Définition 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 sur $\mathbb{Z}^n$.

I Équations diophantiennes linéaires

1) Arithmétique dans $\mathbb{Z}$

Proposition 2. *Soient $a, b \in \mathbb{Z}$ non nuls simultanément. L'équation $ax = b$ possède une unique solution si, et seulement si $a \mid b$. Dans ce cas, cette unique solution est $x = \frac{b}{a} \in \mathbb{Z}$.*

Proposition 3 (Bézout)**.** *Soient $a_1, \dots, a_n \in \mathbb{Z}$ et $d = \text{pgcd}(a_1, \dots, a_n)$. Alors il existe $u_1, \dots, u_n \in \mathbb{Z}$ tels que $a_1u_1 + \dots + a_nu_n = d$.*

Définition 4. Soient $a_1, \dots, a_n \in \mathbb{Z}$. On dit que $a_1, \dots, a_n$ sont premiers entre eux si $\text{pgcd}(a_1, \dots, a_n) = 1$.

Théorème 5 (Bézout)**.** *$a_1, \dots, a_n \in \mathbb{Z}$ sont premiers entre eux si, et seulement si, il existe $u_1, \dots, u_n \in \mathbb{Z}$ tels que $a_1u_1 + \dots + a_nu_n = 1$.*

Lemme 6 (Gauss)**.** *Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.*

Lemme 7 (Euclide)**.** *Soit p premier. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.*

2) Équations diophantiennes de degré 1

On s'intéresse à l'équation de la forme $ax + by = c$, avec $a, b, c \in \mathbb{Z}$.

Méthode 8. *On effectue l'algorithme d'Euclide pour trouver le* pgcd *de a et b, noté d. En remontant les étapes de l'algorithme, trouver une solution de $au' + bv' = d$ puis de $au + bv = c$. Si (x_0, y_0) est une solution générale, on obtient $a(x - u_0) = b(v - y_0)$ et par le lemme de Gauss, $a \mid v - y_0$ et $b \mid u - x_0$, donc $v = y_0 + ak$ et $u = x_0 - bk$.*

Théorème 9. *Soient $a, b \in \mathbb{Z}$. L'équation $ax + by = c$ admet des solutions si, et seulement si, $d = \text{pgcd}(a, b) \mid c$. Dans ce cas, soit (x_0, y_0) une solution particulière donnée par l'identité de Bézout. L'ensemble des solutions est donné par :*

$$\left\{ \left(x_0 + k \times \frac{b}{d}, y_0 - k \times \frac{a}{d} \right) \middle| \, k \in \mathbb{Z} \right\}$$

Exemple 10. *(i) $42x + 66y = 10$ n'admet pas de solutions.*
(ii) $112x + 70y = 14$ a pour solutions les $(2 + 5k, -3 - 8k)$ pour $k \in \mathbb{Z}$.

Proposition 11. *L'équation $a_1x_1 + \dots + a_nx_n = b$ admet une solution si, et seulement si,* $\text{pgcd}(a_1, \dots, a_n) \mid b$.

II Équations modulaires

On fixe $n \geqslant 2$ et p premier. On travaille par défaut dans $\mathbb{Z}/n\mathbb{Z}$.

1) Systèmes de congruences

Méthode 12. *Pour résoudre l'équation $ax \equiv b\,[n]$, on peut résoudre dans $\mathbb{Z}$ l'équation $ax = b + kn, k \in \mathbb{Z}$, reformulée en $ax - nk = b$. On retrouve alors une équation vue dans la première partie.*

Proposition 13. *L'équation $ax \equiv b\,[n]$ admet des solutions si, et seulement si,* $\text{pgcd}(a, b) \mid b$. *En particulier, $a \in \mathbb{Z}/n\mathbb{Z}$ est inversible si, et seulement si, $a \wedge n = 1$.*

Corollaire 14. *$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.*

Théorème 15 (Restes chinois)**.** *Soient $m_1, \dots, m_k$ des entiers premiers entre eux deux à deux, et $m = m_1 \dots m_k$. Alors l'application définie par :*

$$\Phi : \left| \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z} \\ \overline{n}^m & \longmapsto & (\overline{n}^{m_1}, \dots, \overline{n}^{m_k}) \end{array} \right.$$

est un isomorphisme d'anneaux.

Exemple 16. *Résolution de systèmes de congruences :*

$$\begin{cases} x & \equiv & 2 & [3] \\ x & \equiv & 4 & [5] \end{cases} \Leftrightarrow x = 14 + 15k,\ k \in \mathbb{Z}$$

2) Carrés dans $\mathbb{Z}/p\mathbb{Z}$

Définition 17. On pose $(\mathbb{F}_q)^2 = \left\{ x^2 \in \mathbb{F}_q \,\middle|\, x \in \mathbb{F}_q \right\}$ l'ensemble des carrés de $\mathbb{F}_q$, et $\mathbb{F}_q^{\star 2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^\star$.

