

S

tar *Trek*, *Doctor Who*, *Les Simpsons*... ces trois séries ont en commun d'avoir mis à l'honneur lors d'au moins un épisode l'un des plus célèbres théorèmes mathématiques. Quel résultat a-t-il mérité une telle récupération populaire? Le dernier théorème de Fermat, selon lequel $x^n + y^n = z^n$ n'admet pas de solution quel que soit $n > 2$. L'énoncé est simple, la démonstration, beaucoup moins.

Tout commence en 1637 quand Pierre de Fermat, magistrat et mathématicien, note dans la marge de son édition des *Arithmétiques*, de Diophante: «Au contraire, il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré: j'en ai découvert une démonstration véritablement

Dans le corps $\mathbb{C}$ des nombres complexes, l'équation de Fermat engendre une surface fermée et orientable, caractérisée par son genre, c'est-à-dire le nombre de trous qu'elle possède. Deux surfaces qui présentent le même nombre de trous sont topologiquement équivalentes: elles sont de genre égal. Si deux surfaces ont le même genre, on passe de l'une à l'autre à l'aide d'une succession de transformations continues comme les déformations d'une surface en caoutchouc.

merveilleuse que cette marge est trop étroite pour contenir.» On peut douter qu'il l'ait vraiment démontré, car ce n'est qu'en 1995 qu'un autre mathématicien, l'anglais Andrew Wiles, a pu en venir à bout à l'aide d'outils mathématiques très complexes. Ce fut l'épilogue d'une longue histoire riche en détours et en rebondissements.

Remontons le cours de l'histoire, et revenons au début du XIX^e siècle. À cette époque, les mathématiciens savent qu'il suffit de prouver le théorème pour les nombres premiers pour qu'il soit valide quel que soit n . Grâce à Ernst Kummer (1810-1893), ils savent en outre que le théorème est vrai pour les nombres premiers p qu'il a qualifiés de «réguliers» (une certaine propriété liée aux racines du polynôme $x^p - 1$ doit être vérifiée), et qu'il suffit donc de le démontrer pour les nombres premiers «irréguliers».

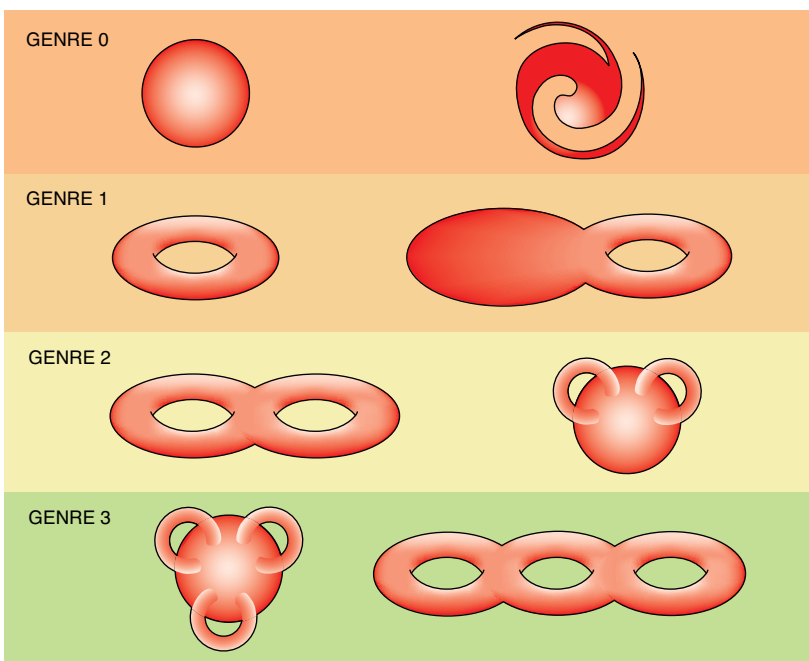
Toutefois, deux problèmes persistent. D'abord, il n'est pas facile de déterminer si un nombre premier est «régulier». Kummer a trouvé un critère permettant de déduire cette caractéristique, mais plus le nombre premier est grand, plus ce critère est lourd à déterminer. Il s'en est toutefois servi pour démontrer le théorème de Fermat pour tous les nombres premiers réguliers inférieurs à 100. Il est en revanche difficile d'aller plus loin à la main.

