

nombres. Il s'agit en général de problèmes diophantiens, du nom du mathématicien du III^e siècle Diophante d'Alexandrie. Ces problèmes font intervenir des équations polynomiales à coefficients entiers, dont on cherche les solutions parmi les nombres entiers (on parle d'équations diophantiennes). Une démonstration de la conjecture ABC fournirait en particulier une solution simple aux problèmes suivants :

- La conjecture de Catalan, selon laquelle l'équation $x^m - y^n = 1$ n'a qu'une seule solution parmi les entiers naturels : $3^2 - 2^3 = 1$. Elle a été démontrée en 2002 par le mathématicien roumain Preda Mihăilescu.

- La conjecture de Mordell, démontrée en 1983 par Gerd Faltings, affirme que chaque courbe dont le « genre » est plus grand que 1, définie par une équation polynomiale à coefficients rationnels, ne peut contenir qu'un nombre fini de points dont les coordonnées sont rationnelles (le genre peut être vu comme le nombre de fois où il est possible de couper la courbe sans obtenir deux morceaux séparés). Noam Elkies, de l'Université Harvard, a démontré en 1991 que la conjecture de Mordell est une conséquence de la conjecture ABC. Si la conjecture ABC était valable dans sa version la plus forte, cela prouverait non seulement l'existence de ces points rationnels, mais donnerait aussi un procédé effectif pour les déterminer.

- Un grand nombre de généralisations de ces problèmes. La preuve de la conjecture ABC entraînerait par exemple celle que chaque égalité (dite de Fermat) $ax^n + by^n = cz^n$ pour $n \geq 4$ (et a, b, c entiers relatifs) n'a qu'un nombre fini de solutions. Il en est de même pour l'équation de Catalan-Fermat $x^n + y^m = z^k$, si les exposants sont « grands », c'est-à-dire si $1/n + 1/m + 1/k < 1$.

Il reste qu'à ce jour, la conjecture ABC n'est pas démontrée – du moins tant que les affirmations de S. Mochizuki n'ont pas été vérifiées. Pourquoi serait-elle vraie ? Et quels sont les résultats intermédiaires atteints à ce stade ?

Comme on l'a vu, de nombreuses données numériques soutiennent la validité de la conjecture, mais elles n'aident en rien à la prouver. En mathématiques, on cherche à obtenir des énoncés qui ne concernent pas seulement un comportement moyen, mais qui sont valables dans tous les cas. Or la difficulté de la conjecture ABC vient des nombres exceptionnels qui échappent à la statistique.

Des pistes ténues vers une démonstration

En utilisant des méthodes de ce qu'on appelle la théorie des nombres transcendants, Cameron Stewart, Robert Tijdeman et Kunrui Yu ont pu montrer que le taux de croissance de C en fonction de $\text{Rad}(ABC)$ est au plus exponentiel. D'après la conjecture ABC, cette croissance est polynomiale, avec un exposant égal au plus à 2 ou $1 + \varepsilon$, suivant la version de la conjecture. On sait donc au moins que la croissance de C n'est pas illimitée, mais cela est insuffisant pour des grandes valeurs de C . Et il semble hors de portée de gravir, avec les méthodes utilisées, la marche séparant la croissance exponentielle de la croissance polynomiale.

Une autre approche emprunte un chemin *a priori* paradoxal. En généralisant la conjecture ABC, donc en la rendant en quelque sorte plus difficile, on a l'espoir de faciliter la démonstration. La généralisation consiste à remplacer les nombres naturels usuels par des structures abstraites plus compliquées. Les propriétés des entiers

naturels utilisées dans la conjecture sont la structure additive, la structure multiplicative et l'ordre total : deux entiers peuvent toujours être comparés, au sens que l'un est forcément plus petit ou égal à l'autre. Ces trois propriétés se retrouvent dans beaucoup d'autres structures mathématiques, par exemple :

- Les nombres rationnels, c'est-à-dire les fractions de la forme r/s , où r et s sont des entiers relatifs. On utilise l'addition et la multiplication usuelles, mais au lieu de l'ordre habituel, on ordonne ici les rationnels par leur « hauteur », c'est-à-dire le maximum entre le numérateur et le dénominateur de la fraction sous forme réduite (sans tenir compte du signe). La hauteur est en quelque sorte une mesure de la complexité d'un nombre rationnel.

