Leçon 126 : Exemples d'équations en arithmétiques.

RM

2022-2023

1 Équations diophantiennes linéaires

1.1 Notion d'équation diophantienne

Définition 1 : On appelle équation diophantienne une équation polynomiales à coefficients entiers telles que les solutions soit des solutions entières.

Exemple 2 : Soient $n \geq 2$ un entier, a un entier naturel non nul et b un entier relatif. Alors $ax \equiv b \pmod{n}$ est une équation diophantienne.

Théorème 3 : Soit $a_1, ..., a_n \in \mathbb{Z}$ et $d = pgcd(a_1, ..., a_n)$. Alors il existe $u_i \in \mathbb{Z}$ telle que $\sum_{i=1}^{n} u_i a_i = d$.

Théorème (de Bézout) 4 : $a_1, ..., a_n \in \mathbb{Z}$ sont premiers entre eux si et seulement si il existe $u_i \in \mathbb{Z}$ tels que $\sum_{i=1}^{n} u_i a_i = 1$.

Remarque/Algorithme 5 : On peut utiliser l'algorithme d'Euclide et Euclide étendue pour trouver le pgcd et les coefficients de Bézout de deux nombres a et b dans $\mathbb{Z}$.

Proposition 6 : Dans le cas ou $b = 1$, alors cette équation a des solutions si et seulement si $\overline{a}$ est inversible dans dans $\mathbb{Z}/n\mathbb{Z}$, ie $a \wedge n = 1$.
L'algorithme d'Euclide nous permet alors de trouver une solutions particulière $x_0 \in \mathbb{Z}$.

Corollaire 7 : L'ensemble des solutions de $ax \equiv 1 \pmod{n}$ si $a \wedge n = 1$ est alors $S = \{x_0 + kn | k \in \mathbb{Z}\}$.

Proposition 8 : Si $a \wedge n = 1$ et $b \in \mathbb{Z}$, alors $u_0 = bx_0$ est solution particulière de $ax \equiv b \pmod{n}$ où x_0 est une solution particulière de $ax \equiv 1 \pmod{n}$. Les solutions sont alors $S = \{bx_0 + kn | k \in \mathbb{Z}\}$.

Proposition 9 : Dans le cas générale, on a pour $\delta = a \wedge n$ avec $a = \delta a'$,$n = \delta n'$ que a' et n' sont premiers entre eux. L'équation diophantienne à alors des solutions si et seulement si δ divise b. L'ensemble des solutions est $S = \{b'x'_0 + kn' | k \in \mathbb{Z}\}$, ou x'_0 est une solution particulière de $a'x \equiv 1 \pmod{n'}$ et $b = \delta b'$.

Remarque 10 : On peut ici remarquer que $ax \equiv b \pmod{n}$ revient à il existe $y \in \mathbb{Z}$ tel que $ax - ny = b$. Résoudre cette équation diophantienne est donc équivalente à résoudre $ax + by = c$ avec $a, b, c \in \mathbb{Z}$.

1.2 Système de congruence

Théorème (Chinois) 11 : Soient $(n_j)_{1 \leq j \leq r}$ une suite de $r \geq 2$ entiers naturels distincts de 0 et 1, et $n = \prod_{j=1}^{r} n_j$. Les entiers $n_1, .., n_r$ sont deux à deux premiers entre eux si et seulement si, les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $\prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z}$ sont isomorphes. Dans ce cas l'application

$$\begin{array}{rccc} \psi : & \mathbb{Z}/n\mathbb{Z} & \to & \prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z} \\ & \pi_n(k) & \mapsto & (\pi_1(k), ..., \pi_r(k)) \end{array} .$$

est un isomorphisme.

Remarque 12 : On dispose même de l'application inverse de ψ, qui est

$$\begin{array}{rccc} \psi^{-1} : & \prod_{j=1}^{r} \mathbb{Z}/n_j\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ & (\pi_1(a_1), ..., \pi_r(a_r)) & \mapsto & \pi_n\left(\sum_{i=1}^{r} a_i u_i \frac{n}{n_i}\right) \end{array} .$$

Remarque 13 : Le théorème chinois nous permet alors de résoudre certains systèmes de congruences. Il nous garantit alors une de l'existence d'une solution et même son unicité dans $\mathbb{Z}/n\mathbb{Z}$. On alors que toutes solutions sont de la $x_0 + kn$ ou x_0 est une solution particulière.

Exemple 14 : On considère le système suivant

$$\begin{cases} k \equiv 2 \pmod{4} \\ k \equiv 3 \pmod{5} \\ k \equiv 1 \pmod{9} \end{cases} .$$

On a alors comme solution $k = 118 + 180q$ ou $q \in \mathbb{Z}$.

Remarque 15 : Dans la pratique, pour trouver la solution de ce système, on pose $x = x_1 + 4x_2 + x_3 20$ et on cherche x_1, x_2, x_3 pour avoir une solution particulière.

