Andrew Wiles, Premio Abel 2016 por su demostración del Último Teorema de Fermat

El pasado 15 de marzo, la Academia de Ciencias y Letras de Noruega anunció que había resuelto conceder el Premio Abel 2016 a Sir Andrew J. Wiles (U. de Oxford) "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".

Adolfo Quirós, profesor del Departamento de Matemáticas de nuestra Facultad, nos cuenta algo más sobre el trabajo de Wiles, sus antecedentes y sus consecuencias.

El problema

Se conoce como Último Teorema de Fermat la afirmación de que, si n es un entero mayor o igual que 3, no existen enteros positivos x, y, z que satisfagan la ecuación:

$$x^n+y^n=z^n.$$

Para n=2, la ecuación es la que aparece en el Teorema de Pitágoras, y ya los griegos clásicos (el propio Pitágoras, Platón o Euclides) sabían que existen infinitas ternas pitagóricas esencialmente distintas (correspondientes a triángulos rectángulos no semejantes con lados enteros). Alrededor de 1637, un abogado francés muy aficionado a las matemáticas, Pierre de Fermat, estaba leyendo la *Aritmética* de Diofanto, que había sido recientemente recuperada y traducida al latín por Bachet, quien la había enriquecido con anotaciones del estilo "dado un número que es un cuadrado, escribirlo como suma de otros dos cuadrados". A esto Fermat apostillaba, en una nota manuscrita al margen,

> *"Por otra parte es imposible descomponer un cubo como suma de dos cubos, o un bicuadrado [potencia cuarta] como suma de dos bicuadrados, o en general una potencia mayor que dos como suma de potencias de igual exponente. He encontrado una demostración realmente maravillosa de este hecho, que desgraciadamente no cabe en este estrecho margen."*

Tras la muerte de Fermat su hijo publicó, en 1670, una nueva edición de la *Aritmética*, a la que añadió como apéndice las notas de su padre. Así fue como una anotación de trabajo en el margen de un libro se dio a conocer y capturó la imaginación de muchos profesionales e innumerables aficionados a las matemáticas durante más de 300 años.

Algunos resultados anteriores a Wiles

Aclaremos en primer lugar que Fermat nunca dijo en público que tuviese la demostración "anunciada". Únicamente habló de los casos n=3 y n=4, y sólo publicó una demostración para el segundo, en la que utilizaba el *método de descenso infinito*, que en sus manos era una poderosa herramienta. Hace mucho tiempo que ningún experto considera que Fermat tuviese realmente una demostración general, y la conjetura más razonable es que pensó que podría hacerlo por descenso, pero luego se dio cuenta de que no funcionaba para todos los casos. Si se puede utilizar, como hizo más tarde Euler (1753), para n=3, y es muy probable que eso también lo supiese Fermat.

El problema se reduce fácilmente a los casos n=4 y n=p, un primo impar, por lo que, tras Fermat y Euler, sólo hay que preocuparse por los exponentes primos mayores o iguales que 5. El progreso fue lento: se demostró el teorema para n=5 (1828, Legendre y Dirichlet), n=7 (1839, Lamé), para todos los primos menores que 100, excepto 37, 59 y 67 (1850, Kummer), para los primos menores que 125.000 (1978, Wagstaff),...

Vale la pena mencionar el primer resultado de tipo general. En 1815 Sophie Germain, una de las pocas mujeres matemáticas anteriores a la II Guerra Mundial, demostró que el llamado "primer caso del Último Teorema de Fermat" era válido para los exponentes primos p tales que 2p+1 también fuese primo. Estos p se llaman ahora *primos de Germain* (ejemplos son 2, 3, 5, 11, 23,..., pero no 7, 13 o 19). Los correspondientes primos 2p+1 se conocen como *primos seguros* y, en uno de esos giros de guión que hacen las matemáticas ubicuas, son 200 años después muy importantes en criptografía.

