

Fermat enfin démontré

YVES HELLEGOUARCH

La démonstration du théorème de Fermat par Andrew Wiles s'appuie sur un faisceau de méthodes mathématiques qui bouleverse le paysage de la théorie des nombres.

Vers la fin de sa vie, Pierre de Fermat (1601-1665), écrivait, dans ses *Défis aux mathématiciens* : « On sait qu'Archimède n'a pas dédaigné de travailler sur des propositions de Conon, qui étaient vraies, mais non prouvées, et qu'il a su les munir de démonstrations d'une haute subtilité. Pourquoi n'espérerais-je pas un semblable secours de vos éminents correspondants, pourquoi, Conon français, ne trouverais-je pas des Archimède anglais? »

Le 23 juin 1993, plus de 300 ans après la note marginale de Fermat, Andrew Wiles, professeur à Princeton (États-Unis), mais fils d'un professeur de théologie anglais, pensait pouvoir annoncer à l'Institut Newton, à Cambridge (Grande-Bretagne) qu'une des propositions que Fermat nous avait léguées – peut-être involontairement, car on peut se demander si la remarque qu'il avait faite en marge d'un exemplaire des *Arithmétiques* de Diophante était destinée à être publiée – était désormais munie d'une démonstration d'une haute subtilité et d'une éblouissante beauté. Il semblait que Fermat avait trouvé son Archimède anglais.

Pourtant, un des artifices d'Andrew Wiles était encore en porte-à-faux, et ce n'est que le 19 septembre 1994, à l'issue d'un labeur intense et grâce au renfort de son collègue Richard Taylor de l'Université de Cambridge, que la magnifique cathédrale édiflée par A. Wiles était enfin libérée de tout échafaudage et s'élevait triomphante dans le ciel mathématique, symbole d'un labeur de trois siècles (ce qui n'est pas exceptionnellement long pour une cathédrale). Cette dernière hésitation du destin illustre bien les mystères et les surprises recelées par le « dernier théorème de Fermat ».

Position du problème

L'article de Christian Houzel du mois dernier nous a rappelé l'Histoire de la recherche des triplets pythagoriciens, les entiers x, y et z , solutions en nombres entiers de l'équation $x^2 + y^2 = z^2$ (1). Ces triplets pythagoriciens sont en correspondance avec les points du cercle centré sur l'origine, de rayon unité et d'équation $u^2 + v^2 = 1$, points dont les deux coordonnées sont rationnelles, c'est-à-dire de la forme a/b où a et b sont entiers. Il suffit, pour s'en convaincre, de diviser les deux membres de l'équation (1) par z^2 .

La résolution de cette équation (1), dite diophantienne, est connue depuis fort longtemps. Pour les exposants supérieurs à 2, les équations de la forme $x^n + y^n = z^n$, la solution est radicalement différente. L'assertion de Fermat est que, pour les valeurs de l'exposant n supérieures à 2, les seules solutions entières sont « triviales » : l'un des trois nombres entiers est nul (par exemple, $x = 0$ et $y = z$), ce que l'on exprime en notant que le produit xyz est alors égal à zéro.

Revenons à l'interprétation géométrique : les courbes représentant l'équation $u^n + v^n = 1$ appartiennent à deux familles : une première famille où l'exposant est pair (n est égal à $2p$), et la seconde où l'exposant est impair (n est égal à $2p + 1$). Le cas n égal à 4 a été résolu par Fermat lui-même. Le cas où n est égal à $2p$ avec p impair résulte du cas où n est impair. En effet, en posant $u' = u^2$ et $v' = v^2$ et en remplaçant dans l'équation, on voit qu'il ne reste plus qu'à traiter le cas impair.

On peut même se limiter au cas où n est premier (et évidemment différent de 2), bien que la spécification que le nombre p doit être premier semble très restrictive. En fait cette limi-

tation de la portée du théorème est trompeuse : si l'équation de Fermat pour le nombre p premier n'a pas de solution, alors comme $(x)^{kp}$ est égal à $(x^k)^p$ la solution n'existe pour aucun multiple de p .

