126

Exemples d'équations en arithmétique.

# I) Equations entières du premier ordre

## A] Cas de une ou deux variables

Le but ici est de résoudre $ax+by=c$ dans $\mathbb{Z}$.

**Prop 1 :** $ax+b=0$ admet une solution si et seulement si $a|b$ et alors $x=-b/a$.

On suppose maintenant $a,b\neq 0$.

**Thm 2 :** Soient $a_1,\dots,a_n\in\mathbb{Z}^*$ et $d=PGCD(a_1,\dots,a_n)$. Alors $\exists (u_1,\dots,u_n)\in\mathbb{Z}^n, d=\sum_{i=1}^{n} u_i a_i$ (Formule de Bézout).

**Cor 3 :** (Théorème de Bézout) $(a_1,\dots,a_n)$ sont premiers entre eux si et seulement si $\exists (u_1,\dots,u_n)\in\mathbb{Z}^n / \sum u_i a_i = 1$

**Thm 4 :** (d'Euclide) Soient $a\in\mathbb{Z}$ et $b\in\mathbb{Z}^*$. $\exists!(q,r)\in\mathbb{Z}\times\mathbb{N} / a=bq+r$ et $0\leq r<b$.

**Alg 5 :** En itérant cet algorithme avec $a\to b$ et $b\to r$, on peut ainsi obtenir le PGCD de $a$ et $b$ ainsi que les coefficients de Bézout. [4]

**Rem 6 :** Cet algorithme se généralise pour $n$ entiers distincts, en utilisant l'associativité du PGCD.

**Lem 7 :** (de Gauss) Soient $a,b,c\in\mathbb{Z}$. On suppose que $a|bc$ et $a\wedge b=1$. Alors $a|c$.

**Thm 8 :** Soient $a,b,c\in\mathbb{Z}$, $a,b\neq 0$, $a\wedge b=1$. L'ensemble des solutions de $ax+by=c$ est non vide et est $\{(x_0+kb\,;\,y_0-ka) \mid k\in\mathbb{Z}\}$ où $(x_0;y_0)$ est une solution particulière.

**Rem 9 :** $(x_0;y_0)$ s'obtient via Alg 5.

**Ex 10 :** L'ensemble des solutions de $47x+111y=1$ est $\{(26+111k\,;\,-11-47k) \mid k\in\mathbb{Z}\}$ [2]

**Rem 11 :** Dans le cas où $a\wedge b\neq 1$, on se ramène à ce type d'équation en divisant par $a\wedge b$.

## B] Systèmes linéaires entiers

On souhaite résoudre dans $\mathbb{Z}^n$ $AX=b$ où $A\in\mathcal{M}_{m,n}(\mathbb{Z})$, $b\in\mathbb{Z}^m$.

**Thm 12 :** Soit $A\in\mathcal{M}_n(\mathbb{Z})$. $A\in GL_n(\mathbb{Z}) \Leftrightarrow \det(A)=\pm 1$. [5]

**Ex 13 :** Si $A=\begin{pmatrix}2&1\\3&8\end{pmatrix}$, $\det A=13$ donc $A^{-1}$ existe dans $GL_2(\mathbb{R})$, mais $A^{-1}\notin\mathcal{M}_2(\mathbb{Z})$

**Rem 14 :** Dans le cas où $\det(A)\neq\pm 1$ mais $\det(A)\neq 0$, on est pas assuré que la solution, qui existe dans $\mathbb{R}^n$, appartienne à $\mathbb{Z}^n$.

**Prop 15 :** (Formules de Cramer) Soit $A=(C_1,\dots,C_n)\in\mathcal{M}_n(\mathbb{R})$ avec $\det A\neq 0$. Alors la solution de $AX=b$ est : [5]

$$x_i=\frac{\det(C_1,\dots,C_{i-1},b,C_{i+1},\dots,C_n)}{\det A} \qquad \forall i\in[\![1,n]\!]$$

**Cor 16 :** Si $A\in\mathcal{M}_n(\mathbb{Z})$ est tel que $\det A\neq 0$, la solution (unique) de $AX=b$ existe si et seulement si $\forall i\in[\![1;n]\!]$, $\det(A) \mid \det(C_1,\dots,C_{i-1},b,C_{i+1},\dots,C_n)$ où $A=(C_1,\dots,C_n)$.

