Leçon 126 : Exemples d'équations en arithmétique.

Dreteon
Rombaldi
Ulmer, Anneaux ...
Gourdon, Analyse (dev 1)

I. Arithmétique dans $\mathbb{Z}$

1. Équations du 1er ordre [Dre]

Lemme 1.1 (Bézout) Soient $a, b \in \mathbb{Z}$. On note $d := \text{pgcd}(a,b)$. Il existe alors $x, y \in \mathbb{Z}$ tels que $ax + by = d$.

Remarque 1.2 Il n'y a pas unicité des solutions $1 = 3\times 1 - 2\times 1 = 3\times 3 - 2\times 4$

Proposition 1.3 Soient $a, b \in \mathbb{Z}$ non tous deux nuls et $d := \text{pgcd}(a,b)$. Pour tout $c \in \mathbb{Z}$, l'équation $ax + by = c$ admet une solution si et seulement si d divise c.

De plus, soit (x_0, y_0) une solution alors l'ensemble des solutions de l'équation est : $\{(x_0 - kb_0, y_0 - ka_0) \mid k \in \mathbb{Z}\}$ où $a_0 = \frac{a}{d}$ et $b_0 = \frac{b}{d}$.

Proposition 1.4 (algorithme d'Euclide étendu) Soient $a, b \in \mathbb{Z}$. On construit par récurrence les suites $(a_n)_n$, $(x_n)_n$, $(y_n)_n$ par $a_0 = a$, $x_0 = 1$, $y_0 = 0$, $a_1 = b$, $x_1 = 0$, $y_1 = 1$ puis : a_{i+1} le reste de la division euclidienne de a_{i-1} par a_i, q_i le quotient de celle-ci, $x_{i+1} = x_{i-1} - q_i x_i$ et $y_{i+1} = y_{i-1} - q_i y_i$

On s'arrête lorsque $a_{n+1} = 0$. On obtient alors : $a_n = d$ et $x_n a + y_n b = d$.

Exemple 1.5

effectuons l'algorithme d'Euclide pour 111 et 47

i	a_i	x_i	y_i
0	111	1	0
1	47	0	1
2	17	1	-2
3	13	-2	5
4	4	3	-7
5	1	-11	26
6	0	47	-111

donc $\text{pgcd}(111, 47) = 1$

et :

$1 = 111 \times (-11) + 47 \times 26$

Proposition 1.6 Soient $a_1, \dots, a_p \in \mathbb{N}^*$ premiers entre eux deux à deux. En considérant S_n le nombre de solutions $(n_1, \dots, n_p) \in \mathbb{N}^p$ de l'équation $a_1 n_1 + \dots + a_p n_p = n$. Alors : $S_n \sim \frac{n^{p-1}}{a_1 \dots a_p (p-1)!}$

développement 1

Application 1.7 Soit $n \in \mathbb{N}^*$. Dans un système monétaire $\{1, 2, 5, 10\}$ le nombre q_n de façons de faire n euros, a un comportement asymptotique $q_n \sim \frac{n^3}{600}$.

2. Système de congruences [Rom] [Ulm]

Lemme 1.8 (lemme chinois) Soient m, n des entiers premiers entre eux alors $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$.

Corollaire 1.9 Soient m, n premiers entre eux et $x, y \in \mathbb{Z}$, il existe alors un unique nombre α modulo mn tel que $x \equiv \alpha\ [m]$ et $y \equiv \alpha\ [n]$.

Théorème 1.10 (théorème chinois) Soient $(n_j)_{1 \leq j \leq r}$ une famille de $r \geq 2$ entiers naturels distincts de 0 et 1 et $n = \prod_{j=1}^{r} n_j$. Alors les entiers $n_1, \dots, n_r$ sont deux à deux premiers entre eux si et seulement si $\mathbb{Z}_n \simeq \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$. Le cas échéant, l'application $\psi : \pi_n(k) \in \mathbb{Z}_n \longmapsto (\pi_{n_1}(k), \dots, \pi_{n_r}(k))$ est un isomorphisme d'anneaux d'inverse $\psi^{-1} : (\pi_{n_1}(a_1), \dots, \pi_{n_r}(a_r)) \longmapsto \pi_n\left(\sum_{i=1}^{r} a_i u_i \frac{n}{n_i}\right)$ où $\sum u_j \frac{n}{n_j} = 1$.

