Leçon 126 - Exemples d'équations diophantiennes.

Def : Une équation diophantienne est une équation de la forme $P(x_1,..,x_n) = 0$, pour $P \in \mathbb{Z}[X_1,..,X_n]$ et dont on cherche les solutions entières.

1. Equations diophantiennes linéaires. —

1. Résolution avec une ou deux variables. —

- Pro : L'équation $ax = b$ pour $(a, b) \neq (0, 0)$ possède une unique solution entière ssi $a|b$. La solution est alors $\frac{b}{a}$.
- Théorème de Bézout : Soient $a, b \in \mathbb{Z}$ et $d = pgcd(a, b)$. Alors il existe $(u, v) \in \mathbb{Z}$ tq $au + bv = d$.
  Réciproquement, si $au' + bv' = c$, alors $d|c$.
- Cor : L'équation $ax + by = c$ admet des solutions ssi $pgcd(a, b)|c$.
  Dans ce cas, pour (u_0, v_0) une solution initiale, $a = a'.pgcd(a, b)$ et $b = b'.pcgd(a, b)$, les solutions sont de la forme $(u_0 + b'.k, v_0 - a'.k)$ pour $k \in \mathbb{Z}$.
- Rem : On peut trouver explicitement une solution initiale grâce à l'algorithme d'Euclide.
- Ex : $42x + 66y = 10$ n'admet aucune solution. $112x + 70y = 14$ admet des solutions, par exemple $(2, -3)$.

2. Equations de degré 1 en n variables. —

- Soient $A \in M_{m,n}(\mathbb{Z})$, $B \in \mathbb{Z}^m$. On veut résoudre $AX = B$ avec $X \in \mathbb{Z}^m$.
- Pro : Si $A = \begin{pmatrix} Diag(d_1,..,d_r) & 0 \\ 0 & 0 \end{pmatrix}$ avec $d_1,..,d_r \in \mathbb{Z}^*$, alors $AX = B$ possède des solutions $\Leftrightarrow \begin{cases} \forall 1 \leq i \leq r, d_i | b_i \\ \forall r + i \leq i \leq m, b_i = 0 \end{cases}$.
  Les solutions sont alors de la forme $(\frac{b_1}{d_1},..,\frac{b_r}{d_r}, x_{r+1},..,x_n)$ pour $x_{r+1},..,x_n \in \mathbb{Z}$.
- Théorème des facteurs invariants : Pour $A \in M_{m,n}(\mathbb{Z})$, il existe une unique famille finie d'entiers strictement positifs $d_1,..,d_r$ telle que $d_1|..|d_r$ et telle qu'il existe $U \in Sl_m(\mathbb{Z}), V \in Sl_n(\mathbb{Z})$ tq $UAV = \begin{pmatrix} Diag(d_1,..,d_r) & 0 \\ 0 & 0 \end{pmatrix}$
- Pro : Pour D la matrice des facteurs invariants de A, on a $AX = B \Leftrightarrow D(VX) = U^{-1}B$.
  On est ramenés à la résolution de $DX' = B'$ pour $X' = VX$ et $B' = U^{-1}B$.
- Rem : On peut calculer explicitement les facteurs invariants de la matrice A en utilisant la division euclidienne dans $\mathbb{Z}$.
- Ex : $\begin{pmatrix} 2 & 4 \\ 3 & 8 \end{pmatrix} = PDiag(1, 4)Q$.
- Ex : L'équation $2x + 4y = -2$, $3x + 8y = 1$ a pour unique solution $(x, y) = (-5, 2)$.

3. Equations modulaires et théorème chinois. —

- Pro : Lien entre équations modulaires et équations diophantiennes.
- Théorème chinois : Pour $n = q_1..q_r$ avec q_i premiers entre eux 2 à 2, on a un isomorphisme d'anneaux entre $\mathbb{Z}/n\mathbb{Z}$ et $\Pi_i \mathbb{Z}/q_i\mathbb{Z}$.
- Exemple de résolution.

