© Sasha Maslov/Quanta magazine

Akshay Venkatesh, dans le parc de l'Institut d'études avancées, à Princeton, avec un café, son pêché mignon.

des « motifs », des formes reliées aux ensembles de solutions des équations polynomiales (de la même façon qu'un cercle représente les solutions à l'équation $x^2 + y^2 = 1$).

PAVÉS ET TORSION

De l'autre, des formes obtenues par le collage des côtés d'un « pavé », comme le tore l'est à partir d'un carré. Cependant, les « pavés » requis par le programme de Langlands sont moins simples et évoquent plus les compositions d'Escher. L'une des correspondances de ce type est au cœur de la preuve du dernier théorème de Fermat, fournie en 1994 par Andrew Wiles (*voir Le tombeur de Fermat, par G. Giorello, page 98*).

Parfois, les pavés collés ont subi une torsion indétectable par les méthodes classiques du programme de Langlands. Quand Akshay Venkatesh entend parler de cette torsion, il est « convaincu qu'il y a quelque chose d'important à découvrir ». En 2009, Akshay Venkatesh et Nicolas Bergeron de l'université Pierre-et-Marie-Curie, à Paris, ont montré que la torsion est fréquente dans les pavés collés prévus dans les correspondances de Langlands.

Étonnamment, un des principaux résultats de Peter Scholze, autre médaillé Fields de la même « promotion » que Akshay Venkatesh (*voir L'oracle de l'arithmétique, par E. Klarreich, page 84*), a été de montrer que des classes de telles torsions sont justement associées à des « motifs », au sens décrit précédemment.

Ces dernières années, avec des collègues, Akshay Venkatesh a exploré d'autres caractéristiques de ces torsions, « mathématiquement plus profondes, mais moins visibles ». « Le programme de Langlands fourni une sorte de dictionnaire pour passer d'un objet à l'autre, déclare Frank Calegari. Akshay nous dit qu'il y a quelque chose d'encore plus précis. » Pour le moment, Akshay Venkatesh n'a prouvé qu'une infime partie de ses conjectures globales. « Mais au moins j'arrive à mieux voir ce qui devrait être vrai », dit-il.

Ce genre d'investigation, qui s'apparente à l'exploration d'un paysage flou, constitue ce qui lui convient le mieux. Plus tôt dans sa carrière, lorsqu'il ressentait le besoin d'impressionner les autres, il travaillait sur des problèmes déjà balisés, le laissant en partie insatisfait. Il a depuis découvert la sensation d'être sur la piste de « quelque chose d'intéressant qui n'a pas encore été exploré, ou quelque chose d'anormal qui n'a pas beaucoup de sens ».

À Princeton, Akshay Venkatesh et Yiannis Sakellaridis ont travaillé sur deux problématiques distinctes : l'une concernant les fonctions L et l'autre étant une extension des travaux récents d'Akshay Venkatesh sur le programme de Langlands. Étrangement, ces deux thèmes semblent converger vers une même question. « C'est un très bon signe estime-t-il. Je ne sais pas exactement où cela va nous mener. Mais quelque chose nous attend au bout de ce chemin, c'est certain. » À suivre donc ! ■

CÉDRIC VILLANI

« Il y a un roman derrière le grand théorème de Fermat »

BIO EXPRESS

1973
Naissance à Brive-la-Gaillarde, en Corrèze.

2009
Directeur de l'institut Henri-Poincaré.

2010
Lauréat de la médaille Fields.

2017
Député (LREM) de l'Essonne.

Pourquoi l'énoncé de Fermat, qui est simple et anodin en apparence, a-t-il acquis une telle célébrité ?

Cédric Villani : Il y a tout d'abord le contraste entre le côté élémentaire de cet énoncé du XVIIe siècle et la difficulté extrême de sa preuve que moi-même, par exemple, serais incapable de comprendre en détail sans avoir fait trois ou quatre années d'études préalables. L'énoncé de Fermat (quel que soit l'entier n supérieur à 2, il n'existe pas d'entiers positifs a, b et c tels que $a^n+b^n=c^n$) a attiré une multitude de mathématiciens amateurs, qui rêvaient de pouvoir entrer dans l'histoire en trouvant, un peu sur un coup de chance, une preuve. C'est encore le cas aujourd'hui, avec des gens persuadés qu'il existe une démonstration beaucoup plus simple que celle d'Andrew Wiles. Et au fil des siècles, plusieurs mathématiciens éminents ont, au détour de leurs travaux, prouvé le théorème de Fermat pour des valeurs particulières de l'exposant n. Un autre élément d'attrait est l'anecdote historique avec, en particulier, l'erreur ou le bluff de Fermat qui, dans la marge d'un livre, a écrit avoir découvert une démonstration merveilleuse, mais trop longue pour figurer dans cette marge. Il y a un roman derrière le grand théorème de Fermat, et il est haut en couleur !

