El Último Teorema de Fermat

Juan Martín Mombelli[1]

A continuación se presenta una traducción de un artículo que apareció en las noticias de 1999 de la Enciclopedia Británica debido a Paul J. Campbell.

La mayor noticia matemática en 1999 fue la demostración de la conjetura de Taniyama-Shimura. En 1993 Andrew Wiles de la Universidad de Princeton probó un caso de de la conjetura que fue lo suficientemente amplia para implicar el último Teorema de Fermat.

Ahora la conjetura de Taniyama-Shimura completa ha sido demostrada por colegas cercanos y antiguos estudiantes de Wiles: Brian Conrad y Richard Taylor de la Universidad de Harvard, Christophe Breil de la Universidad Paris-Sud, y Fred Diamond de la Universidad de Rutgers, New Brunswik, N.J.

En 1955 Yutaka Taniyama de la Universidad de Tokio observó por primera vez una notable relación entre ciertas entidades matemáticas de dos ramas de la matemática no relacionadas anteriormente. Aunque Taniyama no pudo probar que esta relación existía para todos los casos, su conjetura, que *toda curva elíptica racional es modular*, tenía profundas implicaciones para reformular ciertos problemas -tal como el Último Teorema de Fermat- de una rama de la matemática a otra con diferentes herramientas y estructuras matemáticas que tal vez proveyeran una nueva percepción.

Inicialmente, muchos matemáticos fueron escépticos para el caso general, pero despúes del suicidio de Taniyama en 1958, su amigo y colega Goro Shimura (ahora en Princeton) continuó su trabajo realizando avances importantes, y el nombre de Shimura fue agregado: *La conjetura de Taniyama-Shimura.*

Las curvas elípticas tienen ecuaciones de la forma $y^2 = ax^3 + bx^2 + cx + d$. El nombre de curvas elípticas deriva del estudio del perímetro de las elipses. Uno de los mayores logros de la geometría algebraica es identificar soluciones racionales de las curvas elípticas, es decir puntos (x, y) sobre la curva donde ambos números x, y son racionales. Para curvas elípticas con coeficientes racionales,

[1]Nota del traductor: Alrededor de 1630 Pierre de Fermat, un abogado de Tolouse dedicado a la ciencia y a las matemáticas, probó que no existen soluciones enteras para la ecuación $a^3 + b^3 = c^3$. Fermat fue más alla y aseguró que no existen soluciones enteras positivas de la ecuación $a^n + b^n = c^n$, con $n > 2$. En el margen de su copia de *Arithmetica* de Diofanto escribió que tenía una maravillosa demostración. Desde entonces dicha conjetura se la conoce como el Último Teorema de Fermat. Desafortunadamente, no dio una demostración, pero en cambio escribió que *el margen era demasiado angosto para contenerla.* Si Fermat de hecho poseía una demostración, es todavía un misterio. Desde entonces muchos matemáticos han intentado demostrar el último Teorema de Fermat. Muchos dieron soluciones parciales y a veces incorrectas. Pero si hay una lección importante de la historia de la matemática es que el camino a la búsqueda de soluciones a problemas no resueltos invariablemente conduce a descubrimientos importantes.

es decir donde a, b, c, d son racionales, cualquier recta tangente a la curva en un punto racional o cualquier par de puntos sobre la curva, puede ser usado para generar otro punto racional.

Una pregunta clave es cuantos generadores son requeridos para cada curva para determinar todas las soluciones racionales. Una aproximación inicial es ampliar el dominio de x e y para incluir los números complejos $a + bi$, donde a y b son números reales y $i^2 = -1$, para que las curvas de la ecuación ahora ya no sean curvas sino superficies compactas (en otras palabras, la superficie tiene un número finito de partes). Tales superficies pueden ser clasificadas por su género topológico, el número de agujeros a través de la superficie. Las ecuaciones para rectas y secciones cónicas (círculos, elipses, hipérbolas y parábolas) son superficies de género 0, y tales curvas o bien no tienen puntos racionales o son familias infinitas fáciles de describir. Para curvas elípticas al género es 1, son ejemplos de toros, esto es, tienen la forma de una donna, no hay forma fácil de decir si posee infinitos puntos racionales, finitos o ninguno.

Mientas que una clasificación directa de los generadores de una curva elíptica es difícil, otra rama de la matemática ofreció una promesa de un nuevo acercamiento al problema. Aunque difícil de visualizar, las numerosas simetrías de las funciones modulares producen una estructura rica que facilita el análisis. Shimura observó que la sucesión de números que caracterizan por completo a una función modular particular (una función especial a valores complejos) corresponde exactamente a la sucesión de números que caracterizan por completo ciertas curvas elípticas. Esto es donde empieza la idea de reformular problemas involucrando curvas elípticas a ideas involucrando funciones modulares (o curvas modulares).

A cada solución de la ecuación de Fermat $a^n + b^n = c^n$ con $n > 2$ le corresponde un punto racional de la curva elíptica $y^2 = x(x - a^n)(x - b^n)$. Gerhard Frey de la Universidad de Saarland, conjeturó en 1985, y luego Kenneth Ribet de la Universidad de California, Berkeley, probó en 1986, que tal curva asociada a una solución de la ecuación de Fermat no podría ser modular. Wiles, sin embargo, mostró que cierto tipo de curvas elípticas (las llamadas *semiestables*) son modulares. Como las curvas asociadas a la ecuación de Fermat son semiestables esto lleva a una contradicción y por lo tanto a la conclusión de que el último Teorema de Fermat es cierto.

Conrad y otros extendieron el resultado de Wiles para probar la conjetura completa de Taniyama-Shimura. En particular, ellos mostraron que cualquier curva elíptica racional $y^2 = ax^3 + bx^2 + cx + d$ puede ser parametrizada por funciones modulares; esto significa que hay funciones modulares ϕ, ψ con $y = \psi(z), x = \phi(z)$ tal que la curva es de la forma $\psi(z)^2 = a\phi(z)^3 + b\phi(z)^2 + c\phi(z) + d$. Por lo tanto la curva elíptica es una proyección de una curva modular; por lo tanto, los puntos racionales de la curva elíptica corresponden a puntos racionales de la curva modular. Resultados previamente probados para curvas elípticas

modulares, tales como decidir si todos los puntos racionales provienen de un solo generador, ahora se aplican a las curvas elípticas.

Facultad de Matemática, Astronomía y Física (FaMAF)
Universidad Nacional de Córdoba
Ciudad Universitaria (5000), Córdoba, Argentina.