I- Equations diophantiennes et de degré 1

Déf 1: Une équation diophantienne est une équation polynomiale à coefficients dans $\mathbb{Z}$ dont on cherche des solutions dans $\mathbb{Z}$ (on peut aussi un système d'équations polynomiales)

1- Equations du type $ax+by=c$ $[E_1]$, $a,b,c \in \mathbb{Z}$

Th 2 (Théorème de Bézout)
Soient $a,b \in \mathbb{Z}$. Soit $d = a \wedge b$. Alors $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$

Ex 2: $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$

Prop 3: (Lemme de Gauss) Si $d \mid bc$ et si $a \wedge b = 1$, alors $a \mid c$.

Th 4: Soit $d = a \wedge b$. Alors $[E_1]$ admet des solutions ssi $d \mid c$. De plus, si (x_0, y_0) est une solution particulière, alors l'ensemble des solutions est donné par:

$$\{(x_0 + kb', y_0 - ka') \mid k \in \mathbb{Z}\}, \quad a' = \frac{a}{d}, \quad b' = \frac{b}{d}$$

Th 5: (Algorithme d'Euclide étendu)
Soient $a,b \in \mathbb{Z}$. Posons $w_0 = \begin{bmatrix} a \\ 1 \\ 0 \end{bmatrix}$, $w_1 = \begin{bmatrix} b \\ 0 \\ 1 \end{bmatrix}$, ainsi que $w_i = \begin{bmatrix} r_i \\ u_i \\ v_i \end{bmatrix}$, $i \in \mathbb{N}$, où (r_i) est telle que:

$r_0 \in \mathbb{N}$, $r_i = q_{i+2} r_{i+1} + r_{i+2}$ (division euclidienne)
On pose $u_{i+2} = u_i - q_{i+2} u_{i+1}$; $v_{i+2} = v_i - q_{i+2} v_{i+1}$
Alors, $\exists n_0 \in \mathbb{N}$, $\forall n \geq n_0 + 1$, $r_n = 0$ et $r_{n_0} \neq 0$
On a donc $a u_{n_0} + b v_{n_0} = r_{n_0} = a \wedge b$.

Ex 6: L'équation $11x + 16y = 23$ a pour solutions l'ensemble:

$$\{(21k+1, -31k+1) \mid k \in \mathbb{Z}\}$$

2- Système d'équations

On considère le système suivant:

$$\begin{cases} a_{1,1} x_1 + \dots + a_{1,n} x_n = b_1 \\ \vdots \\ a_{m,1} x_1 + \dots + a_{m,n} x_n = b_m \end{cases} \quad [E_2]$$

que l'on peut réécrire sous la forme $AX = B$, où

$$A = [a_{i,j}]_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in \mathcal{M}_{m,n}(\mathbb{Z}), \quad B = [b_i]_{1 \leq i \leq m} \in \mathbb{Z}^m$$

$$X = [x_i]_{1 \leq i \leq n} \in \mathbb{Z}^n$$

Th 7: (Forme normale de Smith)
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:

$$UAV = D = \begin{bmatrix} d_1 & & (0) \\ & \ddots & \\ (0) & & d_r \\ & (0) & \end{bmatrix}, \quad d_1 \mid \dots \mid d_r$$

Prop 8: Le système $[E_2]$ est donc équivalent à:

$$\begin{cases} DX' = B' = UB \\ X = VX' \end{cases}$$ système diagonal en X'

Ex 9: On veut résoudre $\underbrace{\begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} x \\ y \end{bmatrix}}_{X} = \underbrace{\begin{bmatrix} 8 \\ 14 \end{bmatrix}}_{B}$

On obtient ainsi:

$$UAV = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \text{ où } U = \begin{bmatrix} -5 & 3 \\ 2 & -1 \end{bmatrix}, \quad V = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad UB = \begin{bmatrix} -5 & 3 \\ 2 & -1 \end{bmatrix} \begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \end{bmatrix}$$

Donc le système équivaut à $\begin{cases} x' = 2 \\ 2y' = 2 \end{cases}$, $VX' = X \Rightarrow X = VX' = VX$

