THE ABEL PRIZE 2016

A Academia Norueguesa de Ciências e Letras
decidiu atribuir o Prémio Abel de 2016 a

Sir Andrew J. Wiles

Universidade de Oxford

"pela sua impressionante demonstração do Último Teorema de Fermat por meio da conjetura da modularidade para curvas elípticas semiestáveis, dando início a uma nova era na teoria dos números."

A Academia Norueguesa de Ciências e Letras decidiu atribuir o Prémio Abel de 2016 a Sir Andrew J. Wiles, Universidade de Oxford,

"pela sua impressionante demonstração do Último Teorema de Fermat por meio da conjetura da modularidade para curvas elípticas semiestáveis, dando início a uma nova era na teoria dos números."

A teoria dos números, um antigo e belo ramo da Matemática, ocupa-se com o estudo das propriedades aritméticas dos números inteiros. Na sua forma moderna, a disciplina está estreitamente ligada à análise complexa, à geometria algébrica e à teoria de representação. Os resultados da teoria dos números desempenham um papel importante no nosso quotidiano mediante os algoritmos de criptografia usados nas comunicações, nas transações financeiras e na segurança digital.

O Último Teorema de Fermat, formulado pela primeira vez no século XVII por Pierre de Fermat, é a asserção de que para n>2 a equação $x^n + y^n = z^n$ não tem solução em inteiros positivos. Fermat demonstrou a sua afirmação para n=4, Leonhard Euler encontrou uma prova para n=3, e Sophie Germain provou o primeiro resultado geral que se aplica a um número infinito de expoentes primos. O estudo de Ernst Kummer sobre o problema revelou diversas noções básicas da teoria algébrica dos números, tais como os números ideais e as subtilezas da fatorização única. A demonstração completa encontrada por Andrew Wiles conta com três outros conceitos da teoria dos números, a saber, as curvas elípticas, as formas modulares e as representações galoisianas.

As curvas elípticas são definidas por equações cúbicas em duas variáveis. São os domínios naturais de definição das funções elípticas introduzidas por Niels Henrik Abel. As formas modulares são funções analíticas altamente simétricas, definidas na metade superior do plano complexo, e fatorizam-se naturalmente através de formas conhecidas por curvas modulares. Uma curva elíptica é considerada modular se puder ser parametrizada por uma função de uma destas curvas modulares. A conjetura da modularidade, proposta por Goro Shimura, Yutaka Taniyama e André Weil nas décadas de 1950 e 1960, afirma que toda curva elíptica definida sobre os números racionais é modular.

Em 1984, Gerhard Frey associou uma curva elíptica semiestável a qualquer contraexemplo hipotético do Último Teorema de Fermat e teve uma forte suspeita de que esta curva elíptica não seria modular. Mediante a conjetura épsilon de Jean-Pierre Serre, a não modularidade de Frey foi demonstrada por Kenneth

Ribet em 1986. Por conseguinte, uma prova da conjetura da modularidade de Shimura-Taniyama-Weil para curvas elípticas semiestáveis também constituiria uma demonstração do Último Teorema de Fermat. No entanto, na época, a opinião geral ditava que a conjetura da modularidade era completamente inacessível. Portanto foi um avanço formidável quando Andrew Wiles, num artigo pioneiro publicado em 1995, apresentou a sua técnica de levantamento modular, demonstrando o caso semiestável da conjetura da modularidade.

A técnica de levantamento modular de Wiles diz respeito às simetrias de Galois dos pontos de ordem finita da estrutura de grupo abeliano numa curva elíptica. Com base na teoria de deformação de Barry Mazur para tais representações galoisianas, Wiles identificou um critério numérico que garante que a modularidade para pontos de ordem p pode ser elevada à modularidade para pontos de ordem de qualquer potência de p, em que p é um número primo ímpar. Esta modularidade elevada é então suficiente para provar que a curva elíptica é modular. O critério numérico foi confirmado no caso semiestável usando um importante artigo complementar escrito em coautoria com Richard Taylor. Os teoremas de Robert Langlands e Jerrold Tunnell mostram que em muitos casos a representação galoisiana dada pelos pontos de ordem três é modular. Substituindo de forma engenhosa um número primo por outro, Wiles demonstrou que nos restantes casos a representação galoisiana dada pelos pontos de ordem cinco é modular. Isto completou a sua demonstração da conjetura da modularidade e, portanto, também a do Último Teorema de Fermat.

As novas ideias apresentadas por Wiles foram decisivas para muitos avanços subsequentes, incluindo a prova de 2001 do caso geral da conjetura da modularidade por Christophe Breuil, Brian Conrad, Fred Diamond e Richard Taylor. Ainda em 2015, Nuno Freitas, Bao V. Le Hung e Samir Siksek demonstraram a afirmação de modularidade análoga sobre corpos quadráticos reais. Poucos resultados têm uma história matemática tão rica e uma demonstração tão dramática como o Último Teorema de Fermat.