Ensuite, Kummer espérait qu'une infinité de nombres p étaient réguliers, faisant de ceux qui ne le sont pas des exceptions. Or, en 1915, le mathématicien danois Johan Jensen montre qu'il existe une infinité de nombres irréguliers.

UNE GOUTTE DANS L'OcéAN

Avec l'avènement de l'informatique, le seuil des nombres premiers réguliers connus croît progressivement: les recherches sur ordinateur montrent que la plupart des nombres premiers inférieurs à un certain seuil sont réguliers et que les exceptions jouissent d'une propriété supplémentaire, une sorte de régularité faible qui fait que le théorème de Fermat s'applique aussi à ces entiers. Cela réduit d'autant le nombre de cas à traiter au-dessous d'un certain seuil pour démontrer la validité du théorème de Fermat sous ce seuil. Ainsi, en 1983, le théorème est vérifié pour n inférieur à 1 million, puis, en 1992, pour n inférieur à 4 millions.

Ces imposants résultats ne sont cependant qu'une goutte dans l'océan infini des nombres, et le problème de la démonstration du théorème dans sa généralité reste entier.



LA THÉORIE DES GROUPES DE GALOIS

En 1831, un mathématicien français d'une vingtaine d'années, Évariste Galois (1811-1832), soumet à l'Académie des sciences un manuscrit sur la résolution des équations algébriques. Son manuscrit est refusé, qualifié d'inintelligible par ses examinateurs Lacroix et Poisson. Le jeune homme décède un an plus tard au cours d'un duel. Ses travaux ne seront redécouverts que dans les années 1840, par Joseph Liouville, qui les publie en 1846 dans son propre journal, intitulé *Journal de mathématiques pures et appliquées*. La théorie de Galois deviendra un élément incontournable des mathématiques modernes. De quoi s'agit-il ?

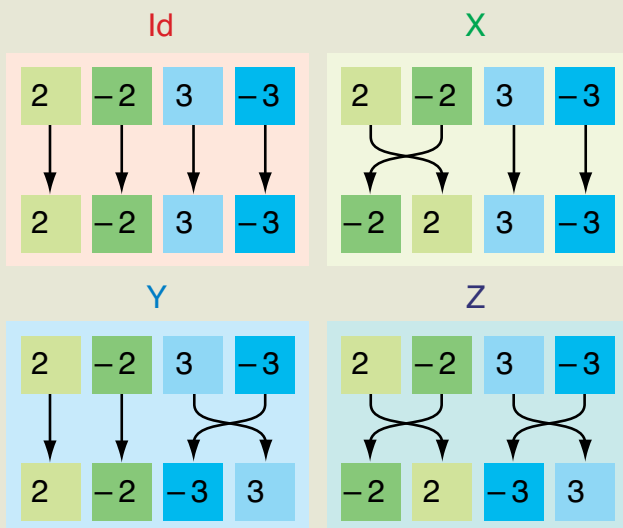
Galois a élaboré une théorie pour déterminer si une équation polynomiale de degré n à coefficients rationnels est résoluble par radicaux, c'est-à-dire à l'aide de ses coefficients et d'un nombre fini d'opérations classiques (addition, soustraction, multiplication, division et extraction de racines). Pour cela, il a associé à chaque équation un objet, qui constitue une « carte génétique » de l'équation. Cet objet est un groupe, le « groupe de l'équation » aujourd'hui baptisé « groupe de Galois ». Galois sait que si une fonction des solutions d'une équation est invariable quand on permute les solutions qu'elle renferme, elle s'exprime rationnellement à l'aide des coefficients de l'équation. Par exemple, la fonction $V(x_1, x_2) = x_1^2 + x_2^2$, où x_1 et x_2 sont les solutions de l'équation du second degré $x^2 + px + q = 0$, est invariante par les permutations du groupe S_2 , ensemble des permutations de deux éléments. Ces permutations sont l'identité, et la transposition qui échange x_1 et x_2 . Pour Galois, un groupe (fini) est un ensemble où la composition de deux éléments est un élément du groupe. Cette notion n'est pas si éloignée de la conception moderne du mot groupe (voir l'encadré page suivante). La fonction V

