126 Exemples d'équations en arithmétique.

Refs : [Li] Liret Arithmétique. [OA] Beck Malick Peyré Objectif Agrégation [FGN2] Analyse 2. [Pen] Perrin Algèbre [Serre] Serre Cours d'arithmétique [Sam] Samuel Théorie algébrique des nombres. [FGN1] Algèbre

Dev't :
- 31 Réciprocité quadratique [Serre]
- 33 34 Chevalley Warning [Serre]
- III.3 Deux carrés [Per]

I. Équations entières du premier degré.

Prop 1 : Pour $(a,b)\neq(0,0)$, l'équation $ax+b=0$ pour $x\in\mathbb{Z}$ admet des solutions si et seulement si $a|b$, avec $x=-b/a$ alors.

1) Équations en deux variables.

[Li] 16 19

On s'intéresse ici aux équations de la forme $au+bv=d$ (E) avec $a,b,d\in\mathbb{Z}$ et $(u,v)\in\mathbb{Z}^2$

Théo 2 Bézout Soit $(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}$, l'idéal (a,b) dans $\mathbb{Z}$ est donné par $\mathrm{pgcd}(a,b)\mathbb{Z}$. On a les équivalences
- $\exists u,v\in\mathbb{Z}^2 \mid au+bv=1$
- $\mathrm{pgcd}(a,b)=1$

Cor 3 : L'équation (E) admet des solutions si et seulement si le pgcd de a et b divise d.

Lemme 4 (Gauss) Soient $a,b,c\in\mathbb{Z}\setminus\{0\}$, si $a|bc$ et si $\mathrm{pgcd}(a,b)=1$, on a $a|c$

Méthode de résolution

On effectue l'algorithme d'Euclide pour trouver le pgcd de a et b, noté c

En remontant les étapes de l'algorithme, trouver une solution de $au'+bv'=c$ (et donc une solution (x,y) de (E) en multipliant par d/c).

Si (u,v) est une solution générale, on obtient $a(x-u)=b(v-y)$ et par le lemme de Gauss, $a|v-y$, donc $v=ak+y$, $k\in\mathbb{Z}$, on trouve de même $u=x-bk$. D'où

Prop 5 : Les solutions de $au+bv=d$ où $c|d$ sont les entiers de la forme $(x-bk, ak+y)$ pour $k\in\mathbb{Z}$, et (x,y) une solution particulière de l'équation.

Exemple 6 : Les solutions de $5x+7y=11$ sont $(7k+5,-2-5k)$ $k\in\mathbb{Z}$

2) Équations linéaires en n variables.

On s'intéresse ici aux équations linéaires à plusieurs variables de la forme $AX=B$ (E) $A,B\in\mathcal{M}_{m,n}(\mathbb{Z})\times\mathbb{Z}^m$.

La situation des corps est bien connue, et s'adapte à un certain degré aux anneaux, en particulier à $\mathbb{Z}$.

[OA] 285 287

Prop 7 : Si A est de la forme $\begin{pmatrix}D&0\\0&0\end{pmatrix}$ où $D=\mathrm{diag}(d_1,\dots,d_r)$. Alors (E) admet des solutions si et seulement si :

$d_i \mid B_i\ \forall i\in[\![1,r]\!]$ et $B_j=0\ \forall j\in[\![r+1,m]\!]$

(en supposant $d_1,\dots,d_r$ tous non nuls).

Ce résultat n'est utile que si l'on arrive à se ramener à ce cas de figure précis, ce qu'on fait dans le cas d'un corps par des éléments de $GL_n(k)$, on adapte cette méthode.

Rappel : $A\in\mathcal{M}_n(\mathbb{Z})$ est inversible si et seulement si $\det A=\pm1$.

Théo 8 (Facteurs invariants) Soit $U\in\mathcal{M}_{m,n}(\mathbb{Z})$, il existe une unique famille $(d_1,\dots,d_r)$ d'entiers positifs strictement telle que.
- $d_i|d_{i+1}$ pour $i\in[\![1,r-1]\!]$
- Il existe $(P,Q)\in GL_m(\mathbb{Z})\times GL_n(\mathbb{Z})$ telles que $PUQ^{-1}=\begin{pmatrix}D&0\\0&0\end{pmatrix}$ avec $D=\mathrm{diag}(d_1,\dots,d_r)$

La suite $d_1,\dots,d_r$ est la suite des facteurs invariants de U.

Rq 9. On peut retrouver les facteurs invariants par divisions euclidiennes successives.

Ex 10. Le système $\begin{cases}2x+y=a\\3x+8y=b\end{cases}$ a des solutions si et seulement si $3a-2b$ est divisible par 13.

Cor 12 : Une équation entière de la forme $\sum_{i=1}^{m} a_ix_i=b$ admet des solutions si et seulement si $\mathrm{pgcd}(a_1\dots a_m)$ divise b.

