Leçon 114 :
Equations diophantiennes du premier degré $ax + by = c$. Autres exemples d'équations diophantiennes.

par Stephanie Maurel

0.0.1. Définition – *Une équation diophantienne est une équation polynomiale $P(x_1, .., x_n) = 0$ à coefficients dans $\mathbb{Z}$ (ou $\mathbb{Q}$) dont on cherche les solutions entières (ou rationnelles).*

0.1 Equation $ax + by = c$

0.1.1. Théorème – *L'équation diophantienne $ax + by = c$, $(a, b, c) \in \mathbb{Z}^3$, admet des solutions si et seulement si $d = pgcd(a, b)$ divise c. Dans ce cas, les solutions sont données par $(x = x_0 + \frac{bt}{d}, y = y_0 - \frac{at}{d})$, où $t \in \mathbb{Z}$ et (x_0, y_0) est une solution particulière de l'équation.*

0.1.2. Proposition – *Algorithme d'Euclide : Soient $a, b \in \mathbb{Z}$,*

$$a = bq_1 + r_1 \text{ où } 0 \leq r_1 < b$$
$$b = r_1q_2 + r_2 \text{ où } 0 \leq r_2 < r_1$$
$$etc...$$
$$r_k = r_{k+1}q_{k+2} + r_{k+2} \text{ où } 0 \leq r_{k+2} < r_{k+1}$$

Il existe $k \in \mathbb{N}$ tel que $r_k = 0$, donc $pgcd(a, b) = pgcd(b, r_1) = .. = r_{k-1}$

0.1.3. Théorème – *(Bezout)*
Soient $a, b \in \mathbb{Z}$ premiers entre eux, alors $\exists u, v \in \mathbb{Z}$, $au + bv = 1$.

0.1.4. Exemples –
1) Les solutions de $11x + 43y = 10$ sont les couples $(-3 + 43t, 1 - 11t)$ où t parcourt $\mathbb{Z}$.
2) Les solutions entières positives de $5x + 7y = 83$ sont les couples $(249 + 7t, -166 - 5t)$ où t parcourt $\mathbb{Z}$ quand les couples sont positifs, ce qui ne laisse en fait que les solutions $(4, 9)$ et $(11, 4)$.
3) L'équation $21x + 49y = 5$ n'a pas de solution car $pgcd(21, 49) = 7$ qui ne divise pas 5.

0.1.5. Applications –
1) L'ensemble des solutions de $ax + by = 11$ est $E = (x, y); x = 5 - 4t, y = 1 - 3t; t \in \mathbb{Z}$. Trouver a et b.
2) Le système $x + y + z = 100, 2x + 5y + \frac{5}{10} = 100$ admet une unique solution entière positive.
3) Soient $(a, b) \in \mathbb{N}^2$, $pgcd(a, b) = 1$. Montrer que le nombre de solutions positives de $ax + by = n$ où $n \in \mathbb{N}$ est égal à $[\frac{n}{ab}]$ ou $[\frac{n}{ab}] + 1$.

0.1.6. Proposition – *Equation $ax + by + cz = d$*
1)Soient $(a, b, c, d) \in \mathbb{Z}^4$. L'équation diophantienne $ax + bt + cz = d$ admet des solutions si et seulement si

$pgcd(a,b,c) = \delta$ divise d.

2)Résolution :
a)Montrer que l'on peut se ramener au cas où a, b, c sont premiers entre eux dans leur ensemble.
b)Supposons a, b, c premiers entre eux. Montrer que, quitte à modifier la troisième inconnue, on peut se ramener au cas où $pgcd(a,b) = 1$.
c)Supposons $pgcd(a,b) = 1$. Trouver une solution de la forme $(x, y, 0)$.
d)Supposons $pgcd(a,b) = 1$ et $d = 0$. Déterminer les solutions de $ax + by + cz = d$.
e)Trouver toutes les solutions lorsque $pgcd(a,b) = 1$

0.2 L'équation de Fermat

L'équation de Fermat est de la forme $x^n + y^n = z^n$, $n \in \mathbb{N}$.

0.2.1. Théorème – *Les solutions de l'équation diophantienne $x^2 + y^2 = z^2$ sont données par, à permutation près de x et y, $(x = K(u^2 - v^2), y = 2Kuv, z = K(u^2 + v^2))$, $K, u, v \in \mathbb{Z}$, u et v de parités différentes et permiers entre eux.*
Si x, y, z sont premiers entre eux, alors $K = 1$.
On appelle ces solutions les triplets pythagoriciens.

