QUELQUES ÉQUATIONS DIOPHANTIENNES

RÉSUMÉ. Une équation diophantienne est une équation algébrique dont ont cherche des solutions en nombres entiers. L'histoire des équations diophantiennes est aussi ancienne que l'histoire de l'écriture. Nous examinons quelques équations diophantiennes ainsi que les notions algébriques qui ont émergé de leur étude, et permettent d'en formaliser la résolution.

TABLE DES MATIÈRES

1. GÉNÉRALITÉS

Une *équation* est une égalité entre deux expressions qui contiennent une ou plusieurs *inconnues*. *Résoudre* l'équation c'est déterminer les valeurs de l'inconnue (des inconnues) pour lesquelles l'égalité est vraie.

Nous allons nous intéresser aux équations *algébriques*. Cela signifie que les deux membres de l'équation sont des polynômes en les inconnues (parfois des fractions rationnelles). On se restreindra au cas où les *coefficients* de ces polynômes sont des nombres entiers relatifs.

Il est primordial de préciser dans quel ensemble on recherche des solutions.

Par exemple l'équation

$$x^2 = -1$$

est algébrique à coefficients entiers. Elle n'admet pas de solution dans l'ensemble $\mathbf{R}$ des nombres réels. Elle admet des solutions dans l'ensemble $\mathbf{C}$ des nombres complexes.

L'équation

$$x^2 = 2$$

est algébrique à coefficients entiers. Elle n'admet pas de solution dans l'ensemble $\mathbf{Q}$ des nombres rationnels. Elle admet des solutions dans l'ensemble $\mathbf{R}$ des nombres réels.

L'équation

$$2x = 3$$

est algébrique à coefficients entiers. Elle n'admet pas de solution dans l'ensemble $\mathbf{Z}$ des nombres entiers relatifs. Elle admet des solutions dans l'ensemble $\mathbf{Q}$ des nombres rationnels.

Comme les équations algébriques s'écrivent à l'aide des opérations $+$, $\times$ et parfois $\div$, il est naturel de chercher des solutions dans un ensemble muni d'une addition et d'une multiplication (et éventuellement d'une division). C'est donc dans un anneau ou dans un corps que l'on cherche les solutions d'une équation algébrique.

2. Équations diophantiennes

Ce sont des équations algébriques à coefficients entiers. On recherche des solutions dans l'ensemble $\mathbf{Z}$ des entiers et parfois aussi dans l'ensemble $\mathbf{Q}$ des nombres rationnels.

Rechercher des solutions dans $\mathbf{R}$ ou $\mathbf{C}$ n'est pas inutile pour autant. Par exemple, toute solution dans $\mathbf{Q}$ est a fortiori une solution dans $\mathbf{R}$. Si l'on prouve qu'il n'y a pas de solution dans $\mathbf{R}$ alors il n'est plus nécessaire de chercher des solutions dans $\mathbf{Q}$.

Les problèmes résolus dans certaines tablettes babyloniennes (deuxième millénaire avant notre ère) peuvent être interprétés dans le langage de l'algèbre moderne comme des équations. Les méthodes de résolution sont présentées à l'aide d'une succession d'exemples de difficulté croissante.

La notion de nombre inconnu est explicitée dans les *Arithmétiques* de Diophante d'Alexandrie (entre le premier et le quatrième siècle de notre ère). La présentation de Diophante est beaucoup plus systématique que celle des tablettes : énoncé du problème, conditions à l'existence de solutions, mise en équation, résolution, synthèse.

La convention de désigner par des lettres les quantités connues ou inconnues, et les diverses notations pour les opérations arithmétiques apparaissent progressivement entre le quinzième et le dix-septième siècle. Les notations utilisées par René Descartes sont proches de celles utilisées aujourd'hui : $a + b$, ab, $\frac{a}{b}$, a^3, $\sqrt{a}$, ...

Le *degré* d'une équation est le plus grand degré total de ses termes. Par exemple le degré total de x^2y est $2 + 1 = 3$. Donc l'équation $x^2y + yx + 1 = x - y$ est de degré 3. En général, la difficulté d'une équation croît avec le degré.