Rq 13. Cette approche ne fait appel qu'à la structure euclidienne de $\mathbb{Z}$.

[FGN2] 297

Prop 14 : Soient $a_1\dots a_k$ des entiers naturels non nuls premiers entre eux dans leur ensemble. Si $U_n=|\{x_1\dots x_k\in\mathbb{N}^k \mid \sum a_ix_i=n\}|$ Alors $U_n\underset{n\to\infty}{\sim}(a_1\dots a_k)^{-1}\dfrac{n^{k-1}}{(k-1)!}$

II. Équations modulaires.

On fixe ici $n\geq 2$ et p un nombre premier, on travaille par défaut dans $\mathbb{Z}/n\mathbb{Z}$. Pour résoudre l'équation $ax\equiv b[n]$, on peut résoudre dans $\mathbb{Z}$ l'équation $ax=b+kn$, $k\in\mathbb{Z}$ reformulée en $ax-nk=b$. On retrouve une équation vue dans la première partie.

Prop 15: L'équation $ax \equiv b[n]$ admet des solutions si et seulement si $a \wedge n$ divise b. En particulier, $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si a et n sont premiers entre eux.

Cor 16: $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Rq 17: La méthode développée à la partie précédente permet de calculer des inverses modulaires.

Ex 18: Dans $\mathbb{Z}/8\mathbb{Z}$, l'inverse de $\bar{5}$ est $\bar{5}$ lui-même.

1) Systèmes de congruence.

[Liz] 91 101

Théo 19 Si p et q sont des entiers premiers entre eux, l'application $f : \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ envoyant $\bar{k}^{pq}$ sur $(\bar{k}^{p}, \bar{k}^{q})$ est bien définie et est un isomorphisme d'anneau.

Cor 20: Si $n, m \in \mathbb{Z}$, on a un isomorphisme $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/\mathrm{ppcm}(n,m)\mathbb{Z}$.

Cor 21: Si $n_1, \dots, n_r$ sont des entiers premiers entre eux deux à deux, alors $\mathbb{Z}/n_1 \dots n_r\mathbb{Z}$ est isomorphe comme anneau à $\bigoplus_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$.

Ces résultats permettent de résoudre des systèmes de congruence

Ex 22: Les solutions de $\begin{cases} x \equiv 2 \,[5] \\ x \equiv -1 \,[7] \\ x \equiv 9 \,[13] \end{cases}$ sont exactement les $x \equiv 237 [455]$.

2) Résidus quadratiques.

Parmi les équations classiques sont les équations de degré 2 du type $X^2 - d = 0$ qui donnent les racines carrées. Dans $\mathbb{Z}$, on a :

Prop 23 Pour $d \in \mathbb{Z}$, les racines de $X^2 - d$ dans $\mathbb{C}$ sont
- irrationnelles ou entières si $d \geq 0$
- imaginaires pures sinon.

Cette situation est plus délicate sur les corps finis. (On rappelle que $\mathbb{Z}/p^n\mathbb{Z}$ n'est pas homéomorphe à $\mathbb{F}_{p^n}$ pour $n > 1$).

[Pen] 74

Def 24: On pose, pour $q = p^\alpha$ un nombre primaire, $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q \mid \exists y \in \mathbb{F}_q, y^2 = x\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

Prop 25. Si $p = 2$, alors $\mathbb{F}_q^{2} = \mathbb{F}_q$ à cause du morphisme de Frobenius $x \mapsto x^2$, qui est bijectif pour un corps fini de caractéristique 2.

[Pen]

Prop 26: Pour $p > 2$, $q = p^\alpha$, on a $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$ et $|\mathbb{F}_q^2| = \frac{q+1}{2}$. Plus précisément, on a une suite exacte courte de groupes abéliens

$$\{\pm 1\} \hookrightarrow \mathbb{F}_q^* \twoheadrightarrow \mathbb{F}_q^{*2}, \quad x \mapsto x^2$$

Prop 27: Pour $p > 2$, on a $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1 \in \mathbb{F}_q$.

Cor 28: Sous les mêmes hypothèses, -1 est un carré dans $\mathbb{F}_q$ si et seulement si q est congru à 1 modulo 4.

[Serre]

Def 29: Pour p premier, et $a \in \mathbb{F}_q$, on pose $\left(\frac{a}{p}\right) = a^{\frac{q-1}{2}}$ le symbole de Legendre de a modulo p (on le voit comme un élément de $\{0, 1, -1\}$). On pose $\left(\frac{a}{p}\right) = \left(\frac{\bar{a}}{p}\right)$ pour $a \in \mathbb{Z}$.

Prop 30: On a $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$ si $p > 2$, où $\omega(p) = \frac{p^2-1}{8} [2]$. Donc 2 est un carré modulo p si et seulement si $p = \pm 1 [8]$.

