126

Exemples d'équations en arithmétique.

Nt : $a \mid b$ signifie a divise b. $a \wedge b$ signifie $\operatorname{pgcd}(a,b)$. $a \vee b$ signifie $\operatorname{ppcm}(a,b)$.

I) Méthodes pour les équations linéaires.

1) Équations linéaires dans $\mathbb{Z}$.

<u>Thm 1</u> : (Bézout) Soient $a, b \in \mathbb{Z}$. Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b$.

<u>Rq 2</u> : La preuve est construite autour de l'algorithme d'Euclide étendu décrit en annexe.

<u>Lemme 3</u> : (Gauss) Soient $a, b, c \in \mathbb{Z}$ tels que $a \wedge b = 1$. Si $a \mid bc$ alors $a \mid c$.

<u>Thm 4</u> : Soient $(a, b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$, $c \in \mathbb{Z}$. L'équation diophantienne d'inconnues $x, y \in \mathbb{Z}$ $ax + by = c$ admet au moins une solution si et seulement si $a \wedge b \mid c$. Une solution est alors $\frac{c}{a \wedge b}(u, v)$ avec les notations du théorème 1.
Si (x_0, y_0) est une solution particulière, alors l'ensemble des solutions est $\left\{\left(x_0 + \frac{kb}{a \wedge b}, y_0 - \frac{ka}{a \wedge b}\right), k \in \mathbb{Z}\right\}$.

<u>Ex 5</u> : $12x + 8y = 28$ admet pour ensemble de solutions $\{(1+2k, 2-3k), k \in \mathbb{Z}\}$.

2) Systèmes de congruences.

<u>Thm 6</u> : Soient $m, n \in \mathbb{N}^*$, $a, b \in \mathbb{Z}$. Le système d'inconnue $x \in \mathbb{Z}$ $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ admet au moins une solution si et seulement si $a \equiv b \pmod{m \wedge n}$.
Si x_0 est une solution particulière, alors l'ensemble des solutions est $\{x \in \mathbb{Z}, x \equiv x_0 \pmod{m \vee n}\}$.

<u>Rq 7</u> : Si $a - b = c(m \wedge n)$ et $mu + nv = m \wedge n$ (Bézout) alors $nvc + b$ est une solution.

<u>Cor 8</u> : (restes chinois) Soit $k \in \mathbb{N}^*$. Soient $a_1, \dots, a_k \in \mathbb{Z}$. Soient $m_1, \dots, m_k \in \mathbb{N}^*$ tels que : $\forall i \neq j$ $m_i \wedge m_j = 1$. Le système d'inconnue $x \in \mathbb{Z}$ $\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$ admet des solutions, et si x_0 est une solution particulière, alors l'ensemble des solutions est $\{x \in \mathbb{Z}, x \equiv x_0 \pmod{m_1 \dots m_k}\}$.

<u>Rq 9</u> : On peut construire une solution à $\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_\ell \pmod{m_\ell} \end{cases}$ grâce à une solution à $\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_{\ell-1} \pmod{m_{\ell-1}} \end{cases}$ et à la remarque 7.

<u>Ex 10</u> : $\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases}$ admet pour ensemble de solutions $\{x \in \mathbb{Z}, x \equiv 18 \pmod{35}\}$.

II) Autres méthodes élémentaires.

1) Méthodes arithmétiques.

Soit $n \in \mathbb{N} \setminus \{0,1\}$. Notons $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ le morphisme surjectif canonique. Soit $k \in \mathbb{N}^*$. Soit $f : \mathbb{Z}^k \to \mathbb{Z}$.
Si $f(x_1, \dots, x_k) = 0$ alors $\pi(f(x_1, \dots, x_k)) = 0$. Par contraposition, si $\pi \circ f$ n'a pas de zéro dans $\mathbb{Z}^k$ alors f n'a pas de zéro dans $\mathbb{Z}^k$.

Ex 11: i) $x^2+3y=5$ (réduction modulo 3)

ii) $x^2+(x+1)^2=2y$ (réduction modulo 2)

iii) $3^a+1=5^b+7^c$ (réduction modulo 3, on est ramené à $a=0$, et donc à $2=5^b+7^c$. On obtient $a=b=c=0$ qui conviennent)

Thm 12: Les solutions de l'équation $x^2+y^2=z^2$ où $(x,y,z)\in\mathbb{N}^3$ de pgcd 1 sont les triplets $(p^2-q^2, 2pq, p^2+q^2)$ où $(p,q)\in\mathbb{N}^2$ avec $\mathrm{pgcd}(p,q)=1$ et $p>q$ ainsi que les triplets $(2pq, p^2-q^2, p^2+q^2)$ où p et q vérifient les mêmes conditions.