s'exprime donc rationnellement à l'aide des deux coefficients p et q de l'équation. Ici, le calcul est simple : $V(x_1, x_2) = (x_1 + x_2)^2 - 2x_1x_2$, avec $x_1 + x_2 = -p$ et $x_1x_2 = q$. Galois étend ce résultat et démontre que toute fonction des solutions d'une équation, invariable par certaines permutations de ces solutions, mais pas toutes, s'exprime rationnellement en fonction des coefficients de l'équation. Il démontre ensuite que les permutations des racines d'une équation qui conservent les relations rationnelles entre ces racines constituent un groupe, le groupe de Galois. Enfin, il démontre qu'à toute équation algébrique, on peut associer un tel groupe. Galois a ainsi établi une correspondance entre une fonction déterminable rationnellement et les permutations du groupe de l'équation. C'est cette correspondance entre fonctions et groupes finis, adaptée aux courbes elliptiques et aux fonctions modulaires, que Wiles utilise dans sa démonstration de la conjecture de Shimura-Taniyama-Weil. Plus précisément, il utilise la correspondance entre le groupe de Galois absolu $G_{\mathbb{Q}}$ et des sous-ensembles de points des courbes elliptiques et des fonctions modulaires (voir l'encadré page 103). Le groupe de Galois absolu réunit toutes les « cartes génétiques » des équations polynomiales à coefficients rationnels : un élément de $G_{\mathbb{Q}}$ détermine ainsi sur chaque équation une permutation particulière des racines.



Évariste Galois, mathématicien malheureux (1811-1832).

Norbert Verdier, IUT de Cachan



o	Id	X	Y	Z
Id	Id	X	Y	Z
X	X	Id	Z	Y
Y	Y	Z	Id	X
Z	Z	Y	X	Id

L'ensemble des permutations Id, X, Y, Z constitue un groupe de l'équation $x^4 - 5x^2 + 6 = 0$, car la composition de deux éléments donne un élément de l'ensemble (les quatre racines de l'équation sont $\pm\sqrt{2}$ et $\pm\sqrt{3}$ car l'équation s'écrit $(x^2 - 2)(x^2 - 3) = 0$). En outre, en examinant la table d'opération du groupe, on remarque que l'ensemble {Id, X} est aussi un groupe : c'est un sous-groupe du groupe {Id, X, Y, Z}.

LA NOTION MODERNE DE GROUPE

La structure de groupe est centrale dans les branches les plus variées des mathématiques (groupes de Lie, géométrie algébrique, topologie algébrique et différentielle, théorie des nombres...). Un groupe est un ensemble d'éléments fermé pour une loi de composition $\times$ associative, c'est-à-dire que $(x \times y) \times z = x \times (y \times z)$ pour tous x, y, z de l'ensemble. En outre il existe un élément neutre u (unité) de l'ensemble tel que $u \times x = x \times u = x$ pour tout élément x , et chaque élément x possède un inverse x' dans l'ensemble tel que $x \times x' = x' \times x = u$. Enfin, le groupe est commutatif si pour tout couple (x, y) , on a $x \times y = y \times x$. Il est aisé de vérifier que l'ensemble $\mathbb{Z}$ des entiers relatifs (ayant un signe) forme un groupe commutatif pour la loi de composition « addition » ; l'élément neutre est $u=0$ et l'inverse de x est l'entier $-x$. En revanche, l'ensemble $\mathbb{N}$ des entiers naturels muni de la loi de composition $+$ n'est pas un groupe. Cette notion abstraite de groupe fut introduite par l'Anglais Arthur Cayley en 1854.

