Formas Modulares: why do we care?

João Rafael de Melo Ruiz
joaorm.ruiz@gmail.com
Sorbonne Université

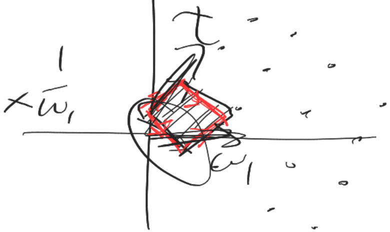
17/05/2022

Overview

1. Como apareceu isso
2. Um problema bem pé no chão
3. Curvas modulares
4. Modularidade
5. Representações de Galois e funções L

Parametrização de curvas elípticas $/\mathbb{C}$

Def. $\boxed{\mathbb{C}/\Lambda}$ $\quad \Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$



$\Lambda \subseteq \mathbb{C}$ uno $\quad \boxed{E = \mathbb{C}/\Lambda}$

$$\begin{tikzcd}
\mathbb{C} \arrow[r, "\times\alpha"] \arrow[d] & \mathbb{C} \arrow[d] \\
E = \mathbb{C}/\Lambda \arrow[r, "(\exists ?)", "\times\alpha"'] & \mathbb{C}/\Lambda' = E'
\end{tikzcd}$$

$\underline{\underline{\alpha\Lambda \subseteq \Lambda'}}$

$$\mathbb{C}/\Lambda \xrightarrow[\times\alpha]{\sim} \mathbb{C}/\Lambda'$$

$$\boxed{\underline{\underline{\alpha\Lambda = \Lambda'}}}$$

Parametrização de curvas elípticas $/\mathbb{C}$

- Reticulado $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subseteq \mathbb{C} \longrightarrow$ curva elíptica $E/\mathbb{C}$.

Parametrização de curvas elípticas $/\mathbb{C}$

- Reticulado $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subseteq \mathbb{C} \longrightarrow$ curva elíptica $E/\mathbb{C}$.
- Todo morfismo de curvas $E/\Lambda \to E/\Lambda'$ vem de multiplicação por um $\alpha \in \mathbb{C}$ tal que $\alpha\Lambda \subseteq \Lambda'$

Parametrização de curvas elípticas $/\mathbb{C}$

- Reticulado $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subseteq \mathbb{C} \longrightarrow$ curva elíptica $E/\mathbb{C}$.
- Todo morfismo de curvas $E/\Lambda \to E/\Lambda'$ vem de multiplicação por um $\alpha \in \mathbb{C}$ tal que $\alpha\Lambda \subseteq \Lambda'$
- $\mathbb{C}/\Lambda \simeq \mathbb{C}/\Lambda'$ se e somente se $\Lambda = \alpha\Lambda'$.

Parametrização de curvas elípticas $/\mathbb{C}$

- Reticulado $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subseteq \mathbb{C} \longrightarrow$ curva elíptica $E/\mathbb{C}$.
- Todo morfismo de curvas $E/\Lambda \to E/\Lambda'$ vem de multiplicação por um $\alpha \in \mathbb{C}$ tal que $\alpha\Lambda \subseteq \Lambda'$
- $\mathbb{C}/\Lambda \simeq \mathbb{C}/\Lambda'$ se e somente se $\Lambda = \alpha\Lambda'$.
- Conclusão:

$$\{\text{Classes de isomorfismo de curvas elípticas}/\mathbb{C}\} \longleftrightarrow \{\text{Reticulados} \subseteq \mathbb{C}\}/\text{homotetia}$$

$E = \dfrac{\mathbb{C}}{\mathbb{Z} \oplus \mathbb{Z}\tau}$ $\quad \tau \in \mathbb{H}$

$\operatorname{Im} \tau > 0$

Parametrização de curvas elípticas $/\mathbb{C}$

- Reticulado $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subseteq \mathbb{C} \longrightarrow$ curva elíptica $E/\mathbb{C}$.
- Todo morfismo de curvas $E/\Lambda \to E/\Lambda'$ vem de multiplicação por um $\alpha \in \mathbb{C}$ tal que $\alpha\Lambda \subseteq \Lambda'$
- $\mathbb{C}/\Lambda \simeq \mathbb{C}/\Lambda'$ se e somente se $\Lambda = \alpha\Lambda'$.
- Conclusão:

$$\{\text{Classes de isomorfismo de curvas elípticas}/\mathbb{C}\} \longleftrightarrow \{\text{Reticulados} \subseteq \mathbb{C}\}/\text{homotetia}$$

- SPG olhamos reticulados da forma $\Lambda = \Lambda\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$, $\tau \in \mathbb{H} := \{z \in \mathbb{C} |\ \mathrm{Im}\, z > 0\}$.

Então $\mathbb{H}$ parametriza curvas elípticas?

$$\alpha \underline{\Lambda_\tau} = \underline{\Lambda_{\tau'}}$$

$$\tau' = \alpha \cdot (a\tau + b)$$

$$1 = \alpha \cdot (c\tau + d)$$

$$\tau' = \frac{a\tau + b}{c\tau + d} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \tau$$

$$\boxed{SL_2\mathbb{Z} \backslash \mathbb{H} =: Y(1)}$$

$$Y(N) := \underline{\Gamma(N)} \backslash \mathbb{H}$$

$$\ker(SL_2\mathbb{Z} \to SL_2 \mathbb{Z}/N\mathbb{Z})$$

Não!

