Curvas elípticas e integrales multiplicativas sobre campos no arquimedianos

Yamidt Bermúdez Tobón
Centro Interdisciplinario de Cómputo Científico
Universidad de Heidelberg
e-mail: yamidt.bermudez-tobon@iwr.uni-heidelberg.de

ALTENCOA6
San Juan de Pasto, 14.08.2014

Contenido

1 Algunas definiciones básicas

Contenido

1 Algunas definiciones básicas

2 Parametrización de curvas elípticas

Contenido

1. Algunas definiciones básicas
2. Parametrización de curvas elípticas
3. Curvas sobre $\mathbb{F}_q[T]$

Curvas elípticas y formas modulares

Una curva elíptica E sobre un campo K es una curva proyectiva suave cuya curva afín está dada por la ecuación

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \tag{1}$$

Esta ecuación se llama *forma de Weierstrass*. Si la característica de K es diferente de $2, 3$ entonces se puede simplificar

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

Formas modulares

Una **forma modular de peso k** para el grupo modular $SL_2(\mathbb{Z})$ es una función analítica $f : \mathfrak{H} \longrightarrow \mathbb{C}$ de el semiplano superior $\mathfrak{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ tal que f satisface

Formas modulares

Una **forma modular de peso k** para el grupo modular $SL_2(\mathbb{Z})$ es una función analítica $f : \mathfrak{H} \longrightarrow \mathbb{C}$ de el semiplano superior $\mathfrak{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ tal que f satisface

1) f es holomorfa en $\mathfrak{H}$.

Formas modulares

Una **forma modular de peso k** para el grupo modular $SL_2(\mathbb{Z})$ es una función analítica $f : \mathfrak{H} \longrightarrow \mathbb{C}$ de el semiplano superior $\mathfrak{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ tal que f satisface

1) f es holomorfa en $\mathfrak{H}$.

2) $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ para todo $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$.

Formas modulares

Una **forma modular de peso k** para el grupo modular $SL_2(\mathbb{Z})$ es una función analítica $f : \mathfrak{H} \longrightarrow \mathbb{C}$ de el semiplano superior $\mathfrak{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ tal que f satisface

1) f es holomorfa en $\mathfrak{H}$.

2) $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ para todo $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$.

3) f es holomorfa cuando z va a ∞ en el eje imaginario.

Formas modulares

Una **forma modular de peso k** para el grupo modular $SL_2(\mathbb{Z})$ es una función analítica $f : \mathfrak{H} \longrightarrow \mathbb{C}$ de el semiplano superior $\mathfrak{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ tal que f satisface

1) f es holomorfa en $\mathfrak{H}$.

2) $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ para todo $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$.

3) f es holomorfa cuando z va a ∞ en el eje imaginario.

- La condición 2) implica que f es períodica y por lo tanto tiene expansión en series de Fourier $f(z) = \sum_{n=-m}^{\infty} a_n q^n$ donde $q = 2\pi i z$.

- La ecuación funcional $z \mapsto \frac{az+b}{cz+d}$ se puede relajar considerando subgrupos de $SL_2(Z)$. En particular, estamos interesados en $\Gamma_0(N)$ (grupo de matrices en $SL_2(Z)$) las cuales son triangulares superiores modulo N.

- La ecuación funcional $z \mapsto \frac{az+b}{cz+d}$ se puede relajar considerando subgrupos de $SL_2(Z)$. En particular, estamos interesados en $\Gamma_0(N)$ (grupo de matrices en $SL_2(Z)$) las cuales son triangulares superiores modulo N.
- Si el coeficiente $a_0 = 0$ de f en la expansion de Fourier es 0, entonces f se es llamada una **forma cuspidal**.

- La ecuación funcional $z \mapsto \frac{az+b}{cz+d}$ se puede relajar considerando subgrupos de $SL_2(Z)$. En particular, estamos interesados en $\Gamma_0(N)$ (grupo de matrices en $SL_2(Z)$) las cuales son triangulares superiores modulo N.
- Si el coeficiente $a_0 = 0$ de f en la expansion de Fourier es 0, entonces f se es llamada una **forma cuspidal**.
- El conjunto de formas modulares es un espacio vectorial complejo finito dimensional.

