Exemples d'équations en arithmétiques.

Sans plus de précision, les équations seront à inconnues entières ou dans un anneau $\mathbb{Z}/n\mathbb{Z}$.

I - Méthodes élémentaires.

1) Quelques exemples

Rmq 1 : Dans $\mathbb{Z}/4\mathbb{Z}$, les carrés sont 0 et 1.

Ex 2 : L'équation $x^2 - 25y^2 = 42$ n'admet pas de solutions.

Prop 3 : Toute suite décroissante d'entiers naturels est stationnaire.

Ex 4 : $\sqrt{2}$ est irrationnel (i.e. $p^2 = 2q^2$ n'a pas de solutions)

Ex 5 : Si $\alpha > n \geq 2$, $x_1^2 + \cdots + x_n^2 = \alpha x_1 \cdots x_n$ admet $(0, \ldots, 0)$ comme unique solution. [FGN 1]

2) L'équation diophantienne $ax + by = c$.

Prop 6 : (Thm de Bézout) Deux entiers a, b sont premiers entre eux ssi il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Prop 7 : (Thm de Gauss) Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Appl 8 : Si $a, b, c \in \mathbb{Z}$, l'équation $ax + by = c$ admet une solution ssi $a \wedge b$ divise c et dans ce cas, les solutions sont les couples $(x_0 + b'k, y_0 - a'k)$, k décrivant $\mathbb{Z}$, où (x_0, y_0) est une solution particulière et $\begin{cases} a' = \frac{a}{a \wedge b} \\ b' = \frac{b}{a \wedge b} \end{cases}$.

Rm 9 : On trouve (x_0, y_0) grâce à l'algorithme d'Euclide étendu.

3) Le théorème des restes et les systèmes de congruence [Rom] DVP 1

$\boxed{\text{Prop 10 : (Sophie Germain) Soit } p \text{ un nombre premier impair tel que } 2p+1 \text{ soit premier. Il n'existe pas de triplet } (x,y,z) \in \mathbb{Z}^3 \text{ tq } xyz \not\equiv 0 [p] \text{ et } x^p + y^p + z^p = 0.}$

Thm 11 : (des restes) Soit $m_1, \ldots, m_r \in \mathbb{N} \setminus \{0, 1\}$ et $m = \prod_{j=1}^{r} m_j$. Les entiers $m_1, \ldots, m_r$ sont premiers entre eux deux à deux ssi les anneaux $\mathbb{Z}/m\mathbb{Z}$ et $\prod_{j=1}^{r} \mathbb{Z}/m_j\mathbb{Z}$ sont isomorphes. Dans ce cas, l'application

$$\psi : \begin{cases} \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z} \\ [k]_m \longmapsto ([k]_{m_1}, \ldots, [k]_{m_r}) \end{cases}$$

est un isomorphisme d'anneaux d'inverse

$$\psi^{-1} : ([a_1]_{m_1}, \ldots, [a_r]_{m_r}) \longmapsto \left[\sum_{i=1}^{r} a_i u_i \frac{m}{m_i} \right]_m$$

où $u_1, \ldots, u_r \in \mathbb{Z}$ sont tq $\sum_{j=1}^{r} u_j \frac{m}{m_j} = 1$.

Prop 12 : Soit $n \geq 2$, $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$. L'équation $ax \equiv b [n]$ admet une solution ssi $a \wedge n$ divise b. Dans ce cas, l'ensemble des solutions est

$$\{ b' x_0' + k n' \mid k \in \mathbb{Z} \}, \text{ où } b' = b / a \wedge b, \ n' = \frac{n}{a \wedge b}$$

et x_0' est une solution particulière de $\frac{a}{a \wedge b} \cdot x \equiv 1 [n']$.

