126 : Exemples d'équations en arithmétique.

I Equations diophantiennes linéaires

A Définition et premiers exemples Rom

Définition 1 : Une équation diophantienne est une équation polynomiale à coefficients entiers et d'inconnues entières

Exemple 2 : Soient $m \geq 2$ un entier, a un entier naturel non nul et b un entier relatif. Alors $ax \equiv b\ [m]$ est une équation diophantienne.

Proposition 3 : L'équation $ax \equiv 1\ [m]$ a des solutions si et seulement si $\bar{a}$ est inversible dans $\mathbb{Z}/m\mathbb{Z}$ si et seulement si $a \wedge m = 1$. Dans ce cas l'algorithme d'Euclide nous permet de trouver une solution $x_0 \in \mathbb{Z}$.

Corollaire 4 : Si $a \wedge m = 1$, l'ensemble des solutions de $ax \equiv 1\ [m]$ est l'ensemble $S = \{x_0 + km \mid k \in \mathbb{Z}\}$ où x_0 est une solution particulière.

Corollaire 5 : Si $a \wedge m = 1$ et $b \in \mathbb{Z}$, les solutions de $ax \equiv b\ [m]$ sont les $bx_0 + km$ avec $k \in \mathbb{Z}$ et x_0 une solution particulière.

Théorème 6 : On note $\delta = a \wedge m$ et $a = \delta a'$, $m = \delta m'$. L'équation de l'exemple 2 a des solutions entières si et seulement si $\delta \mid b$. Dans ce cas l'ensemble des solutions de cette équation est $S = \{b'x_0 + km' \mid k \in \mathbb{Z}\}$ où x_0 est une solution particulière de $a'x \equiv 1\ [m']$.

B Systèmes de congruence Rom

Lemme 7 : Soient $(m_i)_{1 \leq i \leq n}$ une suite de $n \geq 2$ entiers naturels distincts de 0 et de 1.

i) Si les entiers $m_1, \dots, m_n$ sont deux à deux premiers entre eux, leur ppcm est alors $\prod_{i=1}^{n} m_i$

ii) Si les entiers $m_1, \dots, m_n$ ne sont pas deux à deux premiers entre eux on a alors $\mathrm{ppcm}(m_1, \dots, m_n) < \prod_{i=1}^{n} m_i$

Remarque 8 : C'est faux si on suppose seulement que les (m_i) sont premiers dans leur ensemble. Par exemple $2 \vee 3 \vee 4 = 12 < 2 \cdot 3 \cdot 4 = 24$.

Théorème 9 : (chinois) Soient $(m_i)_{1 \leq i \leq n}$ une suite $n \geq 2$ entiers naturels distincts de 0 et 1 et $m = \prod_{i=1}^{n} m_i$.
Les entiers $m_1, \dots, m_n$ sont deux à deux premiers entre eux si et seulement si les anneaux $\mathbb{Z}/m$ et $\prod \mathbb{Z}/m_i$ sont isomorphes. Dans ce cas, l'application :

$$\begin{aligned} \psi : \mathbb{Z}/n &\longrightarrow \prod \mathbb{Z}/m_i \\ \pi_n(k) &\longmapsto (\pi_1(k), \dots, \pi_n(k)) \end{aligned}$$

(où on a noté π_k la surjection canonique π_{m_k}) est un isomorphisme d'anneaux d'inverse :

$$\begin{aligned} \psi^{-1} : \prod \mathbb{Z}/m_i &\longrightarrow \mathbb{Z}/n \\ (\pi_1(a_1), \dots, \pi_n(a_n)) &\longmapsto \pi_n\left(\sum_{i=1}^{n} a_i u_i \frac{m}{m_i}\right) \end{aligned}$$

où $(u_i) \in \mathbb{Z}$ telle que $\sum_{i=1}^{n} u_i \frac{m}{m_i} = 1$

Application 10 : On considère le système de congruences $\begin{cases} x \equiv a\ [n] \\ x \equiv b\ [m] \end{cases}$ d'inconnue $x \in \mathbb{Z}$ et de paramètres $(a, b, n, m) \in \mathbb{Z}^4$ avec $n \wedge m = 1$. Alors il existe une solution $X \in \mathbb{Z}$ (unique modulo nm) de ce système.

Application 11 : exercice de la bande de pirates [Annexe]

Exemple 12 : Le système de congruences $\begin{cases} k \equiv 2\ [4] \\ k \equiv 3\ [5] \\ k \equiv 1\ [3] \end{cases}$ a pour solutions $S = \{118 + 180q,\ q \in \mathbb{Z}\}$.

II Equations diophantiennes non linéaire

A Equations de Fermat. Com

Proposition 13 : Soit $x, y, z \in \mathbb{N}^3$, alors $x^2 + y^2 = z^2$ si et seulement si il existe $d \in \mathbb{N}$ et $u, v \in \mathbb{N}^*$, $u \wedge v = 1$ tels que $x = d(u^2 - v^2)$, $y = 2duv$ et $z = d(u^2 + v^2)$ ou $[x, y, z] = [2duv, d(u^2 - v^2), d(u^2 + v^2)]$.

Méthode 14 (descente infinie) On cherche à montrer qu'une équation n'a pas de solutions. Pour cela on suppose par l'absurde qu'il y en a une. On construit à partir de cette solution une autre solution strictement plus petite au sens où pour $\varphi : \mathbb{Z}^n \to \mathbb{N}$ bien choisie et une solution $(x_1, \dots, x_n) \in \mathbb{Z}^n$, il existe une solution $(x_1', \dots, x_n') \in \mathbb{Z}^n$ telle que $\varphi(x_1', \dots, x_n') < \varphi(x_1, \dots, x_n)$. Par récurrence on obtient une suite (infinie) strictement décroissante. C'est absurde.