- La ecuación funcional $z \mapsto \frac{az+b}{cz+d}$ se puede relajar considerando subgrupos de $SL_2(Z)$. En particular, estamos interesados en $\Gamma_0(N)$ (grupo de matrices en $SL_2(Z)$) las cuales son triangulares superiores modulo N.
- Si el coeficiente $a_0 = 0$ de f en la expansion de Fourier es 0, entonces f se es llamada una **forma cuspidal**.
- El conjunto de formas modulares es un espacio vectorial complejo finito dimensional.
- El espacio vectorial de formas modulares esta dotado de un operador (**Operador de Hecke**) que conserva formas cuspidales.

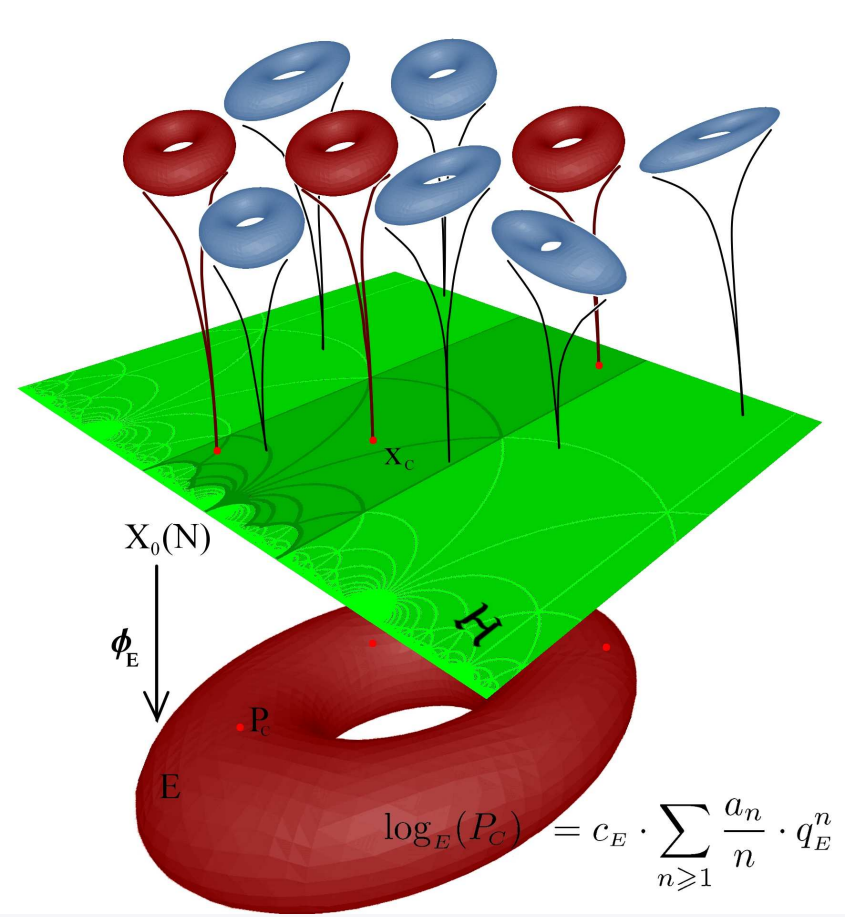
Definición

Una ***curva modular*** *para el subgrupo de congruencia* $\Gamma_0(N)$ *es la superficie de Riemmann, o la correspondiente curva algebraica, construida como el cociente del semiplano superior complejo* $\mathfrak{H}$ *por la accion de* $\Gamma_0(N)$.

Definición

Una ***curva modular*** *para el subgrupo de congruencia* $\Gamma_0(N)$ *es la superficie de Riemmann, o la correspondiente curva algebraica, construida como el cociente del semiplano superior complejo* $\mathfrak{H}$ *por la accion de* $\Gamma_0(N)$.

Como espacio moduli los puntos de una curva modular parametrizan clases de isomorfismos de curvas elípticas junto con una estructura adicional que depende del grupo $\Gamma_0(N)$.


X_C
X_0(N)
φ_E
H
P_C
E
log_E(P_C) = c_E · Σ_{n≥1} (a_n / n) · q_E^n

La conjetura de Taniyama-Shimura y parametrizaciones de curvas elípticas

Teorema (Breuil, Conrad, Diamond, Taylor, (Wiles), 2000)

La conjetura de Taniyama-Shimura es cierta para curvas definidas sobre $\mathbb{Q}$: Toda curva elíptica definida sobre $\mathbb{Q}$ de conductor N es factor (modulo isogenia) de la Jacobiana de la curva modular $X_0(N)$ de nivel N.