El Último Teorema de Fermat trata de resolver una ecuación diofántica. Es, por tanto, un problema clásico de Teoría de Números, pero ha tenido una gran influencia en otros campos de las matemáticas. Por dar dos ejemplos, los intentos de resolución mediante factorización dieron lugar, a partir de los trabajos de Kummer, a la teoría de ideales, esencial en Álgebra. Por otra parte, dividir entre z^n nos lleva a buscar puntos con coordenadas racionales en la curva algebraica de ecuación $X^n+Y^n=1$ (para n=2 sería la circunferencia de radio 1). Esta idea llevo a Weil y Grothendieck, entre otros, a desarrollar una versión de la Geometría Algebraica que pudiese abordar este tipo de problemas aritméticos. De hecho, hoy en día hay un campo muy activo de investigación que se conoce como Geometría Algebraica Aritméticas (a los matemáticos nos gustan especialmente los problemas que requieren utilizar herramientas de diversas áreas).

No obstante, el Último Teorema de Fermat no se consideraba un resultado central de las matemáticas, en el sentido de que no era especialmente importante saber si Fermat tenía razón o no. De hecho Hilbert no lo incluyó en su famosa lista de 23 problemas enunciados en el Congreso Mundial de Matemáticas de 1900 como reto para los matemáticos del siglo XX. Había motivos para pensar que Fermat estaba en lo cierto, pero si alguien hubiese encontrado un contraejemplo no habría pasado nada. Hasta que...

La Conjetura de Modularidad y el Último Teorema de Fermat

Hablemos de otro tipo de curvas algebraicas. Simplificando un poco, una *curva elíptica* es una curva plana definida por una ecuación de la forma

$$Y^2=X^3+AX+B.$$

Si A y B son números racionales (que de hecho podemos suponer enteros) diremos que la curva está definida sobre los racionales.

En 1955, Yutaka Taniyama propuso una relación inesperada entre las curvas elípticas y unos objetos totalmente distintos, las llamadas *formas modulares*, que son funciones de variable compleja con notables propiedades de simetría. Simplificando de nuevo (¡esta vez mucho!) lo que Taniyama sugirió es que, para cualquier curva elíptica definida sobre los racionales existe una forma modular que codifica la información aritmética de la curva. Esta relación se puede hacer explícita a través de las conocidas como funciones-L, una para la curva y otra para la forma modular.

La idea de Taniyama fue posteriormente reformulada y completada por Goro Shimura y André Weil, llegando así a la conocida como Conjetura de Shimura-Taniyama-Weil (o variaciones de este nombre) o Conjetura de Modularidad: *toda curva elíptica definida sobre los racionales es modular*, es decir, existe una forma modular cuya función-L coincide con la de la curva.

De entre las ecuaciones implicadas en el Último Teorema de Fermat, la única que, tras un cambio de variable, da una curva elíptica, es la que corresponde a n=3. ¿Por qué entonces está relacionado el Último Teorema con la Conjetura de Modularidad?

En 1972 Yves Hellegouarch tuvo la idea de asociar a una hipotética solución (a,b,c) en enteros positivos de la ecuación de Fermat para exponente primo p la curva elíptica de ecuación $Y^2=X(X+a^p)(x-b^p)$, y observó que debería tener propiedades muy especiales. En 1984 Gerhard Frey dio un paso fundamental: observó que las propiedades de la curva de Hellegouarch (conocida hoy habitualmente, quizás de manera un poco injusta, como *curva de Frey*) son tan particulares que la curva no podía ser modular. El año siguiente Jean Pierre Serre afina la idea de Frey y muestra que, si se demuestra un pequeño detalle, la verdad de la Conjetura de Modularidad implicaría que la curva de Hellegouarch-Frey no puede existir, y por tanto tampoco existen soluciones del tipo buscado para la ecuación de Fermat.

La modularidad de las curvas elípticas tendría otras muchas e importantes consecuencias. Por tanto, que el Último Teorema de Fermat fuese cierto o falso dejaba de ser irrelevante: si fuese falso, lo sería la Conjetura de Modularidad, lo que resultaría muy desagradable.

El pequeño detalle indicado por Serre, la conocida como *Conjetura Épsilon*, fue demostrado en 1986 por Ken Ribet, y provocó que Andrew Wiles, entonces profesor en la Universidad de Princeton, se encerrase en su ático para intentar demostrar la Conjetura de Modularidad y, con ella, el Último Teorema de Fermat.

Andrew Wiles había nacido en Cambridge en 1953 y, según él mismo cuenta, desde que a los diez años sacó de la biblioteca un libro sobre el Último Teorema de Fermat había estado cautivado por un problema que un muchacho podía entender, pero que los más grandes matemáticos no sabían resolver. No obstante, lo consideraba fuera de su alcance. Hasta que pensó que la línea de ataque de Hellegouarch-Frey-Serre-Ribet le abría la puerta para utilizar técnicas que él manejaba con maestría.