➤ Retour au début du xx^e siècle. L'examen de l'équation (1) $x^n + y^n = z^n$ montre que, pour n'importe quel n (y compris 2), lui trouver des solutions entières est équivalent à chercher des solutions rationnelles à l'équation (2) : $x^n + y^n = 1$.

Quel est l'intérêt de ce décalage ? Il est avantageux de travailler sur l'équation (2) dans le corps $\mathbb{Q}$ des nombres rationnels plutôt que sur (1) dans l'anneau $\mathbb{Z}$ des entiers, car cette équation se prête à une interprétation géométrique immédiate. Ainsi, pour $n=2$, l'équation (2) devient (3) $x^2 + y^2 = 1$, qui représente l'équation d'un cercle de rayon unité et de centre l'origine du plan. Dans ce cas, déterminer les triplets d'entiers vérifiant $x^2 + y^2 = z^2$ (les triplets pythagoriciens) revient à chercher les points du cercle dont les deux coordonnées sont rationnelles, ce qui est plutôt facile.

Pour $n > 2$ en revanche, les courbes associées à l'équation (2) sont plus compliquées qu'un simple cercle, comme on peut déjà le voir pour $n=3$. L'énigme de Fermat devient un cas particulier du problème général de la recherche des solutions rationnelles (c'est-à-dire dans $\mathbb{Q}$) de n'importe quelle équation polynomiale à deux inconnues x, y . En termes géométriques, cela revient à déterminer les points de coordonnées rationnelles sur les courbes réelles associées à ces équations.

DES COURBES AUX SURFACES

L'intuition qui se révélera gagnante (esquissée par Euler) consiste à immerger $\mathbb{Q}$ non dans le corps $\mathbb{R}$ des nombres réels, mais dans celui des nombres complexes, $\mathbb{C}$. De cette façon, on associe non plus des courbes aux équations (2), mais des surfaces fermées et orientables nommées surfaces de Riemann. Ces surfaces furent

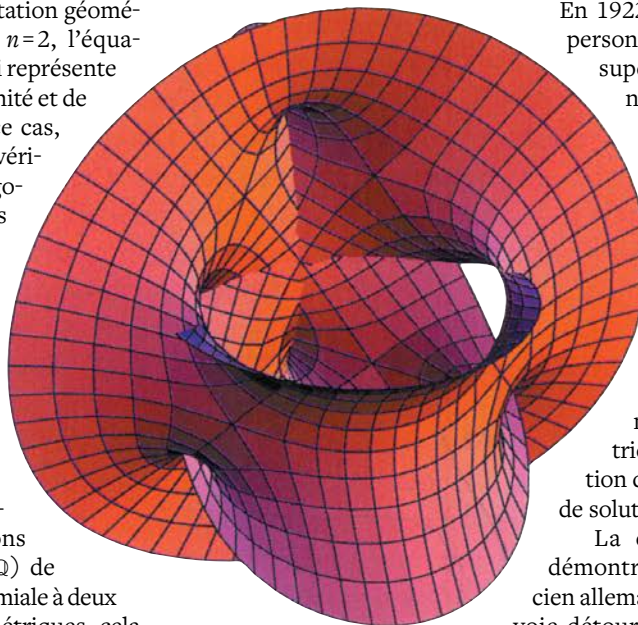
classifiées au xix^e siècle : une surface fermée, orientable et lisse est équivalente, du point de vue topologique, à une sphère avec un certain nombre d'anses (voir la figure page 100). Le nombre d'anses est le genre de la surface. Lorsque la surface est associée à une équation algébrique, le genre est aussi appelé genre de l'équation. Plus le genre est élevé, plus la géométrie de la surface est compliquée et plus il est difficile de trouver les points rationnels de celle-ci. Pour l'équation (2), le genre est donné par la formule $(n-1)(n-2)/2$.