2 Équations de partition d'entiers

2.1 l'anneau $\mathbb{Z}[i]$ et le théorème des deux carrés

Définition 16 : On pose $\sum = \{n \in \mathbb{N} | n = a^2 + b^2; a, b \in \mathbb{N}\}$ et $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} | a, b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss.
Exemple 17 : On a $0, 1, 2, 4, 5, 8, 9, 10$ dans $\sum$ mais pas $3, 6, 7, 11, 12$.

Remarque 18 : Si $n \equiv 3 \pmod{4}$, alors $n \notin \sum$.

Proposition 19 : On a $\mathbb{Z}[i]^{\times} = \{-1, +1, -i, +i\}$.

Proposition 20 : L'ensemble $\sum$ des sommes de deux carrés est stable par multiplication.

Proposition 21 : L'anneau $\mathbb{Z}[i]$ est euclidien, donc principal.

Théorème 22 : Soit $p \in \mathbb{N}$ un nombre premier. On a alors que $p \in \sum$ si et seulement si $p = 2$ ou $p \equiv 1 \pmod 4$.

Lemme 23 : On a que $p \in \sum$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.

Exemple 24 : On a bien que $41 = 5^2 + 4^2$,$53 = 7^2 + 2^2$,$61 = 6^2 + 5^2$ sont dans $\sum$.

Développement (Théorèmes des deux carrés de Fermat) 25 : Soit $n \in \mathbb{N}^*$ avec $n > 1$, on décompose n en facteurs premiers $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$. Alors on a $n \in \sum$ si et seulement si $v_p(n)$ pair pour $p \equiv 3 \pmod 4$. **Dev 1**

2.2 Équation de Fermat

On s'intéresse à l'équation de Fermat $x^n = y^n + z^n$.

Théorème (petit théorème de Fermat) 26 : Soit $a \in \mathbb{Z}^*$ et p un nombre premier tel que p ne divise pas a. Alors $a^{p-1} \equiv 1 \pmod p$.

Développement 27 : Soit p un nombre premier de Sophie Germain, c'est-à-dire un nombre premier impair tel que $q = 2p+1$ soit premier. Alors il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0[p]$ et $x^p+y^p+z^p = 0$. **Dev 2**

Théorème (de Fermat) 28 : Il n'existe pas de nombre entiers strictement positifs x, y, z solution de l'équation de Fermat pour $n > 2$.

3 Résidus quadratique

3.1 Carrés dans un corps fini

On prends $p \geq 2$ un nombre premiers, n un entier naturel non nul et $\mathbb{F}_q$ est un corps fini de cardinal $q = p^n$.

Définition 29 : On pose $P_2 = \{x^2 | x \in \mathbb{F}_q^*\}$ l'ensemble des carrés dans $\mathbb{F}_q^*$.

Théorème 30 : Il y a $q - 1/2$ carrés dans $\mathbb{F}_q^*$ et $q + 1/2$ carrés dans $\mathbb{F}_q$. De plus, les carrés de $\mathbb{F}_q^*$ sont les racines de $X^{q-1/2} - 1$.

Corollaire 31 : *i)* -1 est un carré dans $\mathbb{F}_q^*$ si et seulement si q est congrus à 1 modulo 4.

ii) Pour tous a, b dans $\mathbb{F}_q^*$ et tout $c \in \mathbb{F}_q$, il existe x, y dans $\mathbb{F}_q$ tels que $c = ax^2+by^2$ (prenant $a = b = 1$, on en déduit que tout élément de $\mathbb{F}_q$ est somme de deux carrés).

3.2 Symbole de Legendre

On prends $p \geq 3$ un nombre premier.

Définition 32 : On dit qu'un entier k non multiple de p est un résidus quadratique modulo p si $\overline{k}$ est un carré dans $\mathbb{F}_p^*$.

Exemple 33 : On a que $4^2 \equiv 1[5]$, donc que 4 est un résidus quadratique modulo 5.

Définition 34 : Pour tout $a \in \mathbb{Z}$, le symbole de Legendre est l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } \overline{a} \text{ est un carré dans } \mathbb{F}_p^* \\ 0 \text{ si } p|a \\ -1 \text{ sinon} \end{cases}.$$

Exemple 35 : On en déduit que $\left(\frac{4}{5}\right) = 1$.

Lemme 36 : Soit p un nombre premier impair. Alors :

i) Pour tous $a, b \in \mathbb{Z}$ tels que $a \equiv b \pmod p$, on a $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

ii) Pour tous $a, b \in \mathbb{Z}$, on a $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Théorème 37 : Pour tout $a \in \mathbb{Z}$, on a $\overline{a}^{p-1/2} = \overline{\left(\frac{a}{p}\right)}$ dans $\mathbb{F}_p$ et l'application $a \mapsto \left(\frac{a}{p}\right)$ est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^*$ sur $\{-1, 1\}$.

Application 38 : Pour tout $a \in \mathbb{F}_p^*$, le nombre de solutions de l'équation $ax^2 = 1$ dans $\mathbb{F}_p^*$ est $\left(\frac{a}{p}\right) + 1$.

