Formas modulares y la curva $y^2 = x^3 - 35x - 98$

Dulcinea Raboso Paniagua

Trabajo de fin de Máster
Curso 2008–2009

Director: Fernando Chamizo Lorente
Universidad Autónoma de Madrid

Goro Shimura.

Yutaka Taniyama.

André Weil.

Conjetura de Shimura-Taniyama-Weil

Toda curva elíptica sobre $\mathbb{Q}$ es modular.

Goro Shimura.

Yutaka Taniyama.

André Weil.

Conjetura de Shimura-Taniyama-Weil

Toda curva elíptica sobre $\mathbb{Q}$ es modular.

¿Qué es una curva elíptica?

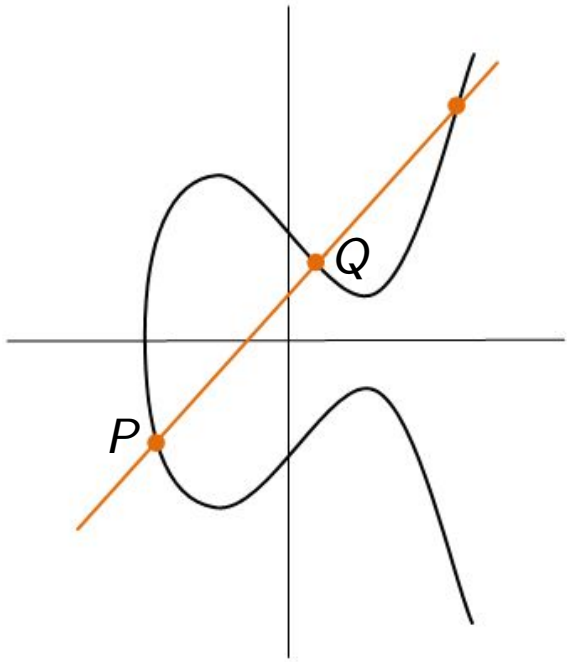
Una curva elíptica es una curva cúbica no singular.

En teoría de números son especialmente importantes las definidas sobre $\mathbb{Q}$,

$$y^2 = x^3 + Ax + B$$

con A y B racionales (o incluso enteros).

Dados dos puntos racionales de la curva, el tercer punto de intersección de la recta que los une será de nuevo racional.

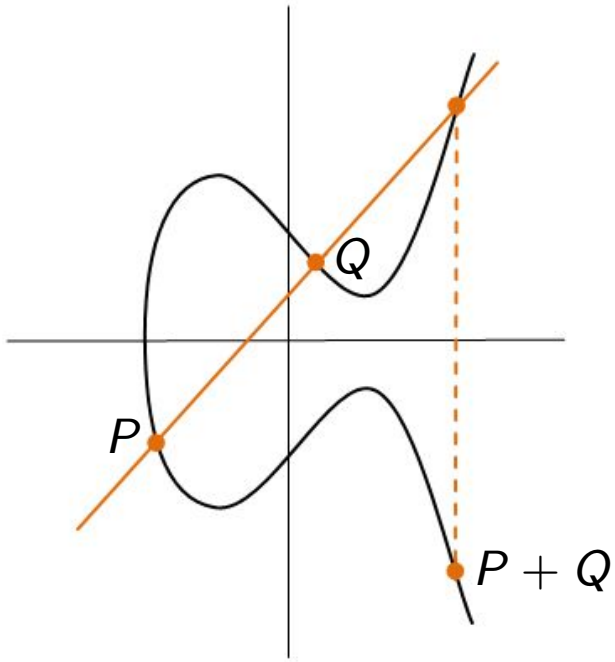


De este modo es posible dotar al conjunto de puntos racionales de la curva de una estructura de grupo abeliano.

Construyendo una $\phi : \mathbb{C} \to E$ cuyas coordenadas son funciones meromorfas doblemente periódicas con ciertos periodos ω_1 y ω_2, la suma habitual de números complejos se transforma en la suma de puntos en la curva elíptica.