Quand le genre est nul ($n=1$ ou 2), notre problème est simple. Comme nous l'avons vu dans le cas de l'équation (3), si l'équation admet une solution rationnelle, alors elle en admet un nombre infini (il existe bien sûr des équations de genre nul qui n'admettent aucune solution rationnelle, par exemple $x^2 + y^2 = -1$). L'affaire se complique dès lors qu'on considère une équation de genre 1 (c'est-à-dire pour $n=3$). Comme dans le cas précédent, une surface peut ne pas avoir de points rationnels. Mais si elle en a, alors ils sont en nombre fini ou, s'ils sont en nombre infini, ils peuvent être obtenus de manière canonique à partir d'un nombre fini de points rationnels appelés générateurs, comme le démontra le mathématicien anglais Louis Mordell.

En 1922, le même Mordell constate que personne n'a trouvé de courbe de genre supérieur ou égal à 2 possédant un nombre infini de points à coordonnées rationnelles. Il fait de cette constatation empirique une conjecture : aucune équation de genre supérieur ou égal à deux ne peut avoir un nombre infini de solutions « génératrices ». Dans notre contexte, la conjecture de Mordell implique que pour n supérieur ou égal à quatre, l'équation (2) a au plus un nombre fini de solutions « génératrices » et, par conséquent, que l'équation de Fermat a au plus un nombre fini de solutions primitives.

La conjecture de Mordell ne fut démontrée qu'en 1983 par le mathématicien allemand Gerd Faltings, au moyen d'une voie détournée. Qu'on en juge. En 1962, le mathématicien Igor Chafarevich avait proposé la conjecture suivante, qui prit ensuite son nom : sous certaines conditions, on peut reconstruire les solutions entières (c'est-à-dire dans $\mathbb{Z}$) d'une équation à partir de l'étude de cette équation modulo p , pour divers nombres premiers p .

En 1968, A. N. Parshin démontra que la conjecture de Chafarevich impliquait celle de Mordell. Et en 1983, Faltings s'attaqua avec succès à la conjecture de Chafarevich, prouvant comme corollaire celle de Mordell ! La



Surface engendrée par l'équation de Fermat $x^3 + y^3 = 1$ quand x et y sont des variables complexes.