Coro 13 : Soient $a_1, \ldots, a_r \in \mathbb{Z}$ et $m_1, \ldots, m_r \in \mathbb{N}^*$ deux à deux premiers entre eux. Les solutions du système d'équations $k \equiv a_j [m_j]$, $1 \leq j \leq r$ sont les $\{ k_0 + q \cdot m \mid q \in \mathbb{Z} \}$ où $m = \prod_{j=1}^{r} m_j$ et $k_0 \in \mathbb{Z}$ est tel que $[k_0]_m = \psi^{-1}([a_1]_{m_1}, \ldots, [a_r]_{m_r})$ avec $\psi : \mathbb{Z}/m\mathbb{Z} \to \prod_{j=1}^{r} (\mathbb{Z}/m_j\mathbb{Z})$ est l'isomorphisme du Thm 11.

II - Carrés dans un corps fini

1) Cas général [Rom]

Thm 14 : Soit p un nombre premier et $n \in \mathbb{N}^*$. Soit $q = p^n$. Il y a $\frac{q-1}{2}$ carrés (resp. non carrés) dans $\mathbb{F}_q^\times$ et ce sont les racines du polynôme $X^{\frac{q-1}{2}} - 1$ (resp. $X^{\frac{q-1}{2}} + 1$).

Coro 15 : -1 est un carré dans $\mathbb{F}_q^\times$ ssi $q \equiv 1 [4]$

Coro 16 : Pour tous $a, b \in \mathbb{F}_q^\times$ et $c \in \mathbb{F}_q$, il existe $x, y \in \mathbb{F}_q$ tq $c = ax^2 + by^2$.

Appl 17 : Classification des formes quadratiques sur les corps finis.

2) La loi de réciprocité quadratique [Rom]

Def 18 : (symbole de Legendre) Si $a \in \mathbb{F}_p^*$, on note $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré} \\ -1 & \text{sinon} \end{cases}$

Prop 19 : Pour tout $a \in \mathbb{F}_p^\times$, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ et l'application

$$\begin{cases} \mathbb{F}_p^\times \longrightarrow \{\pm 1\} \\ a \longmapsto \left(\frac{a}{p}\right) \end{cases}$$

est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^\times$ dans $\{\pm 1\}$.

Thm 20 : (loi de réciprocité quadratique) Si $p \neq q$ sont deux nombres premiers impairs, alors $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

Prop 21 : (lois complémentaires) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ et $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Appl 22 : Soit $n \in \mathbb{N}^\times$ et $F_n = 2^{2^n} + 1$. Le nombre F_n est premier ssi $3^{\frac{F_n-1}{2}} \equiv -1\,[F_n]$. + réciproque

Ex 23 : L'équation $x^2 + 41y = 13$ n'admet pas de solutions.

Appl 24 : Il existe une infinité de nombres premiers congrus à 1 modulo 12.

III - Anneaux factoriels et euclidiens

1) Définitions et propriétés [Per]

Def 25 : Soit A un anneau intègre et $\mathcal{P}$ un système de représentants des irréductibles de A. On dit que A est factoriel si tout élément $a \in A$ s'écrit de manière unique sous la forme $a = u \prod_{p\in\mathcal{P}} p^{v_p(a)}$ avec $u \in A^\times$ et les $v_p(a) \in \mathbb{N}$ presque tous nuls.

Ex 26 : $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel, $9 = 3^2 = (2+i\sqrt{5})(2-i\sqrt{5})$.

Prop 27 : Soit A un anneau intègre vérifiant la condition d'existence de la def 25. Les conditions suivantes sont équivalentes.
 i) A est factoriel
 ii) Si p est irréductible et $p \mid ab$, alors $p \mid a$ ou $p \mid b$
 iii) Si $a \mid bc$ et a et b sont premiers entre eux, alors $a \mid c$.

Def 28 : Un anneau intègre A est dit euclidien si A est muni d'une division euclidienne, i.e. il existe $v : A\setminus\{0\} \to \mathbb{N}$ tq si $a, b \in A\setminus\{0\}$, alors il existe $q, r \in A$ tq $a = bq + r$ et $r = 0$ ou $v(r) < v(b)$.

