

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.

Si l'énoncé de Fermat est indécidable, alors il est vrai !

Une question naturelle se pose à propos des énoncés arithmétiques E tels que celui affirmant que tout nombre pair à partir de 4 est somme de deux nombres premiers (conjecture de Goldbach) ou l'énoncé du théorème de Fermat : « Se peut-il que E soit indécidable, c'est-à-dire que ni E ni sa négation, $\neg(E)$, ne soient démontrables ? »

La question, posée dans l'absolu, n'a pas de sens. Il n'y a pas de notion de démonstration dans l'absolu, mais seulement des notions relatives à des systèmes formels comme PEANO, ZFC ou INAC évoqués dans l'article. Il faut donc reformuler la question et se demander par exemple : Est-il possible que le système PEANO ne puisse démontrer ni E , ni $\neg(E)$? Autrement dit : E est-il un indécidable de PEANO ?

On connaît des indécidables de PEANO (par exemple l'énoncé qui affirme que

PEANO est non contradictoire). La question n'est donc pas absurde et c'est d'ailleurs cette question qui est posée par les recherches évoquées dans l'article à propos du théorème de Fermat. La plupart des mathématiciens pensent que l'énoncé de Fermat n'est sans doute pas un indécidable de PEANO, bien qu'aujourd'hui ce ne soit pas démontré.

Cependant, si, en utilisant par exemple les moyens de ZFC (ou INAC), on démontrait que l'énoncé de Fermat est indécidable dans PEANO, alors on disposerait

automatiquement d'une nouvelle preuve du théorème de Fermat dans la théorie qui aurait prouvé l'indécidabilité.

En effet, PEANO a la propriété que tous les énoncés élémentaires du type « $3 + 7 = 10$ », « $2^3 + 3^3 \neq 5^3$ », « 13 est un nombre premier » sont démontrables dans PEANO quand ils sont vrais. PEANO ne passe à côté d'aucune démonstration pour des vérités arithmétiques aussi élémentaires.

La preuve dans ZFC (ou dans INAC) de l'indécidabilité dans PEANO du théorème de Fermat démontrerait, pour chaque quadruplet d'entiers n, x, y, z avec $n > 2$ et x, y, z non nuls, que PEANO n'établit pas $x^n + y^n = z^n$ (dans le cas contraire, PEANO fournirait un contre-exemple à l'énoncé de Fermat, lequel serait donc

décidable), donc que PEANO démontrerait que $x^n + y^n \neq z^n$ (puisque PEANO ne manque aucun énoncé de cette forme). En simplifiant un peu : si l'énoncé de Fermat est indécidable, alors il est vrai.

La même propriété est vraie pour la conjecture de Goldbach. Celui qui démontrerait qu'elle est indécidable dans PEANO en utilisant les moyens d'un système formel F , démontrerait du même coup la conjecture de Goldbach dans le système F . Il ne serait donc pas très malin, face à la difficulté qu'on a à établir la conjecture de Goldbach, de se mettre à rechercher la preuve que la conjecture est indécidable dans PEANO. L'indécidabilité de ce type d'énoncés E dans PEANO est une affirmation plus difficile à prouver que E lui-même.

On adoptera par exemple l'axiome des « cardinaux fortement inaccessibles » qui autorise certaines formes d'ensemble de tous les ensembles et autres grosses collections. Notons INAC un tel système. Si l'on admet qu'il est non contradictoire, alors on sait démontrer que ZFC l'est aussi, alors que l'inverse est impossible.

Quand on passe de PEANO à ZFC puis à INAC, on accepte l'existence d'objets de plus en plus nombreux et gros, mais le monde mathématique supposé devient aussi plus difficilement contrôlable, et on peut même, au-delà d'un certain point (qui varie selon la sensibilité de chacun), considérer ces mondes mathématiques surabondants comme illusoire. Qu'il puisse exister des entités abstraites telles que les entiers est facile à accepter. Pour les nombres réels et leurs décimales qui se prolongent à l'infini, c'est un peu plus difficile, et certains physiciens considèrent ces nombres comme

des fictions commodées sans contrepartie dans le monde réel. Passer au niveau supérieur avec INAC devient un peu déraisonnable, même si les mathématiciens réussissent à penser et à démontrer des choses dans ces univers follement étendus.

Ces trois points de repère, PEANO, ZFC, INAC, ne sont que des échelons d'une série plus riche de systèmes formels envisagés par les mathématiciens et les logiciens.

Ontologie risquée

Un système formel décrit un ensemble de possibilités de manipulations de formules qui donnent à l'arrivée les théorèmes. Il ne faut pas qu'il permette de démontrer une formule absurde du type $0 = 1$, qui serait en contradiction avec la formule $0 \neq 1$ (le système serait alors incohérent, « inconsistant » ou contradictoire). En effet, dès qu'on a une contradiction, tout devient vrai et tout devient

faux à la fois : plus rien n'a de sens. Passer d'un système faible (par exemple PEANO) à un système plus puissant fait prendre des risques, puisqu'on accroît l'ensemble des énoncés que l'on peut démontrer.

On sait aussi que prouver qu'on ne prend pas de risques (de rencontrer une contradiction qui détruirait tout) est impossible ou nécessairement insatisfaisant. En effet, l'une des conséquences des théorèmes d'incomplétude de Gödel est que, pour démontrer qu'un système est non contradictoire, on doit se placer dans un système plus puissant (donc plus risqué !). S'élever dans la puissance des systèmes formels fait prendre des risques de non-sens.

Ainsi, lorsqu'on s'intéresse à des énoncés sur les entiers, il est souhaitable de ne pas s'aventurer à utiliser des objets infinis, ou, ce qui revient au même, il faut rester sage dans PEANO ou un système formel sans infini plus faible encore.