

➤ 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.

Des nombres et des énigmes

Les dernières énigmes préparées
par Ana Retchman et Sébastien Kernivinen.

Solutions page 106.

Ana
Retchman



Sébastien
Kernivinen



ÉNIGME 10

Trouver le plus petit
nombre divisible
par 999 qui ne contienne
pas de 9 parmi
ses chiffres.

ÉNIGME 12

Si p et $p^2 + 8$ sont
des nombres premiers,
quelle est la valeur
de $p^3 + 4$?

ÉNIGME 11

Calculer la somme
de tous les nombres
palindromes
à 3 chiffres.

ÉNIGME 13

Combien de chiffres
a le plus petit nombre entier
qui se termine par 2 tel que
si on déplace le chiffre 2
en tête du nombre on obtient
un nombre deux fois
plus grand ?

ÉNIGME 14

Écrire le nombre
2019 sous la forme
d'une somme
de cinq nombres
entiers au cube.