Ultimo teorema de fermat

un acercamiento a la demostración

Joab Hernández

Universidad del valle de Guatemala

Tabla de contenidos

Intro

Historia

El ultimo teorema de fermat que dicta

$$\nexists x, y, z \ni x^n + y^n = z^n \text{ para } n > 2$$

Este teorema fue enunciado por Pierre de Fermat, un jurista francés del siglo XVII. Se descubrió en uno de sus ejemplares de Arithmetica, un libro del matemático griego Diofanto. En 1637, Fermat escribió en el margen de este libro una nota en latín en la que formulaba su teorema, dejando enunciado el problema sin ofrecer una demostración. Hasta que en 1995 Andrew Wiles dio su demostración.

entendiendo el origen de las herramientas

Curva de Frey

La **Curva de Frey**, también conocida como la curva de Frey-Hellegouarch, es una curva elíptica de la forma

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

asociado con $a+b=c$ Esto relaciona las propiedades de las soluciones de ecuaciones con las curvas elípticas.
en 1975 Yves Hellegouarch propuso asociar la curva de frey con el ultimo teorema de Fermat donde a, b,c son enteros positivos y l es un numero primo impar tal que $a^l + b^l = c^l$
entonces una curva de Frey correspondiente es una curva algebraica dada por la ecuación

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

nota: La idea principal es que, si existiera una solución entera para la ecuación de Fermat, la curva de Frey asociada tendría ciertas propiedades que podrían contradecir el Teorema de Modularidad.

Discriminante de una Curva Elíptica

El **discriminante** de una curva elíptica es un invariante algebraico que nos proporciona información sobre las singularidades de la curva.

por ejemplo, una curva elíptica está definida por una ecuación de la forma

$$y^2 = x^3 + ax + b,$$

después de un cambio lineal de variables (donde a y b son números reales). Este tipo de ecuación se denomina ecuación de Weierstrass. Para que la curva sea elíptica, se requiere que sea no singular, es decir:

- que no tenga cúspides
- que no tenga auto-intersecciones
- puntos aislados

Discriminante de una Curva Elíptica

Algebraicamente esto se garantiza si y solo si el discriminante, Δ, no es igual a cero. El discriminante está dado por

$$\Delta = -16(4a^3 + 27b^2) \neq 0,$$

lo cual asegura que la curva sea suave. Si el discriminante es cero, la curva tiene singularidades y no puede considerarse una curva elíptica.

nota:En el contexto de la Curva de Frey, el discriminante es importante para analizar las propiedades de la curva y determinar si cumple con los requisitos para ser considerada modular.

Curva Elíptica Modular

Una **curva elíptica modular** es una curva elíptica E que admite una parametrización $X_0(N) \to E$ mediante una curva modular.
nota:Esto no es lo mismo que una curva modular que resulta ser una curva elíptica.

Curva Modular y Grupo Modular

En teoría de números y geometría algebraica, una **curva modular** $Y(\Gamma)$ es una superficie de Riemann, o la correspondiente curva algebraica, construida como el cociente del semiplano superior complejo H mediante la acción de un subgrupo de congruencia Γ del grupo modular de matrices $2x2$ con coeficientes enteros $SL(2, \mathbb{Z})$.

Los puntos de una curva modular parametrizan clases de isomorfismo de curvas elípticas, junto con alguna estructura adicional que depende del grupo Γ. Esta interpretación permite dar una definición puramente algebraica de curvas modulares, sin referencia a los números complejos, y además, probar que las curvas modulares están definidas tanto sobre el campo de los números racionales $\mathbb{Q}$ como sobre un campo ciclotómico $\mathbb{Q}(\zeta_n)$. Este hecho y sus generalizaciones son de importancia fundamental en la teoría de números.

Grupo $SL(2, \mathbb{Z})$

El **grupo** $SL(2, \mathbb{Z})$ es un grupo de matrices 2×2 con coeficientes enteros y determinante igual a 1. Cada matriz A en $SL(2, \mathbb{Z})$ tiene la forma:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

donde $a, b, c, d \in \mathbb{Z}$ son números enteros y satisfacen la condición:

$$\det(A) = ad - bc = 1$$

Superficies de Riemann

En geometría algebraica, una **superficie de Riemann** es una variedad compleja de dimensión (compleja) uno. Consecuentemente, la variedad real subyacente será de dimensión 2.

Las superficies de Riemann se pueden considerar como versiones deformadas del plano complejo: localmente, cerca de cada punto, parecen parches del plano complejo, pero la topología global puede ser bastante diferente. Por ejemplo, pueden parecer una esfera o un toro o varias láminas pegadas entre sí.

El principal interés de las superficies de Riemann radica en que entre ellas pueden definirse funciones holomorfas.

Superficies de Riemann

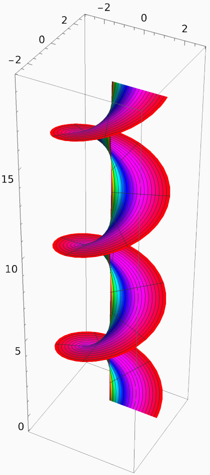

Figure 1: superficie de Riemann

Teorema de Modularidad (Conjetura de Taniyama-Shimura-Weil)

El **Teorema de Modularidad**, también conocido como la **Conjetura de Taniyama-Shimura-Weil**, establece que toda curva elíptica definida sobre los números racionales es modular. Esto significa que cada curva elíptica puede asociarse a una forma modular, lo cual conecta de manera profunda la teoría de números y la teoría de formas modulares.