La conjetura de Taniyama-Shimura y parametrizaciones de curvas elípticas

Teorema (Breuil, Conrad, Diamond, Taylor, (Wiles), 2000)

La conjetura de Taniyama-Shimura es cierta para curvas definidas sobre $\mathbb{Q}$: Toda curva elíptica definida sobre $\mathbb{Q}$ de conductor N es factor (modulo isogenia) de la Jacobiana de la curva modular $X_0(N)$ de nivel N.

Dada una forma modular f de nivel N y peso 2 que es una autoforma para el operador de Hecke a uno le gustaría tener un procedimiento para construir una curva elíptica en la clase de isogenia que corresponda con f.

Sea $E/\mathbb{Q}$ una curva modular de conductor N.

Teorema (Shimura 1950's)

Existe una uniformización modular explícita $X_0(N) \longrightarrow E_f$ *sobre* $\mathbb{C}$.

Sea $E/\mathbb{Q}$ una curva modular de conductor N.

Teorema (Shimura 1950's)

Existe una uniformización modular explícita $X_0(N) \longrightarrow E_f$ sobre $\mathbb{C}$.

El siguiente diagama es commutativo

$$\begin{array}{ccc} \Gamma \setminus \mathcal{H}^* & \xrightarrow{z_0 \mapsto \int_\infty^{z_0} f_E(z)\,dz} & \mathbb{C}/\Lambda_E \\ \Big\downarrow{\scriptstyle j} & & \Big\downarrow{\scriptstyle \eta} \\ X_0(N)(\mathbb{C}) & \xrightarrow{\Phi_N} & E(\mathbb{C}). \end{array} \tag{2}$$

Donde $\eta : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$ es el isomorfismo complejo descrito por la fórmula $\eta = (\wp_\Lambda : \wp'_\Lambda : 1)$ donde $\wp_\Lambda$ es la función de Weierstrass $\wp$ asociada a Λ_E.

Sea $E/\mathbb{Q}$ una curva modular de conductor N.

Teorema (Shimura 1950's)

Existe una uniformización modular explícita $X_0(N) \longrightarrow E_f$ sobre $\mathbb{C}$.

El siguiente diagama es commutativo

$$\begin{array}{ccc} \Gamma \setminus \mathcal{H}^* & \xrightarrow{z_0 \mapsto \int_\infty^{z_0} f_E(z)\,dz} & \mathbb{C}/\Lambda_E \\ \Big\downarrow j & & \Big\downarrow \eta \\ X_0(N)(\mathbb{C}) & \xrightarrow{\Phi_N} & E(\mathbb{C}). \end{array} \tag{2}$$

Donde $\eta : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$ es el isomorfismo complejo descrito por la fórmula $\eta = (\wp_\Lambda : \wp'_\Lambda : 1)$ donde $\wp_\Lambda$ es la función de Weierstrass $\wp$ asociada a Λ_E. Aquí $\Lambda_E = \{\int_\infty^{\gamma\infty} \mid \gamma \in \Gamma_0(N)\}$.

Efectividad Definamos la serie de Eisenstein como

$$G_k(\Lambda) = \sum_{\omega \in \Lambda,\, \omega \neq 0} w^{-k}$$

para k un enero par. Sea

$$g_2(\Lambda) = 60\, G_4(\Lambda) \quad \textit{and} \quad g_3(\Lambda) = 140\, G_6(\Lambda).$$

Teorema (Edixhoven)

Para $y^2 = 4x^3 - c_4 x - c_6$ la ecuación de la curva fuerte de Weil $E = E_f$ para el lattice Λ_E uno tiene

$$c_4 := g_2(\Lambda_E),\ c_6 := g_3(\Lambda_E) \in Z.$$

Esto permite a Cremona encontrar ecuaciones para todas las curvas elípticas hasta conductor 130,000. (Los cálculos de f,Λ_E y $\wp_E$ son muy efectivos).

Sobre campos de funciones tenemos las siguientes correspondencias

$$\mathbb{Z} \rightsquigarrow \mathbb{F}_q[T] \tag{3}$$
$$\mathbb{Q} \rightsquigarrow \mathbb{F}_q(T) \tag{4}$$
$$\mathbb{R} \rightsquigarrow K_\infty = \mathbb{F}_q((\pi)),\ \pi = 1/T \tag{5}$$
$$\mathbb{C} \rightsquigarrow \mathbb{C}_\infty \tag{6}$$

donde $\mathbb{C}_\infty$ es la completación de una clausura algebráica de $\mathbb{F}_q((\pi))$.