Théo 31: (Réciprocité quadratique) Pour p et q deux nombres premiers impairs distincts, on a $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}}$ DVP

Ex 32 La multiplicativité du symbole de Legendre et la loi de réciprocité quadratique permettent de calculer en pratique les symboles de Legendre :

$$\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1.$$

3) Équations polynomiales dans les corps finis.

[Serre]

Théo 33 (Chevalley Warning) Soient $(f_\alpha)_{\alpha \in A} \in \mathbb{F}_q[X_1, \dots, X_n]$ des polynômes à plusieurs variables avec $\sum_{\alpha \in A} d^\circ f_\alpha < n$, et soit V l'ensemble de leurs zéros communs dans $\mathbb{F}_q^n$. On a $|V| \equiv 0 [p]$. DVP

Cor 34 (Erdős-Ginzburg-Ziv) Soient $2n-1$ entiers $a_1, \dots, a_{2n-1}$, on peut choisir n entiers parmi ceux-ci dont la somme soit divisible par n.

Cor 35: Toute forme quadratique d'au moins trois variables sur $\mathbb{F}_q$ a au moins un zéro non trivial.

III. Exemples de méthodes de résolution

On appelle équation diophantienne les équations polynomiales à coefficients entiers, nous en avons vu certains exemples en première partie. Mais il est en toute généralité particulièrement difficile de savoir même de l'existence ou non de solution.

Ex 36 : Pour $n \geq 3$, l'équation $x^n + y^n = z^n$ n'admet pas de solution. Conjecture de Pierre de Fermat prouvée par Andrew Wiles en 1995.

1) Descente infinie.

[Gom] 18 21

Méthode pour montrer qu'une équation n'a pas de solution :

- On suppose par l'absurde qu'il existe une solution non triviale.
- On construit à partir de cette solution une autre solution plus petite
- Par récurrence on obtient une suite décroissante infinie de solution non triviales (impossible car une suite de $\mathbb{N}$ est stationnaire).

Rq 37 : On peut aussi d'emblée supposer avoir une solution minimale et ainsi avoir une contradiction dès la deuxième étape.

Théo 38 : L'équation $x^4 + y^4 = z^2$ n'a pas de solution entière $x, y, z \geq 1$.

Théo 39 : Soit (x,y,z) un triplet pythagoricien (solution de $x^2+y^2=z^2$). Il existe $d \in \mathbb{Z}$ et u, v premiers entre eux tels que (à permutation près de x et y) $x = d(u^2-v^2)$ $y = 2duv$, $z = d(u^2+v^2)$.

Théo 40 L'équation de Fermat n'a pas de solutions pour $n=4$.

[FGN1] 165

Ex 41 (Théorème de Sophie Germain) Si p est premier avec $2p+1$ premier lui aussi. Alors toute solution entière de $x^p + y^p = z^p$ est telle que $xyz \equiv 0 [p]$.

2) Réduction modulaire

Une autre méthode consiste à réduire une équation modulaire dans un anneau $\mathbb{Z}/n\mathbb{Z}$ pour trouver (ou pas) une solution.

Ex 42 La résolution de $x^2 + py = z$ nous ramène à la recherche d'une racine de z modulo p.

Ex 43 : L'équation $x^3 + 5 = 117 y^3$ n'a pas de solution (en réduisant modulo 7)

Ex 44 : Les équations $x^3 + y^3 + z^3 = 4$ ou 5 n'ont pas de solution entière (modulo 9).

Ex 45 : Si $p \equiv 3 [4]$, $x^2 + y^2 = pz^2$ n'a pas de solution non triviale (réduction et descente infinie) et si $p \equiv 1 [4]$ ou $p = 2$, il y a une infinité de solution.

3) Un exemple : les sommes de deux carrés.

[Perrin] 56

On pose $\Sigma = \{ n \in \mathbb{Z} \mid \exists u, v \in \mathbb{Z} \mid u^2 + v^2 = n \}$ les entiers s'écrivant comme somme de deux carrés.

On introduit l'anneau $\mathbb{Z}[i] = \{ a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z} \}$.

Théo 46 : $\mathbb{Z}[i]$ est un anneau euclidien pour le stathme $z \mapsto N(z) = |z|^2$.

Et pour p premier, on a $p \in \Sigma$ si et seulement si p est réductible dans $\mathbb{Z}[i]$

Théo 47. (Deux carrés). Un nombre premier p est somme de deux carrés si et seulement si il est pair ou congru à $1 [4]$.

Cor 48 : Pour $n \in \mathbb{N}$, on pose $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ sa décomposition en produit de facteurs premiers. On a

$$n \in \Sigma \iff \forall p_i \equiv 3 [4], \ \alpha_i \in 2\mathbb{N}.$$

DVP