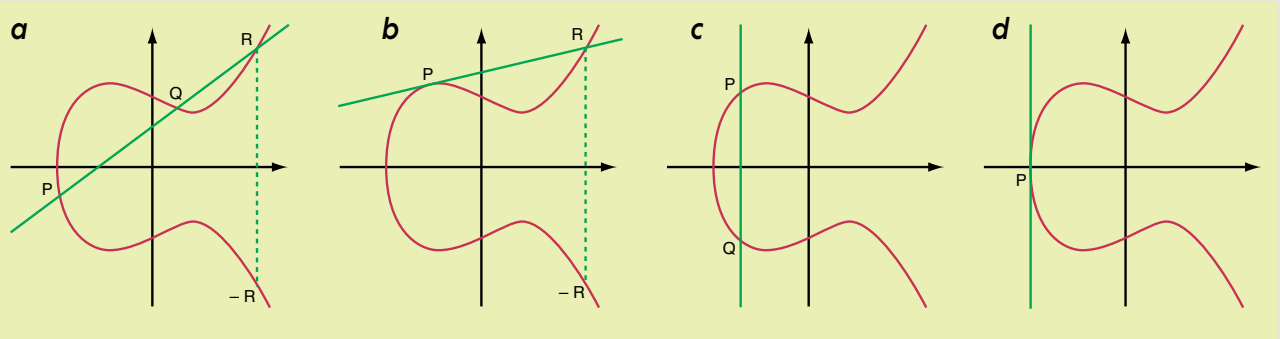
COURBES ELLIPTIQUES ET LOI DE GROUPE

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 pour 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 XIXe 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 elliptics 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 Hecker algebras » (« Les propriétés théoriques annulaires de certaines algèbres de Hecker »), 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, *Mnémosyne* n° 7, pp. 34-61, 1994.