Leçon 126. Exemples d'équations en arithmétiques.

I. Équations diophantiennes linéaires

1. Définition. Une *équation diophantienne* est la donnée d'une fonction $f\colon \mathbf{Z}^r \longrightarrow \mathbf{Z}^s$ dont on cherche ses zéros dans $\mathbf{Z}^r$, c'est-à-dire les r-uplet $x \in \mathbf{Z}^r$ vérifiant $f(x) = 0$.

I.1. Une seule équation linéaire

2. Proposition. Soient $a, b \in \mathbf{Z}$ deux entiers avec $a \neq 0$. Alors l'équation $ax = b$ admet une solution entière si et seulement si $a \mid b$.
3. Exemple. L'équation $2x = 4$ admet la solution $x = 2$.
4. Proposition. Soient $a, b, c \in \mathbf{Z}$ trois entiers avec $(a, b) \neq (0, 0)$. Alors l'équation $ax + by = c$ admet une solution entière si et seulement si $\operatorname{pgcd}(a, b) \mid c$.
5. Exemple. L'équation $6x + 4y = 10$ admet au moins une solution entière.
6. Théorème *(Bezout)*. Soient $a, b \in \mathbf{Z}$ deux entiers avec nous tous nuls. Alors il existe deux entiers $u, v \in \mathbf{Z}$ tels que $au + bv = \operatorname{pgcd}(a, b)$.
7. Théorème *(algorithme d'Euclide étendu)*. Soient $a, b \in \mathbf{Z}$ deux entiers non tous nuls. On définit les trois suites entières $(r_i)_{n\in\mathbf{N}}$, $(u_i)_{i\in\mathbf{N}}$ et $(v_i)_{i\in\mathbf{N}}$ telles que
   - $r_0 = a$ et $r_1 = b$;
   - si $r_i \neq 0$, alors
     - $u_{i+1} = u_{i-1} - qu_i$;
     - $v_{i+1} = v_{i-1} - qu_i$;

     où les entiers q et r_{i+1} sont respectivement le quotient et le reste de la division euclidienne de r_{i-1} par r_i ;
   - si $r_i = 0$, alors $r_{i+1} = 0$.

Alors il existe un plus petit entier $N \in \mathbf{N}$ tel que $r_{N+1} = 0$ et on a
$$\operatorname{pgcd}(a, b) = \pm r_N \quad \text{et} \quad r_N = au_N + bv_N.$$
8. Exemple. On a $2 = 6 \times 1 - 4 \times 1$.
9. Remarque. L'algorithme d'Euclide étendu appliqué aux entiers a et b permet de trouver une solution particulière à l'équation $ax + by = 0$.
10. Proposition. Soient $a, b, c \in \mathbf{Z}$ trois entiers avec $(a, b) \neq (0, 0)$ et $\operatorname{pgcd}(a, b) \mid c$. Soit $(x_0, y_0) \in \mathbf{Z}^2$ une solution particulière de l'équation $ax+by = c$. Alors les solutions de cette dernière sont de la forme
$$(x_0 - kb/d, y_0 + ka/d) \quad \text{avec} \quad k \in \mathbf{Z} \quad \text{et} \quad d := \operatorname{pgcd}(a, b).$$
11. Exemple. Une solution particulière de l'équation $6x+4y = 10$ est le couple $(5, -5)$, donc les solutions de cette équation s'écrivent $(5 - 2k, 3k - 5)$ avec $k \in \mathbf{Z}$.
12. Proposition. Soient $a_1, \dots, a_n \in \mathbf{Z}$ des entiers non tous nuls et $c \in \mathbf{Z}$. Alors l'équation $a_1x_1 + \cdots + a_nx_n = c$ admet une solution si et seulement si $\operatorname{pgcd}(a_1, \dots, a_n) \mid c$.

