Le Dernier Théorème de Fermat

H. Darmon

September 9, 2007

Le 23 Juin 1993, dans une salle de conférences bondée de l'Institut Isaac Newton à Cambridge, Andrew Wiles achève le dernier de ses trois exposés sur les "Courbes elliptiques, formes modulaires, et représentations Galoisiennes". Sujet passionnant... pour les initiés. Mais pourquoi ces journalistes des plus grands quotidiens britanniques, conviés en hâte? Pourquoi cette atmosphère d'attente presque fièvreuse?

De sa belle écriture soignée, Andrew Wiles inscrit au tableau noir: "Corollaire: si $u^n + v^n = w^n$, et $n \geq 3$, alors $uvw = 0$."

Ce que vient d'accomplir ce professeur de l'Université Princeton, ce n'est rien de moins que la solution d'un des problèmes les plus célèbres des mathématiques. La question est apparue en 1637 sous la plume de Pierre de Fermat, juriste Toulousain et mathématicien amateur, qui, presque à lui seul, a ressucité la théorie des nombres, délaissée depuis l'antiquité. Plongé dans la lecture de sa traduction latine de l'*Arithmetica* du grec Diophante, Fermat tombe sur une étude des solutions en *entiers positifs* de l'équation $x^2 + y^2 = z^2$. Selon Diophante, il y en a une infinité: $(x, y, z) = (3, 4, 5)$, $(5, 12, 13)$, $(15, 8, 17)$, ... Fermat démontre que l'équation $x^4 + y^4 = z^4$ ne possède par contre *aucune* solution entière. Enhardi peut-être par ce succès, d'où est née sa célèbre méthode de la *descente*, Fermat affirme qu'il en va de même pour l'équation $x^n + y^n = z^n$ lorsque l'exposant n est plus grand que 2. Sa démontration, à supposer qu'elle ait existée, demeure une énigme, car Fermat n'en publie rien... et les plus grands mathématiciens s'acharneront, pendant plus de 350 ans, à la retrouver! Non sans quelques succès partiels notables: les cas des exposants $n = 3$, 5 et 7 sont traités par Euler, Legendre, Cauchy et Lamé, par des variations de plus en plus byzantines sur le thème de la descente de Fermat. L'Académie des Sciences de Paris, puis la fondation Wolfskehl en

1908, offrent des récompenses pour la démonstration du théorème de Fermat, conférant à ce problème un prestige considérable.

Il reste quand même des sceptiques. Gauss écrit que "le théorème de Fermat, en tant que proposition isolée, représente peu d'interêt pour moi, car il me serait aisé d'énoncer une foule de propositions semblables, tout aussi difficiles à démontrer ou à réfuter." Pour Kummer, il s'agit davantage d'une "curiosité que d'une question centrale de la science des nombres".

C'est pourtant Kummer qui franchit un pas décisif en démontrant le théorème de Fermat pour tout exposant plus petit que 100 en 1857. Déja Euler, pour le cas $n = 3$, a été amené à travailler avec des nombres (complexes) de la forme $a + b\sqrt{-3}$, où a et b sont des entiers naturels. Kummer se lance dans une étude approfondie des nombres, dits *cyclotomiques*, qui aparaissent dans la factorisation de $x^n + y^n$. L'étude de tels systèmes de nombres reste une préoccupation centrale de la théorie, et l'importance du travail de Kummer va bien au delà de son application au dernier théorème de Fermat.

Quarante ans plus tôt, Evariste Galois découvre que la complexité d'un système de nombres se discerne à travers l'ensemble des transformations, ou *symétries*, qui en préservent la structure. Cette collection de symétries, appelée *groupe de Galois*, est particulièrement simple dans le cas des nombres cyclotomiques de Kummer: il s'agit d'un *groupe abélien*, tout comme l'ensemble des rotations du plan préservant les sommets d'un polygone régulier.

Au début du 20ème siècle, la théorie des systèmes de nombres ayant des groupes de Galois abéliens est développée par un cercle de mathématiciens distingué – Artin, Hasse, Hilbert, Takagi, Tate, Weber – dont les travaux culminent dans les années 50, avec la formulation définitive de la théorie du *corps de classe.*

Dans la seconde moitié du 20ème siècle, les théoriciens tournent leur attention vers le cas non-abélien, plus difficile. (Un cas particulier, déjà très riche, est celui où le groupe de Galois ressemble aux rotations de l'espace préservant les sommets d'un icosaèdre régulier.) Les idées de Weil, Shimura et Langlands laissent entrevoir une vaste généralisation de la théorie du corps de classe. Dans son cours à l'Université McGill en 1968, Jean-Pierre Serre insiste sur l'importance de certains systèmes des nombres associés à des *courbes elliptiques.* Dans ce contexte particulier, la vision de Langlands s'exprime à travers la conjecture de Shimura-Taniyama qui relie les courbes elliptiques aux *formes modulaires.*

Ces développements s'inscrivent dans le même grand mouvement d'idées que l'oeuvre de Kummer – mais on semble bien loin du problème de Fermat. En 1985, coup de théatre: Frey présente un argument convaincant selon lequel la conjecture de Shimura-Taniyama impliquerait le dernier théorème de Fermat. Argument formulé de facon plus précise par Serre, et démontré presque aussitôt par Ribet. Sans avoir l'air d'y toucher, la théorie des nombres est revenue à une de ses sources originales d'inspiration, armée de persectives nouvelles. Mais la conjecture de Shimura-Taniyama, de l'avis de (presque) tous, semble rester inviolable... jusqu'aux révélations de ce 23 Juin 1993.

A l'institut Isaac Newton, le tonerre d'applaudissements s'apaise; l'assistance absorbe l'impact des exposés de Wiles. Les uns, pessimistes, s'inquiètent de la solidité des démonstrations - car, en trois heures, impossible d'en présenter tous les détails. (Il y aura effectivement une lacune, comblée un an plus tard par Taylor et Wiles.) Les autres imaginent les découvertes nouvelles qui, inévitablement, suivront cette percée. Mais dans l'allégresse du moment, on se soucie assez peu des embuches ou des opportunités à venir. Le triomphe de Wiles, c'est surtout un couronnement de la théorie des nombres du 20ème siècle, un témoignage de la grandeur et de l'unité des mathématiques.