El semiplano superior complejo se reemplaza por el **semiplano superior de Drinfeld**

$$\Omega := \mathbb{P}^1(\mathbb{C}_\infty) \setminus \mathbb{P}^1(K_\infty).$$

- Sea $\mathfrak{n}$ un ideal de $\mathbb{F}_q[T]$ considere $\Gamma_0(\mathfrak{n})$ el subgrupo de $GL_2(\mathbb{F}_q[T])$ consistente de matrices triangulares superiores modulo $\mathfrak{n}$.

- Sea $\mathfrak{n}$ un ideal de $\mathbb{F}_q[T]$ considere $\Gamma_0(\mathfrak{n})$ el subgrupo de $GL_2(\mathbb{F}_q[T])$ consistente de matrices triangulares superiores modulo $\mathfrak{n}$.
- En lugar de formas modulares consideramos formas analíticas rígidas $f : \Omega \longrightarrow \mathbb{C}_\infty$ con la acción de $\Gamma_0(\mathfrak{n})$ definida como en el caso clásico.

- Sea $\mathfrak{n}$ un ideal de $\mathbb{F}_q[T]$ considere $\Gamma_0(\mathfrak{n})$ el subgrupo de $GL_2(\mathbb{F}_q[T])$ consistente de matrices triangulares superiores modulo $\mathfrak{n}$.
- En lugar de formas modulares consideramos formas analíticas rígidas $f : \Omega \longrightarrow \mathbb{C}_\infty$ con la acción de $\Gamma_0(\mathfrak{n})$ definida como en el caso clásico.
- El cociente $\Gamma_0(\mathfrak{n}) \setminus \Omega$ es una curva algebráica sobre $\mathbb{C}_\infty$.

- Sea $\mathfrak{n}$ un ideal de $\mathbb{F}_q[T]$ considere $\Gamma_0(\mathfrak{n})$ el subgrupo de $GL_2(\mathbb{F}_q[T])$ consistente de matrices triangulares superiores modulo $\mathfrak{n}$.
- En lugar de formas modulares consideramos formas analíticas rígidas $f : \Omega \longrightarrow \mathbb{C}_\infty$ con la acción de $\Gamma_0(\mathfrak{n})$ definida como en el caso clásico.
- El cociente $\Gamma_0(\mathfrak{n}) \setminus \Omega$ es una curva algebráica sobre $\mathbb{C}_\infty$.

Definamos el árbol de Bruhat-Tits $\mathcal{T}$ para $PGL_2(K_\infty)$ como el árbol regular de grado $q+1$, cuyos vértices y lados son

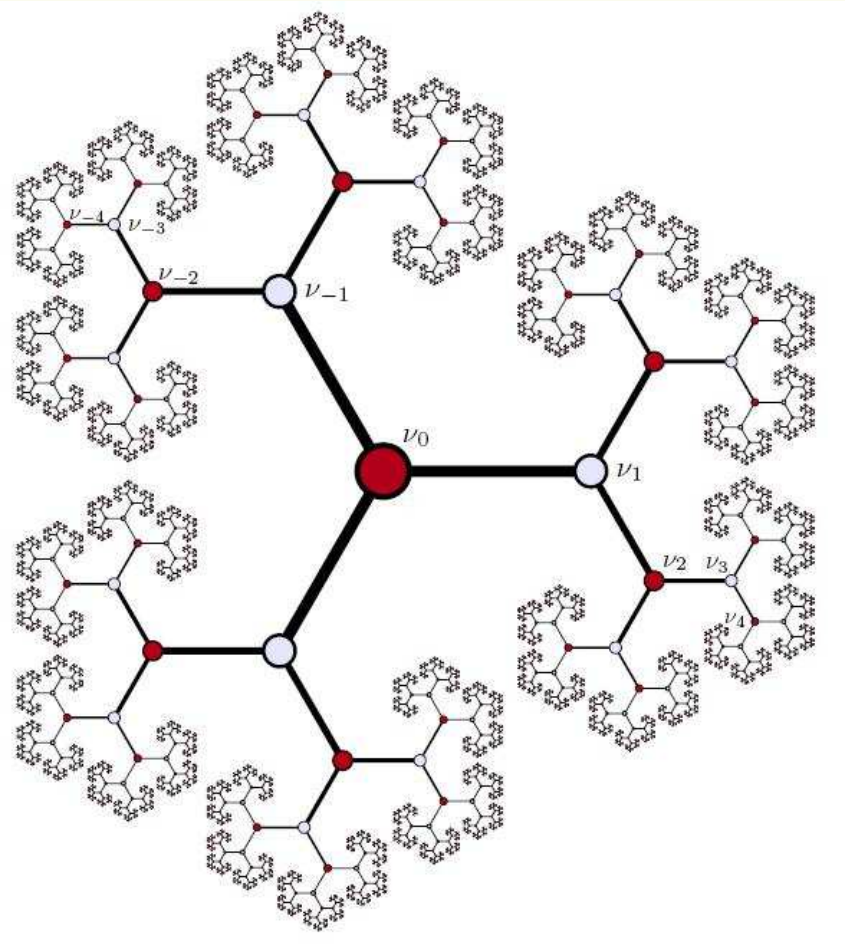
- **Vértices:** clases de homotecia $[L]$ de O_∞-latices en K_∞^2, donde O_∞ es el anillo de enteros de K_∞.