I.2. Les systèmes d'équations linéaires

13. Définition. Un *système linéaire diophantien* est un système $Ax = b$ d'inconnue $x \in \mathbf{Z}^n$ pour une matrice $A \in \mathscr{M}_{m,n}(\mathbf{Z})$ et un vecteur $b \in \mathbf{Z}^m$.
14. Proposition. Une matrice est inversible dans l'anneau $\mathscr{M}_n(\mathbf{Z})$, c'est-à-dire appartient au groupe $\mathscr{M}_n(\mathbf{Z})^\times = \mathrm{GL}_n(\mathbf{Q}) \cap \mathscr{M}_n(\mathbf{Z})$ si et seulement si son déterminant vaut ± 1.
15. Proposition. Soient $A \in \mathscr{M}_n(\mathbf{Z})$ une matrice et $b \in \mathbf{Z}^n$ un vecteur. Si $\det A = \pm 1$, alors le système $Ax = b$ admet une unique solution entière.
16. Proposition. Soient $d_1, \dots, d_r \in \mathbf{Z}^*$ deux entiers et $b := (b_1, \dots, b_n) \in \mathbf{Z}^n$ une vecteur. Alors le système $Ax = b$ avec $A := \operatorname{diag}(d_1, \dots, d_r, 0, \dots, 0)$ admet des solutions si et seulement si
$$\forall i \leqslant r,\ d_i \mid b_i \qquad \text{et} \qquad \forall i > r,\ b_i = 0.$$
17. Théorème *(forme normale de Smith)*. Soit $A \in \mathscr{M}_{m,n}(\mathbf{Z})$ une matrice. Alors elle est équivalente à une matrice $\operatorname{diag}(d_1, \dots, d_r, 0, \dots, 0)$ pour des entiers $d_1, \dots, d_r \in \mathbf{Z}$ vérifiant $d_1 \mid \cdots \mid d_r$.

II. Équations modulaires

II.1. Théorème des restes chinois et systèmes de congruences

18. Théorème *(des restes chinois)*. Soient A un anneau unitaire et $I_1, \dots, I_n \subset A$ des idéaux deux à deux étrangers ($I_i + I_j = A$ si $i \neq j$). Alors l'application
$$\left|\begin{array}{l} A \longrightarrow A/I_1 \times \cdots \times A/I_n, \\ x \longmapsto (x \mod I_1, \dots, x \mod I_n) \end{array}\right.$$
est un morphisme d'anneaux surjectif de noyau $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$. En particulier, il induit un isomorphisme d'anneaux
$$A/I_1 \cdots I_n \longrightarrow A/I_1 \times \cdots \times A/I_n.$$
19. Corollaire *(des restes chinois dans $\mathbf{Z}$)*. Soient $m_1, \dots, m_n \in \mathbf{N}^*$ des entiers deux à deux premiers entre eux et $v_1, \dots, v_n \in \mathbf{Z}$ d'autres entiers. Alors il existe une unique solution $x \in [\![0, m_1 \cdots m_n - 1]\!]$ du système
$$\forall i \in [\![1, r]\!], \qquad x \equiv v_i \mod m_i. \tag{1}$$
20. Proposition *(interpolation de Lagrange)*. En reprenant les notations précédentes, pour tout indice $i \in [\![1, r]\!]$, il existe un entier $N_i \in [\![0, m_i - 1]\!]$ tel que $N_iM_i \equiv 1 \mod m_i$ avec $M_i = m_1 \cdots m_r / m_i$. Alors l'unique solution du système (1) est l'entier
$$\sum_{i=1}^{n} v_i N_i M_i.$$
21. Exemple. On souhaite résoudre le système
$$\begin{cases} x \equiv 0 & \mod 2, \\ x \equiv 2 & \mod 3, \\ x \equiv -2 & \mod 7. \end{cases}$$
On calcul d'abord $M := 2 \times 3 \times 7 = 42$. Les entiers 2, 3 et 7 étant premiers, ce système admet une unique solution dans l'intervalle $[\![0, 41]\!]$.
   - L'élément $M_1 := M/2 = 21 \equiv 1$ est d'inverse $N_1 = 1$ dans $\mathbf{Z}/2\mathbf{Z}$.

