P. Maurer
ENS Rennes

Leçon 226. Exemples d'équations en arithmétique.

Devs :

- Théorème des deux carrés
- Loi de réciprocité quadratique

Références :

1. Objectif Agrégation
2. Gozard, Théorie de Galois
3. Perrin, Cours d'algèbre
4. Combes, Algèbre et géométrie
5. Gourdon, Algèbre

1 Equations diophantiennes linéaires

1.1 Equations diophantiennes linéaires à deux variables

Proposition 1. *Soit $a, b \in \mathbb{Z}$. L'équation $ax = b$ admet des solutions si et seulement si $a|b$, et dans ce cas, l'unique solution est donnée par $x = \frac{b}{a}$.*

Théorème 2. *(Bézout). Soit $a, b \in \mathbb{Z}$ premiers entre eux. Il existe un couple $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$.*

Corollaire 3. *Soit $a, b \geq 2$ deux entiers premiers entre eux. L'équation $ua - vb = 1$ admet pour uniques solutions les couples $(u + kb, v + ka)$ où le couple (u, v) est donné par le théorème de Bézout et k est un entier relatif.*

Remarque 4. En pratique, on obtient u et v grâce à l'algorithme d'Euclide.

Exemple 5. L'équation $47u + 111v = 1$ a pour solutions $(26 + 111k, -11 + 47k)$ pour $k \in \mathbb{Z}$.

1.2 Méthode générale pour les équations linéaires à n variables

Cadre 6. *Soit $n, m \in \mathbb{N}$, $A \in \mathcal{M}_{m,n}(\mathbb{Z})$ et $B \in \mathcal{M}_{m,1}(\mathbb{Z})$. On souhaite résoudre l'équation $AX = B$.*

Proposition 7. *On suppose que $A = \mathrm{diag}(d_1, \dots, d_r, 0, \dots, 0)$ avec $d_1, \dots, d_r \in \mathbb{Z}$. Alors l'équation $AX = B$ a des solutions si et seulement si $d_i | b_i$ pour tout $i \in [\![1, r]\!]$ et $b_{r+1} = \cdots = b_m = 0$, et dans ce cas, les solutions sont les n-uplets $\left(\frac{b_1}{d_1}, \dots, \frac{b_r}{d_r}, k_{r+1}, \dots, k_n\right)$ avec $k_{r+1}, \dots, k_n \in \mathbb{Z}$.*

Théorème 8. *(Invariants de similitude). Soit $A \in \mathcal{M}_{m,n}(\mathbb{Z})$. Il existe une famille $(d_1, \dots, d_r)$ d'entiers non nuls tels que $d_1 | \cdots | d_r$ telle que A soit équivalente à $\mathrm{diag}(d_1, \dots, d_r, 0, \dots, 0)$.*

Remarque 9. On obtient les invariants de similitude de A de manière algorithmique, sur une méthode similaire au pivot de Gauss, en utilisant des divisions euclidiennes successives.

Proposition 10. *Soit $P \in \mathrm{GL}_m(\mathbb{Z})$ et $Q \in \mathrm{GL}_n(\mathbb{Z})$ tels que $PAQ = D$, où D est de la forme du théorème 8. Alors X est solution de $AX = B$ si et seulement si $Q^{-1}X$ est solution de $DQ^{-1}X = PB$.*

Remarque 11. Ceci donne une méthode de résolution pour les équations diophantiennes linéaires à n variables.

2 Equations modulaires

2.1 Système de congruences

Théorème 12. *(Théorème Chinois). Soient $n, m \in \mathbb{N}$ deux entiers non nuls premiers entre eux. Alors on a l'isomorphisme d'anneau $f : (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/(nm)\mathbb{Z}$.*

Remarque 13. La surjectivité de l'application f du théorème 12 prouve que si $n \wedge m = 1$, alors $\forall a, b \in \mathbb{Z} \quad \exists x \in \mathbb{Z} \quad x \equiv a[m]$ et $x \equiv b[n]$. Dans la pratique, on obtient un tel x grâce à l'algorithme d'Euclide, en cherchant u et v tels que $um + vn = 1$ puis en posant par exemple $x = a + um(b-a)$.