- Sea $\mathfrak{n}$ un ideal de $\mathbb{F}_q[T]$ considere $\Gamma_0(\mathfrak{n})$ el subgrupo de $GL_2(\mathbb{F}_q[T])$ consistente de matrices triangulares superiores modulo $\mathfrak{n}$.
- En lugar de formas modulares consideramos formas analíticas rígidas $f : \Omega \longrightarrow \mathbb{C}_\infty$ con la acción de $\Gamma_0(\mathfrak{n})$ definida como en el caso clásico.
- El cociente $\Gamma_0(\mathfrak{n}) \setminus \Omega$ es una curva algebráica sobre $\mathbb{C}_\infty$.

Definamos el árbol de Bruhat-Tits $\mathcal{T}$ para $PGL_2(K_\infty)$ como el árbol regular de grado $q+1$, cuyos vértices y lados son

- **Vértices:** clases de homotecia $[L]$ de O_∞-latices en K_∞^2, donde O_∞ es el anillo de enteros de K_∞.
- **Lados orientados:** pares $([L_1], [L_2])$ tal que $L_1 \supsetneq L_2 \supsetneq \pi L_1$.

Árbol de Bruhat-Tits para $q = 2$



Existe una aplicación $Red : \Omega \longrightarrow \mathcal{T}$ que es $\Gamma_0(\mathfrak{n})$-invariante.

Un cociclo armónico $\Gamma_0(\mathfrak{n})$-invariante con valores en $\mathbb{Z}$, es una función $\varphi : \text{lados}(\mathcal{T}) \longrightarrow \mathbb{Z}$ tal que para todo lado orientado e se tiene

Existe una aplicación $Red : \Omega \longrightarrow \mathcal{T}$ que es $\Gamma_0(\mathfrak{n})$-invariante.

Un cociclo armónico $\Gamma_0(\mathfrak{n})$-invariante con valores en $\mathbb{Z}$, es una función $\varphi : \text{lados}(\mathcal{T}) \longrightarrow \mathbb{Z}$ tal que para todo lado orientado e se tiene

1) $\varphi(\bar{e}) = -\varphi(e)$ donde $\bar{e}$ es el lado opuesto a e.

Existe una aplicación $Red : \Omega \longrightarrow \mathcal{T}$ que es $\Gamma_0(\mathfrak{n})$-invariante.

Un cociclo armónico $\Gamma_0(\mathfrak{n})$-invariante con valores en $\mathbb{Z}$, es una función $\varphi : \text{lados}(\mathcal{T}) \longrightarrow \mathbb{Z}$ tal que para todo lado orientado e se tiene

1) $\varphi(\bar{e}) = -\varphi(e)$ donde $\bar{e}$ es el lado opuesto a e.

2) $\sum_{t(e)=v} \varphi(e) = 0$, donde $t(e)$ es el terminal de e.

Existe una aplicación $Red : \Omega \longrightarrow \mathcal{T}$ que es $\Gamma_0(\mathfrak{n})$-invariante.

Un cociclo armónico $\Gamma_0(\mathfrak{n})$-invariante con valores en $\mathbb{Z}$, es una función $\varphi : \text{lados}(\mathcal{T}) \longrightarrow \mathbb{Z}$ tal que para todo lado orientado e se tiene

1) $\varphi(\bar{e}) = -\varphi(e)$ donde $\bar{e}$ es el lado opuesto a e.

2) $\sum_{t(e)=v} \varphi(e) = 0$, donde $t(e)$ es el terminal de e.

3) $\varphi(\gamma e) = \varphi(e)$ para todo $\gamma \in \Gamma_0(\mathfrak{n})$.