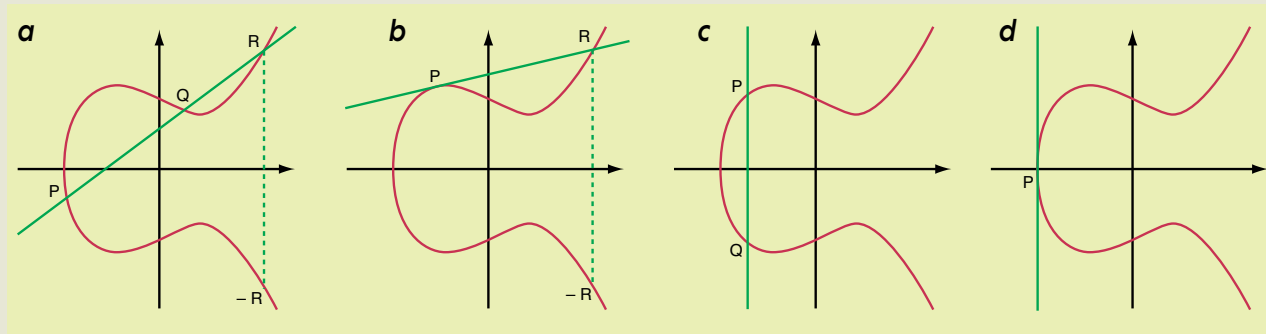
COURBES ELLIPTIQUES ET LOI DE GROUPE

Les courbes elliptiques sont un des outils clés de la démonstration du théorème de Fermat par Andrew Wiles. Voyons de plus près leurs caractéristiques. Une courbe elliptique E est une courbe de genre 1 dont l'équation se ramène à : $y^2 + axy + by = x^3 + cx^2 + dx + e$, où a, b, c, d et e sont des entiers. Une telle équation définit une courbe de genre 1 si elle n'a pas de points singuliers, c'est-à-dire si les dérivées partielles par rapport à x et à y de l'équation ne s'annulent pas en même temps (ce qui impose une condition sur les coefficients). Un point de la courbe E est n'importe quel couple de nombres complexes vérifiant l'équation associée. Si certains points ont des coordonnées réelles (respectivement rationnels), on dit qu'ils sont réels (rationnels). Une propriété cruciale des courbes elliptiques est la suivante : l'ensemble de leurs points forme un groupe commutatif, et il en est de même pour l'ensemble de leurs points réels et celui de leurs points rationnels. En d'autres termes, l'«addition» ou la «soustraction» de deux points de la courbe donne un point de la courbe. Qu'est-ce que l'addition de deux points ? Considérons par exemple la courbe elliptique d'équation : $y^2 = x^3 - x - 1$, et deux points distincts P et Q sur cette courbe (voir la figure). La droite qui les joint recoupe en général la courbe en un troisième point R . On définit la somme des points P et Q comme étant le point symétrique de R par rapport à l'axe des abscisses. Si $P=Q$, on utilise la tangente à la courbe : le point $P+P=2P$ est le symétrique par rapport à l'axe des abscisses du point d'intersection de la tangente en P avec la courbe. L'opposé d'un point P , noté $-P$, est le symétrique de P par rapport à l'axe des abscisses. Et l'élément

neutre du groupe commutatif est le point ∞ , point de rencontre des verticales à l'infini. Ainsi, la somme de P et de son opposé est bien nulle, puisque la droite qui joint ces points est verticale. Autre propriété importante des courbes elliptiques : elles présentent des points de torsion, c'est-à-dire des points dont un multiple entier est nul. Pour un entier $n > 2$, l'ensemble $E[n]$ des points à coordonnées complexes de la courbe E dont le n -ième multiple est 0 (les points de n -torsion), associés au point ∞ , l'élément neutre, constitue un groupe commutatif dit de n -torsion.

On montre, à partir de l'expression des coordonnées de la somme de plusieurs points, que les abscisses x des points de $E[n]$ vérifient une équation polynomiale à coefficients rationnels. Or, par définition, le groupe de Galois absolu conserve les relations algébriques, en particulier l'équation vérifiée par les abscisses des points de $E[n]$, et celle vérifiée par leurs ordonnées – l'équation de E . Par conséquent, il permute les points de $E[n]$ entre eux. C'est grâce à cette propriété que l'on peut établir une correspondance entre le groupe $E[n]$ et le groupe de Galois absolu. On a ainsi construit une représentation galoisienne des courbes elliptiques. Andrew Wiles démontra la conjecture de Shimura-Taniyama-Weil en établissant une correspondance similaire entre le groupe de Galois absolu et les fonctions modulaires, et en montrant que ces deux représentations galoisiennes sont isomorphes.

Catherine Goldstein, institut de mathématiques de Jussieu-Paris-Rive-gauche.



Différents cas d'addition de points P et Q sur la courbe elliptique d'équation $y^2 = x^3 - x - 1$, représentée dans le plan réel. Quand P et Q sont distincts, $P+Q = -R$ (a). Quand $P=Q$, $P+P = -R$ (b). Quand P et Q ont la même abscisse (c), leur somme est égale au point ∞ (là où les droites verticales se rencontrent à l'infini). Quand P et Q sont confondus en un point de tangente verticale, $P+P$ vaut le point ∞ (d).

démonstration de Faltings exploite la résolution, due à Pierre Deligne en 1978, de la conjecture de Weil. André Weil avait proposé en 1949 un analogue pour les corps finis de la célèbre hypothèse de Riemann, formulée à l'origine pour le corps $\mathbb{C}$ des nombres complexes (voir *L'hypothèse qui valait un million*, par P. Meier, page 68).

