126

Exemples d'équations en arithmétiques

[Lamartin classique] p. 336

[Gourdon Algèbre]

Idée: Résoudre des équations sur $\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$

(I) Equations linéaires et arithmétique

1) Equations diophantiennes linéaires (sur $\mathbb{Z}$)

Def 1: Soient $a, b \in \mathbb{Z}$, on dit que a divise b s'il existe $n \in \mathbb{Z}$ tel que $b = an$
on note $a \mid b$ (dans le cas contraire $a \nmid b$)

Prop 2: Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que
$a = bq + r$ et $0 \leq r < b$

Def 3: Soient $a_1, \dots, a_n \in \mathbb{Z}$. Il existe un unique $d \in \mathbb{N}$ tel que $a_1\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$, on appelle d le pgcd de $a_1 \dots a_n$ noté $\text{pgcd}(a_1, \dots, a_n)$

Def 4: Si $\text{pgcd}(a_1 \dots a_n) = 1$ on dit que les a_i sont premiers entre eux

Thm 5: Des entiers $a_1, \dots, a_n$ dans leur ensemble SSi il existe des entiers $u_1 \dots u_n$ tels que $\sum_{i=1}^{n} a_i u_i = 1$

Ex 6: 12 et 35 sont premiers entre eux
et $3 \times 12 - 35 = 1$

Rmq 7: L'algorithme d'Euclide qui utilise des divisions euclidiennes (Prop 2) successives permet de trouver le pgcd de deux nbrs et les coefficients de Bézout (Thm 5)

Prop 8: L'équation diophantienne linéaire $ax + by = c$ admet un solution SSi $\text{pgcd}(a,b) \mid c$

Méthode 9: Pour trouver les solutions on divise a et b par $d = \text{pgcd}(a,b)$, on a $au + bv = 1$ (Bézout) puis $auc' + bvc' = c'$, on a une solution particulière puisque $aX + bY = 0$ admet comme solution $-bk, ak$ $k \in \mathbb{Z}$ on a finalement $uc' - bk$ et $vc' + ak$, $k \in \mathbb{Z}$ comme ensemble de solutions.
$c' = c/\text{pgcd}(a,b)$.

Ex 10: $35x + 11y = 149$ admet comme solutions
$x = -745 + 11k$ $y = 2384 - 35k$ $k \in \mathbb{Z}$
$6x + 15y = 56$ n'a pas de solution.

Thm 11: Soit $A \in \mathcal{M}_{n,m}(\mathbb{Z})$ $n, m \geq 0$
le système $AX = 0$ admet une solution dans $\mathbb{N}^m$ SSi $0_{\mathbb{R}^n} \in \text{Conv}(A_1, \dots A_m)$ où A_i sont les colonnes de A.

[DEV]

2) Equations linéaires aux congruences (sur $\mathbb{Z}/n\mathbb{Z}$)

Def 12: On appelle équation linéaire aux congruences une équation du type $ax \equiv b\ [p]$
où x est l'inconnue et a, b, p sont des entiers connus

Thm 13: $ax \equiv 1\ [n]$ admet une solution $a, n \geq 2$
SSi a et n sont premiers entre eux.

Ex 14: $3x \equiv 1\ [4]$ admet pour solution $x \equiv 3\ [4]$
$6x \equiv 1\ [9]$ n'admet pas de solution.

Thm 15 (chinois des restes): Soient $m_1, \dots m_r$ strictement positifs et premiers entre eux 2 à 2.
Alors $\begin{cases} x \equiv a_1\ [m_1] \\ \vdots \\ x \equiv a_r\ [m_r] \end{cases}$ admet une unique solution x modulo $M = \prod_{i=1}^{r} m_i$
qui est $x \equiv a_1 M_1 y_1 + \dots + a_r \Pi_r y_r$
$M_i = M/m_i$ $y_i \Pi_i \equiv 1\ [m_i]$

Ex 16: $x \equiv 1\ [2]$
$x \equiv 2\ [3]$ a pour solution $x \equiv 29\ [30]$
$x \equiv 4\ [5]$

[Lamartin modulaire] p 163

II Méthodes plus poussées

1) Réduction modulaire

Thrm 17 : Si une équation linéaire admet une solution sur $\mathbb{Z}$, alors en plongeant tous les coefficients dans $\mathbb{Z}/n\mathbb{Z}$, l'équation a une solution dans $\mathbb{Z}/n\mathbb{Z}$ $\forall n \in \mathbb{Z}$

Appli 18 : Si une équation (E) n'a pas de solution dans $\mathbb{Z}/n\mathbb{Z}$, alors elle n'en a pas dans $\mathbb{Z}$.

Ex 19 : $3x+6y=5$ n'a pas de solution car modulo 3 on a $0 \neq 2$

2) Utilisation de l'analyse

Idée 20 : Pour certaines équations (E), on peut les résoudre sur $\mathbb{R}$ explicitement, si aucune solution n'est entière alors l'équation (E) n'admet pas de solution sur $\mathbb{Z}$.