2. Quelques méthodes pratiques. —

1. Réduction modulaire. —

- Rem : Dans le cas où certains termes de P de petit degré total sont multiples d'un nombre premier p, on peut chercher à résoudre $\overline{P}(x_1,..,x_n) = 0$ dans $\mathbb{F}_p$.
  Si $\overline{P}$ n'a pas de zéros dans $\mathbb{F}_p$, alors il n'a pas de zéros dans $\mathbb{Z}$.
  Si $\overline{P}$ a des zéros dans $\mathbb{F}_p$, on cherche alors à voir si ces zéros peuvent être étendus en des zéros dans $\mathbb{Z}$.
- Ex : $X^2 + 1 = p$ n'a pas de solutions pour p premier tq $p \equiv 3 \ mod(4)$.
- Ex : Les équations $x^3 + 5 = 117y^3$, $x^2 + y^2 = 8z + 7$, n'ont pas de solutions.
- Théorème de Sophie-Germain : Soit p un nombre premier impair tel que $q = 2p + 1$ soit premier.
  Alors l'équation $x^p + y^p + z^p = 0$ n'admet aucune solution entière telle que $xyz = 0$.
- Def+Pro : Pour tout $x \in \mathbb{F}_p$, on définit $(\frac{x}{p}) = \begin{cases} 1 \text{ si x} \in (\mathbb{F}_p^*)^2 \\ 0 \text{ si } x = 0 \\ -1 \text{ sinon} \end{cases}$
  le symbole de Legendre.
  Le symbole de Legendre définit un morphisme de groupes de $\mathbb{F}_p^*$ vers $\{-1, 1\}$.
  Ainsi, pour $n = p_1^{a_1}..p_r^{a_r}$ et p premier aux p_i, $(\frac{n}{p}) = \Pi_i (\frac{p_i}{p})^{a_i}$.
- Ex : $(\frac{-1}{p}) = (-1)^{\frac{p-1}{4}}$.
- Pro : $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.
- **Dev** : Loi de réciprocité quadratique : Soient p,m des nombres premiers impairs distincts.
  Alors $(\frac{p}{m}) = (\frac{m}{p}).(-1)^{\frac{p-1}{2}.\frac{m-1}{2}}$.
- App : Les équations de la forme $x^2 + py = q$, pour p premier impair et q non-multiple de p, ont une solution si et seulement si $(\frac{q}{p}) = 1$.
  Pour $x_0 \in \mathbb{Z}$ tel que $x_0^2 \equiv q \ mod(p)$, les solutions sont de la forme $(x_0 + k.p, \frac{(x_0+k.p)^2-q}{p})$.
  La loi de réciprocité quadratique, les formules pour -1 et 2, et la division euclidienne permettent de toujours calculer le symbole de Legendre $(\frac{q}{p})$.
- Ex : $x^2 + 59y = 23$ n'a pas de solutions.
- App : Les équations de la forme $ax^2 + bx + c = 0$ pour a,b,c non divisibles par p ont des solutions dans $\mathbb{F}_p$ ssi $(\frac{b^2-4ac}{p}) = 1$.
  Si $(\frac{b^2-4ac}{p}) = -1$ pour un certain p premier, alors $ax^2 + bx + c = 0$ n'a pas de solutions dans $\mathbb{Z}$.

2. Méthode de descente infinie. —

- Principe : On suppose que l'équation admet une solution $(x_1, .., x_n)$ vérifiant certaines propriétés (non-triviale par ex), et l'on dispose d'une fonction w qui à $(x_1, .., x_n)$ associe un entier strictement positif.
  Si l'on est capable de montrer que l'existence de cette solution implique l'existence d'une autre solution $(y_1, .., y_n)$ vérifiant les mêmes propriétés, et pour laquelle l'image par w est un entier strictement positif inférieur à $w(x_1, .., x_n)$, alors cela veut dire que l'équation n'admet aucune solution vérifiant lesdites propriétés, car une sous-partie majorée de $\mathbb{N}^*$ ne contient pas un nombre infini d'éléments distincts.
- App : Il n'existe pas de solution non-triviale eux équations $x^4+y^4 = z^4$, $x^4+y^4 = z^2$, et $x^2 + y^2 = p.z^2$ pour p premier, $p \equiv 3 \ mod(4)$.

3. Méthodes géométriques. —

- Rem : Résoudre $P(x, y, z) = 0$ avec P polynôme homogène revient à chercher les solutions rationnelles de la courbe $P(x, y, 1) = 0$.
  Si la courbe possède une paramétrisation faite de fractions rationnelles à coefficients dans $\mathbb{Q}$, alors on peut déterminer les points rationnels de celle-ci en fonction du paramétrage.
- Pro : Une paramétrisation rationnelle du cercle C d'équation $X^2 + Y^2 = 1$ est $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}) \cup \{(-1, 0)\}$, c'est-à-dire : $C = \{(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}), t \in \mathbb{R}\} \cup \{(-1, 0)\}$ et $t \in \mathbb{Q}$ $\Leftrightarrow (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}) \in \mathbb{Q}^2$.
- Thm : Les solutions de $x^2 + y^2 = z^2$ dont les coefficients sont premiers entre eux dans leur ensemble sont exactement les triplets $(u^2 - v^2, 2uv, u^2 + v^2)$ pour $u \wedge v = 1$.
  L'ensemble des solutions de $x^2 + y^2 = z^2$ est donc :
  $\{(d(u^2 - v^2), 2duv, d(u^2 + v^2)), u, v, d \in \mathbb{Z}, u \wedge v = 1\}$.
- Ex : En prenant $u = 2, v = 1$, on obtient le triplet $(3, 4, 5)$. Avec $u = 7, v = 2$ on a $(45, 28, 53)$.
- Def : On définit le folium de Descartes F comme la courbe d'équation $X^3+Y^3 = XY$.
- Pro : $(\frac{t}{1+t^3}, \frac{t^2}{1+t^3})$ est une paramétrisation rationnelle de F.
- Thm : Les triplets $(uv^2, u^2v, u^3 + v^3)$ où $u \wedge v = 1$ sont exactement les solutions de $x^3 + y^3 = xyz$ avec $pgcd(x, y, z) = 1$.
- Ex : $u = 1, v = 1 \Rightarrow (1, 1, 2)$ est solution. $u = 3, v = 5 \Rightarrow (75, 45, 152)$ est solution.