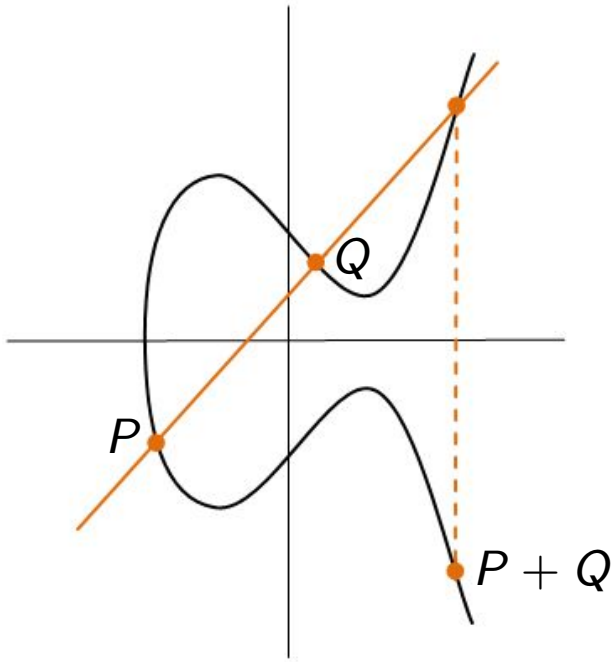
Dados dos puntos racionales de la curva, el tercer punto de intersección de la recta que los une será de nuevo racional.

De este modo es posible dotar al conjunto de puntos racionales de la curva de una estructura de grupo abeliano.



Construyendo una $\phi : \mathbb{C} \to E$ cuyas coordenadas son funciones meromorfas doblemente periódicas con ciertos periodos ω_1 y ω_2, la suma habitual de números complejos se transforma en la suma de puntos en la curva elíptica.

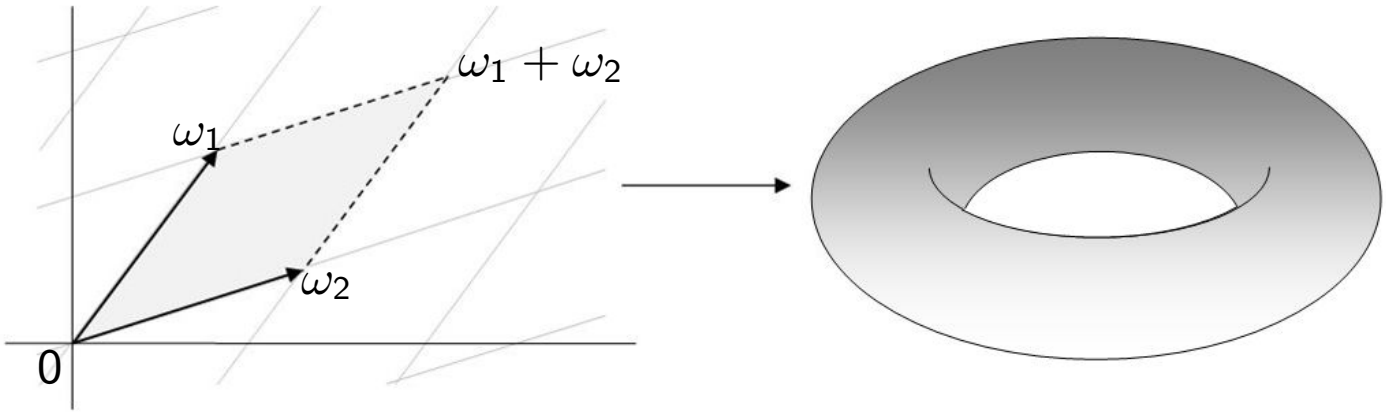
Dados dos puntos racionales de la curva, el tercer punto de intersección de la recta que los une será de nuevo racional.



De este modo es posible dotar al conjunto de puntos racionales de la curva de una estructura de grupo abeliano.

Construyendo una $\phi : \mathbb{C} \to E$ cuyas coordenadas son funciones meromorfas doblemente periódicas con ciertos periodos ω_1 y ω_2, la suma habitual de números complejos se transforma en la suma de puntos en la curva elíptica.

La función ϕ es sobreyectiva e inyectiva cuando se restringe al paralelogramo generado por ω_1 y ω_2 donde se identifica el lado superior con el inferior y el derecho con el izquierdo.



De este modo vemos que E es topológicamente un toro.

$$E \leftrightarrow \Lambda = \{n\omega_1 + m\omega_2 \ : \ n, m \in \mathbb{Z}\}$$

¿Qué es una forma modular?