**Ex 17 :** Si $A=\begin{pmatrix}2&1\\3&8\end{pmatrix}$, $AX=\begin{pmatrix}a\\b\end{pmatrix}$ admet une solution si et seulement si $13|(8a-b)$ et $13|(2b-3a)$

**Thm 18 :** Soit $A\in\mathcal{M}_{n,m}(\mathbb{Z})$. Il existe une unique suite d'entiers $d_s|\dots|d_1$ de $\mathbb{N}^*$ tels que $A$ est équivalente dans $\mathcal{M}_{n,m}(\mathbb{Z})$ à $\begin{pmatrix}\mathrm{Diag}(d_s,\dots,d_1)&0\\0&0\end{pmatrix}$. Les entiers sont les facteurs invariants de $A$. [5]

**Rem 19 :** On ramène alors l'étude de $AX=b$ du cas de $n$ équations à une variable.

## II) Equations modulaires

On s'intéresse ici à certaines équations dans les anneaux $\mathbb{Z}/n\mathbb{Z}$.

### A] Systèmes de Congruence

**Thm 20 :** Soient $a \in \mathbb{N}^*$, $b \in \mathbb{Z}$ et $n \geq 2$. $ax \equiv b\ [n]$ admet une solution si et seulement si $a \wedge n \mid b$. Dans ce cas, si $a = (a \wedge n)a'$, $n = (a \wedge n)n'$ et $b = (a \wedge n)b'$, l'ensemble des solutions est $\{b'x_0 + kn' \mid k \in \mathbb{Z}\}$ où $x_0$ vérifie $a'x_0 \equiv 1\ [n']$

**Rem 21 :** On aurait pu retrouver ce résultat avec Th 8

**Ex 22 :** Les solutions de $47x \equiv 1\ [111]$ sont $\{130 + 111k \mid k \in \mathbb{Z}\}$.

**Rem 23 :** La résolution de ces équations trouve son utilité pour calculer un inverse dans $\mathbb{Z}/n\mathbb{Z}$.

On souhaite maintenant résoudre, étant donnés $n_1, \dots, n_r$ 2 à 2 premiers entre eux, résoudre $x \equiv a_i\ [n_i]$ $\forall i \in [\![1; r]\!]$. Soit $n = \prod_{i=1}^{r} n_i$.

**Thm 24 :** (dit chinois) On a l'isomorphisme $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$.

**Rem 25 :** Soient $m_i = \frac{n}{n_i}$ et $u_1, \dots, u_r \in \mathbb{Z}$, tels que $\sum_{i=1}^{r} u_i m_i = 1$. Alors $\Psi : \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $(\overline{x_1}, \dots, \overline{x_r}) \mapsto \sum_{i=1}^{r} u_i m_i x_i$ est un isomorphisme.

**Cor 26 :** Le système de congruences admet une solution particulière $x_0$. L'ensemble des solutions est alors $\{x_0 + nk \mid k \in \mathbb{Z}\}$.

### B] Résidus quadratique

On souhaite ici résoudre $x^2 = a$ dans $\mathbb{F}_q$, $q = p^n$, $p$ premier.

**Def 27 :** Soit $q = p^n$, $n \neq 0$. $a \in \mathbb{F}_q$ est un carré si $\exists x \in \mathbb{F}_q / a = x^2$. On notera $\mathbb{F}_q^2$ l'ensemble des carrés, et $\mathbb{F}_q^{*2}$ les carrés non nuls.

**Ex 28 :** 0 et 1 sont dans $\mathbb{F}_q^2$ et $x^2 = 0 \Leftrightarrow x = 0$, $x^2 = 1 \Leftrightarrow x = \pm 1$.

**Prop 29 :** Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$. Si $p \geq 3$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$.

On suppose maintenant $p \geq 2$.

