

Le dernier théorème de Fermat

L'énoncé de ce théorème est simple : « Si n est un entier supérieur à 2, il n'existe pas d'entiers positifs (non nuls) x, y, z tels que $x^n + y^n = z^n$. Pour $n=2$, il existe une infinité de tels triplets, par exemple (3, 4, 5) puisque $3^2 + 4^2 = 5^2$. On pense que Fermat disposait de la démonstration pour $n=4$.

Le cas $n=3$ a été démontré par Leonhard Euler vers 1760. Le cas $n=5$ a été prouvé par Adrien-Marie Legendre et Johann Dirichlet en 1825. Le théorème a été démontré jusqu'à $n=36$ par Ernst Kummer en 1847. En 1976, Samuel Wagstaff publia une preuve du théorème de Fermat pour tous les entiers compris entre 3 et 1 million.

L'énoncé a été formulé par Pierre de Fermat dans une note écrite dans la marge d'un livre de Diophante, dont l'exemplaire est aujourd'hui perdu.

Plus de trois siècles ont été nécessaires pour qu'une preuve publiée soit reconnue correcte.

Elle est due, pour la partie finale, au mathématicien britannique Andrew Wiles qui en présenta une première version en 1993, et en compléta certaines insuffisances en 1994 avec l'aide de Richard Taylor. Le fait que Fermat ait écrit qu'il disposait d'une jolie preuve du théorème est aujourd'hui considéré comme très probablement dû à une erreur de sa part. C'est principalement par les idées et outils mis en œuvre pour démontrer le résultat qu'il est considéré comme mathématiquement très important.

La preuve repose, entre autres, sur des méthodes et

résultats d'Alexandre Grothendieck et Pierre Deligne. Elle est en définitive fondée sur des systèmes logiques puissants mettant en œuvre des objets mathématiques infinis allant bien au-delà des entiers.

Les logiciens s'interrogent aujourd'hui sur l'utilisation de ces objets à la fois très abstraits et logiquement plus risqués que les entiers. Ils tentent de formuler des preuves du théorème de Fermat qui n'utilisent que les entiers (donc jamais explicitement d'objets infinis).

Ils essaient même de se limiter à des raisonnements simples sur ces entiers tels qu'ils sont définis par le système formel EFA (voir page 83). Obtenir une preuve du théorème de Fermat vérifiable par ordinateur semble aujourd'hui encore hors de portée.



PIERRE DE FERMAT



ANDREW WILES, EN 2016

d'Andrew Wiles a un sens, revenons à la notion de système formel. Les progrès de la logique mathématique ont conduit, au début du XX^e siècle, à une situation étonnante et à vrai dire inattendue. On a réussi à identifier de manière parfaite les règles de raisonnement mises en œuvre en mathématiques, et à les exprimer de façon suffisamment précise pour que la vérification d'une démonstration, dont le mathématicien écrit chaque pas dans ce système de règles, soit faisable mécaniquement, c'est-à-dire sans intelligence. Aujourd'hui, bien sûr, ce « faisable mécaniquement » renvoie à des ordinateurs et des programmes informatiques.

Quand on s'intéresse aux nombres entiers, on tente de formaliser les raisonnements dans le système de l'arithmétique de Giuseppe Peano (qu'on notera PEANO) qui, en particulier, permet les raisonnements par récurrence. On envisage parfois des

systèmes plus faibles, c'est-à-dire disposant de moins de moyens de raisonnement.

Pour traiter d'ensembles infinis d'entiers, de nombres réels comportant une infinité de décimales, de fonctions continues et d'objets plus riches encore tels que des ensembles de fonctions ou des espaces de dimension infinie, on envisage divers systèmes formels.

Plusieurs systèmes formels

Le système le plus souvent retenu est celui de la théorie des ensembles, formalisé au début du XX^e siècle et noté ZFC pour « Zermelo-Fraenkel avec axiome du choix ». Il permet de manipuler directement des objets infinis qui n'existent pas dans PEANO, mais il est plus puissant pour une autre raison : supposer que ZFC est non contradictoire permet de démontrer que PEANO

est non contradictoire, alors que l'inverse est impossible.

Rarement, mais cela arrive, la théorie des ensembles usuelle ZFC n'est pas suffisante. Si, par exemple, on veut parler de toutes les fonctions, ou de tous les groupes et raisonner globalement sur leurs structures et les liens entre ce type de structures (c'est ce que fait la théorie des catégories), on rencontre une ennuyeuse difficulté. En effet, ni « L'ensemble de tous les ensembles », ni « L'ensemble de toutes les fonctions », ni « L'ensemble de tous les groupes », etc., ne sont des ensembles au sens de ZFC, qui ne connaît que les collections d'objets mathématiques de taille limitée. Exprimer les propriétés des grandes structures et les raisonnements qui les concernent exige alors des systèmes formels plus puissants. On utilisera par exemple ceux qu'on obtient à partir de ZFC en ajoutant des axiomes affirmant l'existence d'ensembles très grands.