Cor 13: Les solutions de l'équation $x^2+y^2=z^2$ où $(x,y,z)\in\mathbb{Z}^3$ sont les triplets $(\varepsilon_1 a(p^2-q^2), \varepsilon_2 a2pq, \varepsilon_3(p^2+q^2))$ et $(\varepsilon_1 a(2pq), a\varepsilon_2(p^2-q^2), a\,\varepsilon_3(p^2+q^2))$ où $a\in\mathbb{N}$, $(\varepsilon_1,\varepsilon_2,\varepsilon_3)\in\{-1;1\}^3$ et $(p,q)\in\mathbb{N}^2$ avec $p>q$ et $\mathrm{pgcd}(p,q)=1$.

On va à présent utiliser la méthode de la descente de Fermat qui repose sur le fait que toute partie non vide de $\mathbb{N}$ admet un minimum.

Ex 14: L'équation $x^3+2y^3=4z^3$ n'a pas de solution sur $\mathbb{Z}^3\setminus\{(0;0;0)\}$

Thm 15: L'équation $x^4+y^4=z^2$ d'inconnue $(x,y,z)\in(\mathbb{Z}\setminus\{0\})^3$ n'a pas de solution

Cor 16: L'équation $x^4+y^4=z^4$ n'a pas de solution dans $(\mathbb{Z}\setminus\{0\})^3$.

2°) Méthodes venant de l'analyse

Ex 17: $\left(\sum_{i=1}^{n} x_i\right)^n = \prod_{i=1}^{n} x_i$ n'a pas de solution dans $\mathbb{N}^n$ autre que $(0)_{1\leq i\leq n}$ si $n>1$. (On utilise l'inégalité arithmético-géométrique)

Ex 18: L'ensemble des solutions (où $(x,y)\in\mathbb{Z}^2$) $y^2+y=x^4+x^3+x^2+x$ est $\{(-1;-1);(-1;0);(0;-1);(0;0);(2;-6);(2;5)\}$

(On multiplie l'équation par 4 puis on lui ajoute 1: $(2y+1)^2=4(x^4+x^3+x^2+x)+1$ et on vérifie par l'étude de deux trinômes du second degré si $x<-1$ ou $x>2$ alors $(2x^2+x)^2<4(x^4+x^3+x^2+x)+1<(2x^2+x+1)^2$. Donc on est ramené à $x\in\{-1;0;1;2\}$)

III) Les carrés dans les anneaux cycliques et les corps finis.

1) Les anneaux cycliques.

Not 19 : Soient p premier impair, $a \in \mathbb{Z} \setminus p\mathbb{Z}$. $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

Prop 20 : $\left(\frac{a}{p}\right) = 1$ si et seulement si a est un carré mod p.

Les deux théorèmes suivants vont nous permettre de calculer $\left(\frac{a}{p}\right)$ pour p premier impair.

Thm 21 : Soit p premier impair. Soient $a, b \in \mathbb{Z} \setminus p\mathbb{Z}$.
(i) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. (ii) $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 4$.
(iii) $\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod 8$.

Ex : $y^2 = x^3 + 7$ (on utilise (ii)).
Ex : $y^2 = x^3 - 6$ (on utilise (iii)).

Thm 22 : (réciprocité quadratique) Soient p, q premiers impairs
$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$. DEVELOPPEMENT 1.

Thm 23 : Soit $n \in \mathbb{N} \setminus \{0,1\}$. Soit $a \in \mathbb{Z}$ tel que $a \wedge n = 1$.
Soient $p_1, \dots, p_k$ premiers distincts, $n_1, \dots, n_k \in \mathbb{N}^*$ tels que $n = \prod_{i=1}^{k} p_i^{n_i}$.
(i) a est un carré modulo $n \Leftrightarrow \forall i \in \{1, \dots, k\}$ a est un carré mod. $p_i^{n_i}$.
(ii) Si $p_i \neq 2$, a est un carré mod. $p_i^{n_i} \Leftrightarrow a$ est un carré mod p_i.
(iii) Si $p_i = 2$ et $n_i \geq 3$, a est un carré mod. $2^{n_i} \Leftrightarrow a \equiv 1 \pmod 8$.
$n_i = 2$: a est un carré mod 4 $\Leftrightarrow a \equiv 1 \pmod 4$.
$n_i = 1$: a est un carré mod. 2.

Ex : $x^2 = 7 + 333y$ admet une infinité de solutions car 7 est un carré modulo 333.
$x^2 = 5 + 333y$ n'admet pas de solution car 5 n'est pas un carré modulo 333.

2) Recherche de racine carrée dans les corps finis.

Prop 24 : Soient $n \in \mathbb{N}^*$, $a \in (\mathbb{F}_{2^n})^*$. a admet une unique racine carrée : $a^{2^{n-1}}$

Prop 25 : Soient p un nombre premier impair, $n \in \mathbb{N}^*$.
Le sous-groupe des carrés d'éléments de $(\mathbb{F}_{p^n})^*$ est d'indice deux dans $(\mathbb{F}_{p^n})^*$; ses éléments sont les racines de $X^{\frac{p^n-1}{2}} - 1$.
Si $p^n \equiv 3 \pmod 4$ et a carré dans $(\mathbb{F}_{p^n})^*$ alors $\left(a^{\frac{p^n+1}{4}}\right)^2 = a$.
Dans le cas général, l'algorithme de Cipolla (cf. annexe) donne une racine carrée de a.

