THE ABEL PRIZE 2016

L'académie norvégienne des sciences et des lettres
a décidé de décerner le prix Abel 2016 à

Sir Andrew J. Wiles

de l'université d'Oxford

« pour avoir démontré de manière éclatante le dernier théorème de Fermat par le biais de la conjecture de modularité pour les courbes elliptiques semi-stables, ouvrant ainsi une nouvelle ère dans la théorie des nombres. »

La théorie des nombres, une belle et ancienne branche des mathématiques, se penche sur l'étude des propriétés arithmétiques des nombres entiers. Dans sa forme moderne, le sujet est fondamentalement lié à l'analyse complexe, la géométrie algébrique et la théorie de la représentation. Les résultats de la théorie des nombres jouent un rôle important dans nos vies quotidiennes par le biais des algorithmes de cryptage pour les communications, les transactions financières et la sécurité numérique.

Le dernier théorème de Fermat, formulé la première fois par Pierre de Fermat au 17ème siècle, est l'affirmation selon laquelle l'équation $x^n + y^n = z^n$ n'a pas de solutions dans les nombres entiers positifs quand $n > 2$. Fermat a apporté la preuve de son affirmation pour $n = 4$, Leonhard Euler a trouvé la preuve pour $n = 3$, et Sophie Germain a démontré le premier résultat général qui s'applique à une infinité d'exposants premiers. L'étude du problème par Ernst Kummer a dévoilé plusieurs notions de base dans la théorie algébrique des nombres, telles que les nombres idéaux et les subtilités de la factorisation unique. La démonstration complète trouvée par Andrew Wiles repose sur trois autres concepts dans la théorie des nombres, à savoir les courbes elliptiques, les formes modulaires et les représentations de Galois.

Les courbes elliptiques sont définies par des équations cubiques à deux variables. Elles sont les domaines naturels de définition des fonctions elliptiques introduites par Niels Henrik Abel. Les formes modulaires sont des fonctions analytiques hautement symétriques définies sur la partie supérieure du plan complexe. Elles factorisent naturellement à travers des formes appelées courbes modulaires. Une courbe elliptique est dite modulaire si elle peut être paramétrée par une application de l'une de ces courbes modulaires. La conjecture de modularité proposée par Goro Shimura, Yutaka Taniyama, et André Weil dans les années 1950 et 1960, affirme que toute courbe elliptique définie sur les nombres rationnels est modulaire.

En 1984, Gerhard Frey a associé une courbe elliptique semi-stable à tout contre-exemple hypothétique au dernier théorème de Fermat, et a fortement suspecté cette courbe elliptique de ne pas être modulaire. La non-modularité de Frey a été démontrée via la conjecture epsilon de Jean-Pierre Serre par Kenneth Ribet en 1986. Ainsi, une preuve de la conjecture de modularité de Shimura-Taniyama-Weil pour les courbes elliptiques semi-stables permettrait également de démontrer le dernier théorème de Fermat. Cependant, à cette époque, la conjecture de modularité était considérée par beaucoup comme totalement inaccessible. Par conséquent, ce fut une avancée majeure lorsqu'Andrew Wiles, dans une publication révolutionnaire publiée en 1995, a introduit sa technique de relèvement modulaire et démontré le cas semi-stable de la conjecture de modularité.

La technique de relèvement modulaire de Wiles concerne les symétries de Galois des points d'ordre fini dans la structure de groupe abélien sur une courbe elliptique. En s'appuyant sur la théorie des déformations de Barry Mazur pour de telles représentations de Galois, Wiles a identifié un critère numérique qui assure que la modularité des points d'ordre p peut être relevée à la modularité des points d'ordre de n'importe quelle puissance de p, où p est un nombre premier impair. Cette modularité relevée est alors suffisante pour démontrer que la courbe elliptique est modulaire. Le critère numérique a été confirmé dans le cas semi-stable en utilisant un important article complémentaire écrit conjointement avec Richard Taylor. Les théorèmes de Robert Langland et Jerrold Tunnell montrent que, dans de nombreux cas, la représentation de Galois donnée par les points d'ordre trois est modulaire. Par le passage ingénieux d'un nombre premier à un autre, Wiles a démontré que dans les cas restants, la représentation de Galois donnée par les points d'ordre cinq est modulaire. Ceci lui a permis d'achever sa démonstration de la conjecture de modularité, et ainsi également du dernier théorème de Fermat.

Les idées novatrices introduites par Wiles ont eu une importance cruciale pour de nombreux développements ultérieurs, y compris la démonstration en 2001 du cas général de la conjecture de modularité par Christophe Breuil, Brian Conrad, Fred Diamond et Richard Taylor. Pas plus tard qu'en 2015, Nuno Freitas, Bao V. Le Hung et Samir Siksek ont apporté une démonstration de la conjecture de modularité sur corps de nombres réels quadratiques. Peu de résultats ont une histoire mathématique aussi riche et une démonstration aussi éclatante que le dernier théorème de Fermat.