**Thm 30 :** Soit $x \in \mathbb{F}_q^*$. $x \in \mathbb{F}_q^{*2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.

**Ex 31 :** 2 est un carré modulo 7.

**Cor 32 :** $(-1) \in \mathbb{F}_q^{*2} \Leftrightarrow q \equiv 1\ [4]$

**App 33 :** Il existe une infinité de nombres premiers de la forme $4n+1$, $n \in \mathbb{N}^*$.

**Def 34 :** Soit $a \in \mathbb{F}_p^*$. On définit son symbole de Legendre par : $\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } a \in \mathbb{F}_p^{*2} \\ -1 \text{ sinon} \end{cases}$ $a^{\frac{p-1}{2}}$

**Prop 35 :** $\forall a \in \mathbb{F}_p^*$, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$

**Cor 36 :** $\mathbb{F}_p^* \to \{\pm 1\}$, $a \mapsto \left(\frac{a}{p}\right)$ est un morphisme de groupes.

**Lem 37 :** (DEV 1) Soit $q \geq 2$ premier. L'équation $ax^2 = 1$ où $a \in \mathbb{N}^*$ admet exactement $1 + \left(\frac{a}{q}\right)$ solutions dans $\mathbb{F}_q^*$.

**Thm 38 :** (Loi de réciprocité quadratique)
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

[1] [3] [1]

## III) Exemples de méthodes de résolution

### A] Descente infinie de Fermat

**Thm 39 :** Les solutions de $x^2+y^2=z^2$ sont les triplets $(d(u^2-v^2); 2duv; d(u^2+v^2))$ où $d \in \mathbb{N}$ et $u, v \in \mathbb{Z}$ sont premiers entre eux.

**Meth 40 :** Soit $P \in \mathbb{Z}[X,Y,Z]$. Considérons l'équation $P(x,y,z)=0$. On souhaite montrer qu'elle n'admet aucune solution non triviale. Le principe de la descente infinie de Fermat est le suivant :

- On suppose que l'ensemble des solutions est non trivial. On prends une solution non triviale $(x,y,z)$ avec $z$ minimal non nul.
- On trouve une solution $(x',y',z')$, avec $z'<z$ et $z' \neq 0$.
- On a une suite décroissante d'entiers de $\mathbb{N}^*$ qui ne stationne pas : c'est absurde.

[4]

**Ex 41 :** L'équation $x^4+y^4=z^2$ n'admet aucune solution telle que $xyz \neq 0$.

**App 42 :** $x^4+y^4=z^4$ n'admet aucune solution non triviale.

### B] Réduction modulo p

**Meth 43 :** On peut parfois projeter l'égalité $P(x,y,z)=0$ dans $\mathbb{F}_p$ pour obtenir des informations sur les solutions éventuelles.

[2]

**Ex 44 :** Soit $p \in \mathbb{N}^*$ premier tel que $p \equiv 3 [4]$. Alors l'équation $x^2+y^2=pz^2$ n'admet pas de solutions non triviales, puisque $(-1) \notin \mathbb{F}_p^2$.

## C] Théorème des deux carrés de Fermat

Soit $n \in \mathbb{N}$. On souhaite savoir si $x^2+y^2=n$ admet des solutions dans $\mathbb{Z}^2$.

**Def 45 :** On définit l'anneau des entiers de Gauss par $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\}$. On note :

$$N : \mathbb{Z}[i] \to \mathbb{N}, \quad a+ib \mapsto |a+ib|^2 = a^2+b^2$$

[3]

**Lem 46 : (DEV 2)** $\mathbb{Z}[i]$ est euclidien et $\mathbb{Z}[i]^\times = \{\pm 1; \pm i\}$

**Thm 47 :** Soit $p \in \mathbb{N}^*$, $p$ est somme de deux carrés si et seulement si $p=2$ ou $p \equiv 1 [4]$.

**Thm 48 :** Soit $n \in \mathbb{N}^*$. $n$ est somme de deux carrés si et seulement si pour tout $p$ premier tel que $p \equiv 3 [4]$, $v_p(n)$ est pair.

Références :


- Algèbre et géométrie, Rombaldi [1]
- Algèbre, Gourdon [2]
- Cours d'algèbre, Perrin [3]
- Algèbre et géométrie, Combes [4]
- Objectif agrégation, Beck [5]