Exemples d'équations en arithmétique.

126

# I - Équations de degré 1

## A - Équations diophantiennes

**Prop 1** : Soit $(a,b)\in\mathbb{Z}^2$. L'équation $ax=b$ admet une solution si, et seulement si $a\mid b$. Le cas échéant, son unique solution est $x=b/a$

[Bu 84] **Thm 2** (de Bézout) : $\forall (a,b)\in\mathbb{Z}^2$, $(\exists (u,v)\in\mathbb{Z}^2 : au+bv=1) \iff a\wedge b=1$

[Bu 85] **Thm 3** (de Gauss) : $\forall (a,b,c)\in\mathbb{Z}^3$, $\begin{cases} a\mid bc \\ a\wedge b=1 \end{cases} \Rightarrow a\mid c$.

[Bu 86] **Appli 4** : Résolution dans $\mathbb{Z}^2$ de $ax+by=c$, $(a,b,c)\in\mathbb{Z}^3$ :

- Si $a\wedge b\nmid c$, alors l'équation n'a pas de solution
- Sinon, sans perte de généralité, on peut remplacer $a,b,c$ par $\frac{a}{a\wedge b}$, $\frac{b}{a\wedge b}$ et $\frac{c}{a\wedge b}$.
  - On trouve $(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1$ (avec l'algorithme d'Euclide).
  - Si $ax+by=c$, alors $ax+by=acu+bcv$, donc $a\mid b(cv-y)$, mais $a\wedge b=1$ donc $a\mid cv-y$, donc $\exists k\in\mathbb{Z}$ : $y=cv-ak$.
  - On injecte $y$ dans $ax+by=c$.

[Go 12] **Ex 5** : $\{(x,y)\in\mathbb{Z}^2 \mid 47x+111y=1\} = \{(26+111k, 47k-11)\}_{k\in\mathbb{Z}}$.

[Gu 163] **Def 6** : Soit $M\in\mathcal{M}_{n,m}(\mathbb{Z})$. On dit que $M$ est sous forme normale d'Hermite si elle est sous la forme :

$$\begin{pmatrix} 0\cdots 0 & p_1 & * & \cdots & * & + & * & \cdots & * & + \\ & & & & p_2 & * & \cdots & * & + & \\ & & & & & & p_3 & \cdots & & \\ & & & & & & & & \cdots + & * \cdots * \\ & & & & & & & & p_r & * \cdots * \\ & & & & & & & & & 0 \\ & & & & & & & & & \vdots \\ & & & & & & & & & 0 \end{pmatrix}$$

où les pivots $p_i$ sont $>0$, et les coefficients au-dessus de chaque pivot sont $\geq 0$ et inférieurs au pivot.

[Gu 164] **Thm 7** : Il existe $P\in GL_n(\mathbb{Z})$ telle que $PM$ est sous forme normale de Hermite.

**Appli 8** : Résolution d'un système linéaire d'équations diophantiennes : on se ramène à résoudre 1 équation, les autres se déduisant de celle-ci par propagation.

Cas d'une seule équation : $(a_1 \cdots a_n)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = b$ :

- Si $a_1\wedge\cdots\wedge a_n \nmid b$, alors il n'y a pas de solution.
- Sinon, quitte à diviser par $a_1\wedge\cdots\wedge a_n$, supposons que $a_1\wedge\cdots\wedge a_n=1$.
  - De l'algorithme d'Euclide, on déduit $P\in GL_n(\mathbb{Z})$ telle que $P\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.
  - De là, $(a_1 \cdots a_n)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = b \iff (1\,0\cdots 0)\begin{pmatrix} \tilde{x}_1 \\ \vdots \\ \tilde{x}_n \end{pmatrix} = b \iff \tilde{x}_1 = b$ où $\begin{pmatrix} \tilde{x}_1 \\ \vdots \\ \tilde{x}_n \end{pmatrix} = P^{-1}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.
  - Ainsi, $\{{}^t(x_1 \cdots x_n)\in\mathbb{Z}^n \mid \sum_{k=1}^{n} a_k x_k = b\} = \{P\,{}^t(b\ \tilde{x}_2 \cdots \tilde{x}_n) : (\tilde{x}_2 \cdots \tilde{x}_n)\in\mathbb{Z}^{n-1}\}$.

## B - Systèmes de congruence

[Rb 283-290] [Bu 87]

**Prop 9** : Soit $(a,b,n)\in\mathbb{Z}^3$. L'équation $ax\equiv b\ [n]$ a des solutions si, et seulement si $a\wedge b\mid n$.