Existe una aplicación $Red : \Omega \longrightarrow \mathcal{T}$ que es $\Gamma_0(\mathfrak{n})$-invariante.

Un cociclo armónico $\Gamma_0(\mathfrak{n})$-invariante con valores en $\mathbb{Z}$, es una función $\varphi : \text{lados}(\mathcal{T}) \longrightarrow \mathbb{Z}$ tal que para todo lado orientado e se tiene

1) $\varphi(\bar{e}) = -\varphi(e)$ donde $\bar{e}$ es el lado opuesto a e.

2) $\sum_{t(e)=v} \varphi(e) = 0$, donde $t(e)$ es el terminal de e.

3) $\varphi(\gamma e) = \varphi(e)$ para todo $\gamma \in \Gamma_0(\mathfrak{n})$.

- Los cociclos armónicos están en correspondencia 1-1 con medidas en $\mathbb{P}^1(K_\infty)$.

Existe una aplicación $Red : \Omega \longrightarrow \mathcal{T}$ que es $\Gamma_0(\mathfrak{n})$-invariante.

Un cociclo armónico $\Gamma_0(\mathfrak{n})$-invariante con valores en $\mathbb{Z}$, es una función $\varphi : \text{lados}(\mathcal{T}) \longrightarrow \mathbb{Z}$ tal que para todo lado orientado e se tiene

1) $\varphi(\bar{e}) = -\varphi(e)$ donde $\bar{e}$ es el lado opuesto a e.

2) $\sum_{t(e)=v} \varphi(e) = 0$, donde $t(e)$ es el terminal de e.

3) $\varphi(\gamma e) = \varphi(e)$ para todo $\gamma \in \Gamma_0(\mathfrak{n})$.

- Los cociclos armónicos están en correspondencia 1-1 con medidas en $\mathbb{P}^1(K_\infty)$.
- Cada lado e del árbol $\mathcal{T}$ está en correspondencia con un abierto compacto de $\mathbb{P}^1(K_\infty)$.

Parametrizaciones modulares de curvas elípticas

Teorema (Drinfeld 1974)

La conjetura de Taniyama-Shimura es cierta para curvas elípticas definidas sobre $\mathbb{F}_q(T)$: Toda curva elíptica E definida sobre $\mathbb{F}_q(T)$ de conductor $\mathfrak{n}\infty$ es un factor (modulo una isogenia) de la Jacobiana J de la curva modular de Drinfeld $X(\mathfrak{n})$ de nivel $\mathfrak{n}$.

Sea $E/\mathbb{F}_q(T)$ con conductor $\mathfrak{n}\infty$ y correspondiente a una Hecke autoforma modular f de nivel $\mathfrak{n}$

Teorema (Gekeler-Reversat, 1996)

Existe una parametrización modular explícita $X_0(\mathfrak{n}) \longrightarrow E_f$ sobre $\mathbb{C}_\infty$.

Integrales multiplicativas

Definición

Dada una función continua $f : \mathbb{P}^1(K_\infty) \to \mathbb{C}_\infty^\times$, *su integral multiplicativa con respecto a una medida* $\mu \in \mathcal{M}_0(\mathbb{P}^1(K_\infty), \mathbb{Z})$ *es*

$$\oint_{\mathbb{P}^1(K_\infty)} f(t)\, d\mu(t) := \varinjlim_{\alpha} \prod_{U \in \mathcal{C}_\alpha} f(u)^{\mu(U)} \tag{7}$$

donde $\{\mathcal{C}_\alpha\}_\alpha$ *es el sistema directo de cubrimientos finitos de* $\mathbb{P}^1(K_\infty)$ *por subconjuntos abiertos compactos* U *y* u *es un punto arbitrario en* U.

Esta integral se puede usar para definir la parametrización explícita

$$\Gamma_0(\mathfrak{n}) \setminus \Omega \longrightarrow \mathbb{C}_\infty^\times / \mathbf{q}^{\mathbb{Z}} \tag{8}$$

$$z \longmapsto \int\!\!\!\!\!\!\diagup_{\mathbb{P}^1(K_\infty)} \frac{z_0 - t}{z_1 - t}\, d\mu(t) \tag{9}$$

donde

$$\mathbf{q}^{\mathbb{Z}} = \{ \int\!\!\!\!\!\!\diagup_{\mathbb{P}^1(K_\infty)} \frac{z_0 - t}{\gamma z_0 - t}\, d\mu(t) \mid \gamma \in \Gamma_0(\mathfrak{n}) \}$$

