Exemples d'équations diophantiennes.

Déf 1 : Soit $P \in \mathbb{Z}[X_1, \dots, X_n]$. On appelle équation diophantienne toute équation de la forme $P(x_1, \dots, x_n) = 0$ dont on cherche les solutions $(x_1, \dots, x_n) \in \mathbb{Z}^n$.

I Equations diophantiennes linéaires

1) Arithmétique dans l'anneau principal $\mathbb{Z}$

Prop 2 : Soit $(a,b) \neq (0,0)$. L'équation $ax = b$ possède une unique solution ssi $a \mid b$. Dans ce cas, cette unique solution est $x = \frac{b}{a} \in \mathbb{Z}$.

Identité de Bézout : Soient $(a_1, \dots, a_n) \in \mathbb{Z}^n$. On note $d = \text{pgcd}(a_1, \dots, a_n)$.
alors $\exists (u_1, \dots, u_n) \in \mathbb{Z}^n$ tq $a_1 u_1 + \dots + a_n u_n = d$

Déf 4 : Soient $(a_1, \dots, a_n) \in \mathbb{Z}^n$. On dit que $a_1, \dots, a_n$ sont (mutuellement) 1ers entre eux si $\text{pgcd}(a_i) = 1$.

Th de Bézout : $(a_1, \dots, a_n) \in \mathbb{Z}^n$ sont 1ers entre eux $\Leftrightarrow \exists (u_1, \dots, u_n) \in \mathbb{Z}^n$ tq $a_1 u_1 + \dots + a_n u_n = 1$

Lemme de Gauss : Soient $a, b, c \in \mathbb{Z}$ tq $a \mid bc$ et $a \wedge b = 1$ alors $a \mid c$

Lemme d'Euclide : Soient $a, b \in \mathbb{Z}$, $p \in \mathbb{P}$ tq $p \mid ab$ alors $p \mid a$ ou $p \mid b$

2) Equations diophantiennes de degré 1

Th 8 : Soient $a, b, c \in \mathbb{Z}$. L'équation $ax + by = c$ admet des solutions ssi $\text{pgcd}(a,b) \mid c$
Dans ce cas, soit (x_0, y_0) une solution particulière donnée par l'identité de Bézout
L'ensemble des solutions est donné par : $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} + \frac{k}{\text{pgcd}(a,b)} \cdot \begin{pmatrix} b \\ -a \end{pmatrix}$, $k \in \mathbb{Z}$

Exple 9 : $42x + 66y = 10$ n'admet aucune solution
$112x + 70y = 14$ admet une infinité de solutions de la forme : $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2+5k \\ -3-8k \end{pmatrix}$, $k \in \mathbb{Z}$

Prop 10 : L'équation $a_1 x_1 + \dots + a_n x_n = b$ admet une solution ssi $\text{pgcd}(a_1, \dots, a_n) \mid b$

Th 11 : Soient $(a_1, \dots, a_n) \in (\mathbb{N}^*)^n$ tq $\text{pgcd}(a_1, \dots, a_n) = 1$.
$\forall N \in \mathbb{N}^*$, on note $u_N = \text{Card}\{(x_1, \dots, x_n) \in \mathbb{N}^n : a_1 x_1 + \dots + a_n x_n = N\}$, alors $u_N \underset{+\infty}{\sim} \frac{1}{a_1 \dots a_n} \cdot \frac{N^{n-1}}{(n-1)!}$

II Approche géométrique

1) Solutions entières sur une courbe

Déf 12 : Soit $d \in \mathbb{N}^*$, sans facteur carré. On appelle équation de Pell-Fermat : $x^2 - dy^2 = 1$

Déf 13 : Soit $\mathcal{H}$ l'hyperbole d'équation $\mathcal{H} : X^2 - dY^2 = 1$.
On définit une Loi sur $\mathcal{H}$ en posant, pour $M\begin{pmatrix} x \\ y \end{pmatrix}$, $M'\begin{pmatrix} x' \\ y' \end{pmatrix}$, $M * M' = \begin{pmatrix} xx' + dyy' \\ xy' + x'y \end{pmatrix} \in \mathcal{H}$.