Dans le cas où p est premier impair, la courbe $u^p + v^p = 1$ possède trois points rationnels triviaux, le point $(u,v) = (1,0)$, le point $(u,v) = (0,1)$, et le point à l'infini de la courbe, lequel correspond à la solution $(x,y,z) = (1,-1,0)$ de l'équation diophantienne $x^p + y^p = z^p$. L'assertion de Fermat revient à dire que si p est premier et différent de 2, la courbe $u^p + v^p = 1$ n'admet pas d'autre point rationnel : il faut démontrer qu'il n'y a que trois points rationnels sur la courbe.

Les derniers résultats classiques

Lorsqu'ils sont bloqués dans leurs recherches, les mathématiciens ont une stratégie particulière : ils étudient des variations du problème qu'ils présentent sous des formes différentes. Le grand mathématicien Niels Henrik Abel écrivait que l'on devait donner à un problème d'impossibilité « une forme telle qu'il soit toujours possible de le résoudre, ce que l'on peut toujours faire... Au lieu de demander une relation dont on ne sait pas si elle existe ou non, il faut (se) demander si une telle relation est en effet possible ». On en déduit alors les limites de possibilité du problème original.

C'est ainsi que les algébristes italiens du XVI^e siècle ont introduits les nombres « imaginaires » pour étudier les solutions réelles des équations algébriques. Pragmatique, Newton écrivait : « il faut bien que dans les équations, il y ait des racines impossibles (entendez « imaginaires ») sans quoi, dans les problèmes (physiques), cer-

tains cas impossibles se trouveraient possibles».

En théorie des nombres, les mathématiciens varient la structure : au lieu d'examiner les solutions entières des équations, ils examinent les solutions modulo k . Ils regroupent dans une même classe les nombres qui ont le même reste après division par k . Ainsi la classe des nombres pairs est constituée par les nombres égaux à zéro modulo 2.

Les entiers modulo k ont une structure d'anneau, c'est-à-dire qu'ils sont munis d'une addition et d'une multiplication reflétant l'addition et la multiplication ordinaires. Lorsque k est égal à 2 les restes sont 0 et 1, et l'on a :

+	0	1
0	0	1
1	1	0
ADDITION		

×	0	1
0	0	0
1	0	1
MULTIPLICATION		

En utilisant la loi de réciprocité quadratique due à Euler, Legendre et Gauss, le mathématicien Gérard Terjanian a su faire resplendir, en 1977, les méthodes traditionnelles d'un éclat particulier.

Il a démontré que, si n est égal à $2p$, où p est un nombre premier impair, alors l'un des trois nombres x, y, z vérifiant l'équation de Fermat pour l'exposant $2p$, est égal à zéro modulo $2p$, c'est-à-dire est divisible par n . C'était la première fois qu'un résultat aussi général était obtenu pour ce qu'il est convenu d'appeler le «premier cas du théorème de Fermat».

Dans les méthodes classiques, mais pas dans la méthode de A. Wiles, la démonstration de Fermat comporte toujours deux étapes. La première, que l'on appelle le «premier cas» est la plus facile ; elle consiste à démontrer, lorsque l'exposant est un nombre premier p , que p divise l'un des trois nombres x, y, z vérifiant l'équation de Fermat.

Donnons un exemple d'une telle démonstration. Par exemple, si p est égal à 3, on examine les solutions modulo 9 de l'équation $x^3 + y^3 = z^3$; on voit alors facilement que 3 divise x, y ou z .

En présentant les choses négativement (raisonnement par l'absurde), on prouverait le premier cas de Fermat en disant que si p ne divise pas xyz , alors l'équation $x^p + y^p = z^p$ est impossible. Comme zéro est divisible par tous les nombres, y compris p , les solutions tri-

viales sont éliminées d'emblée. Cet avantage se retrouvera dans la méthode de Andrew Wiles.

Dans le second cas, beaucoup plus difficile, il s'agit de démontrer que, non seulement p divise xyz , mais que toutes les puissances de p divisent xyz , ce qui implique que xyz est égal à 0 (un nombre non nul n'étant pas indéfiniment divisible).