Una forma modular f de peso k es una función holomorfa en el semiplano superior que verifica

$$f(z) = f(z+1), \qquad f(z) = z^{-k} f(-1/z)$$

y que en cierta forma es también holomorfa en el infinito.

Estas relaciones implican

$$f(z) = (cz+d)^{-k} f\left(\frac{az+d}{cz+d}\right) \qquad \text{para toda } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

La definición se extiende cambiando el grupo $\mathrm{SL}_2(\mathbb{Z})$ por algunos subgrupos suyos, especialmente

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{N} \right\}, \qquad \text{con } N \in \mathbb{Z}^+.$$

Al ser funciones periódicas, tienen un desarrollo de Fourier

$$f(z) = \sum a_n e^{2\pi i n z}$$

y son estos coeficientes a_n los que a menudo aportan información aritmética.

¿Qué dice entonces la conjetura?

Conjetura de Shimura-Taniyama-Weil

Si N_p es el número de puntos de una curva elíptica sobre $\mathbb{Q}$ al considerarla módulo un primo p, entonces existe una forma modular de peso dos

$$f(z) = \sum a_n e^{2\pi inz}$$

con ciertas características tal que sus coeficientes de Fourier a_p coinciden con $p + 1 - N_p$.

La conjetura y el último teorema de Fermat.

1985 G. Frey

$$\underbrace{a^n + b^n = c^n}_{\text{Ecuación de Fermat}} \quad \leftrightarrow \quad \underbrace{y^2 = x(x + a^n)(x - b^n)}_{\text{Curva elíptica}}$$

A partir de estos coeficientes, el discriminante

$$\Delta = \sqrt{(a^n - b^n)^2 + 4a^n b^n} = a^n + b^n = c^n$$

es una potencia n-ésima perfecta.

1986 K. Ribet

La curva de Frey no puede ser parametrizada por funciones modulares.

Conjetura $\Rightarrow$ UTF

La conjetura y el último teorema de Fermat.

1985 G. Frey

$$\underbrace{a^n + b^n = c^n}_{\text{Ecuación de Fermat}} \quad \leftrightarrow \quad \underbrace{y^2 = x(x + a^n)(x - b^n)}_{\text{Curva elíptica}}$$

A partir de estos coeficientes, el discriminante

$$\Delta = \sqrt{(a^n - b^n)^2 + 4a^n b^n} = a^n + b^n = c^n$$

es una potencia n-ésima perfecta. ???

1986 K. Ribet

La curva de Frey no puede ser parametrizada por funciones modulares.

Conjetura $\Rightarrow$ UTF

La conjetura y el último teorema de Fermat.

1985 G. Frey

$$\underbrace{a^n + b^n = c^n}_{\text{Ecuación de Fermat}} \quad \leftrightarrow \quad \underbrace{y^2 = x(x + a^n)(x - b^n)}_{\text{Curva elíptica}}$$

A partir de estos coeficientes, el discriminante

$$\Delta = \sqrt{(a^n - b^n)^2 + 4a^n b^n} = a^n + b^n = c^n$$

es una potencia n-ésima perfecta. ???

1986 K. Ribet

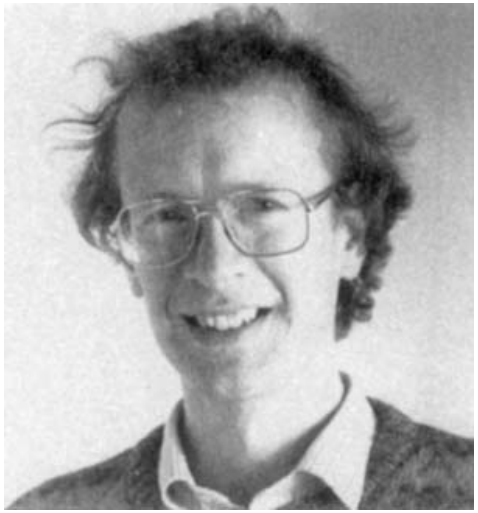
La curva de Frey no puede ser parametrizada por funciones modulares.

Conjetura $\Rightarrow$ UTF

1995 A. Wiles, con la ayuda de R. Taylor, demuestra la conjetura para una clase de curvas elípticas llamadas semiestables.

$$\Downarrow$$

UTF



Andrew Wiles.

