El Último Teorema de Fermat-Wiles

Nicolle Escobar

Universidad del Valle de Guatemala

esc20647@uvg.edu.gt

18 de noviembre de 2023

Tabla de contenido

1. Fermat
   - Biografía
2. Resultados anteriores a Wiles
   - Antecedentes
3. Resultado de Wiles
   - Conjetura de Modularidad
   - Andrew Wiles

Pierre de Fermat (1601-1665) . Jurista y matemático francés. Estudió derecho civil en la Universidad de Orleans

Fermat anotó al margen: *"Por otra parte, es imposible descomponer un cubo como suma de dos cubos, o un bicuadrado 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"*

Tabla de contenido

1. Fermat
   - Biografía
2. Resultados anteriores a Wiles
   - Antecedentes
3. Resultado de Wiles
   - Conjetura de Modularidad
   - Andrew Wiles

Antecedentes

Fermat nunca publicó ni anunció la demostración. Únicamente habló de los casos con $n = 3$ y $n = 4$ y demostró formalmente la demostración para $n = 4$, mediante el método del descenso infinito.
A continuación, una breve cronología del progreso por demostrar este teorema, antes del resultado de Wiles.

- (1637) Fermat hace su planteamiento y demuestra el caso con $n = 4$
- (1753) Euler lo demuestra para $n = 3$
- (1800s) Germain demuestra $x^p + y^p = z^p$, con p primo impar en dos casos:
  - x, y, z son primos relativos a pares y $p \not| xyz$
  - x, y, z son primos relativos a pares y $p | xyz$

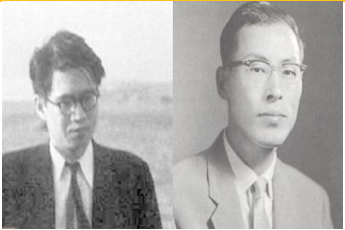
  Logrando demostrar el primer caso para primos impares $p \leq 197$.

Antecedentes

- (1825) Dirichlet y Legendre completan una demostración con $n = 5$
- (1839) Lamé toma el caso $n = 7$
- (1954-1993) Se demuestra el teorema computacionalmente $\forall n < 4,000,000$

Tabla de contenido

1. Fermat
   - Biografía
2. Resultados anteriores a Wiles
   - Antecedentes
3. Resultado de Wiles
   - Conjetura de Modularidad
   - Andrew Wiles



Taniyama y Shimura. Matemáticos que conectaron las curvas elípticas definidas sobre el Shimura-Weil.

En 1955, Taniyama propuso la relación entre curvas elípticas y formas modulares. Las formas modulares son funciones de variable compleja con propiedades de simetría.
Taniyama sugirió que para cualquier curva elíptica definida sobre los racionales existe una forma modular que codifica la información aritmética de la curva.

Curvas elípticas

Curvas elípticas

Una curva elíptica es una curva plana definida por la ecuación de la forma

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

donde $A, B \in \mathbb{Q}$ (se pueden suponer enteros) y la curva está definida sobre los racionales.

Esta idea fue posteriormente reformulada y completada por Taniyama y Shimura, permitiendo una relación entre las formas modulares y las curvas elípticas, para las cuales observaron que toda curva elíptica sobre los racionales podría ser parametrizada por medio de dos formas modulares.

Taniyama-Shimura

La idea de Taniyama fue reformulada por Shimura y Weil, llegando a la conjetura de Shimura-Taniyama-Weil

Conjetura de Modularidad

Toda curva elíptica definida sobre los racionales es modular

Esta relación se hace conoce como funciones-L (y se asigna una función para la curva y otra para la forma modular).

Taniyama-Shimura

Teorema de Taniyama-Shimura

Para toda curva elíptica E con coeficientes racionales existe una forma modular f (peso 2) tal que la serie L asociada a E y la serie L asociada a f coinciden. Esto equivale a que los coeficientes a_p asociados a la curva E coinciden con los coeficientes del desarrollo de Fourier en el infinito de f.

La primera persona en sugerir una conexión entre las curvas elípticas y el UTF fue Yves Hellegouarch (1972). Asocia una solución no trivial (a, b, c) de $x^p + y^p = z^p$, siendo p un primo impar, se considera la curva elíptica de ecuación

$$Y^2 = X(X + a^p)(x - b^p)$$

Sin pérdida de generalidad, asúmase (a,b,c)=1, con $a \equiv 3 \pmod 4$ y $b \equiv 0 \pmod 2$.

Curvas de Frey

En 1984, Gerhard Frey dio un paso fundamental: sugirió que las propiedades de la curva de Hellegouarch son tan particulares que la curva no podía ser modular.
Entonces, Hellegouarch define las curvas de Frey.

Curva de Frey

Sea l un primo impar y $a, b, c \in \mathbb{Z}^+$, tales que

$$a^l + b^l = c^l$$

entonces, una curva de Frey correspondiente es una curva algebraica dada por la ecuación

$$y^2 = x(x - a^l)(x + b^l)$$

Conjetura Épsilon (Jean Pierre Serre)

A partir de la idea de Frey, Serre, si se demuestra un pequeño detalle **(la conjetura Épsilon)** la conjetura de Modularidad implicaría que la curva de Hellegouarch-Frey no puede existir, y tampoco existen soluciones del tipo buscado para la ecuación de Fermat.
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.

Conjetura Épsilon

Si se asume que una determinada curva elíptica E sobre Q es modular, predice el nivel minimal que tendrá una forma modular cuya serie L es congruente con la de E módulo l.

Conjetura Épsilon

La conjetura Épsilon fue demostrada por Ken Ribet en 1986. Esto provocó que Andrew Wiles, entonces profesor en la Princeton, demostrar la conjetura de modularidad $\implies$ el último teorema de Fermat.

Andrew Wiles

Andrew Wiles (1953) Desde los diez años sacó de la biblioteca un libro sobre el Último Teorema de Fermat.

Trabajó durante siete años en total aislamiento hasta que en 1993, anunció la demostración de la Conjetura de Modularidad para curvas elípticas semiestables. Los revisores encontraron un punto incompleto.
En 1995, él y Richard Taylor lograron publicar el artículo titulado ”Modular elliptic curves and Fermat’s last theorem”, estableciendo la veracidad de la conjetura de modularidad y quedando el teorema demostrado.

References

F Doménech (2019)
Fermat y el mayor problema de las matemáticas.

Andrew Sutherland (2017)
Fermat's last theorem.