Les équations de degré 1 sont dites linéaires. La résolution sur un corps, par exemple le corps $\mathbf{Q}$ des rationnels, d'un système d'équations linéaires est facile. On utilise la méthode du pivot de Gauss. Observons que l'opération de division joue un rôle capital dans cette méthode. Cette méthode ne permet donc pas de trouver les solutions entières d'un système d'équations linéaires à coefficients entiers.

3. Une équation homogène de degré 1

On s'intéresse à l'équation

$$15x + 12y = 0 \tag{1}$$

et plus généralement à une équation de la forme

$$ax + by = 0$$

où a et b sont des entiers donnés. Donc a et b sont des coefficients. Et x et y sont les inconnues. On dit que l'équation est homogène car tous ses termes sont de degré total 1.

Les solutions dans $\mathbf{Q}$ sont les couples $(x, -5x/4)$ avec x parcourant $\mathbf{Q}$. L'ensemble des solutions est un sous-espace vectoriel du $\mathbf{Q}$-espace vectoriel $\mathbf{Q}^2$.

Mais toutes ces solutions ne sont pas des solutions entières. On aimerait dire que l'ensemble des (x, y) dans $\mathbf{Z}^2$ qui satisfont l'équation 1 est un sous-espace vectoriel du $\mathbf{Z}$-espace vectoriel $\mathbf{Z}^2$. Mais $\mathbf{Z}^2$ n'est pas un espace vectoriel et $\mathbf{Z}$ n'est pas un corps.

On définit la notion d'anneau unitaire commutatif, qui généralise la notion de corps. Si A est un anneau unitaire commutatif on peut définir la notion de A-module en imitant la définition des K-espaces vectoriels pour un corps K. Les notions de corps et d'anneaux sont apparues progressivement à la fin du dix-neuvième siècle et au début du vingtième notamment grâce à Richard Dedekind, Leopold Kronecker, Emmy Noether, David Hilbert.

On peut dire que l'ensemble des solutions entières de l'équation 1 est un sous-module du $\mathbf{Z}$-module $\mathbf{Z}^2$. En effet si (x, y) et (x', y') sont des solutions entières alors la somme $(x, y) + (x', y')$ est une solution entière. Si λ est un entier et si (x, y) est une solution entière alors $\lambda(x, y)$ est une solution entière.

Pour résoudre l'équation 1 on divise par le pgcd des coefficients 15 et 12. On obtient l'équation équivalente

$$5x = -4y \tag{2}$$

En utilisant le lemme de Gauss, on vérifie que les solutions de l'équation 1 sont les $(4u, -5u)$ avec u parcourant l'ensemble des entiers relatifs.

4. Des équation linéaires inhomogènes

On s'intéresse à l'équation

$$15x + 12y = 3 \tag{3}$$

C'est une équation linéaire inhomogène. Comme 3 est le pgcd de 15 et de 12, cette équation admet une solution. C'est le théorème de Bezout. L'algorithme d'Euclide (330 avant notre ère) étendu permet de trouver un λ et un μ tels que $15\lambda + 12\mu = 3$. Par exemple $\lambda = 1$ et $\mu = -1$. Le couple $(1, -1)$ est solution de l'équation (3).

On s'intéresse maintenant à l'équation

$$15x + 12y = 7 \tag{4}$$

Si x et y sont entiers alors le membre de gauche est un multiple de 3. Or le membre de droite n'est pas un multiple de 3. Donc cette équation homogène n'a pas de solution entière.

On se demande quels sont les entiers c tels que l'équation

$$15x + 12y = c \tag{5}$$

ait une solution entière.

On note Eq_c cette équation. Il est clair que si Eq_c et $\mathrm{Eq}_{c'}$ ont chacune une solution alors $\mathrm{Eq}_{c+c'}$ a une solution. Et pour tout entier a l'équation Eq_{ac} a une solution. Donc l'ensemble $\mathcal{C}$ des c tels que Eq_c ait une solution entière est stable par addition et par multiplication par n'importe quel entier. On dit que c'est un idéal de l'anneau $\mathbf{Z}$.

Essayons de préciser quel est cet ensemble. Il est évident que pour avoir une solution à Eq_c l'entier c doit être un multiple de 3. Réciproquement si c est un multiple de 3 alors Eq_c a une solution puisque Eq_3 a une solution.