Th 14 : Soient $\mathcal{H} : X^2 - dY^2 = 1$; $M_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $M_1 = \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \in \mathcal{H}$ avec $x_1, y_1 \in \mathbb{N}^*$ tq $x_1^2 + y_1^2$ aussi petit que possible
L'ensemble des points entiers de la branche de $\mathcal{H}$ qui contient M_0 est le groupe engendré par M_1.
L'ensemble des points entiers de $\mathcal{H}$ est un sous groupe de $\mathcal{H}$, isomorphe à $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exple 15 : Soit $P_2 : x^2 - 2y^2 = 1$. $M_0(1,0)$ et $M_1(3,2)$ sont deux solutions de P_2.
alors P_2 admet une infinité de solutions, parmi lesquelles $M_2\begin{pmatrix} 17 \\ 12 \end{pmatrix}$, $M_3\begin{pmatrix} 99 \\ 70 \end{pmatrix}$

2) Points rationnels sur une courbe

Déf 15 : Soit $n \geq 2$. On appelle équation de Fermat de degré n : $(F_n) : x^n + y^n = z^n$

Rq 16 : Les triplet $(x,y,z) \in \mathbb{Z}^3$ tq $xyz = 0$ sont des solutions dites triviales de (F_n).

Déf 17 : On dit que $(x,y,z) \in \mathbb{Z}^3$ est une solution primitive de (F_n) si $pgcd(x,y,z) = 1$.

Prop 19 : Les solutions de (F_2) sont les points du cercle unité à coordonnées rationnelles.

Th 19 : L'équation $(F_2) : x^2 + y^2 = z^2$ admet comme solutions primitives (avec y pair) les triplets pythagoriciens : $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} r^2 - s^2 \\ 2rs \\ r^2 + s^2 \end{pmatrix}$ avec $r, s \in \mathbb{Z}$, $r \wedge s = 1$.

Exples 20 : Les triplets $(3,4,5)$ et $(5,12,13)$ sont des solutions primitives de (F_2).

Déf 21 : On appelle folium de Descartes la courbe plane $\mathcal{C} : X^3 + Y^3 = XY$.

Exple 22 : Les solutions primitives de : $x^3 + y^3 = xyz$ sont de la forme : $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} uv^2 \\ u^2 v \\ u^3 + v^3 \end{pmatrix}$, $u \wedge v = 1$

3) Méthode de la descente infinie

Th 23 : Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Exple 24 : L'équation $y^2 - 2x^2 = 0$ n'admet pas de solutions non triviale, ie $\sqrt{2} \notin \mathbb{Q}$.

Exple 25 : L'équation $x^4 + y^4 = z^2$ n'admet pas de solutions non triviale,
A fortiori, $(F_4) : x^4 + y^4 = z^4$ non plus

III Réduction modulaire

1) Equations dans $\mathbb{Z}/d\mathbb{Z}$

Prop 27 : Soit $(x_1, \dots, x_n) \in \mathbb{Z}^n$ tq $P(x_1, \dots, x_n) = 0$ alors $\forall d \in \mathbb{N}^*$, $\overline{P}(\overline{x_1}, \dots, \overline{x_n}) = \overline{0}$ dans $\mathbb{Z}/d\mathbb{Z}$

Exples 28 : Les équations $x^2 + y^2 = 4z + 7$ et $x^2 + 3y = 5$ n'admettent pas de solutions

Th des restes chinois : Soient $n_1, \dots, n_k \in \mathbb{N}^*$ 2 à 2 premiers entre eux, alors $\mathbb{Z}/n_1 \dots n_k\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$
En d'autres termes, le système $\begin{cases} x \equiv a_1 \ [n_1] \\ \vdots \\ x \equiv a_k \ [n_k] \end{cases}$ admet une unique solution.

Exple 30 : L'équation $39x^2 + 3x - 77 = 385y$ admet 8 familles de solutions données par : $x \in \{231\mathbb{Z} ; 301\mathbb{Z} ; 286\mathbb{Z} ; 356\mathbb{Z} ; 77\mathbb{Z} ; 147\mathbb{Z} ; 132\mathbb{Z}, 202\mathbb{Z}\}$

Petit th de Fermat : Soit $p \in \mathbb{P}$ et $a \notin p\mathbb{Z}$ alors : $a^{p-1} \equiv 1 \ [p]$.

DVPT ①

Exple 32 : Th de Sophie-Germain : Soit p un nb 1er impair tel que $q = 2p + 1$ est 1er
alors $x^p + y^p + z^p = 0$ ne possède pas de solutions tq $xyz \not\equiv 0 \ [p]$

2) Loi de la réciprocité quadratique

Déf 33 : $\forall x \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, on définit le symbole de Legendre : $\left(\frac{x}{p}\right) = \begin{cases} 1 \text{ si } x \in (\mathbb{F}_p^*)^2 \\ 0 \text{ si } x = \overline{0} \\ -1 \text{ sinon} \end{cases}$

Prop 34 : $\left(\frac{\cdot}{p}\right)$ définit un morphisme de groupes de $\mathbb{F}_p^*$ sur $\{-1;1\}$.
De plus, $\forall x \in \mathbb{F}_p^*$, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$.