- Les polynômes, c'est-à-dire des sommes de produits de puissances des variables et de constantes. L'ordre est donné par le degré du polynôme, la plus élevée des sommes des exposants d'un terme du polynôme.

- Les fonctions rationnelles, c'est-à-dire les fractions dont le numérateur et le dénominateur sont des polynômes.

- Les extensions algébriques des nombres rationnels (corps de nombres algébriques) et des fonctions rationnelles (corps de fonctions algébriques).

Il est possible de transposer la conjecture ABC pour ces structures ; le contexte devient ainsi plus clair. R. Mason et W. Stothers ont prouvé l'équivalent de la conjecture ABC pour les polynômes par des méthodes élémentaires en 1981, avant que la conjecture sur les entiers n'ait été énoncée. Et dans le cadre général des corps de fonctions, la relation avec les courbes elliptiques, qui avaient déjà joué un grand rôle dans la preuve du théorème de Fermat, devient évidente.

Considérons une courbe elliptique E . On peut définir trois nombres qui la caractérisent : son invariant modulaire, noté j_E , son discriminant, noté Δ_E , et sa hauteur, notée h_E (voir l'encadré ci-contre). Le comportement de la courbe E est décrit par le radical du discriminant, aussi appelé conducteur de la courbe.

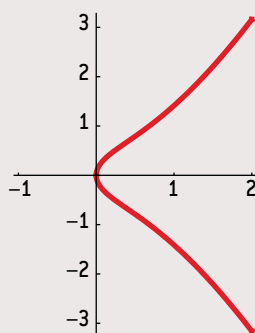
Lucien Szpiro, de l'Université de New York, a conjecturé qu'il existe un nombre k tel que pour toute courbe elliptique E , $\delta(|\Delta_E|) \leq k$ (la puissance moyenne du discriminant est bornée). Il est remarquable que L. Szpiro ait observé ce comportement dans le cas des corps de fonctions, et ait formulé un analogue pour le cas des corps de nombres.

Un lien intime avec les courbes elliptiques

Une courbe elliptique E (ci-contre un exemple) est l'ensemble des points de coordonnées (x, y) solutions d'une équation de la forme $y^2 = x^3 + ax + b$, où a et b sont des entiers tels que le « discriminant » $\Delta_E = 4a^3 - 27b^2$ soit non nul (cela garantit que la courbe n'ait pas de points singuliers).

On peut définir une hauteur de Faltings h_E pour une courbe elliptique E . Lorsque la courbe est « semi-stable », h_E est reliée à la hauteur du nombre $j_E = 12^3 \cdot 4a^3 / \Delta_E$, nommé invariant modulaire.

La « conjecture sur la hauteur des courbes elliptiques », formulée par l'auteur, énonce que la hauteur h_E est bornée par une quantité qui dépend du radical du discriminant Δ_E ($h_E \leq k \log \text{Rad}(|\Delta_E|)$). La conjecture ABC découle de celle sur les hauteurs.



L. Szpiro a prouvé cette conjecture dans le cas des corps de fonctions (pour $k = 6$), si bien que la version forte de la conjecture *ABC* est vraie pour ces corps (ce qui généralise le résultat de R. Mason et W. Stothers). Cela justifie l'espoir que la conjecture soit valable pour les nombres rationnels qui, du point de vue arithmétique, sont assez semblables aux fonctions rationnelles.

J'ai généralisé la conjecture de L. Szpiro en affirmant que la hauteur h_E est bornée par un multiple de $\log \text{Rad}(|\Delta_E|)$. J'ai ensuite prouvé que cette « conjecture sur la hauteur des courbes elliptiques » entraîne la conjecture *ABC*. Ces deux dernières sont même équivalentes dans le cadre des fonctions rationnelles.

En exploitant la très riche théorie des courbes elliptiques, développée depuis plus de 200 ans, notamment en utilisant des résultats qui ont conduit G. Faltings à la preuve de la conjecture de Mordell, j'ai ainsi trouvé une borne – malheureusement toujours exponentielle – de C en fonction de $\text{Rad}(ABC)$.

