126

Exemples d'équations en arithmétique

[Rom]

X.4

Soit $n \in \mathbb{N}^*$, A anneau principal, $\mathcal{P}$ l'ensemble des entiers premiers

I] Équations diophantiennes linéaires

1] Notion d'équation diophantienne

Définition 1 : On appelle équation diophantienne toute équation polynomiale à coefficients entiers et d'inconnues entières.

Exemple 2 : Pour $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$, $ax \equiv b\,[n]$ définit une équation diophantienne.

Proposition 3 : Soit $a \in \mathbb{N}^*$

Alors : $ax \equiv 1\,[n]$ a des solutions ssi $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$

ssi $a \wedge n = 1$

Dans ce cas, l'algorithme d'Euclide étendu permet de trouver $x_0 \in \mathbb{Z}$ solution particulière $ax_0 \equiv 1\,[n]$.

Corollaire 4 : Soit $a \in \mathbb{N}^*$ tel que $a \wedge n = 1$.

Alors : les solutions de $ax \equiv 1\,[n]$ sont $S = \{x_0 + kn \mid k \in \mathbb{Z}\}$ avec x_0 une solution particulière

Corollaire 5 : Soit $a \in \mathbb{N}^*$ tel que $a \wedge n = 1$, $b \in \mathbb{Z}$.

Alors : les solutions de $ax \equiv b\,[n]$ sont $S = \{bx_0 + kn \mid k \in \mathbb{Z}\}$ avec x_0 solution particulière

Théorème 6 : Soit $a, b \in \mathbb{N}^* \times \mathbb{Z}$.

Alors : $ax \equiv b\,[n]$ a des solutions ssi $a \wedge n \mid b$

Dans ce cas, les solutions de $ax \equiv b\,[n]$ sont $S = \left\{\frac{b}{a \wedge n} x_0 + k\frac{n}{a \wedge n} \mid k \in \mathbb{Z}\right\}$ avec x_0 solution particulière de $\frac{a}{a \wedge n} x \equiv b\left[\frac{n}{a \wedge n}\right]$.

[Rom]

X.4

2] Systèmes de congruences

Lemme 7 : Soit $(a_i)_{i=1}^r \in A^* \setminus A^\times$ deux à deux premiers entre eux

Alors : les $\left(b_j := \prod_{\substack{i=1 \\ i \neq j}}^r a_i\right)_{j=1}^r$ sont premiers entre eux

Théorème 8 : (des restes chinois) Soit $(a_i)_{i=1}^r \in A^* \setminus A^\times$ deux à deux premiers entre eux, $\left(b_j = \prod_{\substack{i=1 \\ i \neq j}}^r a_i\right)_{j=1}^r$.

Alors : l'application $\varphi : A \to \prod_{j=1}^r A/\langle a_j \rangle$, $x \mapsto (\pi_j(a))_{j=1}^r$ est un morphisme d'anneaux surjectif de noyau $\ker(\varphi) = \langle \prod a_j \rangle$ qui induit un isomorphisme d'anneaux $\overline{\varphi} : A/\langle \prod a_j \rangle \to \prod A/\langle a_j \rangle$, $\pi(x) \mapsto (\pi(x))_{j=1}^r$ d'inverse $\overline{\varphi}^{-1} : \prod A/\langle a_j \rangle \to A/\langle \prod a_i \rangle$, $(\pi_j(x_j))_{j=1}^r \mapsto \sum x_i u_i b_i$ avec $(u_i)_{i=1}^r$ telle que $\sum u_i b_i = 1$ (coefficients de Bezout).

Exemple 9 : Le système $\begin{cases} x \equiv 2\,[4] \\ x \equiv 3\,[5] \\ x \equiv 1\,[3] \end{cases}$ a pour ensemble de solutions $\{838 + 180k \mid k \in \mathbb{Z}\}$ car $1 = 1 \times 5 \times 9 + 11 \times 4 \times 9 + \underbrace{(-22)}_{\times 4 \times 5}$

II] Équations de partition d'entiers

1] Équation des 2 carrés et anneau des entiers de Gauss

Définition 10 : On note $\square = \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N},\ n = a^2 + b^2\}$.

On appelle anneau des entiers de Gauss l'ensemble :

$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$

Remarque 11 : Si $n \equiv 3\,[4]$, alors $n \notin \square$

Proposition 12 : $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Proposition 13 : $\square$ est stable par multiplication

Lemme 14 : Soit $p \in \mathbb{N}$ premier.

Alors : $p \in \square$ ssi p n'est pas irréductible dans $\mathbb{Z}[i]$

[Rom]

VIII.3

[Rom]

X.4

II.6

[Rec]

II.6 [Per]

Théorème 15 : Soit $p \in \mathbb{N}$ premier.
Alors : $p \in \Sigma_1$ ssi $p = 2$ ou $p \equiv 1 [4]$

Exemple 16 : $41 = 5^2 + 4^2$; $53 = 7^2 + 2^2$; $61 = 6^2 + 5^2$

Théorème 17 : Soit $n = \prod_{p \in \mathcal{P}} p^{v_p(n)} \in \mathbb{N} \setminus \{0;1\}$.
Alors : $n \in \Sigma_1$ ssi $\forall p \in \mathcal{P}$, $p \equiv 3 [4] \Rightarrow v_p(n)$ est pair.