L'ensemble $\mathcal{C}$ est donc l'ensemble des entiers multiples de 3.

Supposons maintenant que $c \in \mathcal{C}$. On sait comment trouver une solution à l'aide de l'algorithme d'Euclide étendu. Si (x_0, y_0) est une solution quelconque de Eq_c alors $(x-x_0, y-y_0)$ est solution de (1). Comme on connaît les solution de cette équation homogène, on en déduit l'ensemble des solutions de Eq_c.

On sait donc quand une équation linéaire a des solutions. Et l'on dispose d'un algorithme pour les calculer toutes.

Cette méthode s'étend à la résolution en nombres entiers de systèmes d'équations linéaires inhomogènes en plusieurs inconnues. La méthode utilisée est un hybride entre l'algorithme d'Euclide étendu et l'algorithme du pivot de Gauss pour la résolution des systèmes linéaires sur un corps. Cette méthode remonte au milieu du dix-neuvième siècle (Charles Hermite) et elle a été rendue plus efficace avec les progrès de l'arithmétique des ordinateurs. Elle est exposée dans le texte [1] disponible ici :

`https://agreg-maths.univ-rennes1.fr/documentation/docs/alglinent.pdf`

5. Une équation de degré deux

On considère l'équation

$$x^2 + y^2 = 1. \tag{6}$$

L'ensemble des solutions réelles est le cercle C de centre $(0,0)$ et de rayon 1. On peut écrire

$$C = \{(x, \pm\sqrt{1-x^2}), x \in [-1,-1]\}.$$

On s'intéresse à l'ensemble des solutions rationnelles. Autrement dit les couples $(x,y) \in \mathbf{Q}^2$ solutions de l'équation (6).

On appelle A le point $(1,0)$ qui est rationnel, et sur le cercle. Si B est un autre point rationnel sur le cercle C alors la droite (AB) admet une équation à coefficients dans $\mathbf{Q}$. Sa pente en particulier est dans $\mathbf{Q}$. Réciproquement, pour tout rationnel t soit D_t la droite de pente t passant par A. Cette droite coupe le cercle en deux points : A et un autre point P_t. Un paramétrisation des points rationnels de D_t est $x = 1+z$, $y = zt$ pour z parcourant $\mathbf{Q}$. On substitue $1+z$ à x et zt à y dans l'équation de C. On trouve $z(2+z(1+t^2)) = 0$. La valeur $z = 0$ correspond au point A. La valeur

$$z = \frac{-2}{1+t^2}$$

correspond au point P_t. On en déduit que

$$P_t = (\frac{t^2-1}{t^2+1}, \frac{-2t}{1+t^2})$$

parcourt l'ensemble des points rationnels de $C - \{A\}$ quand t parcourt $\mathbf{Q}$.

Pour trouver les points entiers on remarque que si (x, y) est sur C alors x et y sont dans $[-1, 1]$. On cherche donc des points à coordonnées -1, 0 ou 1 sur le cercle C. Il y en a exactement 4 qui sont $(1, 1)$, $(1, -1)$, $(-1, 1)$, $(-1, -1)$.

Nous retenons de cet exemple que la géométrie joue un rôle important pour la résolution des équations algébriques. À toute équation en deux inconnues on peut associer une courbe dans le plan. Les solutions de l'équation correspondent à des points sur la courbe. Si la courbe est de degré 2, la connaissance d'un point rationnel suffit à déterminer tous les autres car on peut construire une paramétrisation.

6. Une autre équation de degré 2

On considère l'équation

$$x^2 - 2y^2 = 1. \tag{7}$$

La recherche des solutions rationnelles se fait comme pour l'équation précédente. La recherche des solutions entières est plus délicate. En effet on ne sait pas borner la valeur absolue de y et de x cette fois.