Remarque 14. Par récurrence, on peut généraliser le théorème Chinois : si n_1,..., n_p sont premiers entre eux deux à deux et $n = n_1 \cdots n_p$, alors $(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_p\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}$.

Exemple 15. Le système $x \equiv 2[4]$, $x \equiv 3[5]$, $x \equiv 1[9]$ a pour solutions $x = 118 + 180k$, avec $k \in \mathbb{Z}$.

2.2 Equations polynomiales et réduction modulaire

Théorème 16. *(Critère d'Eisenstein)*

Soit $P = \sum_{i=1}^{n} a_i X^i \in \mathbb{Z}[X]$, avec $n \geq 1$. On suppose qu'il existe p premier tel que :

- *p divise a_i pour tout $i \in [\![0, n-1]\!]$.*
- *p ne divise pas a_n.*
- *p^2 ne divise pas a_0.*

Alors P est irréductible dans $\mathbb{Q}[X]$.

Corollaire 17. *L'équation $a_n x^n + \cdots + a_0 = 0$ avec $a_0, \ldots, a_n \in \mathbb{Z}$ admet des solutions rationnelles de la forme p/q avec $p \wedge q = 1$ si et seulement si $p | a_0$ et $q | a_n$.*

Théorème 18. *Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, et $\overline{P}$ sa réduction sur $\mathbb{F}_p$ avec p premier, c'est-à-dire $\overline{P} = \sum_{i=0}^{n} \overline{a_i} X^i$. Si $\overline{P}$ est irréductible sur $\mathbb{F}_p$, alors P est irréductible sur $\mathbb{Z}$.*

Exemple 19. $X^3 + X + 1$ est irréductible sur $\mathbb{Z}$.

Remarque 20. La réciproque est fausse, par exemple en prenant $P = X^4 + 1$.

Remarque 21. On en déduit que si une équation de la forme $P(x) = 0$ avec $P \in \mathbb{Z}[X]$ n'a pas de solutions sur $\mathbb{F}_p$, alors elle n'en a pas non plus sur $\mathbb{Z}$. Dans le cas où elle admet des solutions sur $\mathbb{F}_p$, on regarde si ces solutions peuvent être étendues à $\mathbb{Z}$.

2.3 Résidus quadratiques

On se donne p un nombre premier.

Cadre 22. *On cherche à résoudre l'équation $ax^2 + bx + c \equiv 0[p]$, où $a, b, c \in \mathbb{Z}$. Ceci est équivalent à chercher les racines de $\overline{a} X^2 + \overline{b} X + \overline{c} \in \mathbb{F}_p[X]$. Si $p > 2$ et $\overline{a} \neq 0$, ce polynôme admet des racines si et seulement si $\Delta = \overline{b}^2 - 4\overline{a}\,\overline{c}$ est un carré α^2 dans $\mathbb{F}_p$. Si tel est le cas, l'intégrité de $\mathbb{F}_p$ assure l'existence de deux racines, α et $-\alpha$. On se pose alors la question de caractériser les carrés dans $\mathbb{F}_p$.*

Notation 23. *On pose $\mathbb{F}_p^2 := \{y \in \mathbb{F}_p : \exists x \in \mathbb{F}_p,\ y = x^2\}$, et $\mathbb{F}_p^{*2} := \mathbb{F}_p^* \cap \mathbb{F}_p^2$.*

Proposition 24. *Si $p = 2$, on a $\mathbb{F}_p^2 = \mathbb{F}_p$. Si $p > 2$, on a $|\mathbb{F}_p^2| = \frac{q+1}{2}$ et $|\mathbb{F}_p^{*2}| = \frac{q-1}{2}$.*

Proposition 25. *On suppose $p > 2$ et on se donne $a \in \mathbb{F}_p^*$. Alors*

$$a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \end{cases}.$$

Définition 26. *On définit le symbole de Legendre pour $p > 2$ et $a \in \mathbb{F}_p$ par*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^*, \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^*, \\ 0 & \text{si } a = 0. \end{cases}$$