0.2.2. Proposition – *Il n'existe pas de triangle pythagoricien dont l'aire soit un carré.*

0.2.3. Théorème – *(Fermat-Wiles)*
L'équation diophantienne $x^n + y^n = z^n$ n'admet pas de solutions non triviales pour $n > 2$.

0.2.4. Théorème – *(Sophie Germain)*
Soit p un nombre premier de Sophie Germain, c'est à dire un nombre premier impair tel que $2p + 1$ soit premier. Il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}$ tel que xyz ne soit pas congru à 0 modulo p et $x^p + y^p = z^p$.

0.2.5. Applications – *Résolution des cas $n = 3$ et $n = 4$.*

0.3 L'équation de Pell-Fermat

Les fractions continues permettent de résoudre l'équation diophantienne (*) $x^2 - Dy^2 = L$ où $1 \leq \mid L \mid < \sqrt{D}$, D entier positif qui n'est pas un carré parfait.

0.3.1. Théorème – *Si $(x, y) \in \mathbb{N}^2$, $pgcd(x, y) = 1$, est solution de $(*)$, alors $x = P_n$ et $y = Q_n$ où $\frac{P_n}{Q_n}$ est une réduite du développement de $\sqrt{D}$ en fraction continue.*

On cherche donc les réduites $\frac{P_n}{Q_n}$ du développement de $\sqrt{D}$ en fraction continue qui vérifient $P_n^2 - DQ_n^2 = L$. Soit $\alpha_0 = \sqrt{D} = [c_0, c_1, ..]$, $\alpha_n = c_n + \frac{1}{\alpha_{n+1}}$, $c_n = [\alpha_n]$. On a, $\forall n \in \mathbb{N}$ $\alpha_n = \frac{A_n + \sqrt{D}}{B_n}$,$A_n \in \mathbb{N}, B_n \in \mathbb{N}^*$.

0.3.2. Théorème – *L'équation* $(*)$ *admet une solution si et seulement si* $\exists n_0 \in \mathbb{N}^*$ $L = (-1)^{n_0} B_{n_0}$. *Dans ce cas, une solution de* $(*)$ *est* $(x = P_{n_0-1}, y = Q_{n_0-1})$, *où* $\frac{P_{n_0-1}}{Q_{n_0-1}}$ *est la réduite d'ordre* $n_0 - 1$ *du développement de* $\sqrt{D}$ *en fraction continue.*
De plus, soit T *la période de ce développement, alors* $\forall k \in \mathbb{N}$, $(x = P_{n_0+2kT-1}, y = Q_{n_0+2kT-1})$ *est solution de* $(*)$.

0.3.3. Théorème – *L'équation de Pell* $x^2 - Dy^2 = 1$ *admet une infinité de solutions.*

0.3.4. Théorème – *Soit* (x_1, y_1) *la solution fondamentale de l'équation* $x^2 - Dy^2 = 1$. *Soient* (x_n, y_n) *les solutions vérifiant* $x_n \geq 0, y_n \geq 0$, *rangées dans l'ordre croissant. Alors :*
a) $x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n, \forall n \in \mathbb{N}$
b) $x_{n+2} = 2x_1x_{n+1} - x_n$ *et* $y_{n+2} = 2y_1y_{n+1} - y_n, \forall n \in \mathbb{N}$

0.3.5. Exemple – L'équation $x^2 - 34y^2 = L, 1 \leq \mid L \mid < 5$, admet des solutions si $L \in \{1, 2\}$

0.4 L'équation de Mordell $y^2 = x^3 + K$

0.4.1. Théorème – *L'équation diophantienne* $y^2 = x^3 - 1$ *admet une unique solution* $(x = 1, y = 0)$

0.4.2. Théorème – *Soit* $K < -1$, *sans facteur carré, avec* $K \equiv 2$ *ou* 3 $[4]$. *Supposons que le nombre de classes* $h(\mathbb{Q}(\sqrt{K}))$ *n'est pas divisible par 3. Alors l'équation* $y^2 = x^3 + K$ *admet une solution entière si et seulement si* $K = \pm 1 - 3a^2$,$a \in \mathbb{N}^*$. *Dans ce cas, les solutions sont* $(x = a^2 - K, y = \pm a(a^2 + 3K))$.