– L'élément $M_2 := M/3 = 14 \equiv -1$ est d'inverse $N_2 = -1$ dans $\mathbf{Z}/3\mathbf{Z}$.
– L'élément $M_3 := M/7 = 6 \equiv -1$ est d'inverse $N_2 = -1$ dans $\mathbf{Z}/7\mathbf{Z}$.
Finalement, l'unique solution est $0 \times 21 \times 1 + 2 \times 14 \times (-1) - 2 \times 6 \times (-1) = -16$.

II.2. Les carrés dans les corps finis

22. Définition. Un élément x d'un corps K est un *carré* s'il existe un élément $y \in K$ tel que $x = y^2$. On note $K^2 \subset K$ l'ensemble des carrés et on pose $K^{\times 2} := K^2 \cap K^\times$.
23. Proposition. Soit q une puissance d'un nombre premier p.
– Si $p = 2$, alors $\mathbf{F}_q^{\times 2} = \mathbf{F}_q$.
– Si $p > 2$, alors $|\mathbf{F}_q^2| = (q+1)/2$ et $|\mathbf{F}_q^{\times 2}| = (q-1)/2$.
24. Exemple. Les carrés dans $\mathbf{F}_9$ sont 0, 1, 4, 9 et 7.
25. Proposition. On suppose que $p > 2$. Pour $x \in \mathbf{F}_q$, on a $x \in \mathbf{F}_q^{\times 2} \Leftrightarrow x^{(q-1)/2} = 1$.
26. Exemple. L'élément 2 est un carré dans $\mathbf{F}_7$ puisque $2^{(7-1)/2} = 2^3 = 1$, mais les éléments -1 et 3 n'en sont pas.
27. Définition. Soient p un nombre premier impair. Pour tout élément $a \in \mathbf{F}_p^\times$, son *symbole de Legendre* est l'entier

$$\left(\frac{a}{p}\right) := a^{(p-1)/2} = \begin{cases} 1 & \text{si } a \in \mathbf{F}_p^{\times 2}, \\ -1 & \text{si } a \in \mathbf{F}_p^\times \setminus \mathbf{F}_p^{\times 2}. \end{cases}$$

28. Exemple. En reprenant l'exemple précédent, on a $(\frac{2}{7}) = 1$ et $(\frac{-1}{7}) = (\frac{3}{7}) = -1$.
29. Lemme. Pour tout élément $a \in \mathbf{F}_p^\times$, on a

$$|\{x \in \mathbf{F}_p \mid ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$

D1

30. Théorème *(loi de réciprocité quadratique)*. Soient p et q deux nombres premiers impairs. Alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \times (q-1)/2}.$$

31. Proposition *(lois spéciales)*. Pour tout nombre premier impair, on a

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \qquad \text{et} \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Autrement dit,
– l'entier -1 est un carré modulo p si et seulement si $p \equiv 1 \mod 4$;
– l'entier 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \mod 8$;
32. Théorème. L'application $a \in \mathbf{F}_p^\times \longmapsto (\frac{a}{p}) \in \{\pm 1\}$ est un morphisme de groupes.
33. Exemple. Avec les trois derniers points, on trouve

$$\left(\frac{14}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{7}{23}\right) = \left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -1.$$

Par conséquent, l'entier 14 n'est pas un carré modulo 23, c'est-à-dire l'équation $x^2 = 14$ dans $\mathbf{Z}/23\mathbf{Z}$ n'admet pas de solution.