Esta integral se puede usar para definir la parametrización explícita

$$\Gamma_0(\mathfrak{n}) \setminus \Omega \longrightarrow \mathbb{C}_\infty^\times / \mathbf{q}^{\mathbb{Z}} \tag{8}$$

$$z \longmapsto \int\!\!\!\!\!\!\diagup_{\mathbb{P}^1(K_\infty)} \frac{z_0 - t}{z_1 - t}\, d\mu(t) \tag{9}$$

donde

$$\mathbf{q}^{\mathbb{Z}} = \{ \int\!\!\!\!\!\!\diagup_{\mathbb{P}^1(K_\infty)} \frac{z_0 - t}{\gamma z_0 - t}\, d\mu(t) \mid \gamma \in \Gamma_0(\mathfrak{n}) \}$$

Problema

Cómo calcular la integral multiplicativa efectivamente?

- Sobre los p-ádicos Darmon y Greenberg encontraron un algoritmo que permite calcular con buena precisión una integral similar en tiempo polinomial.

- Sobre los p-ádicos Darmon y Greenberg encontraron un algoritmo que permite calcular con buena precisión una integral similar en tiempo polinomial.
- La clave en el cálculo de Darmon-Greenberg es la función logaritmo.

- Sobre los p-ádicos Darmon y Greenberg encontraron un algoritmo que permite calcular con buena precisión una integral similar en tiempo polinomial.
- La clave en el cálculo de Darmon-Greenberg es la función logaritmo.

En $\mathbb{F}_q(T)$ no existe una función logaritmo

- Sobre los p-ádicos Darmon y Greenberg encontraron un algoritmo que permite calcular con buena precisión una integral similar en tiempo polinomial.
- La clave en el cálculo de Darmon-Greenberg es la función logaritmo.

En $\mathbb{F}_q(T)$ no existe una función logaritmo

Usando una modificación del algoritmo de Greenberg nosotros encontramos un algoritmo para calcular $\mathbf{q}$.

Teorema (B., Boeckle y Cervino)

El parámetro de Tate $\mathbf{q}$ *se puede calcular en tiempo polinomial.*

Ejemplos

- $p = 2,\ \mathfrak{n} = T^3 \rightsquigarrow\ \mathbf{q} = \pi^{\mathbf{4}} + \pi^{\mathbf{36}} + \pi^{\mathbf{68}} + \mathbf{O}(\pi^{\mathbf{69}})$.
- $p = 2,\ \mathfrak{n} = T^4 + T^3 + T^2 + T + 1 \rightsquigarrow$
  $\mathbf{q} = \pi^{\mathbf{8}} + \pi^{\mathbf{9}} + .. + \pi^{\mathbf{30}} + \mathbf{O}(\pi^{\mathbf{31}})$.
- $p = 3,\ \mathfrak{n} = (T + 2)(T^2 + T + 2) \rightsquigarrow$
  $\mathbf{q} = \pi^{\mathbf{4}} + \pi^{\mathbf{5}} + .. + \pi^{\mathbf{40}} + \mathbf{O}(\pi^{\mathbf{41}})$.
- $p = 5,\ \mathfrak{n} = T^2(T^2 - 1) \rightsquigarrow\ \mathbf{q} = \pi^{\mathbf{2}} + \mathbf{2}\pi^{\mathbf{4}} + .. + \mathbf{2}\pi^{\mathbf{50}} + \mathbf{O}(\pi^{\mathbf{51}})$.
- $p = 7,\ \mathfrak{n} = T^3 - 2 \rightsquigarrow\ \mathbf{q} = \mathbf{5}\pi^{\mathbf{3}} + \mathbf{4}\pi^{\mathbf{6}} + .. + \mathbf{5}\pi^{\mathbf{60}} + \mathbf{O}(\pi^{\mathbf{61}})$.