Ex 21 : $x^2+3x=4$ n'admet pas de solution car les solutions sont $\frac{-3\pm\sqrt{17}}{2}$

solution de $a^b=b^a$ $a \neq b$ [FGNAlg1]

III L'équation de Fermat

But 22 Résoudre $x^n+y^n=z^n$

Def 23 : On dit que $(a,b,c) \in \mathbb{Z}^3$ est un triplet pythagoricien si $a^2+b^2=c^2$
si a,b,c sont premiers entre eux, on dit que le triplet est irréductible

Ex 24 : $(6,8,10)$ est un triplet pythagoricien
$(5,12,13)$ est un triplet pythagoricien irréductible

[Hindry] p.81

Thrm 25 : Si m et n sont deux entiers premiers entre eux et de parités distinctes, alors
$(2mn,\ m^2-n^2,\ m^2+n^2)$ est pythagoricien
Réciproquement, tout triplet pythagoricien irréductible (a,b,c) peut être décomposé sous la forme
$a=m^2-n^2 \quad b=2mn \quad c=m^2+n^2$

Ex 26 : pour $(5,12,13)$ on a $m=3$ et $n=2$

Principe 27 : "Descente infinie" de Fermat
si (x,y,z) vérifie $x^4+y^4=z^2$ avec $xyz \neq 0$
alors il existe (x_1,y_1,z_1) une autre solution avec $z_1 < z$
ABSURDE car les suites décroissantes de $\mathbb{N}$ stationnent

[Lamotte classique]

Thrm 28 : L'équation $x^4+y^4=z^2$ n'a pas de solutions entières avec $xyz \neq 0$

Corollaire 29 : L'équation $x^4+y^4=z^n$ n'a pas de solutions entières avec $xyz \neq 0$.

Thrm 30 (Fermat, Wiles) (admis) pour tout $n \geqslant 3$ l'équation $x^n+y^n=z^n$ n'a pas de solution entières avec $xyz \neq 0$

Thrm 31 : (Fermat modulaire) pour tout $r \in \mathbb{N}^*$, il existe un rang n tel que pour tout p premier supérieur à n
$x^r+y^r=z^r$ a une solution non triviale dans $\mathbb{Z}/p\mathbb{Z}$

DEV 1

[Landmo Robillse]

IV Les carrés de $\mathbb{F}_p$

But 32 : Résoudre $x^2+py=a$

Prop 33 : Soit $\mathbb{K}$ un corps de cardinal fini.
Alors la caractéristique de $\mathbb{K}$ est un nbr premier p
(générateur du noyau de $\mathbb{Z} \to \mathbb{K}$, $n \mapsto \underbrace{1+\dots+1}_{n \text{ fois}}$)

Prop 34 : Un corps fini est de cardinal p^n pour une puissance d'un nombre premier.

Prop 35 : Si p est un nombre premier, $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$

Question 36 : quels sont les carrés de $\mathbb{F}_p$? (pour p premier impair)

Prop 37 : Si p premier impair, on a
x est un carré de $\mathbb{F}_p^\times$ SSi $x^{\frac{p-1}{2}} = 1$

Def 38 : On définit le symbole de Legendre pour $a \in \mathbb{Z}$ et p premier comme

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a \text{ est divisible par } p \\ 1 \text{ si } a \text{ est un carré de } \mathbb{F}_p \\ -1 \text{ sinon} \end{cases}$$

Corollaire 39 : $\left(\frac{a}{p}\right) = 1$ SSi $a^{\frac{p-1}{2}} = 1$

Prop 40 : $\left(\frac{-1}{p}\right) = 1$ SSi $p \equiv 1 [4]$

Corollaire 41 : un nombre premier p est somme de 2 carrés
SSi $p = 2$ ou $p \equiv 1 [4]$.

Prop 42 : pour tout a, b entiers, p premier on a

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \; ; \; \left(\frac{1}{p}\right) = 1 \; ; \; \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Thm 43 : Loi de Réciprocité quadratique
Si p, q premiers distincts impairs, on a

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}$$

DEV 2

[Perrin] [Sauvageot]

[Stewart Tall] p.63

II Théorie algébrique des nombres

But 44 : Résoudre $x^2 - d y^2 = \pm 1$ (Pells Fermat)

Def 45 : Un corps de nombre est une extension finie sur $\mathbb{Q}$

Ex 46 : $\mathbb{Q}(\sqrt[3]{2})$ est un corps de nombre
$\mathbb{Q}(\pi)$ ne l'est pas.

Def 47 : Un corps quadratique est un corps de nombre de degré 2.

Ex 48 : $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$ est un corps quadratique

Prop 49 : Un corps quadratique K peut toujours s'écrire comme $\mathbb{Q}(\sqrt{d})$ où d n'a pas de facteurs carrés ($d \in \mathbb{Z}$)

Def 50 : Un anneau d'entiers d'un corps de nombres K sont les éléments de K qui sont solution d'un polynôme unitaire à coefficients entiers. On le note $\mathcal{O}_K$

Ex 51 : $\phi = \frac{1+\sqrt{5}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ car $\phi^2 - \phi - 1 = 0$ et $\phi \in \mathbb{Q}(\sqrt{5})$

Thm 52 : Si $d \in \mathbb{Z}$ sans facteurs carrés
si $d \neq 1 [4]$ $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$
si $d \equiv 1 [4]$ $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$

Def 53 : On définit $N(a + b\sqrt{d}) = a^2 - db^2$
pour $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$

Ex 54 : $N(1 + 2\sqrt{3}) = 1 - 3 \times 4 = -11$
$N(2 - \sqrt{-5}) = 4 + 5 \times 1 = 9$

Prop 55 : Les inversibles de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ sont les éléments $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ tels que $N(\alpha) = \pm 1$

Thm 56 (admis) : Si $d > 0$ sans carré, il existe $(x_n, y_n) \in \mathbb{N}^* \times \mathbb{N}^*$ à l'équation $x^2 - dy^2 = \pm 1$ telle que toute solution $x_n + \sqrt{d} y_n$ s'écrivant $\pm(x_1 + \sqrt{d} y_1)^n$.