Le « grand théorème de Fermat » est-il important pour la théorie des nombres ?

Cédric Villani : En soi, non. Ce théorème a ici et là quelques conséquences, mais les méthodes développées pour le démontrer sont de loin plus importantes

que le résultat lui-même. Et c'est une histoire qui a été pleine de rebondissements au cours des dernières décennies.

Dans les années 1980, Andrew Wiles, qui était fasciné depuis son enfance par la conjecture de Fermat, a compris que certains développements dans le domaine où il faisait ses recherches (la géométrie algébrique) lui permettraient peut-être d'élaborer une démonstration. Il a alors travaillé en secret durant des années, avant d'annoncer lors d'un séminaire en 1993 y être parvenu. Mais sa preuve comportait une erreur, et il a fallu l'aide de son ancien étudiant Richard Taylor pour la réviser et l'achever en 1995, dans une course de vitesse pour ne pas se faire doubler par quelqu'un d'autre.

Les méthodes mobilisées pour ce théorème continuent d'ailleurs de bouger, afin de réécrire la preuve et mieux relier l'énoncé de Fermat à d'autres sujets. Tout cela touche des domaines parmi les plus prestigieux des mathématiques, ceux qui font le plus rêver – la théorie des nombres, la géométrie algébrique, champs où l'activité est intense et où l'école française a d'ailleurs une forte expertise.

Pouvez-vous donner une idée de la démarche suivie par Andrew Wiles ?

Cédric Villani : Depuis 1986, on savait, à la suite de divers travaux, que la conjecture de Fermat pouvait être vue comme un cas particulier d'un énoncé plus vaste et plus technique, la conjecture de Shimura-Taniyama-Weil. Cette «conjecture STW», datant des années 1960, prédisait une sorte de dictionnaire, de correspondance, entre les «courbes elliptiques» – des courbes (qui ne sont pas des ellipses…) définies par des équations algébriques du troisième degré à coefficients entiers, et dont on ne considère que les points à coordonnées rationnelles – et des fonctions particulières, les «fonctions modulaires». Or on peut associer une certaine courbe elliptique à l'équation de Fermat et on a montré que si cette équation avait des solutions en nombres entiers, alors la courbe elliptique correspondante ne vérifierait pas la conjecture STW. Par conséquent, si la conjecture STW est vraie, il s'ensuit que l'équation de Fermat n'a pas de solutions en nombres entiers et le grand théorème de Fermat serait ainsi prouvé. Andrew Wiles a donc entrepris de démontrer la conjecture STW.

C'est ce qu'il a réussi à faire ?

Cédric Villani : Presque. Andrew Wiles a réussi à démontrer une partie importante de la conjecture STW, qui suffisait à prouver la conjecture de Fermat. La conjecture STW complète a été démontrée plus tard, en 1999, par Christophe Breuil, Brian Conrad, Fred Diamond et Richard Taylor. Cette conjecture est d'ailleurs une brique d'un édifice plus vaste qu'on appelle le programme ou la correspondance de Langlands.

Andrew Wiles était fasciné depuis son enfance par la conjecture de Fermat. Il a alors travaillé en secret durant des années avant d'annoncer son résultat

De quoi s'agit-il ?

Cédric Villani : C'est un ensemble d'idées et de conjectures complexes qui ont été esquissées à la fin des années 1960 par le mathématicien canadien Robert Langlands. Ce programme établit des ponts, ou des correspondances, entre la théorie des nombres et d'autres parties des mathématiques (géométrie algébrique, théorie des groupes, etc.). Il continue à occuper aujourd'hui de nombreux chercheurs brillants, parmi lesquels Laurent Lafforgue (médaille Fields en 2002), Christophe Breuil, Ngô Bao Châu (médaille Fields en 2010)…

Est-il fréquent que la preuve d'un énoncé élémentaire comme celui de Fermat nécessite des mathématiques de très haut niveau ?

Cédric Villani : Oui, j'y ai moi-même été confronté à plusieurs reprises au cours de ma carrière, dans mes travaux sur la stabilité des gaz et des plasmas. Avec mes collègues, nous nous sommes souvent retrouvés avec des preuves plutôt vertigineuses pour des énoncés qui étaient en eux-mêmes peu compliqués. Le cœur de la preuve peut être assez simple, mais c'est l'enrobage technique qui est très élaboré. Ce qu'on préfère, c'est quand l'idée centrale est à la fois simple et inattendue ; mais ce n'est pas toujours le cas ! ■

Propos recueillis par Maurice Mashaal

Le tombeur de Fermat

Le dernier théorème de Fermat ne fut démontré qu'en 1995, par Andrew Wiles, plus de 360 ans après sa première formulation. Une épopée riche en rebondissements et en détours.