Loi de la réciprocité quadratique : Soient p, q deux nombres premiers impairs distincts
alors $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{q-1}{2}}$.

Corollaire 36 : L'équation $x^2 + py = q$ admet une solution $\Leftrightarrow \left(\frac{q}{p}\right) = 1$

Exple 37 : L'équation $x^2 + 59y = 23$ n'admet pas de solutions.

3) Théorème de la progression arithmétique

Déf 38 : Soient $a, b \in \mathbb{N}^*$. On étudie l'équation $p = an + b$ avec $p \in \mathbb{P}$.

Rq 39 : Si a et b ne sont pas premiers entre eux, il n'y a pas de solutions.

Déf 40 : On appelle caractère de Dirichlet modulo a un morphisme de groupe $\chi : (\mathbb{Z}/a\mathbb{Z})^\times \to \mathbb{C}^*$

Prop 41 : On peut prolonger χ en une fonction sur $\mathbb{Z}$, a-périodique, strictement multiplicative.

Th 42 : On a $\forall s \in \mathbb{C}, \mathrm{Re}(s) > 1$, $L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}}$.

- $L(\mathbb{1}_a, \chi)$ a un pole simple en $s = 1$
- Si $\chi \neq \mathbb{1}_a$, on peut prolonger $L(\chi, s)$ sur $\mathrm{Re}(s) > 0$ et alors $L(\chi, 1) \neq 0$.

Th de la progression arithmétique de Dirichlet :

Si $a \wedge b = 1$, l'équation $p = an + b$ admet une infinité de solutions.

(IV) Extensions algébriques de $\mathbb{Z}$

1) L'anneau des entiers de Gauss

Déf 44 : On appelle anneau de Gauss l'anneau : $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2+1)$.

Prop 45 : $\mathbb{Z}[i]$ est euclidien pour le stathme $N(a+ib) = a^2 + b^2$

et $\mathbb{Z}[i]^\times = \{1 ; -1 ; i ; -i\}$

DVPT ②

Th 46 : Soit $p \in \mathbb{P}$. On a équivalence entre :

(1) $\exists a, b \in \mathbb{Z}$ tq $p = a^2 + b^2$

(2) p n'est pas irréductible dans $\mathbb{Z}[i]$

(3) -1 est un carré dans $\mathbb{F}_p$

(4) $p = 2$ ou $p \equiv 1 [4]$

Th des deux carrés : $n \in \mathbb{N}$ est somme de deux carrés $\Leftrightarrow \forall p \in \mathbb{P}, p \equiv 3 [4], p \mid n \Rightarrow v_p(n)$ est pair

Th des 4 carrés : Tout nombre entier est la somme de 4 carrés.

2) L'anneau $\mathbb{Z}[i\sqrt{2}]$

Prop 49 : On définit $\mathbb{Z}[i\sqrt{2}] = \mathbb{Z}[X]/(X^2+2)$

Prop 50 : $\mathbb{Z}[i\sqrt{2}]$ est euclidien pour le stathme $N(a+ib\sqrt{2}) = a^2 + 2b^2$ et $\mathbb{Z}[i\sqrt{2}]^\times = \{\pm 1\}$

Prop 51 : Soit $p \in \mathbb{P}$, alors $p = a + 2b^2 \Leftrightarrow -2$ est un carré modulo p.

Exple 52 : Les solutions de l'équation de Mordell $y^2 = x^3 - 2$ sont $(3;5)$ et $(3;-5)$

3) L'anneau des entiers d'Eisenstein

Déf 53 : On définit l'anneau des entiers de Eisenstein $\mathbb{Z}[j] = \mathbb{Z}[X]/(X^2+X+1)$.

Prop 54 : $\mathbb{Z}[j]$ est euclidien pour le stathme $N(a+jb) = a^2 - ab + b^2 = \frac{(2a-b)^2}{4} + \frac{3b^2}{4}$

Prop 55 : $\mathbb{Z}[j]^\times = \{1 ; -1 ; j, j^2, -j, -j^2\}$

Exple 56 : L'équation de Nagell-Ramanujan $x^2 + 3 = 2^n$

n'admet que deux solutions : $(x, n) = (1 ; 2)$ et $(x, n) = (-1, 2)$.

(V) Grand théorème de Fermat

Th de Fermat-Wiles : 1994, [ADMIS] :

$\forall n \geq 3$, l'équation $x^n + y^n = z^n$ n'admet pas de solution non triviales