Donc $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$

II- Quelques équations diophantiennes de degré supérieur

1- Triplets pythagoriciens

On étudie l'équation suivante:

$$x^2 + y^2 = z^2, \quad (x,y,z) \in \mathbb{Z}^3 \quad [E_3]$$

Lemme 10: (Paramétrage du cercle unité)
On peut paramétrer le cercle ainsi à coordonnées rationnelles par:

$$\mathcal{C} \cap \mathbb{Q}^2 = \left\{(x,y) \in \mathbb{Q}^2 \mid x^2 + y^2 = 1\right\} = \left\{\left(\frac{1-b^2}{1+b^2}, \frac{2b}{1+b^2}\right), \ b \in \mathbb{Q}\right\}$$

Thm (Tuplets pythagoriciens)
Les tuplets solutions de $[E_2]$, appelés tuplets pythagoriciens sont de la forme
$$\left(d(u^2-v^2), 2duv, d(u^2+v^2)\right), \text{ avec } u,v \in \mathbb{N}^*, d \in \mathbb{Z}, u \wedge v = 1$$
DVPT 4

Rq 12: Ce résultat est vrai à permutation près entre x et y

Ex 13: $u=2, v=1$ et $d=1$ donne $(x,y,z)=(3,4,5)$
$u=3, v=2$ et $d=1$ donne $(x,y,z)=(5,12,13)$
(cf Annexe)

2- Méthode de descente infinie

Méthode: On considère une solution qui minimise une grandeur et avec des relations on construit une solution d'après l'image qui est plus petite que celle de départ. Par l'absurde l'équation n'a pas de solution

Prop 15: L'équation $x^4+y^4=z^2$ n'a pas de solution $(x,y,z) \in \mathbb{Z}^3$

3- Somme de deux carrés

Prop 16: L'anneau $\mathbb{Z}[i] = \{a+ib, (a,b) \in \mathbb{Z}^2\}$ est un sous-anneau de $\mathbb{C}$ l'ensemble de ses unités est donné par $\mathbb{Z}[i]^\times = \{-1, 1, -i, i\}$

Th 17: (Théorème des deux carrés)
Soit $p \in \mathbb{N}$ un nombre premier. L'équation $x^2+y^2=p$, d'inconnue $(x,y) \in \mathbb{Z}^2$, admet une solution si et seulement si $p=2$ ou $p \equiv 1 \ [4]$

DVPT 2

Ex 18: L'équation $x^2+y^2=3$, $(x,y) \in \mathbb{Z}^2$ n'admet aucune solution

Ex 19: Nombres premiers congrus à 1 modulo 4, inférieurs à 50
$5 = 1^2+2^2$, $13 = 2^2+3^2$, $17 = 1^2+4^2$, $29 = 2^2+5^2$,
$37 = 1^2+6^2$, $41 = 4^2+5^2$,

III - Equations dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$

1 - Systèmes de congruences

Th 20: (Théorème chinois)
Soient $n, m \in \mathbb{N}^*$ - $n \wedge m = 1$ alors l'application
$$\frac{\mathbb{Z}}{nm\mathbb{Z}} \xrightarrow{\sim} \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$
$$[x]^{nm} \longmapsto \left([x]^n ; [x]^m\right)$$
est un isomorphisme de groupes où $[x]^k$ est la classe de $x \in \mathbb{Z}$ modulo p dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$

Th 21: (Système de congruence)
Soient $m_1, \dots, m_n \in \mathbb{N}^*$ des entiers 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 $\{x_0 + m_1 \dots m_n k, k \in \mathbb{Z}\}$, où x_0 est une solution particulière du système

Ex 22: Le système de congruences
$$\begin{cases} x \equiv 1 \ [2] \\ x \equiv 2 \ [3] \\ x \equiv 3 \ [5] \end{cases}$$
admet pour solutions l'ensemble $\mathcal{S}$ suivant:
$$\mathcal{S} = \{-7 + 30k, k \in \mathbb{Z}\} = -7 + 30\mathbb{Z}$$

2 - Réduction modulaire

Prop 23: (Réduction modulo m)
Soit $P \in \mathbb{Z}[X_1, \dots, X_n]$. Soit l'équation $P(x_1, \dots, x_n) = 0 \ [m]$ d'inconnue $(x_1, \dots, x_n) \in \mathbb{Z}^n$. Alors on a pour tout $m \in \mathbb{N} \setminus \{0,1\}$ l'équation réduite:
$$\overline{P}\left(\overline{x_1}, \dots, \overline{x_n}\right) = 0 \ [m]$$

Prop 24 : Si $\exists m \in \mathbb{N}^*$, $m \geq 2$, $\overline{F}(\overline{x_1}, \dots, \overline{x_n}) = \overline{0}$ n'a pas de solutions dans $\frac{\mathbb{Z}}{m\mathbb{Z}}$ alors l'équation $[E_1]$ n'a pas de solutions dans $\mathbb{Z}$.