Théorème 15 : Les équations de la forme $x^4 + y^4 = z^2$ et $x^4 + y^4 = z^4$ n'ont pas de solutions non triviales.

Théorème 16 (Fermat, Admis) L'équation $x^n + y^n = z^n$ pour $n \geq 2$ n'admet pas de solutions non triviales.

Développement (Sophie Germain) Soit $p \in \mathcal{P}$ impair tel que $q = 2p+1 \in \mathcal{P}$ alors il n'existe pas de triplet $(x,y,z) \in \mathbb{Z}^3$ tel que $p \nmid xyz$ et $x^p + y^p + z^p = 0$.

B L'anneau des entiers de Gauss Per

Définition 17 : On note $\mathbb{Z}[i] = \{a+ib \in \mathbb{C} \mid a,b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss. On définit sur $\mathbb{Z}[i]$ l'application $N : \mathbb{Z}[i] \to \mathbb{N}$ $a+ib \mapsto a^2+b^2$. Pour $z \in \mathbb{Z}[i]$, $N(z)$ est appelé la norme de l'entier de Gauss z. On remarque que N est multiplicative : $N(zz') = N(z)\,N(z')$.

Définition 18 : On note $\Sigma = \{n \in \mathbb{Z} \mid \exists a,b \in \mathbb{Z}\ n = a^2+b^2\}$ l'ensemble des entiers qui s'écrivent comme somme de deux carrés.

Exemple 19 : On a $0, 1, 2, 4, 5, 8, 9, 10 \in \Sigma$ mais $3, 6, 7, \ldots \notin \Sigma$

Remarque 20 : Si $n \equiv 3\ [4]$ on a $n \notin \Sigma$. En effet si a est pair on a $a^2 \equiv 0\ [4]$ et si a est impair, $a^2 \equiv 1\ [4]$ donc $a^2+b^2 \equiv 0, 1, 2\ [4]$.

Proposition 21 : On a $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Proposition 22 : L'ensemble Σ est stable par multiplication.

Proposition 23 : L'anneau $\mathbb{Z}[i]$ (muni de N) est euclidien donc principal

Lemme 24 : On a $p \in \Sigma \iff p$ n'est pas irréductible dans $\mathbb{Z}[i]$.

Développement Soit $p \in \mathcal{P}$ impair. Alors $p \in \Sigma \iff p \equiv 1\ [4]$.

III Carrés dans un corps fini

A Symbole de Legendre Per + Rom

Notation 25 : On note pour $q = p^m$, $m \geq 1, p \in \mathcal{P}$, $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q,\ x = y^2\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

Proposition 26 : i) Pour $p = 2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$
ii) Pour $p > 2$, on a $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$

Proposition 27 (caractérisation des carrés) On suppose $p > 2$. Alors on a :
$$x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$$

Exemple 28 : si $q = 7$ donc $\mathbb{F}_q = \mathbb{Z}/7\mathbb{Z}$, $q^{\frac{q-1}{2}} = 1\ [7]$ donc $2 \in \mathbb{F}_7^{*2}$
Par contre $3^3 \equiv -1\ [7]$ et 3 n'est pas un carré.

Corollaire 29 : -1 est un carré dans $\mathbb{F}_q \iff q \equiv 1\ [4]$.

Application 30 : Il existe une infinité de nombres premiers $p \equiv 1\ [4]$.

Définition 31 : On dit qu'un entier k non multiple de p premier impair est un résidu quadratique modulo p si $\overline{k}$ est un carré dans $\mathbb{F}_p^*$.

Définition 32 : Pour tout $a \in \mathbb{F}_p^*$, le symbole de Legendre est l'entier :
$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{si non} \end{cases}$$

Théorème 33 : i) Pour tout $a \in \mathbb{F}_p^*$, on a $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\ [p]$.
ii) L'application $\mathbb{F}_p^* \to \{-1,1\}$, $a \mapsto \left(\frac{a}{p}\right)$ est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^*$ sur $\{-1,1\}$.

Exemple 34 : $2^{\frac{5-1}{2}} = 2^2 = -1\ [5]$ donc 2 n'est pas un résidu quadratique modulo 5.

Corollaire 35 : Si $n = \pm \prod_{i=1}^{\wedge} p_i^{\alpha_i}$ alors $\left(\frac{n}{p}\right) = (-1)^{\frac{p-1}{2}} \prod_{i=1}^{\wedge} \left(\frac{p_i}{p}\right)^{\alpha_i}$

Proposition 36 : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

B Loi de réciprocité quadratique Caldero

Lemme 37 : Pour tout $a \in \mathbb{F}_p^*$, le nombre de solution de l'équation $ax^2 = 1$ est
$$\left(\frac{a}{p}\right) + 1 = \begin{cases} 2 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ 0 & \text{si non.} \end{cases}$$

Proposition 38 : Soit p et q deux nombres premiers distincts et l'ensemble $X = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p \ , \ \sum x_i^2 = 1\}$, alors $|X| \equiv \left(\frac{p}{q}\right) + 1 \ [p]$

Proposition 39 : On a également $|X| = q^{\frac{p-1}{2}} \left(\frac{(-1)^{\frac{p-1}{2}}}{q} \right) + q^{p-1}$

Théorème 40 (Loi de réciprocité quadratique) Pour tout nombre premier impair $q \neq p$, on a : $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

Exemple 41 : $\left(\frac{219}{383}\right) = 1$ donc 219 est un résidu quadratique modulo 383.

Références :

Rombaldi Mathématiques pour l'agrégation

D. Perrin Cours d'Algèbre

Algèbre et géométrie Combes (pour équation de Fermat)
et descente infinie

N2H2G Caldero