DÉTOUR PAR LE JAPON

Ainsi aucune équation du type (2) ne peut avoir un nombre infini de solutions génératrices pour $n > 2$. Peu après, en 1985, en utilisant le résultat de Faltings, Andrew Granville et Roger Heath-Brown démontrèrent que le nombre de solutions des équations (2), s'il en existe, est une fonction décroissante de l'entier n . Ce point

ne résout cependant pas l'énigme de Fermat. Il suffit en effet d'une seule solution rationnelle de l'équation (2) pour obtenir une solution entière de l'équation (1) et donc un nombre infini de solutions de celle-ci.

La solution de l'énigme de Fermat fut finalement l'œuvre d'un descendant de la vieille Angleterre émigré aux États-Unis, Andrew Wiles. Le chemin tortueux de la découverte passa par le Japon tumultueux de l'après-guerre. Revenons au cas $n=2$ du théorème, exprimé au moyen de l'équation (3) : $x^2 + y^2 = 1$. On peut paramétriser x et y par respectivement les fonctions cosinus et sinus, qui satisfont la relation : (4) $\cos^2 \alpha + \sin^2 \alpha = 1$.

Résoudre l'équation de Fermat pour $n=2$, c'est-à-dire déterminer les triplets de Pythagore, ➤

➤ revient donc à trouver un angle α dont le sinus et le cosinus sont des rationnels. En 1955, le Japonais Yutaka Taniyama énonça une conjecture qui généralisait cette idée aux courbes elliptiques définies sur $\mathbb{Q}$. Ces courbes, ainsi nommées parce qu'elles interviennent dans la rectification d'un segment d'ellipse, sont les courbes de genre 1 dont l'équation peut se ramener à une expression du type : $y^2 + axy + by = x^3 + cx^2 + dx + e$, où a, b, c, d et e sont des entiers (voir l'encadré page précédente). Taniyama conjectura que ces courbes peuvent être paramétrisées par certaines fonctions dites modulaires qui généralisent les fonctions trigonométriques. On retrouva Taniyama, âgé d'à peine 31 ans, mort dans son appartement le matin du 17 novembre 1958. Dans une lettre laissée sur son bureau, il confiait son intention de mettre fin à ses jours.

Précisée par André Weil en 1968 et reprise en 1971 par un autre Japonais, Goro Shimura, cette conjecture prit le nom de «conjecture de Shimura-Taniyama-Weil». Pour le mathématicien japonais, elle est inspirée par l'idée de la bonté intrinsèque des mathématiques. Quel lien existe-t-il entre cette conjecture et le dernier théorème de Fermat ?

En 1985, l'Allemand Gerhard Frey propose d'associer la courbe elliptique d'équation (5) : $y^2 = x(x+a^n)(x-b^n)$ à un triplet de Fermat (a, b, c) , c'est-à-dire un triplet vérifiant l'équation (6) : $a^n + b^n = c^n$ (en supposant qu'il en existe tout un quelconque n).

L'équation (5) est belle, mais infidèle : selon Frey, cette courbe représenterait un contre-exemple de la conjecture de Shimura-Taniyama-Weil. Il serait impossible de la paramétriser avec des fonctions modulaires. La conjecture de Frey (connue sous le nom de «conjecture epsilon») est une métaconjecture, c'est-à-dire une conjecture selon laquelle si une autre conjecture est vraie (la conjecture de Shimura-Taniyama-Weil) alors le théorème de Fermat l'est aussi.

Un an plus tard, l'Américain Kenneth Ribet démontre que la courbe de Frey n'est pas paramétrisable par des fonctions modulaires. Pour résoudre l'énigme de Fermat, il «suffit» donc à présent de démontrer la prémisse de la conjecture epsilon, c'est-à-dire la conjecture de Shimura-Taniyama-Weil.