Le mathématicien Indien Brahmagupta a remarqué au septième siècle de notre ère que si y_1, y_2, x_1, x_2 sont quatre indéterminées on a

$$(x_1^2 - 2y_1^2)(x_2^2 - 2y_2^2) = (x_1x_2 + 2y_1y_2)^2 - 2(y_1x_2 + y_2x_1)^2. \tag{8}$$

On peut retrouver facilement cette identité en remarquant que

$$\begin{aligned}
x_1^2 - 2y_1^2 &= (x_1 + y_1\sqrt{2})(x_1 - y_1\sqrt{2}) \\
x_2^2 - 2y_2^2 &= (x_2 + y_2\sqrt{2})(x_2 - y_2\sqrt{2}) \\
(x_1 + y_1\sqrt{2})(x_2 + y_2\sqrt{2}) &= (x_1x_2 + 2y_1y_2) + (y_1x_2 + y_2x_1)\sqrt{2} \\
(x_1 - y_1\sqrt{2})(x_2 - y_2\sqrt{2}) &= (x_1x_2 + 2y_1y_2) - (y_1x_2 + y_2x_1)\sqrt{2}
\end{aligned}$$

$$((x_1x_2+2y_1y_2)+(y_1x_2+y_2x_1)\sqrt{2})((x_1x_2+2y_1y_2)-(y_1x_2+y_2x_1)\sqrt{2}) = (x_1x_2+2y_1y_2)^2-2(y_1x_2+y_2x_1)^2.$$

Une conséquence est que l'on peut définir une loi de groupe sur l'ensemble des solutions entières de l'équation (7) en posant

$$\begin{aligned}
(x_1, y_1) \oplus (x_2, y_2) &= (x_1x_2 + 2y_1y_2, y_1x_2 + y_2x_1) \\
\ominus(x_1, y_1) &= (x_1, -y_1).
\end{aligned}$$

Une solution presque évidente à l'équation (7) est $(3, 2)$. En utilisant la loi de groupe on construit d'autres solutions :

$$\begin{aligned}
(3, 2) \oplus (3, 2) &= (17, 12) \\
(3, 2) \oplus (17, 12) = [3](3, 2) &= (99, 70) \\
(3, 2) \oplus (99, 70) = [4](3, 2) &= (577, 408)
\end{aligned}$$

On peut montrer qu'il existe une infinité de solutions. Et que le groupe des solutions est engendré par la solution $(3, 2)$ qui est d'ordre infini, et la solution $(-1, 0)$ qui est d'ordre 2.

Une conséquence étonnante est que l'hyperbole d'équation (7) a une infinité de points à coordonnées entières.

Une interprétation algébrique de ce phénomène est possible à l'aide de l'ensemble

$$\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} \,|\, a, b \in \mathbf{Z}\}$$

muni des lois + et ×. C'est un anneau. Une unité de $\mathbf{Z}[\sqrt{2}]$ est par définition un élément de $\mathbf{Z}[\sqrt{2}]$ qui admet un inverse dans $\mathbf{Z}[\sqrt{2}]$ pour la multiplication. L'étude de l'équation (7) revient peu ou prou à étudier le groupe des unités de $\mathbf{Z}[\sqrt{2}]$. Le développement aux alentours de 1900 par les mathématiciens Allemands Klein, Hecke, Minkowski, Hensel, Schur, Noether, Hilbert, Siegel et quelques autres de la théorie algébrique des nombres a constitué un progrès majeur dans l'étude des équations diophantiennes.

7. POUR ALLER PLUS LOIN

Un cours d'histoire des mathématiques très agréable à lire est [2] qui est disponible ici :
`https://irma.math.unistra.fr/~baumann/polyh.pdf`

Le livre [3] propose une introduction élémentaire à la théorie des nombres.

Un traité plus systématique de théorie des nombres est [4]. Le livre [5] est plus synthétique et peut-être plus accessible.

RÉFÉRENCES

[1] Michel COSTE : *Algèbre linéaire sur les entiers*. Université de Rennes, 2008.

[2] Pierre BAUMANN : *Histoire des mathématiques*. Université de Strasbourg, 2004.

[3] G. H. HARDY et E. M. WRIGHT : *An Introduction to the Theory of Numbers*. Oxford, fourth édition, 1975.

[4] A. I. BOREVICH et I. R. SHAFAREVICH : *Number theory*. Pure and Applied Mathematics, Vol. 20. Academic Press, New York-London, 1966. Translated from the Russian by Newcomb Greenleaf.

[5] Pierre SAMUEL : *Théorie algébrique des nombres*. Hermann, collection Méthodes, 1967.