THE ABEL PRIZE 2016

La Academia de Ciencias y Letras de Noruega
ha resuelto conceder el Premio Abel 2016 a

Sir Andrew J. Wiles

Universidad de Oxford, Inglaterra

“por su impresionante demostración del *Último Teorema de Fermat* mediante la conjetura de modularidad para las curvas elípticas semiestables, iniciando una nueva era en la teoría de números”.

La teoría de números, una antigua y hermosa rama de las Matemáticas, estudia las propiedades aritméticas de los números enteros. En su forma actual, está fundamentalmente relacionada con el análisis complejo, la geometría algebraica y la teoría de la representación. Los algoritmos de cifrado para las comunicaciones, las transacciones financieras y la seguridad digital, tan importantes en nuestra vida cotidiana, se basan en resultados teóricos de esta teoría matemática.

El *Último Teorema de Fermat*, formulado por Pierre de Fermat en el siglo XVII, afirma que si n es un número entero mayor o igual que 3, no existen números enteros positivos *x, y y z*, que cumplan la igualdad $x^n + y^n = z^n$. Fermat dió una demostración en el caso n=4 y Leonhard Euler para n=3. Sophie Germain demostró el primer resultado general aplicable a un número infinito de exponentes primos. El estudio del problema por Ernst Kummer reveló varias nociones básicas de la teoría algebraica de números, como los números complejos ideales y las sutilezas de la factorización única. La demostración completa descubierta por Andrew Wiles se apoya en tres conceptos adicionales de la teoría de números, a saber, las curvas elípticas, las formas modulares y las representaciones de Galois.

Las curvas elípticas están definidas por ecuaciones de tercer grado en dos variables. Son los dominios naturales de definición de las funciones elípticas introducidas por Niels Henrik Abel. Las formas modulares son funciones analíticas, extremadamente simétricas, definidas en el semiplano complejo superior, que factorizan de manera natural a través de formas conocidas como curvas modulares. Una curva elíptica es modular si puede ser parametrizada mediante una aplicación definida sobre una curva modular. La conjetura de modularidad, propuesta por Goro Shimura, Yutaka Taniyama y André Weil en los años 1950-1960 afirma que, toda curva elíptica definida sobre el cuerpo de los números racionales, es modular.

En 1984, Gerhard Frey asoció una curva elíptica semiestable a cualquier hipotético contraejemplo del *Último Teorema de Fermat* y sospechó, por razones diversas, que esta curva elíptica no sería modular. Ello fué demostrado por Kenneth Ribet en 1986, mediante la conjetura épsilon de Jean-Pierre Serre. Por tanto, una demostración de la conjetura de Shimura-Taniyama-Weil de modularidad de las curvas elípticas semiestables proporcionaría también una demostración del *Último Teorema de Fermat*. Sin embargo, por aquel entonces, se pensaba que la conjetura de modularidad era totalmente inaccesible. De ahí el avance impresionante que supuso

que Andrew Wiles, en un artículo innovador publicado en 1995, presentara su método de lifting modular y demostrara la veracidad de la conjetura de modularidad en el caso semiestable.

El método de lifting modular de Wiles se refiere a las simetrías de Galois de los puntos de orden finito de la estructura de grupo abeliano de una curva elíptica. Basándose en la teoría de deformación de Barry Mazur para este tipo de representaciones de Galois, Wiles identificó un criterio numérico que asegura que la modularidad de los puntos de orden p puede ser transferida a la modularidad de los puntos cuyo orden es cualquier potencia de p, siendo p un número primo impar. Esta modularidad inducida resulta suficiente para demostrar que la curva elíptica es modular. El criterio numérico fue verificado para el caso semiestable utilizando un importante artículo complementario, escrito conjuntamente con Richard Taylor. Los Teoremas de Robert Langlands y Jerrold Tunnell muestran que, en muchos casos, la representación de Galois dada para los puntos de orden 3 es modular. Mediante un ingenioso intercambio entre primos, Wiles demostró que la representación de Galois dada para los puntos de orden 5 es modular en los casos restantes. Con ello completó su demostración de la conjetura de la modularidad y, por lo tanto, también del *Último Teorema de Fermat*.

Las nuevas ideas aportadas por Wiles han sido decisivas en desarrollos posteriores, como por ejemplo, en la demostración, en 2001, del caso general de la conjetura de modularidad por Christophe Breuil, Brian Conrad, Fred Diamond y Richard Taylor. Recientemente, en 2015, Nuno Freitas, Bao V. Le Hung y Samir Siksek han demostrado la conjetura de modularidad en el campo de los números cuadráticos reales. Son pocos los resultados que tienen una historia matemática tan rica y una demostración tan espectacular como el Último Teorema de Fermat.