[Bu ~87]

**Rq 10** : L'équation $ax\equiv b\ [n]$ est une réécriture de $ax+ny=b$, dans laquelle la valeur de $y$ ne nous intéresse pas.

[Rb 285]

**Thm 11** (des restes chinois) : Soit $(a_1,\dots,a_n)\in(\mathbb{N}_{\geq 2})^d$. Les entiers $a_1,\dots,a_d$ sont deux premiers entre eux si, et seulement si les anneaux $\mathbb{Z}/a_1\mathbb{Z}\times\cdots\times\mathbb{Z}/a_d\mathbb{Z}$ et $\mathbb{Z}/a_1\cdots a_d\mathbb{Z}$ sont isomorphes. Le cas échéant, il existe $(u_1,\dots,u_d)\in\mathbb{Z}^d$ tel que $1=\sum_{k=1}^{d} u_i b_i$, où pour tout $i\in[\![1,d]\!]$, $b_i = (a_1\cdots a_d)/a_i$. L'application :

$$\bar{\varphi} : \mathbb{Z}/a_1\cdots a_d\mathbb{Z} \longrightarrow \mathbb{Z}/a_1\mathbb{Z}\times\cdots\times\mathbb{Z}/a_d\mathbb{Z}$$

$$x \bmod a_1\cdots a_d \longmapsto (x \bmod a_1, \dots, x \bmod a_d)$$

est alors un isomorphisme d'anneau dont la réciproque est :

$$\bar{\varphi} : \mathbb{Z}/a_1\mathbb{Z}\times\cdots\times\mathbb{Z}/a_d\mathbb{Z} \longrightarrow \mathbb{Z}/a_1\cdots a_d\mathbb{Z}$$

$$(x_1 \bmod a_1, \dots, x_d \bmod a_d) \longmapsto \sum_{k=1}^{d} u_k b_k x_k \bmod a_1\cdots a_d$$

[Rb] 291 **Ex 10** : $\{x \in \mathbb{Z} \mid x \equiv 2\ [4],\ x \equiv 3\ [5],\ x \equiv 1\ [9]\} = 118 + 180\mathbb{Z}$

## II - Équations de degré supérieur

### A - Carrés dans les corps finis

Soient $p$ un nombre premier impair, $r \in \mathbb{N}^*$ et $q = p^r$. On pose $c : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $x \longmapsto x^2$ et $\ell : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $x \longmapsto x^{\frac{q-1}{2}}$.

**Prop 11** : $\mathrm{Im}(\ell) = \mathrm{Ker}(c) = \{\pm 1\}$ et $\mathrm{Ker}(\ell) = \mathrm{Im}(c) = \{x^2 : x \in \mathbb{F}_q^*\}$.

[P] 75 **Cor 12** (critère d'EULER) : $x \in \mathbb{F}_q^*$ est un carré *si, et seulement si* $x^{\frac{q-1}{2}} = 1$

[P] 74 **Cor 13** : Il y a $\frac{q-1}{2}$ carrés inversibles dans $\mathbb{F}_q$ (et $\frac{q+1}{2}$ carrés).

[P] 74 **Prop 14** : Tous les éléments de $\mathbb{F}_{2^r}$ sont des carrés.

[P] 75 **Prop 15** : $-1$ est un carré dans $\mathbb{F}_p$ *si, et seulement si* $p \equiv 1\ [4]$.

[Rb] 428 **Def 16** : Le *symbole de* LEGENDRE de $a \in \mathbb{Z}$ modulo $p$ est :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \in p\mathbb{Z} \\ 1 & \text{si } a \text{ est un carré inversible modulo } p \\ -1 & \text{sinon} \end{cases}$$

[Rb] 428 **Prop 17** : $\forall a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$. En particulier, $\left(\frac{\cdot}{p}\right)$ est un morphisme du groupe $\mathbb{F}_p^*$.

**Prop 18** : Soit $a \in \mathbb{F}_p^*$. L'équation de $ax^2 = 1$ a $1 + \left(\frac{a}{p}\right)$ solutions dans $\mathbb{F}_p$.

[Rb] 431-434 **Thm 19** (loi de réciprocité quadratique) : Soient $p$ et $q$ deux nombres premiers impairs distincts.

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

**Appli 20** : $\left(\frac{12}{23}\right) = \left(\frac{3}{23}\right)\left(\frac{2^2}{23}\right) = \left(\frac{23}{3}\right)(-1)^{11 \cdot 1} \cdot 1 = -\left(\frac{2}{3}\right) = 1$ donc 12 est un carré modulo 23.