IV) Utilisation d'anneaux.

1) L'anneau des entiers de Gauss.

Thm 26 : $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$ est euclidien.

Prop 27 : $(\mathbb{Z}[i])^* = \{\pm 1, \pm i\}$.

Ex 28 : $y^2 = x^3 - 1$ a pour unique solution $(1,0)$.

Thm 29 : L'équation diophantienne d'inconnues $x, y \in \mathbb{Z}$ $n = x^2 + y^2$ admet au moins une solution si et seulement si tout nombre premier congru à 3 modulo 4 apparaît avec un exposant pair dans la décomposition en facteurs premiers de n.

2) L'anneau des quaternions.

Déf 30 : $\mathbb{H} = \mathbb{R}^4$ muni de l'addition usuelle et du produit qui vérifie $i^2 = j^2 = k^2 = -1$ et $ij = k$ et 1 élément neutre où $(1, i, j, k)$ est la base canonique de $\mathbb{R}^4$.
$\tilde{\mathbb{H}} = \mathbb{Z}^4 \cup \left(\frac{1}{2} + \mathbb{Z}\right)^4$ (quaternions de Hurwitz).

Thm 31 : $\mathbb{H}$ est une algèbre à division et $\tilde{\mathbb{H}}$ est un sous-anneau de $\mathbb{H}$ où on peut définir une division euclidienne à gauche.

Thm 32 : L'équation diophantienne d'inconnues $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ admet au moins une solution.

3) L'anneau des entiers d'Eisenstein.

Thm 33 : $\mathbb{Z}[j] = \{a + jb,\ a, b \in \mathbb{Z}\}$ est euclidien.

Prop 34 : $(\mathbb{Z}[j])^* = \{\pm 1, \pm j, \pm j^2\}$.

Thm 35 : L'équation $x^3 + y^3 = z^3$ d'inconnues $x, y, z \in \mathbb{Z} \setminus \{0\}$ n'a pas de solution.

Rq 36 : (culturelle) Le grand théorème de Fermat stipule que $x^n + y^n = z^n$ d'inconnues $x, y, z \in \mathbb{Z} \setminus \{0\}$ n'a pas de solution si $n \geq 3$. Il a été démontré par Andrew Wiles en 1995.

Algorithme d'Euclide étendu :

On se ramène au cas où $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$.

On définit par récurrence : $(r_n)_{n\in\mathbb{N}}$ et $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$; des suites d'entiers.

$$r_0 := a \qquad r_1 := b$$
$$u_0 := 1 \qquad u_1 := 0$$
$$v_0 := 0 \qquad v_1 := 1$$

$\forall n \in \mathbb{N}^*$
$$\begin{cases} r_{n+1} = \begin{cases} r_{n-1} - r_n \left\lfloor \dfrac{r_{n-1}}{r_n} \right\rfloor & \text{si } r_n \neq 0 \\ 0 & \text{sinon} \end{cases} \\ u_{n+1} := \begin{cases} u_{n-1} - \left\lfloor \dfrac{r_{n-1}}{r_n} \right\rfloor u_n & \text{si } r_n \neq 0 \\ u_n & \text{si } r_n = 0 \end{cases} \\ v_{n+1} := \begin{cases} -\left\lfloor \dfrac{r_{n-1}}{r_n} \right\rfloor v_n + v_{n-1} & \text{si } r_n \neq 0 \\ v_n & \text{si } r_n \neq 0. \end{cases} \end{cases}$$

On considère : $N = \min \{ n \in \mathbb{N} \mid r_n = 0 \}$

On a alors : $r_{N-1} = \operatorname{pgcd}(a, b)$

et : $r_{N-1} = a u_{N-1} + b v_{N-1}$

Algorithme de Cipolla :

Soit p un nombre premier impair et $n \geq 1$. Soit $a \in (\mathbb{F}_p^\times)^2$.

Pour déterminer une racine carrée de a. On commence par essayer différents éléments u de $\mathbb{F}_p^*$ jusqu'à en trouver un tel que $u^2 - a$ ne soit pas un carré (c'est-à-dire $(u^2-a)^{\frac{q-1}{2}} = -1$). On pose alors : $P = X^2 - 2uX + a$

P est irréductible et $\mathbb{F}_q[X]/(P) \cong \mathbb{F}_{q^2}$.

De plus : en notant $\bar{X}$, la classe de X dans $\mathbb{F}_p[X]/(P)$, on a : $\left(\bar{X}^{\frac{q+1}{2}}\right)^2 = a$. Donc : $\bar{X}^{\frac{q+1}{2}}$ est une racine carrée de a, et a donc un représentant dans $\mathbb{F}_q$ qui convient.

Références :

Elementary methods in number theory, Nathanson (chapitres 2 et 3)

Nouvelles histoires hédonistes de groupes et de géométries, Caldero et Germoni (Tome 1, chapitre V, annexe C).