1999 La conjetura es demostrada en su totalidad.

Teorema (Breuil, Conrad, Diamond, Taylor, Wiles).

Toda curva elíptica sobre $\mathbb{Q}$ es modular.

La curva $E_0 : \ y^2 = x^3 - 35x - 98$.

El objetivo en el trabajo es probar la conjetura de modularidad para una sola curva

$$E_0 : \ y^2 = x^3 - 35x - 98$$

sin utilizar los profundos resultados de Wiles.

¿Qué tiene de especial la curva E_0?

La curva $E_0 : \ y^2 = x^3 - 35x - 98$.

El objetivo en el trabajo es probar la conjetura de modularidad para una sola curva

$$E_0 : \ y^2 = x^3 - 35x - 98$$

sin utilizar los profundos resultados de Wiles.

¿Qué tiene de especial la curva E_0?

La curva E_0 : $y^2 = x^3 - 35x - 98$.

E_0 es una curva de multiplicación compleja (o curva CM).

Esto significa que su retículo Λ se aplica en sí mismo al multiplicar por ciertos números complejos.

Para E_0 y $\xi = (1 + i\sqrt{7})/2$,

Anillo de multiplicación compleja
$\mathbb{Z}[\xi]$

Retículo asociado
$\Lambda = \{n + m\xi\}$
que verifica $\alpha\Lambda \subset \Lambda$ para $\alpha \in \mathbb{Z}[\xi]$.

Pasos de la prueba:

1. Encontrar una fórmula explícita para N_p (usando la multiplicación compleja).
2. Comprobar que cierta función Θ con coeficientes $p + 1 - N_p$ es modular.

¿Cómo se halla N_p?

Los enteros módulo p forman un cuerpo, $\mathbb{F}_p$ y satisfacen $x^p = x$ (pequeño teorema de Fermat). Además son los únicos que lo satisfacen en cualquier extensión finita de $\mathbb{F}_p$.

N_p es el número de puntos fijos del endomorfismo de Frobenius

$$\text{Frob} : E \longrightarrow E, \quad \text{Frob}(x, y) = (x^p, y^p).$$

Si este endomorfismo se interpreta como una aplicación lineal $\mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda$, contar puntos fijos es fácil.

Todos los endomorfismos de E_0 sobre $\mathbb{C}$ son de la forma

$$f(Q) = [n]Q + [m]\phi(Q) = [n + m\xi](Q)$$

con $n, m \in \mathbb{Z}$ y $Q \in E_0$.

Para $p > 7$, distinguimos dos casos:

- $\left(\frac{-7}{p}\right) = 1$ en el que Frob $= [n_0 + m_0\xi]$ para ciertos $n_0, m_0 \in \mathbb{Z}$.
- $\left(\frac{-7}{p}\right) = -1$ en el que no se asegura que Frob provenga de un endomorfismo de E_0 sobre $\mathbb{C}$.

Todos los endomorfismos de E_0 sobre $\mathbb{C}$ son de la forma

$$f(Q) = [n]Q + [m]\phi(Q) = [n + m\xi](Q)$$

con $n, m \in \mathbb{Z}$ y $Q \in E_0$.

Para $p > 7$, distinguimos dos casos:

- $\left(\frac{-7}{p}\right) = 1$ en el que Frob $= [n_0 + m_0\xi]$ para ciertos $n_0, m_0 \in \mathbb{Z}$.
- $\left(\frac{-7}{p}\right) = -1$ en el que no se asegura que Frob provenga de un endomorfismo de E_0 sobre $\mathbb{C}$.

Caso $\left(\frac{-7}{p}\right) = 1$ ($p \equiv 1, 2, 4$ módulo 7).

$$N_p = p + 1 - \left(\frac{2n+m}{7}\right)(2n+m).$$

Caso $\left(\frac{-7}{p}\right) = -1$ ($p \equiv 3, 5, 6$ módulo 7).

$$N_p = p + 1.$$

¿Cómo se prueba la modularidad?

Para la curva $E_0 : y^2 = x^3 - 35x - 98$, $a_p = p + 1 - N_p$ coincide con el p-ésimo coeficiente de Fourier de

$$\Theta(z) = \frac{1}{2} \sum_{n,m \in \mathbb{Z}} n \left(\frac{n}{7}\right) e((n^2 + 7m^2)z)$$

donde $e(z) = e^{2\pi i z}$.