Mais on a fait encore mieux. Par sa relation avec l'arithmétique des courbes elliptiques, la conjecture *ABC* s'intègre à la géométrie algébrique. Cette branche des mathématiques, qui donne une interprétation géométrique à des problèmes de la théorie des nombres et apporte ainsi des éclaircissements surprenants, a été révolutionnée dans les années 1960 par le mathématicien Alexandre Grothendieck.

D'après moi, la conjecture sur la hauteur des courbes elliptiques n'est pas seulement un énoncé profond sur ces objets en question, mais aussi l'arrière-plan structurel recherché pour la conjecture *ABC*. Et pour J. Oesterlé, la motivation essentielle de la conjecture *ABC* était son rapport avec l'arithmétique des courbes elliptiques.

La conjecture sur la hauteur des courbes elliptiques étant vraie pour le corps des fonctions rationnelles, la conjecture *ABC* l'est aussi pour ce corps. Ma démonstration en est simple et courte, mais on ne peut malheureusement pas la transposer du monde géométrique vers celui des nombres. En revanche, la démonstration initiale de L. Szpiro, bien plus compliquée, fournit une ébauche d'une telle transposition.

Cette preuve tire parti de l'arithmétique des surfaces algébriques, bien étudiées en géométrie algébrique. Il existe un analogue à ces surfaces dans le monde des nombres,



Winfried Scharau

5. ALEXANDRE GROTHENDIECK (ici au Vietnam en 1967) a refondé dans les années 1960 la géométrie algébrique. Né en 1928, ce fils d'un anarchiste russe a découvert très jeune des résultats révolutionnaires, malgré une formation sommaire. En 1970, notamment par conviction antimilitariste, il quitte l'Institut des hautes études scientifiques, près de Paris. Depuis 1991, il vit retiré du monde dans les Pyrénées.

appelé « surfaces arithmétiques ». Ces objets jouent un rôle clef dans la démonstration de la conjecture de Mordell, et les propriétés des surfaces arithmétiques qui permettraient de prouver la conjecture sur la hauteur des courbes elliptiques sont bien identifiées. Nous sommes cependant loin d'avoir trouvé ces propriétés...

Les travaux de S. Mochizuki ont-ils changé la donne ? Expert reconnu dans le domaine des surfaces arithmétiques, S. Mochizuki a prouvé des résultats difficiles sur la relation entre les « groupes fondamentaux au sens de Grothendieck » et les surfaces. Derrière ces termes et ces résultats se cachent encore des idées profondes de A. Grothendieck reliant la théorie de Galois à l'arithmétique. De nombreux spécialistes de la théorie des nombres se sont attelés à la vérification des travaux de S. Mochizuki, qui occupent des centaines de pages et qui utilisent des objets et méthodes mathématiques peu classiques. En attendant leur verdict, la conjecture *ABC* reste non démontrée.

On est au moins sûr d'une chose. La conjecture *ABC* n'est pas une bizarrerie gratuite de la théorie des nombres. Elle a de vastes conséquences et découle elle-même d'autres conjectures, dont il y a de bonnes raisons de penser qu'elles sont vraies. La relation entre théorie des nombres et géométrie qui sert de fondation depuis 50 ans à la géométrie algébrique serait mise à rude épreuve si la conjecture *ABC* était fausse. Il est difficile de l'imaginer. ■

■ BIBLIOGRAPHIE

S. Mochizuki, *Inter-universal Teichmüller theory I : Construction of Hodge theatres*, 2012. Prépublication : www.kurims.kyoto-u.ac.jp/~ffmotizuki/Inter-universal/Teichmuller/Theory/I.pdf

G. Frey, *Der Beweis des Fermatschen Theorems*, *Moderne Mathematik*, pp. 166-175, Spektrum Akademischer Verlag, 1996.

G. Frey, *Links between solutions of $A - B = C$ and elliptic curves*, *Number Theory - Lecture Notes in Mathematics*, vol. 1380, pp. 31-62, Springer, 1989.

J. Oesterlé, *Nouvelles approches du théorème de Fermat*, *Séminaire Bourbaki*, exposé 694, 1987-88.

F. Beukers, *Introduction to the ABC conjecture*, conférence donnée le 9 septembre 2005 : www.math.leidenuniv.nl/~fdesmit/ic/abc/fritsABCpresentation.pdf

La liste des bons triplets : www.rekenmeemetabc.nl/?item=h_stats.

Projet de calcul collaboratif des bons triplets : www.abccathome.com