**Prop 21** : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

**Prop 22** : Soit $(a,b,c) \in \mathbb{F}_q^3$ avec $a \neq 0$. L'équation $ax^2 + bx + c = 0$ dans $\mathbb{F}_q$ a des solutions *si, et seulement si* $b^2 - 4ac$ est un carré dans $\mathbb{F}_q$. Le cas échéant, si $\delta \in \mathbb{F}_p$ vérifie $\delta^2 = b^2 - 4ac$, alors les solutions de cette équation sont $\frac{-b \pm \delta}{2a}$.

**Rq 23** : Dans $\mathbb{F}_{2^r}$, l'équation $ax^2 + bx + c = 0$ est bien plus difficile à résoudre, en dehors des cas triviaux !

**Ex 24** : $x^2 + 4x + 1 = 0$ a des solutions dans $\mathbb{Z}/23\mathbb{Z}$. Pour les trouver, il faut déterminer une racine carrée de 12 (difficile...)

### B - Équations diophantiennes

**Prop 25** : Le critère d'EISENSTEIN ou la réduction dans un corps fini permettent de détecter des équations polynomiales diophantiennes sans solutions.

**Ex 26** : Équations de MORDELL

- $\{(x,y) \in \mathbb{Z}^2 \mid x^3 = y^2 + 1\} = \{(1,0)\}$

  ↳ étude dans $\mathbb{Z}[i]$ (euclidien) en écrivant $y^2 + 1 = (y+i)(y-i)$

- $\{(x,y) \in \mathbb{Z}^2 \mid x^3 = y^2 + 2\} = \{(3,5),(3,-5)\}$ [C] 193

  ↳ étude dans $\mathbb{Z}[i\sqrt{2}]$ (euclidien) en écrivant $y^2 + 2 = (y + i\sqrt{2})(y - i\sqrt{2})$

**Ex 27** : Équation de FERMAT pour $n = 3$

On ramène l'étude à $\mathbb{Z}[j] = \mathbb{Z} + \mathbb{Z}j = \mathrm{eval}_j(\mathbb{Z}[X]) \simeq \frac{\mathbb{Z}[X]}{\langle X^2 + X + 1 \rangle}$

($j = e^{\frac{2i\pi}{3}} = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$) en écrivant $x^3 + y^3 = (x+y)(x+jy)(x+j^2y)$

**Rq 28** : $\mathbb{Z}[j]$ est euclidien pour $|.|^2$.

[Rb] 138 [C] 309

**Thm 29** (de WILES-FERMAT) : $\forall n \geqslant 3$, $x^n + y^n = z^n$ n'admet pas de solution non triviale.

**Thm 30** (équations de PELL-FERMAT) : Soit $d \in \mathbb{Z}$. L'équation $x^2 - dy^2 = 1$ admet des solutions non triviales si, et seulement si $d > 0$ et $n$ n'est pas un carré. Le cas échéant, soit $(x_0, y_0)$ une solution avec $x_0 > 1$ minimal. Toutes les solutions sont les couples $(x, y)$ tels que $\exists k \in \mathbb{Z} : x + y\sqrt{d} = \pm (x_0 + y_0\sqrt{d})^k$.

[P] 56
[Rb] 269

**Thm 31** (des deux carrés de FERMAT) : Soit $E = \{n \in \mathbb{N}^* \mid \exists (x,y) \in \mathbb{N}^2 : n = x^2 + y^2\}$.

$n \in E \iff \forall p \in \mathcal{P}, p \equiv 3 [4] \Rightarrow v_p(n)$ pair DEV 1

Autrement dit, l'équation $x^2 + y^2 = n$ a des solutions si, et seulement si $n$ est premier.

## C - Une équation célèbre en arithmétique polynômiale DEV 2

[Rb] 404
([FGN] 179)

**Thm 32** (de LIOUVILLE) : Soit $K$ un corps de caractéristique nulle. L'équation $P^n + Q^n + R^n$ n'admet pas de solution non triviale dans $K[X]$ dès que $n \geqslant 3$.

**Rq 33** : Cela illustre une similitude et une différence entre l'arithmétique entière et l'arithmétique polynomiale : le résultat est le même, mais la preuve est nettement plus simple pour les polynômes !

## RÉFÉRENCES


[Bu] Burg
[Go] Gourdon
[Gu] Guin
[Rb] Rombaldi
[P] Perrin
[C] Carnets de voyage en Algébrie