Soluciones enteras de $n^2 + 7m^2 = p$.

- Si $p < 7$, no tiene soluciones enteras.
- Si $p = 7$, las soluciones son $n = 0$, $m = \pm 1$.
- Si $p > 7$, existe solución si y sólo si $p \equiv 1, 2, 4 \pmod 7$

¿Cómo se prueba la modularidad?

Para la curva $E_0 : y^2 = x^3 - 35x - 98$, $a_p = p + 1 - N_p$ coincide con el p-ésimo coeficiente de Fourier de

$$\Theta(z) = \frac{1}{2} \sum_{n,m \in \mathbb{Z}} n \left(\frac{n}{7}\right) e((n^2 + 7m^2)z)$$

donde $e(z) = e^{2\pi i z}$.

Soluciones enteras de $n^2 + 7m^2 = p$.

- Si $p < 7$, no tiene soluciones enteras.
- Si $p = 7$, las soluciones son $n = 0$, $m = \pm 1$.
- Si $p > 7$, existe solución si y sólo si $p \equiv 1, 2, 4 \pmod 7$

¿Cómo se prueba la modularidad?

Para la curva $E_0 : y^2 = x^3 - 35x - 98$, $a_p = p + 1 - N_p$ coincide con el p-ésimo coeficiente de Fourier de

$$\Theta(z) = \frac{1}{2} \sum_{n,m \in \mathbb{Z}} n \left(\frac{n}{7}\right) e((n^2 + 7m^2)z)$$

donde $e(z) = e^{2\pi i z}$.

Soluciones enteras de $n^2 + 7m^2 = p$.

- Si $p < 7$, no tiene soluciones enteras.
- Si $p = 7$, las soluciones son $n = 0$, $m = \pm 1$.
- Si $p > 7$, existe solución si y sólo si $p \equiv 1, 2, 4 \pmod 7$

¿Cómo se prueba la modularidad?

Para la curva $E_0 : y^2 = x^3 - 35x - 98$, $a_p = p + 1 - N_p$ coincide con el p-ésimo coeficiente de Fourier de

$$\Theta(z) = \frac{1}{2} \sum_{n,m \in \mathbb{Z}} n \left(\frac{n}{7}\right) e((n^2 + 7m^2)z)$$

donde $e(z) = e^{2\pi i z}$.

Soluciones enteras de $n^2 + 7m^2 = p$.

- Si $p < 7$, no tiene soluciones enteras.
- Si $p = 7$, las soluciones son $n = 0$, $m = \pm 1$.
- Si $p > 7$, existe solución si y sólo si $p \equiv 1, 2, 4 \pmod 7$

¿Cómo se prueba la modularidad?

Para la curva $E_0 : y^2 = x^3 - 35x - 98$, $a_p = p + 1 - N_p$ coincide con el p-ésimo coeficiente de Fourier de

$$\Theta(z) = \frac{1}{2} \sum_{n,m \in \mathbb{Z}} n \left(\frac{n}{7}\right) e((n^2 + 7m^2)z)$$

donde $e(z) = e^{2\pi i z}$.

Soluciones enteras de $n^2 + 7m^2 = p$.

- Si $p < 7$, no tiene soluciones enteras.
- Si $p = 7$, las soluciones son $n = 0$, $m = \pm 1$.
- Si $p > 7$, existe solución si y sólo si $p \equiv 1, 2, 4 \pmod 7$

Θ es forma modular de peso 2 con respecto a $\Gamma_0(196)$.

La modularidad de Θ se prueba con varias aplicaciones de la fórmula de sumación de Poisson (que implica $\sum e^{-\pi n^2 x} = x^{-1/2} \sum e^{-\pi n^2/x}$) junto con propiedades aritméticas relacionadas con la ley de reciprocidad cuadrática.

Los cálculos son largos pero finalmente se acaba probando

$$\Theta(z) = (cz+d)^{-2}\Theta\left(\frac{az+d}{cz+d}\right) \qquad \text{para } ad-bc=1, \quad 196|c.$$

La curva elíptica

$$E_0 : \ y^2 = x^3 - 35x - 98$$

es modular.