Efectividad

Defina

$$s_k \quad = \quad \sum_{m \geqslant 1} \frac{m^k \mathbf{q}^m}{1 - \mathbf{q}^m} \quad \text{para } k \in \mathbb{N}. \tag{10}$$

Tome $a_4(\mathbf{q}) = -5s_3$ y $a_6(\mathbf{q}) = \frac{1}{12}(5s_3 + 7s_5)$ y asi la curva de Tate es

$$E_{\mathbf{q}} : y^2 + xy = x^3 + a_4(\mathbf{q})x + a_6(\mathbf{q}).$$

Efectividad

Defina

$$s_k \quad = \quad \sum_{m \geqslant 1} \frac{m^k \mathbf{q}^m}{1 - \mathbf{q}^m} \quad \text{para } k \in \mathbb{N}. \tag{10}$$

Tome $a_4(\mathbf{q}) = -5s_3$ y $a_6(\mathbf{q}) = \frac{1}{12}(5s_3 + 7s_5)$ y asi la curva de Tate es

$$E_{\mathbf{q}} : y^2 + xy = x^3 + a_4(\mathbf{q})x + a_6(\mathbf{q}).$$

Para $p = 2$ y $\mathfrak{n} = T^3$ con $\mathbf{q} = \pi^{\mathbf{4}} + \pi^{\mathbf{36}} + \pi^{\mathbf{68}} + \mathbf{O}(\pi^{\mathbf{69}})$ se obtuvo la curva

$$E : y^2 + xy = y^3 + \frac{1}{T^3}.$$

Efectividad

Defina

$$s_k \quad = \quad \sum_{m \geqslant 1} \frac{m^k \mathbf{q}^m}{1 - \mathbf{q}^m} \quad \text{para } k \in \mathbb{N}. \tag{10}$$

Tome $a_4(\mathbf{q}) = -5s_3$ y $a_6(\mathbf{q}) = \frac{1}{12}(5s_3 + 7s_5)$ y asi la curva de Tate es

$$E_{\mathbf{q}} : y^2 + xy = x^3 + a_4(\mathbf{q})x + a_6(\mathbf{q}).$$

Para $p = 2$ y $\mathfrak{n} = T^3$ con $\mathbf{q} = \pi^{\mathbf{4}} + \pi^{\mathbf{36}} + \pi^{\mathbf{68}} + \mathbf{O}(\pi^{\mathbf{69}})$ se obtuvo la curva

$$E : y^2 + xy = y^3 + \frac{1}{T^3}.$$

Para $p = 3$ y $\mathfrak{n} = (T-1)(T^2 + T + 1)$ con
$\mathbf{q} = \pi^{\mathbf{4}} + \pi^{\mathbf{5}} + .. + \pi^{\mathbf{40}} + \mathbf{O}(\pi^{\mathbf{41}})$ se obtuvo la curva.

$$E : y^2 = x^3 + (T^2 + T)x^2 - \frac{(T-1)^4(T^2 + T - 1)}{(T^2 + T)^3}.$$

Para $p > 3$ no es fácil encontrar un modelo sobre $\mathbb{F}_q(T)$.

Para $p > 3$ no es fácil encontrar un modelo sobre $\mathbb{F}_q(T)$.

Sean $E_4 = 1 + 240 s_3(\mathbf{q})$ y $E_6 = 1 - 504 s_5(\mathbf{q})$ las series de Einsestein.

Serre y Swinnerton-Dyer probaron que existe un polinomio $A \in \mathbb{F}_q[X, Y]$ tal que $A(E_2, E_4) = 1 \bmod p$.

Lo cual implica que existen $n, m \in \mathbb{N}$ tal que $g_2^n, g_3^m \in \mathbb{F}_q(T)$. Entonces usando la ecuación $y^2 = 4x^3 - g_2 x - g_3$ se pueden encontrar las curvas con coefficientes recionales.

Para $p > 3$ no es fácil encontrar un modelo sobre $\mathbb{F}_q(T)$.

Sean $E_4 = 1 + 240 s_3(\mathbf{q})$ y $E_6 = 1 - 504 s_5(\mathbf{q})$ las series de Einsestein.

Serre y Swinnerton-Dyer probaron que existe un polinomio $A \in \mathbb{F}_q[X, Y]$ tal que $A(E_2, E_4) = 1 \bmod p$.

Lo cual implica que existen $n, m \in \mathbb{N}$ tal que $g_2^n, g_3^m \in \mathbb{F}_q(T)$. Entonces usando la ecuación $y^2 = 4x^3 - g_2 x - g_3$ se pueden encontrar las curvas con coefficientes recionales.

Para $p = 5$ y $\mathfrak{n} = T^2(T-1)$ con $\mathbf{q} = \pi^{\mathbf{2}} + \mathbf{2}\pi^{\mathbf{4}} + .. + \mathbf{2}\pi^{\mathbf{50}} + \mathbf{O}(\pi^{\mathbf{51}})$ se obtuvo

$$E : y^2 = x^3 + \frac{3T+4}{T} x + \frac{4T+3}{T}.$$

GRACIAS POR SU ATENCIÓN!