Ex 29 : $\mathbb{Z}$ est euclidien pour $v = |\cdot|$, si k est un corps alors $k[X]$ est euclidien.

Ex 30 : Si $n \in \mathbb{N}\setminus\{1, 2\}$, alors $\mathbb{Z}[i\sqrt{n}]$ n'est pas euclidien.

Prop 31 : Si A est euclidien, alors A est factoriel.

2) Un premier exemple : l'anneau des entiers de Gauss [Per]

Prop 32 : $\mathbb{Z}[i]$ est euclidien muni de $N : z = a+ib \mapsto z\cdot\bar{z} = a^2+b^2$.

Prop 33 : $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Prop 34 : Soit $\Sigma = \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N}, n = a^2+b^2\}$. L'ensemble Σ est stable par multiplication.

Thm 35 : Soit p un nombre premier. $p \in \Sigma$ ssi $p = 2$ ou $p \equiv 1\,[4]$.

Coro 36 : Soit $n \in \mathbb{N}^\times\setminus\{1\}$ et $n = \prod_{p\in\mathcal{P}} p^{v_p(n)}$ sa décomposition en facteurs premiers. $n \in \Sigma$ ssi ($\forall p$ premier, $p \equiv 3\,[4] \Rightarrow v_p(n)$ pair).

Coro 37 : Les irréductibles de $\mathbb{Z}[i]$ sont aux inversibles près :
 i) les entiers premiers p tq $p \equiv 3\,[4]$,
 ii) les $a+ib$ avec a^2+b^2 premier.

Prop 38 : Les uniques solutions de $x^2+4 = y^3$ sont $(\pm 2, 2)$ et $(\pm 11, 5)$.

3) Un second exemple : $\mathbb{Z}[i\sqrt{2}]$ [131]

DVP2

Prop 39 : $\mathbb{Z}[i\sqrt{2}]$ est euclidien et $\mathbb{Z}[i\sqrt{2}]^\times = \{\pm 1\}$.

Thm 40 : Les uniques solutions de $x^2 + 2 = y^3$ sont $(\pm 5, 3)$

Coro 41 : L'unique entier encadré inférieurement par un carré et supérieurement par un cube est 26

IV - Modules sur les anneaux euclidiens [ArE]

1) Définitions

Def 42 : Soit A un anneau. Un A-module M est un groupe abélien pour une loi +, muni d'une multiplication scalaire $A\times M \to M$ telle que
 i) $1\cdot v = v$ ii) $(\lambda\mu)v = \lambda(\mu v)$ iii) $(\lambda+\mu)v = \lambda v + \mu v$
et iv) $\lambda(v+u) = \lambda v + \lambda u$,
où $v, u \in M$ et $\lambda, \mu \in A$

Ex 43 : Un k-ev est un k-module, un groupe abélien est un $\mathbb{Z}$-module.

Rmq 44 : on étend les définitions habituelles des e-v aux modules.

Def 45 : A-module de type fini M est dit libre s'il existe un isomorphisme $\varphi : A^n \to M$ avec $n \in \mathbb{N}$.

Prop 46 : Soit $(e_1, \ldots, e_n)$ la base canonique de A^n et $(v_1, \ldots, v_n) \in M$. L'application $\begin{cases} A^n \longrightarrow M \\ \sum_{i=1}^n x_i e_i \longmapsto \sum_{i=1}^n x_i v_i \end{cases}$ est une application A-linéaire

et donc M admet une base ssi M est libre.
Dans la suite, A est supposé euclidien.

2) Forme normale de Smith et conséquences [Art]

Thm 47 : Soit $M \in \mathcal{M}_{m,n}(A)$ une matrice. Il existe $Q \in GL_m(A)$ et $P \in GL_n(A)$ telle que $M' = QAP^{-1}$ soit diagonale, de la forme $\begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & 0 \end{pmatrix}$ avec $r \leq \min\{m,n\}$ et $d_1, \dots, d_r \in A$ tels que $d_1 \mid d_2 \mid \dots \mid d_r$. Les éléments $d_1, \dots, d_r$ sont uniques à multiplication par un inversible près.