Wiles demostro esto para curvas elipticas semi-estables

Conjetura ϵ de Serre

La **Conjetura ϵ de Serre** es una afirmación que propone que si la Curva de Frey es modular, entonces puede ser asociada a una forma modular de cierto tipo.

y que herramientas hicieron esto posible?

- **Curva de Frey**: Gerhard Frey observó que, si existiera una solución entera positiva (a, b, c) para la ecuación de Fermat $a^n + b^n = c^n$ con $n > 2$, se podría asociar una curva elíptica específica, conocida como la Curva de Frey. Esta observación fue fundamental porque permitió relacionar la ecuación de Fermat con propiedades de las curvas elípticas.
- **Conjetura ε de Serre**: Jean-Pierre Serre propuso que, si la Curva de Frey es modular, entonces se podría establecer una conexión con formas modulares. Este vínculo fue crucial para poder aplicar herramientas de la teoría de formas modulares a la resolución del problema.

- **Teorema de Ribet**: Ken Ribet demostró que, si la Conjetura ε de Serre es cierta, la existencia de una solución a la ecuación de Fermat implicaría la existencia de una curva elíptica semiestable no modular. Este resultado mostró que probar la modularidad de ciertas curvas elípticas sería suficiente para demostrar el Último Teorema de Fermat.
- **Teorema de la Modularidad (Conjetura de Taniyama-Shimura-Weil)**: Esta conjetura establece que toda curva elíptica definida sobre los números racionales es modular, es decir, puede asociarse a una forma modular. La demostración de esta conjetura para el caso de curvas elípticas semiestables fue clave para el éxito de la prueba de Wiles.

herramientas

- **Teoría de Deformaciones de Representaciones de Galois**: Wiles utilizó esta teoría para estudiar cómo las representaciones de Galois pueden deformarse dentro de ciertas familias, lo que le permitió analizar la modularidad de las curvas elípticas. Este enfoque fue esencial para conectar la teoría de números con las propiedades de las formas modulares.
- **Teorema $R = T$ (Anillos de Deformación y Álgebra de Hecke)**: Wiles estableció una correspondencia entre el anillo de deformaciones de una representación de Galois y el álgebra de Hecke asociada a una forma modular, demostrando que estos dos anillos son isomorfos. Esta equivalencia fue un paso fundamental en la demostración de la modularidad de las curvas elípticas semiestables.

- **Demostración de la Modularidad para Curvas Elípticas Semiestables**: Finalmente, Wiles demostró que todas las curvas elípticas semiestables definidas sobre los números racionales son modulares. Este resultado, junto con el Teorema de Ribet, implicó que no pueden existir soluciones a la ecuación de Fermat para $n > 2$.

abordando la demostración

- Por contradicción, asumimos que el Último Teorema de Fermat es falso, lo cual implicaría la existencia de una solución entera positiva a la ecuación $x^n + y^n = z^n$ para $n > 2$. Esta suposición nos lleva a generar una curva con propiedades que no cumplen con ciertas condiciones fundamentales, lo cual resulta en una contradicción.
- Se genera una curva de Frey, cuya estructura sugiere que no puede ser modular según la teoría de formas modulares, debido a que el discriminante de la curva no satisface las propiedades requeridas por el teorema de modularidad. Esto indica una incompatibilidad fundamental con la posibilidad de que sea modular.
- Representamos la curva de Frey mediante sus representaciones de Galois asociadas.

- Las representaciones de Galois asociadas a la curva de Frey describen cómo los elementos del grupo de Galois actúan sobre las soluciones de ecuaciones polinómicas, estableciendo una conexión entre la teoría de números y la geometría algebraica.
- Definimos las representaciones admisibles (es decir, aquellas que cumplen ciertas propiedades necesarias para ser asociadas con formas modulares) y demostramos que todas ellas provienen de formas modulares.
- Se parametrizan subconjuntos de representaciones de Galois mediante anillos locales completos Noetherianos.

esquema

- Mostramos que un mapeo específico entre dichos anillos es un isomorfismo utilizando técnicas de álgebra conmutativa, tales como el lema de Nakayama y la teoría de ideales primarios. Estas herramientas nos permiten demostrar la existencia y unicidad necesarias para establecer el isomorfismo.
- Reducimos el problema a la computación de ciertos invariantes, que se lleva a cabo mediante cohomología de Galois.
- finalmente se encuentra la contradiccion de que la curva de frey debe ser modular
- se prueba que el ultimo teorema de Fermat es correcto

preguntas?

References i

A. D. Aczel.
El último teorema de Fermat: El secreto de un antiguo problema matemático.
Fondo de Cultura Económica, Ciudad de México, México, 2004.

N. Boston.
The proof of fermat's last theorem, 2003.

K. Buzzard and R. Taylor.
A lean proof of fermat's last theorem, 2024.

G. contributors.
Special linear group: Sl(2,z), 2024.

W. contributors.
Modular curve, 2024.

References ii

W. contributors.
Ribet's theorem, 2024.

W. contributors.
Riemann surface, 2024.