LA FIN HEUREUSE D'UNE ÉPOPÉE

On pourrait penser que l'énigme n'a été que simplement déplacée, mais, comme Andrew Wiles le souligne en 1993, travailler sur les courbes elliptiques modulaires, objets géométriques sur lesquels on sait déjà beaucoup et on espère en savoir encore plus, est bien différent de travailler avec les propriétés des nombres, que Fermat qualifiait de fugitives.

La preuve de Wiles s'insère dans ce contexte précis. En premier lieu, il restreint

l'analyse de la conjecture de Shimura-Taniyama-Weil en se limitant à la classe des courbes elliptiques dites semi-stables, classe à laquelle appartient la courbe d'équation (5).

La grande intuition de Wiles consiste à faire appel à un outil fondamental des mathématiques, la théorie des groupes de Galois (voir l'encadré page 101). Au XIX^e siècle, le jeune Évariste Galois a établi une correspondance entre les fonctions rationnelles des solutions d'une équation et le groupe des permutations de ces solutions. L'avantage de cette traduction est qu'un groupe est souvent une structure engendrée par un ensemble fini d'éléments. Wiles propose de comparer les représentations de Galois correspondant aux courbes elliptiques semi-stables avec celles correspondant aux fonctions modulaires.

UN TROU DANS LA DÉMONSTRATION

En 1993, au cours d'une rencontre à l'institut de mathématiques de Cambridge, en Angleterre, il annonce y être parvenu. Mais quelques mois plus tard, en décembre, il reconnaît que sa démonstration présente un «trou». Rentré à Princeton, il se met au travail pour corriger la faille. En octobre 1994, il annonce en être venu à bout en collaboration avec un ex-étudiant de Cambridge, Richard Taylor.

En mai 1995, un long texte de Wiles, intitulé «Modular elliptic curves and Fermat's last theorem» («Les courbes elliptiques modulaires et le dernier théorème de Fermat») et contenant le cœur de son raisonnement, paraît dans la revue *Annals of Mathematics*, suivi d'un autre article écrit en collaboration avec Richard Taylor, «Ring theoretic properties of certain Hecke algebras» («Les propriétés théoriques annulaires de certaines algèbres de Hecke»), qui apporte la solution du point critique. Finalement, en 1999, Taylor, avec Brian Conrad, Christophe Breuil et Fred Diamond complètent le travail de Wiles en montrant que la conjecture de Shimura-Taniyama-Weil est aussi valide pour les courbes elliptiques non semi-stables.

Le dernier théorème de Fermat, qui découle de la conjecture de Shimura-Taniyama-Weil, est enfin démontré. L'épopée séculaire, commencée dans une marge trop étroite, est close. Comme l'écrivit François Rabelais (1494-1553), mieux vaut conclure les controverses par des signes que par des déclamations lorsqu'on recourt à des arguments si compliqués que les paroles humaines ne peuvent suffire à les exposer correctement. C'est pourquoi, après tant d'épisodes personnels bizarres ou dramatiques, la résolution de l'énigme de Fermat confirme le mot du mathématicien américain Hans Lewy : «L'histoire des mathématiques n'est ni tragique ni comique, mais épique.» ■

BIOGRAPHIE

N. VERDIER, Galois : le mathématicien maudit, Belin-Pour la Science, 2011.

R. TAYLOR et A. WILES, Ring-Theoretic Properties of Certain Hecke Algebras, *Annals of Mathematics*, vol. 141, pp. 553-572, 1995.

A. WILES, Modular Elliptic Curves and Fermat's Last Theorem, *Annals of Mathematics*, vol. 141, pp. 443-551, 1995.

C. GOLDSTEIN, Autour du théorème de Fermat, *Mnemosyne* n° 7, pp. 34-61, 1994.