3), où $pgcd(u,v)=1$ sont exactement les solutions de $x^3+y^3=xyz$, avec $pgcd(x,y,z)=1$.

L'ensemble des solutions est donc $\{(duv^2, du^2v, d(u^3+v^3)); u,v,d\in\mathbb{Z}, pgcd(u,v)=1\}$

Exemple 32 : $u=1, v=1, d=1$ donne $(1,1,2)$ comme solution.
$u=2, v=1, d=1$ donne $(2,4,9)$ comme solution.

III / Utilisation de corps quadratique

1) Entiers d'un corps quadratique

Déf 33 : Soit $d\in\mathbb{Z}\setminus\{0,1\}$ sans facteur carré.
$$\mathbb{Q}(\sqrt{d})=\{\alpha+\beta\sqrt{d}\ ;\ \alpha,\beta\in\mathbb{Q}\}\subset\mathbb{C}$$

Déf 34 : Un élément de $\mathbb{Q}(\sqrt{d})$ est appelé un entier algébrique ssi son polynôme minimal sur $\mathbb{Q}$ est à coefficients dans $\mathbb{Z}$. On appelle $\mathcal{O}_d$ l'ensemble des entiers algébriques sur $\mathbb{Q}(\sqrt{d})$.

Théorème 35 : $\mathcal{O}_d=\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ si $d\equiv 1[4]$ et $\mathcal{O}_d=\mathbb{Z}[\sqrt{d}]$ sinon.

2) Entiers de Gauss

Prop 36 : $\mathbb{Z}[i]$ est un anneau euclidien pour le stathme sa norme.
Ses inversibles sont $\mathbb{Z}[i]^\times=\{1,-1,i,-i\}$

Prop 37 : Les irréductibles de $\mathbb{Z}[i]$ sont : les p premiers tels que $p\equiv 3[4]$ et les $a+ib$ tels que a^2+b^2 est premier.

Théorème 38 (des deux carrés) : Soit p un nombre premier.
$x^2+y^2=p$ a des solutions ssi $p=2$ ou $p\equiv 1[4]$. DEV 2

3) Utilisation de la factorialité :

Théorème 39 : On appelle équation de Pell-Fermat une équation de la forme $x^2-dy^2=1$, pour d sans facteur carré.
- Si $d<0$, les solutions possibles sont $(\pm1,0),(0,\pm1)$
- Si $d>0$, il y a une infinité de solutions.

Exemple 40 : $x^2-3y^2=1$ a pour solutions $(1,0),(2,1),(7,4),(26,15),\ldots$

Théorème 41 : On appelle équation de Mordell une équation de la forme $y^2=x^3+k$, $k\in\mathbb{Z}$.
Si $k<1$ est tel que $k\equiv 2,3[4]$ et est sans facteur carré.
Si le nombre de classes d'idéaux de $\mathbb{Q}(\sqrt{k})$ n'est pas divisible par 3.
L'équation de Mordell admet des solutions entières ssi $k=\pm1-3a^2$, $a\in\mathbb{N}^*$.

Exemple 42 : $y^2=x^3-2$ admet $(3,5),(3,-5)$ comme solutions entières.

Références :
- Combes, Algèbre et géométrie
- Duverney, Théorie des nombres
- Beck, Malick, Peyré, Objectif agrégation
- Perrin, Cours d'algèbre
- Francinou, Gianella, Nicolas, Oraux X-ENS algèbre 1