Exemple 1.11

Les solutions de $\begin{cases} u \equiv 1 \mod 3 \\ u \equiv 3 \mod 5 \\ u \equiv 0 \mod 7 \end{cases}$ sont de la forme $28 + 105k$, $k \in \mathbb{Z}$

Remarque 1.12 Lorsqu'il s'agit d'un système à deux équations, on peut appliquer la proposition 1.4 combiné au théorème 1.10 pour donner l'ensemble des solutions.

II - Équations du 2nd ordre

1. Équations de Pell-Fermat [Szp]

On s'intéresse aux équations de la forme $x^2 - dy^2 = 1$ où $d \in \mathbb{Z}$.

Remarque 2.1 Cette solution admet toujours des solutions $(\pm 1, 0)$, que l'on appelle solutions triviales.

Théorème 2.2 (Fermat) Soit $d \in \mathbb{Z}$ avec $d \neq 0, -1$. Alors l'équation de Pell - Fermat admet une solution non triviale si et seulement si $d > 0$ et d n'est pas un carré parfait.

Le cas échéant, soit (x_0, y_0) une telle solution avec $x_0 > 1$ et minimal, alors les solutions $(x, y) \in \mathbb{Z}^2$ sont celles telles que $x + y\sqrt{d} = \pm (x_0 + y_0\sqrt{d})^k$, $k \in \mathbb{Z}$.

Lemme 2.3 Les inversibles de $\mathbb{Z}[\sqrt{d}]$ sont ceux de norme ± 1 où la norme est définie par $N : \mathbb{Z}[\sqrt{d}] \longrightarrow \mathbb{Z}$, $x + y\sqrt{d} \longmapsto x^2 - y^2 d$.

Exemple 2.4

$x^2 - 2y^2 = 1$ admet $(3,2)$ comme solution minimale et l'ensemble des solutions (x,y) est de la forme $x + y\sqrt{2} = \pm (3 + 2\sqrt{2})^k$, $k \in \mathbb{Z}$

2. Somme de deux carrés de Fermat [Ulm]

Définition 2.5 On appelle anneau des entiers de Gauss, $\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}$.

Proposition 2.6 Les inversibles de $\mathbb{Z}[i]$ sont $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Notation 2.7 On note $\sum_2 := \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N}, a^2 + b^2 = n\}$.

Lemme 2.8 Soit $n \in \sum_2$. Alors $n \equiv 0 \mod 4$, $n \equiv 1 \mod 4$ ou $n \equiv 2 \mod 4$.

Lemme 2.9 L'anneau $\mathbb{Z}[i]$ est euclidien.

Théorème 2.10 Soit p un nombre premier. Alors $p \in \sum_2$ si et seulement si $p = 2$ ou $p \equiv 1 \mod 4$.

développement 2

Théorème 2.11 Un entier positif n est somme de deux carrés si, et seulement si, dans la décomposition en facteurs premiers de n chacun de ses facteurs premiers p tel que $p \equiv 3 \mod 4$ apparaît avec une puissance paire.

III. Équations de degré supérieur [Dre]

1. Exemples historiques

Définition 3.1 Un nombre premier p est dit de Sophie - Germain si $q = 2p + 1$ est un nombre premier.

Théorème 3.2 (Sophie Germain) Soit p un nombre premier de Sophie Germain alors il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ vérifiant $xyz \not\equiv 0 \mod p$ et $x^p + y^p + z^p = 0$.

Théorème 3.3 (Fermat) - admis L'équation $x^n + y^n = z^n$, pour $n \geq 3$, n'admet pas de solution $(x, y, z) \in \mathbb{Z}^3$ non triviale.

2. Méthode de descente infinie

Définition 3.4 La méthode de descente infinie consiste en la méthode suivante : On considère un sous-ensemble de $\mathbb{N}$ supposé non vide formé des solutions de l'équation diophantienne. On choisit le plus petit, puis on en exhibe un plus petit, aboutissant à une contradiction : donc l'ensemble est vide.

Exemple 3.5 Soit $d \in \mathbb{N}$ qui n'est pas un carré parfait. Alors $\sqrt{d}$ est irrationnel.

Exemple 3.6

L'équation $x^3 + 2y^3 = 4z^3$ n'admet pas de solution non triviale

Exemple 2.7

soient $n \in \mathbb{N}$, $\alpha \in \mathbb{N}$, $\alpha > n \geq 2$

alors $x_1^2 \dots x_n^2 = \alpha x_1 \dots x_n$ n'admet pas de solution non triviale