Théorème (Réciprocité quadratique) 39 : Pour tout nombre premier impair $q \neq p$, on a $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$.

Proposition 40 : Pour p premier impaire, on a que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. On a alors que 2 est un résidus quadratique modulo p si et seulement si p est congrus à 1 ou -1 modulo 8.

Exemple 41 : Dans $\mathbb{Z}/17\mathbb{Z}$, on a bien que $6^2 \equiv 2 \pmod{17}$.

Exemple 42 : Grâce à la loi de réciprocité quadratique, on calcule $\left(\frac{103}{173}\right) = -1$. Donc 103 n'est pas un carré modulo 173.

4 Systèmes d'équations linéaires à coefficients entiers

Définition 43 : Soit A un anneau. Un système complet de représentants irréductibles(s.r.c.i) est un sous ensemble $\mathscr{P}$ de A tel que :

1) tout élément de $\mathscr{P}$ est irréductible.
2) tout élément irréductible de A est associé à un unique élément de $\mathscr{P}$.

Remarque 44 : Cela revient à munir l'ensemble des irréductibles de A la relation d'équivalence "êtres associés", et de prendre un représentant dans chaque classe d'équivalence.

Exemple 45 : Pour $A = \mathbb{Z}$, on a que $\mathscr{P}_1 = \{2, 3, 5, 7, 11, ...\}$ et
$\mathscr{P}_2 = \{-2, -2, -5, -7, -11, ...\}$ sont tous les deux un s.c.r.i de $\mathbb{Z}$.

On se place dans l'anneau euclidien $\mathbb{Z} = A$ pour la suite.

Théorème (Réduction des matrices) 46 : Toute matrice $C \in \mathcal{M}_{m\times n}(\mathbb{Z})$ est équivalente à une matrice de la forme

$$E(a_1, ..., a_r) = \begin{pmatrix} a_1 & & & 0 \\ & \ddots & & \\ & & a_r & \\ 0 & & & 0 \end{pmatrix}$$

avec $a_1, ..., a_r \in \mathbb{Z}$ non nuls et normalisés (ie produit d'éléments de $\mathscr{P}$) vérifiant

$$a_1|a_2|...|a_r$$

De plus, l'entier r et les éléments $a_1, ..., a_r$ sont uniques.
Plus précisément, il existe des matrices $U \in GL_m(\mathbb{Z})$ et $V \in GL_n(\mathbb{Z})$ qui sont produits de matrices de permutation, de transvection et de dilatation telles que $UCV = E(a_1, ..., a_r)$.

Définition 47 : Soit $C \in \mathcal{M}_{m\times n}(\mathbb{Z})$. La matrice $E(a_1, ..., a_r)$ donnée par le théorème précédent s'appelle la forme normal de Smith de C (par rapport à $\mathscr{P}$).

Exemple 48 : Soit $A = \mathbb{Z}$ et $C = \begin{pmatrix} 10 & 14 \\ 6 & 7 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$. Alors $C \sim \begin{pmatrix} 1 & 0 \\ 0 & 14 \end{pmatrix}$ avec donc $r = 2, a_1 = 1$ et $a_2 = 14$.

Remarque 49 : On peut alors utiliser la forme normal de Smith pour résoudre des systèmes linéaires à coefficients entiers.

Théorème 50 : Soit $a_1, ..., a_n$ des éléments de $\mathbb{Z}$ non tous nuls, et soit $b \in \mathbb{Z}$. Enfin, soit $d \in \mathbb{Z}$ le pgcd normalisé (ie dans $\mathbb{Z}$ le pgcd positif pour le s.c.r.i $\mathscr{P}_1$) de $a_1, ..., a_n$. Alors l'équation

$$a_1x_1 + ... + a_nx_n = b. \quad x_i \in \mathbb{Z}$$

admet une solution si et seulement si $d|b$. Dans ce cas, toute solution de cette équation s'écrit de manière unique sous la forme

$$\alpha.V_1 + x_2.V_2 + ... + x_n.V_n, \quad x_2, ..., x_n \in \mathbb{Z}.$$

où $\alpha \in \mathbb{Z}$ vérifie $b = \alpha d$ et $V_1, ..., V_n$ sont les colonnes d'une matrice inversible $V \in GL_n(\mathbb{Z})$ vérifiant

$$(a_1, ..., a_n)V = (d, 0, ..., 0).$$

Exemple 51 : On veut résoudre $3x+4y+7z = b$ dans $\mathbb{Z}$. Comme le pgcd est de 1, on a l'existence d'une solution pour tout $b \in \mathbb{Z}$. On obtient la matrice $V = \begin{pmatrix} -1 & 4 & -1 \\ 1 & -3 & -1 \\ 0 & 0 & 1 \end{pmatrix}$ et alors on a comme solution

$$x = -b + 4z_1 - z_2, y = b - 3z_1 - z_2, z = z_2 \text{ avec } z_1, Z_2 \in \mathbb{Z}.$$

Références :

1. Algèbre et géométrie Rombaldi
2. Cours d'algèbre Perrin
3. Algèbre le grand combat Berhuy