Proposition 18. *Si $q = p^n$, on a :*
(i) Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$
(ii) Si $p > 2$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{\star 2}| = \frac{q-1}{2}$

Proposition 19. *Si $q = p^n$ et $p > 2$, on a $x \in \mathbb{F}_q^{\star 2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.*

Corollaire 20. *Si $q = p^n$ et $p > 2$, -1 est un carré dans $\mathbb{F}_q$ si, et seulement si, q est congru à 1 modulo 4.*

Corollaire 21. *Il y a une infinité de nombres premiers de la forme $4k+1$.*

Définition 22. Soit p un premier impair et $a \in \mathbb{N}$. On définit le symbole de Legendre de a par p par :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & si \ \overline{a} \in \mathbb{F}_p^{\star 2} \\ -1 & si \ \overline{a} \notin \mathbb{F}_p^{\star 2} \\ 0 & si \ \overline{a} = 0 \end{cases}$$

Proposition 23. *Pour $x, y \in \mathbb{F}_p^\star$, on a $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.*
Le symbole de Legendre donne un morphisme $\mathbb{F}_q^\star \to \{\pm 1\}$.

Proposition 24. *Soit p un premier impair et $a \in \mathbb{N}$, alors $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p]$*

Théorème 25 (Réciprocité quadratique)**.** *Soient p et q deux premiers distincts impairs. Alors $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}}$.*

Proposition 26. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Exemple 27. $\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1$

Exemple 28. *L'équation $x^2 + 59y = 23$ n'a pas de solutions entiers.*

III Équations diophantiennes non linéaires

1) Premiers exemples

Méthode 29 (Descente infinie)**.**

(i) On suppose par l'absurde qu'il existe une solution non triviale.

(ii) On construit à partir de cette solution une autre solution plus petite.

(iii) Par récurrence, on obtient une suite décroissante infinie de solutions non triviales. Ce qui est impossible car toute suite décroissante de $\mathbb{N}$ est stationnaire.

Théorème 30. *L'équation $x^4+y^4+z^2$ n'as pas de solutions entières non triviales*

Théorème 31. *Soit (x, y, z) un triplet pythagoricien, c'est-à-dire solution de $x^2 + y^2 = z^2$. Il existe $d \in \mathbb{Z}$ et u, v premiers entre eux tels que, à permutation près, on a $x = d(u^2 - v^2)$, $y = 2duv$, $z = d(u^2 + v^2)$.*

Théorème 32. *L'équation de Fermat $x^n + y^n = z^n$ n'a pas de solutions pour $n = 4$.*

Remarque 33. *Cette équation n'a en fait pas de solution non triviale pour tout $n \geqslant 3$. Conjecture de Pierre de Fermat, prouvée par Andrew Wiles en 1995.*

Théorème 34 (Sophie Germain)**.** *Soit p un nombre premier impair tel que $2p + 1$ est premier. Si $x^p + y^p + y^p = 0$, alors $xyz \equiv 0[p]$.*

2) Réduction modulaire

Méthode 35. *On peut réduire une équation à une équation modulaire dans $\mathbb{Z}/n\mathbb{Z}$ pour trouver (ou pas) une solution.*

Exemple 36. *La résolution de $x^2 + py = z$ nous ramène à la recherche d'une racine carrée de z modulo p.*

Exemple 37. *L'équation $x^3 + 5 = 117y^3$ n'a pas de solution.*

Exemple 38. *Les équations $x^3 + y^3 + z^3 = 4$ et $x^3 + y^3 + z^3 = 5$ n'ont pas de solutions entières.*

3) L'anneau $\mathbb{Z}[i]$ des entiers de Gauss

Définition 39. On définit $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \,|\, a, b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss.

Proposition 40. $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Proposition 41. $\mathbb{Z}[i]$ *est un anneau euclidien.*

Définition 42. On note $\Sigma = \left\{n = a^2 + b^2 \,\middle|\, a, b \in \mathbb{N}\right\}$.

Lemme 43. *Soit p premier impair. Alors $p \in \Sigma$ si, et seulement si, p est réductible dans $\mathbb{Z}[i]$.*

Lemme 44. Σ *est stable par multiplication.*

Théorème 45. *Soit p premier impair. Alors $p \in \Sigma$ ssi $p \equiv 1[4]$.*

Corollaire 46 (Théorème des deux carrés)**.** *Soit $n \in \mathbb{N}*$. On le décompose en produit de facteurs premiers : $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$. Alors :*

$$n \in \Sigma \Leftrightarrow (\forall p \in \mathbb{P}, p \equiv 3[4] \Rightarrow v_p(n) \equiv 0[2])$$

Développements

— Théorème des deux carrés (40,41,43,44,45,46) [Per96]
— Loi de réciprocité quadratique (25) [Ser13]
— Théorème de Sophie Germain (34) [FGN13a]

Références

[Rom20] J.-E. Rombaldi. *Algèbre et Géométrie*. DeBoeck
[Per96] D. Perrin. *Cours d'Algèbre*. Ellipses
[Ser13] J.-P. Serre. *Cours d'Arithmétique*. PUF
[FGN13a] S. Francinou, H. Gianella, et S. Nicolas. *Oraux X-ENS Algèbre 1*. Cassini