

premiers réguliers. Les seuls nombres premiers irréguliers inférieurs à 100 sont 37, 59 et 67.

Analyse diophantienne et géométrie algébrique

Le travail de Newton précédemment évoqué à propos de tangentes et de sécantes (inconnu jusque dans les années 1960) était resté sans suite, mais la connexion de l'analyse diophantienne avec le calcul intégral fut explicitée pour le cas des intégrales elliptiques par Carl Jacobi (1804-1851) dans une courte note publiée en 1834. Jacobi y interprète la méthode d'Euler pour construire des solutions rationnelles de l'équation $y^2 = P(x)$, où P est un polynôme de degré égal à 4, au moyen de la multiplication par un entier de l'intégrale de la fonction $1/\sqrt{P(x)}$.

James Sylvester (1804-1897), à l'Université de Londres, a consacré des travaux remarquables à l'étude des équations diophantiennes de degré égal à 3 par la géométrie algébrique. Il annonce ses résultats dans une note de 1858 et il les développe dans une série de mémoires en 1879 et en 1880. Sa méthode consiste à construire des points rationnels d'une courbe cubique (voir la figure 5) à partir d'un point rationnel donné en se servant de tangentes et de sécantes.

En 1890, le dernier mathématicien capable d'embrasser l'ensemble des mathématiques, David Hilbert (1862-1943), et son professeur Adolf Hurwitz (1859-1919) étudient systématiquement les équations diophantiennes à l'aide de la notion de genre d'une courbe, introduite par Rudolf Clebsch (1833-1872), à la suite de travaux de Bernhard Riemann : on étend la méthode de la corde en remplaçant la sécante (de degré 1) qui coupe la cubique (de degré 3, soit $1 + 2$) par une courbe de degré inférieur de deux unités au degré n de la courbe étudiée et en imposant que cette courbe passe par tous les points singuliers (points doubles, points de rebroussement, etc). On lui impose en outre de passer par un certain nombre de points ordinaires. Si p est le genre, ce nombre de points imposés doit être égal à $n - 2 + p$, et il reste p points d'intersection. Hilbert et Hurwitz se limitent au genre égal à zéro ; ils trouvent que l'on peut passer, par des quotients de polynômes à coefficient rationnels (des «transformations birationnelles»), de courbes de genre

égal à zéro et de degré n définies sur l'ensemble des nombres rationnels à une droite ou à une conique, et inversement. En réduisant ainsi le degré d'une équation diophantienne, ils arrivent au degré 1 ou 2, que l'on sait résoudre.

Puis, en 1901, Henri Poincaré (1854-1912), sans connaître apparemment le travail de Hilbert et de Hurwitz, consacre un article important à l'analyse diophantienne. Poincaré voulait classer les problèmes diophantiens en problèmes équivalents par certaines transformations adaptées à la nature du problème. Comme il s'intéressait à l'analyse diophantienne rationnelle, les transformations birationnelles à coefficients rationnels se présentèrent naturellement, et le genre, qui n'est pas modifié au cours de telles transformations (on dit que c'est un invariant birationnel) a une signification que n'a pas le degré. Poincaré traite d'abord le cas du genre zéro, obtenant le même résultat que Hilbert et Hurwitz ; puis il passe au genre un, qui occupe l'essentiel de son mémoire.

Poincaré montre que les courbes de genre un qui ont un point rationnel sont birationnellement équivalentes à la cubique déjà considérée, d'équation $y^2 = 4x^3 - ax - b$. Il introduit les fonctions dites elliptiques afin d'exprimer les coordonnées des points de ces courbes.

Un ensemble de points rationnels d'une cubique plane est dit stable par la construction des tangentes et des sécantes si cette construction ne fait pas sortir de l'ensemble. Dans une suite d'articles publiés entre 1906 et 1908, Beppo Levi cherche ces systèmes stables. En termes modernes, il s'agit de déterminer quels sont les groupes de torsion possibles dans le groupe des points rationnels (voir la figure 7). La détermination complète a été faite par Bruno Mazur, en 1978, et il est remarquable que Levi s'en soit approchée.

Contrairement à Poincaré, L. Mordell s'intéressait à l'analyse diophantienne entière ; en 1922, il voulait établir la finitude du nombre de solutions entières d'équations diophantiennes de la forme $y^2 = P(x)$, où P est un polynôme de degré trois ou quatre. Pour le degré trois, la théorie des nombres algébriques lui permettait de se ramener à un théorème d'Axel Thue, lié à la théorie des approximations diophantiennes (comment estimer la rapidité de l'approximation d'un nombre irrationnel par une

suite de nombres rationnels), sur la finitude du nombre de solutions entières d'une équation de la forme $F(u,v) = m$, où F est un polynôme homogène en (u,v) , c'est-à-dire dont le degré total, pour u et pour v soit égal pour tous les termes du polynôme (par exemple, le polynôme $uv^3 + u^2v^2 + 4v^4$ est homogène, et de degré égal à quatre) ; mais cette méthode était inopérante en degré quatre.

Mordell s'est aperçu qu'elle lui donnait un procédé de descente conduisant à établir que les points rationnels s'obtiennent à partir d'un nombre fini d'entre eux par la construction des tangentes et des sécantes ; c'est alors seulement qu'il cite Poincaré et qu'il formule sa célèbre conjecture, sur la finitude du nombre de points rationnels pour les genres strictement supérieurs à un.

André Weil, en 1929, a réinterprété le résultat de Mordell en termes du groupe des points rationnels d'une courbe elliptique. La conjecture de Mordell a fini par être démontrée en 1983, par l'Allemand Gerd Faltings, qui a suivi une autre voie. Comme la courbe de Fermat est de genre supérieur à un lorsque l'exposant est strictement supérieur à trois, le théorème de G. Faltings indique que l'équation de Fermat n'a au plus qu'un nombre fini de solutions.

Le théorème de Fermat proprement dit est sorti de son isolement plus récemment, en 1987, quand on s'est aperçu qu'il se déduisait de conjectures formulées de manière complètement indépendantes. Notamment un théorème de Kenneth Ribet a montré que le théorème de Fermat est une conséquence d'une conjecture de M. Taniyama et de A. Weil sur les courbes elliptiques ; c'est cette conjecture que A. Wiles vient de démontrer.

Christian HOUZEL est professeur de mathématiques à l'IUFM de Paris.

O. NEUGEBAUER et A. SACHS, *Mathematical Cuneiform Texts*, New Haven, 1945.

DIOPHANTE, *Les Arithmétiques*, 4 vol., Éditions Allard et Rashed, Paris, vol. 3 et 4, 1984 ; vol. 1 et 2 à paraître.

G. TERJANIAN, *Fermat et l'analyse diophantienne*, *Sém. d'Hist. des Math. de Toulouse* 8, pp. 57-66, 1986.

P. RIBENBOÏM, *13 Lectures on Fermat's Last Theorem*, Berlin, 1979.