0.4.3. Exemple – Les solutions de $y^2 = x^3 - 2$ sont $(3, \pm 5)$.

0.5 Equations diophantiennes et séries

0.5.1. Proposition – *Soient* $\alpha_1, .., \alpha_p \in \mathbb{N}^*$, *premiers entre eux dans leur ensemble et* $\forall n \in \mathbb{N}$, *on note* S_n *le nombre de solutions* $(n_1, .., n_p) \in \mathbb{N}^p$ *de l'équation* $\alpha_1 n_1 + .. + \alpha_p n_p = n$.

$$S_n \sim \frac{1}{\alpha_1..\alpha_p} \frac{n^{p-1}}{(p-1)!}$$

0.5.2. Exemple – 1) Le nombre de solutions $(x, y, z) \in \mathbb{N}^3$ de $x + 2y + 3z = n$ est $p(n) = \frac{(n+1)(n+5)}{12} + 17/72 + (-1)^n/8 + 2/9cos(2i\pi/3)$

2) Soit V_n le nombre de couples $(p,q) \in \mathbb{N}^2$ tels que $2p+3q=n$.
Si $n=3m$, alors $V_n = 1/4(1+(-1)^m)+1/6(3m+1)+1/3$
Si $n=3m+1$, alors $V_n = 1/4(1+(-1)^{m+1})+1/6(3m+2)-1/3$
Si $n=3m+2$, alors $V_n = 1/4(1+(-1)^m)+(m+1)/2$

0.6 Conjecture de Catalan

Deux nombres consécutifs ne sont jamais des puissances exactes sauf 8 et 9. Autrement dit, $x^n - y^m = 1$,$n,m \geq 2$, n'admet pas de solutions entières à part $(3,2), n=2, m=3$.

0.7 Dixième problème de Hilbert

Il n'existe pas d'algorithme indiquant si une équation diophantienne admet ou non une solution.

0.8 Autres équations diophantiennes

1) Un produit de trois entiers consécutifs n'est jamais une puissance k-ième, $k \geq 2$.
2) Soit $n \in \mathbb{N}$, soit $\alpha \in \mathbb{N}$ tel que $\alpha > n \geq 2$. L'équation $x_1^2 + .. + x_n^2 = \alpha x_1..x_n$ n'a pas de solutions entières autres que $(0,..,0)$.
3) L'équation $x^2+y^2+z^2 = xyz-1$ n'admet pas de solutions $(x,y,z) \in \mathbb{N}^{*3}$.
4) Les solutions telles que $x \neq 0$ de l'équation $x^2+y^2 = x^3+y^3$ sont de la forme :

$$x = \frac{1+a^2}{1+a^3} \text{ et } y = \frac{a(1+a^2)}{1+a^3} \text{ , } a \neq -1$$

0.9 Bibliographie

- Daniel Duverney : *Théorie des nombres,cours et exercices corrigés.*
p 37.38 : équation $ax+by=c$, mais en passant par les fractions continues.
p 43.43.51 : équation de Pell (erreur dans la démonstration du corollaire 4.3).
p 56 : équation de Mordell $y^2 = x^3 - 1$.
p 149 : équation de Mordell $y^2 = x^3 + K$.
p 52 : équation de Fermat pour $n=2$.
p 53 : équation de Fermat pour $n=4$.
p 56.67 : équation de Fermat pour $n=3$.
Cours complet sur les fractions continues et les corps quadratiques, dont la connaissance est nécessaire pour cette leçon. Les démonstrayions sont assez bien expliquées.

- Jean-Marie Koninck, Armel Mercier : *1001 problèmes en théorie classique des nombres*

p 10 : Rappel sur $ax + by = c$ et $x^2 + y^2 = z^2$.
p 100 à 108 : exercices sur les équations diophantiennes tous corrigés.

- Serge Francinou, Hervé Gianella, Serge Nicolas :*Exercices de mathématiques, oraux X-ENS, algèbre 1*
Théorème de Sophie Germain
Un produit de trois entiers consécutifs n'est jamais une puissance k-ième
Une équation diophantienne $x_1^2 + .. + x_n^2 = \alpha x_1..x_n$