4. Utilisation des corps quadratiques. —

1. Entiers d'un corps quadratique. —

- Rem : $\mathbb{Q}(\sqrt{d})$ est un corps.
- Def : Norme d'un élément de $\mathbb{Q}(\sqrt{d})$.
- Def : Trace d'un élément de $\mathbb{Q}(\sqrt{d})$.
- Def : Un élément de $\mathbb{Q}(\sqrt{d})$ est appelé un entier algébrique ssi son polynôme minimal sur $\mathbb{Q}$ est à coefficients dans $\mathbb{Z}$.
  On appelle O_d l'ensemble des entiers algébriques sur $\mathbb{Q}(\sqrt{d})$.
- Pro : O_d est un anneau intègre.
- Thm : $O_d = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \equiv 1 \ mod(4)$, et $O_d = \mathbb{Z}[\sqrt{d}]$ sinon.
- Thm : La norme sur O_d est un stathme si :
  $d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13\}$.
- Application aux equations de Mordell, comme : $y^2 = x^3-2$, $y^2 = x^3-11$, $y^2 = x^3-1$, $x^5 - y^2 = 1$.

2. Entiers de Gauss. —

- Rem : $\mathbb{Z}[i]$ est un anneau euclidien, avec pour stathme sa norme. Ses inversibles sont ± 1 et $\pm i$.
- **Dev** : Théorème des deux carrés de Fermat : Les irréductibles de $\mathbb{Z}[i]$ sont : les p premiers tq $p \equiv 2, 3 \ mod(4)$, et les $a + ib$ tels que $a^2 + b^2$ est premier.
  L'équation diophantienne $x^2 + y^2 = n$ admet des solutions si et seulement si pour tout p premier tq $p \equiv 3$ mod(4), on a $v_p(n)$ pair.

3. Equations de Pell-Fermat. —

- Def : Une équation de Pell-Fermat est une équation de la forme $x^2 - dy^2 = 1$ pour d sans facteurs carrés.
- Rem : Les solutions de l'équation de Pell-Fermat sont en bijection avec les éléments de O_d de norme 1, qui est un sous-groupe du groupe des inversibles de O_d.
- Rem : Si $d < 0$ les seules solutions sont $(\pm 1, 0)$,$(0, \pm 1)$
- Thm : Pour $d > 1$, il existe un $w \in O_d$ de norme 1 tel que tout élément de norme 1 soit de la forme w^k pour $k \in \mathbb{Z}$. w est appelé unité fondamentale.
- Cor Pour $d > 1$, $x^2 - dy^2 = 1$ admet une infinité de solutions, et toute solution (x, y) est de la forme : $x + \sqrt{d}y = (x_0 + \sqrt{d}y_0)^n = (\sum_{k=2m, k \leq n} x_0^k y_0^{n-k} \binom{n}{k} d^m) + \sqrt{d}(\sum_{k=2m+1, k \leq n} x_0^k y_0^{n-k} \binom{n}{k} d^m)$
- Ex : Résolution de $x^2 - 3y^2 = 1$.

Références

Duverney : Corps quadratique, norme/trace/conjugué, entiers quadratiques, propriétés, unités. Equations de Mordell.
Combes : Equations diophantiennes linéaires, exemples. Equations modulaires, Th chinois, lien avec les équations linéaires. Paramétrisation rationnelle d'une équation homogène, cercle, folium de Descartes.
Objectif Agrégation : Equa diophant lin en dimension supérieure, décomposition de Smith.
Perrin : Th des deux carrés.(Dev)
Caldero,Germoni : Loi de réciprocité quadratique.(Dev)
FGN : Partitions d'un entier en parts fixées.

January 23, 2018

Vidal Agniel, École normale supérieure de Rennes