Fermat avait trouvé une «route tout à fait singulière» pour résoudre le second cas et d'autres problèmes de cette nature : la «descente infinie» (voir *De Diophante à Fermat*, par Christian Houzel, *Pour la Science*, janvier 1996).

La descente infinie est un ingrédient essentiel de toutes les preuves classiques du «second cas» du théorème de Fermat, alors qu'elle est inutile pour le «premier cas», comme nous l'avons vu. Ici une véritable mutation va se produire : la méthode de A. Wiles traitera d'un seul coup de baguette magique les premier et deuxième cas, et ceci pour tous les exposants à la fois.

Finalement, en 1985, au moment où l'Histoire semblait hésiter entre tradition et idées à venir, trois hardis mousquetaires, Adleman, Fouvry et Heath-Brown essayèrent de régler définitivement le sort du premier cas. S'ils échouèrent, du moins échouèrent-ils avec panache : ils démontrèrent le premier cas pour une infinité d'exposants premiers. Ce résultat fit beaucoup de bruit, mais les mathématiciens savaient qu'il s'agissait d'un combat

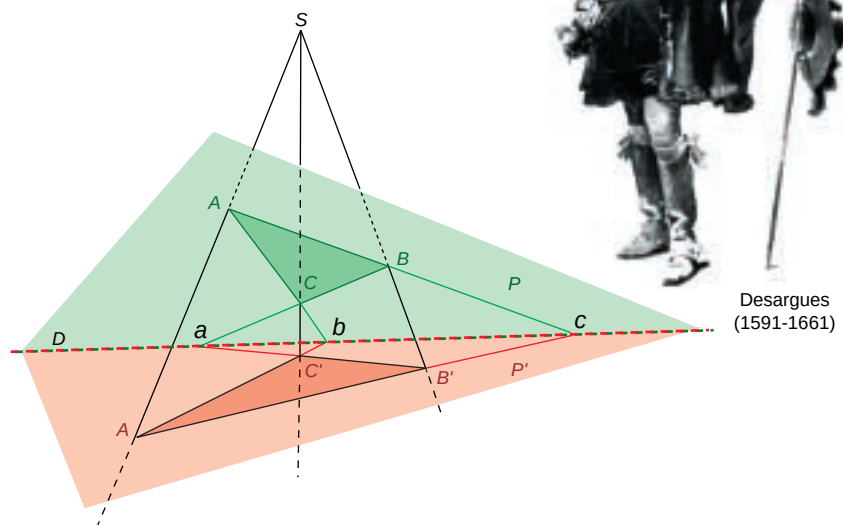
d'arrière-garde et que les batailles futures allaient se livrer sur d'autres fronts.

Le groupe de Galois absolu

À l'époque de Kummer déjà, les nombres algébriques avaient fait leur apparition dans l'étude du théorème de Fermat. Nous allons définir ces nombres mystérieux qui vont jouer un rôle essentiel.

Un titre plus romantique pour ce sujet pourrait être «le corps des nombres algébriques et les représentations de son âme». En effet, la philosophie qui sous-tend ce type de question a d'abord été rêvée par Évariste Galois à la prison de Sainte-Pélagie (en 1831) avant de trouver sa consécration officielle dans le programme d'Erlangen de Félix Klein (en 1872). Cette philosophie consiste à attacher, à tout objet mathématique muni d'une structure, le groupe des transformations de cet objet qui respectent cette structure. On appelle ce groupe, le groupe des automorphismes de l'objet.

Si l'objet est l'ensemble des trois sommets d'un triangle isocèle (et non équilatéral) et sa structure la distance



Desargues (1591-1661)

1. LES GÉNÉRALISATIONS à des dimensions supérieures sont des moyens puissants de démonstration. Ainsi des propriétés de figures planes ne sont que les ombres de propriétés de figures dans l'espace. Si SAA', SBB', SCC' sont alignés, alors a, b, c le sont aussi. Ce théorème, dû à Desargues, est démontré facilement en donnant du relief à la figure : celle-ci est considérée comme la projection plane de deux triangles en perspective dans l'espace, les triangles ABC et $A'B'C'$, situés dans deux plans distincts, P et P' . Alors les points a, b, c sur la droite d'intersection D des plans P et P' , sont alignés.