Appl 48 : Soit $M \in \mathcal{M}_{m,n}(\mathbb{Z})$ et $B \in \mathbb{Z}^m$. On peut appliquer la forme normale de Smith pour résoudre le système $MX = B$

Thm 49 : Soit M un A-module libre et M' un sous module de M. Il existe une base $(e_1, \dots, e_m)$ de M et il existe des éléments $d_1, \dots, d_r \in A$ tels que $(d_1 e_1, \dots, d_r e_r)$ soit une base de M' avec $r \leq m$.

3) Réseaux [S&TO]

Def 50 : Un réseau de dimension m de $\mathbb{R}^m$ est un $\mathbb{Z}$-module Γ engendré par des vecteurs $e_1, \dots, e_m \in \mathbb{R}^m$ linéairement indépendants.

Prop 51 : Un sous-groupe additif Γ de $\mathbb{R}^m$ est un réseau ssi toute intersection de Γ avec un compact est finie.

Def 52 : Si Γ est un réseau engendré par $e_1, \dots, e_m$, le domaine fondamental de Γ est $\{\sum_{i=1}^{m} a_i e_i \mid 0 \leq a_i < 1, \forall i = 1, \dots, m\}$.
(annexe 1)

Def 53 : On définit le covolume d'un réseau $\Gamma \subseteq \mathbb{R}^m$ de dimension m comme le volume de son domaine principal (il ne dépend pas du choix de la base).

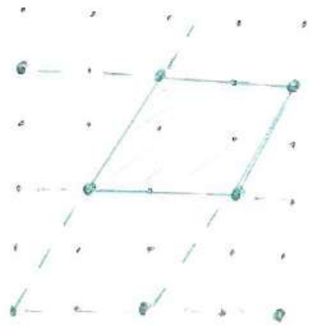
Prop 54 : Soit Γ un réseau de dimension m de $\mathbb{R}^m$ de base $(e_1, \dots, e_m)$. Le volume du domaine fondamental associé est $|\det P_{\mathcal{B} \to (e_1, \dots, e_m)}|$ où $\mathcal{B}$ est la base canonique.

Prop 55 : Soit Γ' un sous-réseau de Γ de dimension m dans $\mathbb{R}^m$. Alors :
$$\mathrm{cov}(\Gamma') = [\Gamma' : \Gamma] \cdot \mathrm{cov}(\Gamma).$$

Thm 56 : (Minkowski) Soit $\Gamma \subset \mathbb{R}^m$ un réseau de dimension m ~~et de domaine fondamental T~~. Soit $X \subset \mathbb{R}^m$ un convexe symétrique. Si $v(X) > 2^m \mathrm{cov}(\Gamma)$, alors X contient un point non nul de Γ.

Appl 57 : Théorème des 2 carrés (item 35) avec le réseau
$$\mathbb{R}^2 \supset \Gamma = \{\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) \in \mathbb{Z}^2 \mid b \equiv ua\,[p]\},$$ où $u \in \mathbb{Z}/p\mathbb{Z}$ est tel que $-1 \equiv u^2\,[p]$. (annexe 2)

Appl 58 : Tout entier naturel est somme de quatre carrés. On utilise le réseau $\Gamma = \{\left(\begin{smallmatrix} a \\ b \\ c \\ d \end{smallmatrix}\right) \in \mathbb{Z}^4 \mid c \equiv ua + vb\,[p]$ et $d \equiv ub - va\,[p]\} \subset \mathbb{R}^4$ avec $u^2 + v^2 + 1 \equiv 0\,[p]$.



annexe 1 - Le réseau engendré par $\{(2,0),(1,2)\}$ et le domaine fondamental associé.

annexe 2 : Le réseau pour $p=5$.