L'ESSENTIEL

- Dans les années 1630, Pierre de Fermat affirma: «Soit n un entier supérieur ou égal à 3. L'équation $x^n+y^n=z^n$ n'a pas de solutions entières non nulles.»
- Plusieurs mathématiciens ont progressé vers la démonstration, parfois au prix de gros efforts intellectuels, mais la preuve définitive n'arriva qu'en 1995.
- Elle passe par des avancées récentes en géométrie arithmétique et notamment dans l'étude des courbes elliptiques et la démonstration de la conjecture de Shimura-Taniyama-Weil.
- Le résultat est important, tant par les méthodes employées, les théories déployées que par les questions soulevées.

LES AUTEURS


GIULIO GIORELLO et CORRADO SINIGAGLIA sont professeurs à l'université de Milan, en Italie.

Andrew Wiles devant le bâtiment qui porte désormais son nom, à l'université d'Oxford.

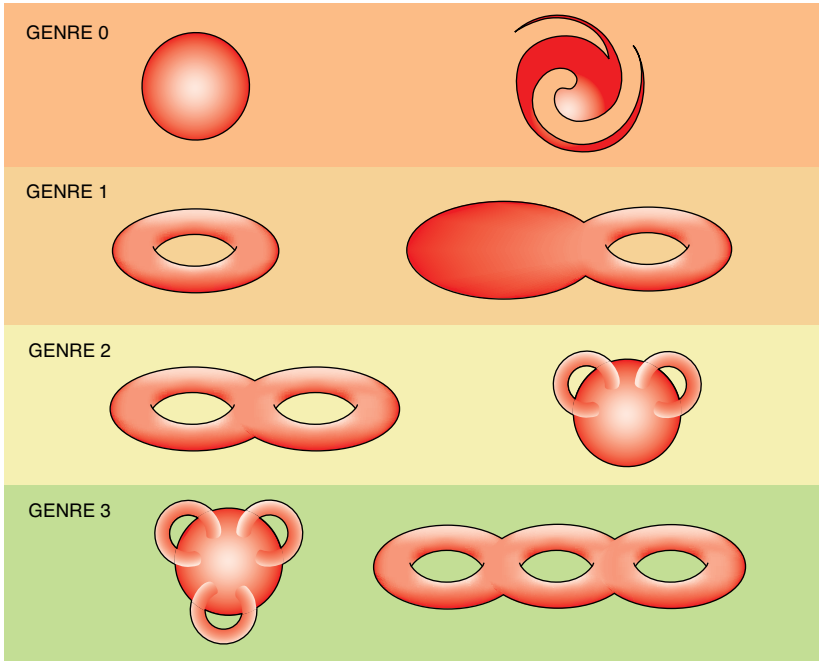
***Star Trek, Doctor Who, Les Simpsons*... ces trois séries ont en commun d'avoir mis à l'honneur lors d'au moins un épisode l'un des plus célèbres théorèmes mathématiques.** Quel résultat a-t-il mérité une telle récupération populaire? Le dernier théorème de Fermat, selon lequel $x^n+y^n=z^n$ n'admet 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 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 XIXe 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.



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.

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 $x_1x_2=q$.

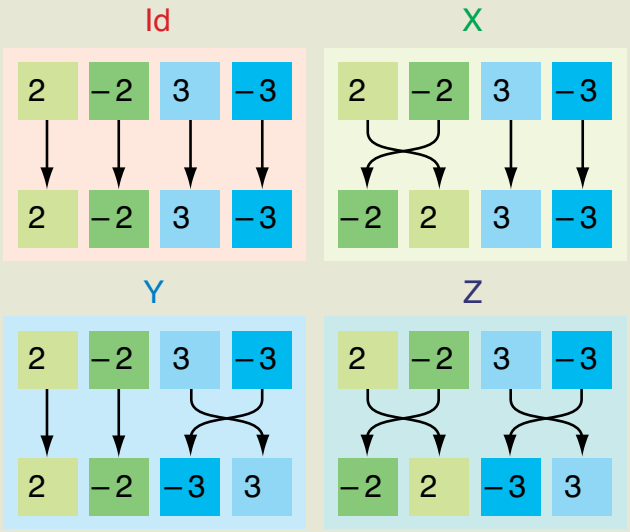
Galois étend ce résultat et démontre que toute fonction des solutions d'une équation, invariable par certaines permutations de ces solutions, mais pas toutes, s'exprime rationnellement en fonction des coefficients de l'équation.

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.

Norbert Verdier, IUT de Cachan

Évariste Galois, mathématicien malheureux (1811-1832).



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}.