Remarque 27. D'après ce qui précède, pour $a \neq 0$ on a donc $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$. En particulier, le symbole de Legendre est multiplicatif, au sens où $\left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Proposition 28. *Soit p un nombre premier impair et a un élément de $\mathbb{F}_p^*$. On a*

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

Développement 1 :

Théorème 29. *(Loi de réciprocité quadratique)*

Soit p et q deux nombres premiers impairs distincts. Alors on a

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

Exemple 30. Calcul du symbol de Legendre :
$\left(\frac{23}{59}\right) = (-1)^{11.29}\left(\frac{59}{23}\right) = -\left(\frac{13}{23}\right) = \cdots = \left(\frac{2}{3}\right) = -1.$

Lemme 31. *Pour tout nombre premier p impair, 8 divise p^2-1.*

Proposition 32. *Pour tout nombre premier p impair, on a $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.*

3 Méthodes de résolution

3.1 Descente infinie

Principe 33. *On cherche à démontrer qu'une équation n'a pas de solution. 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 une fonction $\varphi: \mathbb{Z}^n \to \mathbb{N}$ donnée, et une solution $(x_1,\dots,x_n) \in \mathbb{Z}^n$, il existe une autre solution $(x'_1,\dots,x'_n)$ telle que $\varphi(x'_1,\dots,x'_n) < \varphi(x_1,\dots,x_n)$. Par récurrence, on obtient donc une suite (infinie) $(\varphi(x_1^{(m)},\dots,x_n^{(m)}))_{m\in\mathbb{N}}$ strictement décroissante, ce qui est absurde.*

Théorème 34. *(Fermat). 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 35. *(Fermat-Wiles, Admis bien sûr). L'équation $x^n+y^n=z^n$ pour $n \geq 2$ n'admet pas de solution non triviale.*

3.2 Une méthode géométrique

Proposition 36. *Résoudre l'équation $x^2+y^2=z^2$ pour $(x,y,z) \in \mathbb{Z}^3$ revient à chercher les $(X,Y) \in \mathbb{Q}^2$ tels que $X^2+Y^2=1$.*

Théorème 37. *(Paramétrisation de $\mathbb{U}$)*
L'application $\varphi: t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ est une bijection de $\mathbb{R}$ vers $\mathbb{U}\setminus\{(-1,0)\}$. Elle s'étend en une bijection de $\overline{\mathbb{R}}$ vers $\mathbb{U}$ en posant $\varphi(\infty) = (-1,0)$.

Proposition 38. *Les points de $\mathbb{U}\setminus\{(-1,0)\}$ à coordonnées rationnelles s'écrivent sous la forme $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ avec $t \in \mathbb{Q}$.*

Théorème 39. *Les solutions entières de $x^2+y^2=z^2$ sont de la forme $(u^2-v^2, 2uv, u^2+v^2)$.*

3.3 Utilisation des entiers de Gauss

Définition 40. *On note $\mathbb{Z}[i] := \{a+ib : a \in \mathbb{Z} \text{ et } b \in \mathbb{Z}\}$ 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 : $\forall z, z' \in \mathbb{Z}[i]$, $N(zz') = N(z)N(z')$.*

Définition 41. *On note $\Sigma := \{n \in \mathbb{Z} : \exists a,b \in \mathbb{Z} \quad n = a^2+b^2\}$ l'ensemble des entiers qui s'écrivent comme somme de deux carrés.*

Proposition 42. *$\mathbb{Z}[i]$ est euclidien pour l'application N, donc principal.*

Lemme 43. *L'anneau $\mathbb{Z}[i]^\times$ des inversibles de $\mathbb{Z}[i]$ est $\{\pm 1, \pm i\}$.*

Lemme 44. *Soit p un nombre premier impair.*
On a l'équivalence $p \in \Sigma \iff p$ est réductible dans $\mathbb{Z}[i]$.

Lemme 45. *Σ est stable par multiplication.*

Développement 2 :

Théorème 46. *Soit p un nombre premier impair. Alors $p \in \Sigma \iff p \equiv 1[4]$.*