Appli 25 : On peut alors montrer via cette méthode que certaines équations n'ont pas de solutions

Ex 26 : 1- L'équation $x^2 + 3y = 5$ n'a pas de solution $(x,y) \in \mathbb{Z}^2$ (considérer $m = 3$)

2- L'équation $x^2 + y^2 = 4z + 7$ n'a pas de solution $(x,y,z) \in \mathbb{Z}^3$ (considérer $m = 4$)

3- Résidus quadratiques

Def 27 : Soit $a \in \mathbb{Z}$. On dit que a est un résidu quadratique modulo $p \in \mathbb{N}$ si $\exists b \in \mathbb{N}$: $b^2 \equiv a \ [p]$, et $a \not\equiv 0 \ [p]$.

Def 28 (Symbole de Legendre) :
Soit $n \in \mathbb{Z}$ et $p \in \mathbb{N}$ premier. On définit le symbole de Legendre de n et p, noté $\left(\frac{n}{p}\right)$, par :

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{si } p \mid n \\ 1 & \text{si } n \text{ est un résidu quadratique modulo } p \\ -1 & \text{sinon} \end{cases}$$

Th 29 (Propriétés du symbole de Legendre) :
(i) $\forall a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,

(ii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ (iii) Si $a \equiv b \ [p]$, alors $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(iv) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

(v) Loi de réciprocité quadratique : Soient $p, q \in \mathbb{N}$ deux entiers premiers impairs distincts. Alors $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$

Ex 30 : $\left(\frac{30}{7}\right) = ?$

En effet, $\left(\frac{30}{7}\right) = \left(\frac{2 \cdot 3 \cdot 5}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right)\left(\frac{5}{7}\right)$

- $\left(\frac{2}{7}\right) = (-1)^{\frac{7^2-1}{8}} = (-1)^6 = 1$
- $\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{7-1}{2}} = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -(1) = -1$
- $\left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)(-1)^{\frac{5-1}{2}\cdot\frac{7-1}{2}} = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$

Donc $\left(\frac{30}{7}\right) = 1$. Cela est cohérent puisque $30 \equiv -16 \ [7]$ et $-16 = -4^2$. 30 est bien un résidu quadratique modulo 7.

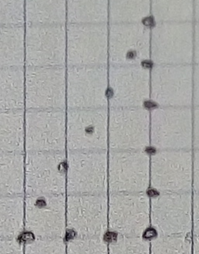
Appli 31 : On peut déterminer l'existence de solutions à certaines équations quadratiques modulo p premier.

Ex 32 : L'équation $x(x+8) \equiv 0 \ [47]$ admet des racines car solution. En effet, en posant $y = x+4$, on a l'équation $x^2 + 8x + 16 \equiv -1 \ [47]$ soit $y^2 \equiv -1 \ [47]$.
On constate en remarquant que $\left(\frac{-1}{47}\right) = 1$.

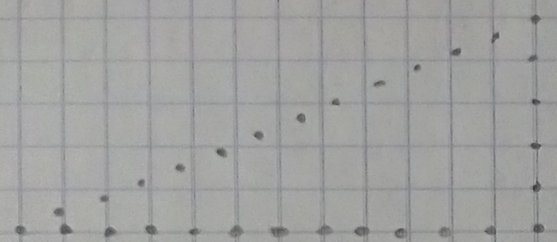
Ex 33 : Si $p, q \in \mathbb{N}^*$ sont deux entiers premiers tels que $\left(\frac{p}{q}\right) = -1$, alors l'équation $x^2 - py^2 = q$, $(x,y) \notin \mathbb{Z}^2$. En effet, en réduit mod p on a $x^2 \equiv q \ [p]$, qui n'a pas de solution. On constate ici l'étude de la propriété de réduction modulaire.

Annexe :

Triplets pythagoriciens :



$(x,y,z) = (3,4,5)$



$(x,y,z) = (5,12,13)$