Trabajó durante siete años en total aislamiento hasta que, a finales de junio de 1993, en un congreso celebrado en Cambridge, anunció una demostración de la Conjetura de Modularidad para curvas elípticas semiestables, suficiente para deducir el Último Teorema de Fermat. Por desgracia, los revisores encontraron un punto no del todo justificado en la demostración, y en diciembre Wiles reconoció que ésta era incompleta. Tras esforzarse en arreglarla él sólo, finalmente reclutó a su antiguo alumno Richard Taylor para que le ayudase. En 1995 la prestigiosa revista *Annals of Mathematics* publicaba en el número 3 de su volumen 141 únicamente dos artículos, uno (108 páginas) de Andrew Wiles titulado "Modular elliptic curves and Fermat's last theorem", y otro (19 páginas) de Taylor y Wiles (en matemáticas los artículos se firman por orden alfbético) con el nombre "Ring-theoretic properties of certain Hecke algebras". Juntos establecían la veracidad de la Conjetura de Modularidad para curvas elípticas semistables y, por tanto, demostraban que lo que Fermat había quizás intuido 350 años antes era cierto.

Una nueva era en la Teoría de Números

La herramientas desarrolladas por Wiles (y Taylor) en su demostración, y en particular las ideas de "levantamiento modular" y "cambio de primo" han resultado ser de lo más fructíferas. Se han utilizado después para probar resultados del calibre de la Conjetura de Langlands local para grupos lineales en característica positiva (Harris y Taylor), la Conjetura de Sato-Tate para (muchas) curvas elípticas (Clozel, Harris, Shepherd-Barron y Taylor) o la Conjetura de Modularidad en toda su generalidad (Breuil, Conrad, Diamond y Taylor). Incluso si Wiles no hubiese sido capaz de arreglar del todo su prueba, sus resultados iniciales habrían sido de enorme importancia, pero seguramente sólo habrían sido conocidos por los especialistas. Debemos estar agradecidos por que su perseverancia (y generosidad al enrolar a Taylor en la tarea) le permitiese alcanzar lo que sin duda es uno de los hitos ("el hito" en el imaginario popular) de las matemáticas de los últimos años.

Los nombres franceses, ingleses, alemanes, japoneses o estadounidenses implicados en esta historia, son clara muestra de la universalidad de las matemáticas. No queremos dejar de señalar que el anuncio oficial de la Academia de Ciencias y Letras de Noruega incluye también una referencia ibérica cuando dice "en 2015, Nuno Freitas, Bao V. Le Hung y Samir Siksek han demostrado la conjetura de modularidad para cuerpos de números cuadráticos reales". Freitas (Guimarães, Portugal, 1984) es doctor por la Universitat de Barcelona y el ganador del último Premio José Luis Rubio de Francia concedido por la Real Sociedad Matemática Española y patrocinado por la Universidad Autónoma de Madrid y la Universidad de Zaragoza.

El Premio Abel y otros premios matemáticos

El Premio Abel se entregó por primera vez en 2003 y, de algún modo, su objetivo era suplir al inexistente Premio Nobel en Matemáticas. Se concede anualmente, se puede compartir, está dotado con 6 millones de coronas noruegas (unos 750.000 euros) y los diecisiete matemáticos que lo han recibido hasta ahora se cuentan entre lo más granado del siglo XX. Todo ello lo hace, efectivamente, parecido al Nobel.

Pero antes de la creación del Premio Abel siempre se había dicho que el "Nobel de Matemáticas" eran las Medallas Fields. Éstas llevan asociadas una pequeña dotación económica (15.000 dólares canadienses, unos 10.000 euros), se entregan cada cuatro años en el Congreso Mundial de Matemáticas (un máximo de cuatro medallas, no compartidas, en cada ocasión) y, la principal diferencia con los Nobel y los Abel, no se pueden conceder a nadie mayor de 40 años.

Como consecuencia, Wiles no pudo ganar la Medalla Fields por los resultados que ahora han sido reconocidos con el Premio Abel. No obstante, la Unión Matemática Internacional (IMU) acordó entregarle en el ICM de 1998 la "IMU Silver Plaque", la única ocasión hasta ahora en que se ha concedido tal galardón.