III. Méthode de résolution

III.1. Utilisation de la factorialité

34. Théorème. L'anneau $\mathbf{Z}$ est euclidien et donc factoriel.
35. Corollaire. Tout entier positif $n \geqslant 2$ s'écrit de manière unique sous la forme $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ pour des nombres premiers distincts p_i et des entiers $\alpha_i \in \mathbf{N}^*$.
36. Proposition. Les solutions entières de l'équation $x^2 + y^2 = z^2$ sont exactement les triplets de la forme

$$(2kmn, k(m^2-n^2), k(m^2+n^2)) \quad \text{ou} \quad (k(m^2-n^2), 2kmn, k(m^2+n^2))$$

pour trois entiers $k, m, n \in \mathbf{N}$ tels que $k \neq 0$ et $m > n$.
37. Corollaire. L'équation $x^4 + y^4 = z^4$ n'admet que la solution nulle.
38. Théorème. Soit $p \geqslant 3$ un nombre premier tel que le nombre $2p+1$ soit premier. Alors il n'existe pas de triplet $(x, y, z) \in \mathbf{Z}^3$ tel que D2

$$xyz \not\equiv 0 \mod p \qquad \text{et} \qquad x^p + y^p + z^p = 0.$$

III.2. Utilisation des anneaux d'entiers

39. Définition. Soit $d \in \mathbf{Z}^*$ un entier sans facteur carré. Un élément $x \in \mathbf{Q}(\sqrt{d}) \subset \mathbf{C}$ est un *entier* s'il est racine d'un polynôme unitaire $P \in \mathbf{Z}[X]$. On note $\mathcal{O}_d \subset \mathbf{Q}(\sqrt{d})$ l'ensemble des éléments entiers du corps $\mathbf{Q}(\sqrt{d})$.
40. Exemple. Le nombre d'or $\varphi := \frac{1}{2}(1+\sqrt{5})$ est un entier du corps $\mathbf{Q}(\sqrt{5})$.
41. Théorème. Soit $d \in \mathbf{Z}^*$ un entier sans facteur carré. Alors

$$\mathcal{O}_d = \begin{cases} \mathbf{Z}[\sqrt{d}] & \text{si } d \equiv 2, 3 \mod 4, \\ \mathbf{Z}[\frac{1}{2}(1+\sqrt{d})] & \text{si } d \equiv 1 \mod 4. \end{cases}$$

42. Proposition. Un élément $\varepsilon := a + b\sqrt{d} \in \mathcal{O}_d$ est inversible dans l'anneau $\mathcal{O}_d$ si et seulement si $N(\varepsilon) := a^2 - db^2 = \pm 1$.
43. Exemple. Les inverses de l'anneau $\mathbf{Z}[i]$ sont les éléments ± 1 et $\pm i$.
44. Application *(équation de Mordell)*. Soit $k \in \mathbf{Z}$. Alors l'équation $y^2 = x^3 + k$ admet une unique solution entière $(1, 0)$.
45. Théorème *(équation de Pell-Fermat)*. L'équation $x^2 - dy^2 = 1$ admet une infinité de solutions.

III.3. Un exemple : la somme de deux carrés

46. Définition. On définit l'ensemble $\Sigma := \{a^2 + b^2 \mid a, b \in \mathbf{Z}\} = \{N(z) \mid z \in \mathbf{Z}[i]\}$.
47. Exemple. On a $0, 1, 2, 4, 5 \in \Sigma$ et $3, 6, 7, 11, 12 \notin \Sigma$.
48. Proposition. L'ensemble Σ est stable par multiplication.
49. Théorème. L'anneau $\mathbf{Z}[i]$ est euclidien et donc principal.
50. Théorème. Soit p un nombre premier. Alors

$$p \in \Sigma \iff p = 2 \quad \text{ou} \quad p \equiv 1 \mod 4.$$

51. Corollaire. Un entier appartient à l'ensemble Σ si et seulement si sa valuation p-adique est paire pour tout nombre premier congrus à 3 modulo 4.

[1] Vincent Beck, Jérôme Malick et Gabriel Peyré. *Objectif Agrégation.* 2e édition. H&K, 2005.
[2] Alin Bostan et al. *Algorithmes Efficaces en Calcul Formel.* 2017.
[3] Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries.* T. Tome premier. Calvage & Mounet, 2017.
[4] Daniel Duverney. *Théorie des nombres.* Dunod, 2007.
[5] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.