2] Partition d'un entier en parts fixés

On s'intéresse à l'équation $a_1 x_1 + \dots + a_k x_k = n$ pour n, $a_1, \dots, a_k$ fixés.

Application 18 : Soit $(a_1, \dots, a_k) \in \mathbb{N}^*$ premiers entre eux et $(u_n := \mathrm{card}(\{(x_1, \dots, x_k) \in \mathbb{N}^k \mid a_1 x_1 + \dots + a_k x_k = n\}))_{n \in \mathbb{N}}$
Alors : $u_n \underset{+\infty}{\sim} \frac{1}{a_1 \times \dots \times a_k} \times \frac{n^{k-1}}{(k-1)!}$

[FGN Anz]

3] Résolubilité de l'équation de Fermat.

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

Théorème 19 : (petit théorème de Fermat) Soit $p \in \mathbb{N}$ premier
Alors : $\forall a \in \mathbb{F}_p^*$, $a^{p-1} \equiv 1 [p]$.

Application 20 : (théorème de Sophie Germain)
Soit $p \in \mathbb{N}$ premier impair tel que $q := 2p + 1$ est premier.
Alors : $\nexists (x;y;z) \in \mathbb{Z}^3 \setminus \begin{cases} xyz \not\equiv 0 [p] \\ x^p + y^p + z^p = 0 \end{cases}$

[FGN Al 1]

III] Carrés dans un corps fini

1] Symbole de Legendre

Théorème 21 : Dans $\mathbb{F}_p$, il y a $\frac{p+1}{2}$ carrés et $\frac{p-1}{2}$ non-carrés.

Théorème 22 : Les carrés dans $\mathbb{F}_p^\times$ sont les solutions de $X^{\frac{p-1}{2}} - 1 = 0$ et les non-carrés sont les solutions de $X^{\frac{p-1}{2}} + 1 = 0$.

Corollaire 23 : -1 est carré dans $\mathbb{F}_p^\times$ ssi $p \equiv 1 [4]$

Définition 24 : On dit que $k \in \mathbb{Z}$ tel que $p \nmid k$ est un résidu quadratique modulo p si $\overline{k}$ est un carré dans $\mathbb{F}_p^\times$.
On appelle symbole de Legendre de $a \in \mathbb{F}_p^\times$ dans $\mathbb{F}_p$:
$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré modulo } p \\ -1 & \text{sinon} \end{cases}$

Exemple 25 : $4^2 \equiv 1 [5]$ donc 4 est un résidu quadratique modulo 5.

Théorème 26 : (1) $\forall a \in \mathbb{F}_p^\times$, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$ dans $\mathbb{F}_p^\times$
(2) L'application $\begin{array}{ccc} \mathbb{F}_p^\times & \to & \{\pm 1\} \\ a & \mapsto & \left(\frac{a}{p}\right) \end{array}$ est l'unique morphisme non-trivial de $\mathbb{F}_p^\times$ dans $\{\pm 1\}$.

Exemple 27 : $2^{\frac{5-1}{2}} \equiv -1 [5]$ donc 2 n'est pas résidu quadratique modulo 5.

Application 28 : (théorème de Frobénius-Zolotarev) Soit p premier impair, V un $\mathbb{F}_p$-espace vectoriel de dimension n.
Alors : $\forall u \in GL(V)$, $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$

Application 29 : A partir du théorème de Frobénius-Zolotarev, on peut montrer que : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

III.5 [Rau]

XIII.6

[Plan]

2] Loi de réciprocité quadratique

Lemme 30 : $\forall a \in \mathbb{F}_p^\times$, le nombre de solutions de l'équation $ax \equiv 1$ est $\left(\frac{a}{p}\right)+1 = \begin{cases} 2 \text{ si } a \text{ est un carré modulo } p \\ 0 \text{ sinon} \end{cases}$

Théorème 31 : (loi de réciprocité quadratique) Soit $p \neq q$ deux premiers impairs.
Alors : $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$

Exemple 32 : $\left(\frac{219}{383}\right) = 1$ donc 219 est résidu quadratique modulo 383.

Remarque 33 : La loi de réciprocité quadratique donne une sorte de dualité entre les solutions $x^2 = p$ modulo q et les solutions de $x^2 + q$ modulo p.

Références :

[Rau] Mathématiques pour l'agrégation Algèbre et Géométrie – Rouvaldi – Perrin

[Per] Cours d'algèbre

[FGN An2] Exercices de mathématiques oraux X-ENS – Francinou
Analyse 2

[FGN Al1] Exercices de mathématiques oraux X-ENS – Francinou
Algèbre 1