A ação de $\mathrm{SL}_2\,\mathbb{Z}$

$\mathrm{PSL}_2\mathbb{Z}$

- $\cancel{\mathrm{SL}_2}\,\mathbb{Z} \circlearrowleft \mathbb{H}$ é uma ação meio zuada (tem pontos com estabilizador não-trivial);

$$\tau = \frac{-\tau}{-1} = \underbrace{\begin{bmatrix} -1 & \\ & -1 \end{bmatrix}}_{-1\cdot\mathbb{1}} \cdot \tau$$

$$i = \frac{-1}{i} = \begin{bmatrix} & -1 \\ 1 & \end{bmatrix} i$$

$$|\mathrm{SL}_2\mathbb{Z}_i|/2$$

$$\rho = \exp\left(\frac{2\pi i}{3}\right)$$

$$|\mathrm{SL}_2\mathbb{Z}_\rho|/2$$

A ação de $\mathrm{SL}_2 \mathbb{Z}$

- $\mathrm{SL}_2 \mathbb{Z} \circlearrowleft \mathbb{H}$ é uma ação meio zuada (tem pontos com estabilizador não-trivial);
- Um domínio fundamental:

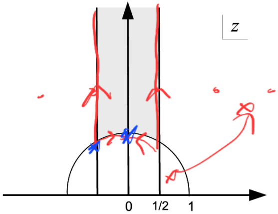
A ação de $SL_2 \mathbb{Z}$

- $SL_2 \mathbb{Z} \circlearrowleft \mathbb{H}$ é uma ação meio zuada (tem pontos com estabilizador não-trivial);
- Um domínio fundamental:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \tau = \tau + 1$$

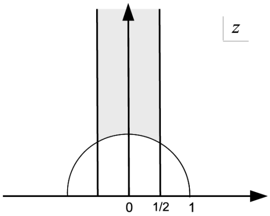
$$\begin{bmatrix} & -1 \\ 1 & \end{bmatrix}$$

$SL_2\mathbb{Z}$



A ação de $\mathrm{SL}_2\,\mathbb{Z}$

- $\mathrm{SL}_2\,\mathbb{Z} \circlearrowleft \mathbb{H}$ é uma ação meio zuada (tem pontos com estabilizador não-trivial);
- Um domínio fundamental:



- Porém $Y(1) := \mathrm{SL}_2\,\mathbb{Z}\backslash\mathbb{H}$ é uma superfície de Riemann!

Tá, mas da onde surgem formas modulares?!

$\boxed{g = 1}$

$\Longrightarrow$ Riemann Roch

$$y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$$

$$G_k(\Lambda) = \sum_{\omega \in \Lambda}{}' \omega^{-k}$$

EISENSTEIN

$$\underline{\underline{G_k(\alpha\Lambda) = \alpha^{-k} G_k(\Lambda)}}$$

$$\mathbb{C}/\Lambda$$

$$G_k(\tau) := G_k(\mathbb{Z} \oplus \mathbb{Z}\tau).$$

Tá, mas da onde surgem formas modulares?!

Quando transformamos o toro numa cúbica!

Tá, mas da onde surgem formas modulares?!

$\alpha\Lambda = \Lambda' \Rightarrow E \simeq E'$

Quando transformamos o toro numa cúbica!

$$\boxed{y^2 = 4x^3 - 60G_4(\alpha\Lambda)\,x - 140G_6(\alpha\Lambda).}$$

$(x, y) \longmapsto (u^2 x, u^3 y)$

$u = \alpha^2$

Tá, mas da onde surgem formas modulares?!

Quando transformamos o toro numa cúbica!

$$y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda).$$

Peraê! Esses caras não são invariantes!!

Tá, mas da onde surgem formas modulares?!

Quando transformamos o toro numa cúbica!

$$y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda).$$

Peraê! Esses caras não são invariantes!!Mas são a menos de mudança de coordenada...

Definição, finalmente!

Definição, finalmente!

Definição

$\Gamma(N) := \ker(\mathrm{SL}_2\,\mathbb{Z} \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$. Um subgrupo $\Gamma \subseteq \mathrm{SL}_2\,\mathbb{Z}$ é dito ser de congruência se existe $N \geqslant 1$ tal que $\Gamma \supseteq \Gamma(N)$.

$$\begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix} \in \Gamma(N)$$

$$f(t+N) = f(t)$$

Definição, finalmente!

Definição

$\Gamma(N) := \ker\left(\mathrm{SL}_2\,\mathbb{Z} \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\right)$. Um subgrupo $\Gamma \subseteq \mathrm{SL}_2\,\mathbb{Z}$ é dito ser de congruência se existe $N \geqslant 1$ tal que $\Gamma \supseteq \Gamma(N)$.

Definição

Sejam $k \in \mathbb{Z}$ e $\Gamma \subseteq \mathrm{SL}_2\,\mathbb{Z}$ um subgrupo de congruência. Uma função holomorfa $f : \mathbb{H} \to \mathbb{C}$ é dita ser **fracamente modular de peso k com respeito a Γ** se, para todo, $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma$,

$$f(\gamma \cdot \tau) = (c\tau + d)^k f(\tau)$$

$f(\alpha N) = \alpha^k f(N)$

Expansão de Fourier e formas modulares

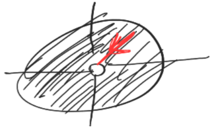
f Mod. form $\quad SL_2\mathbb{Z} \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in SL_2\mathbb{Z}$

$$\boxed{f(t+1) = f(t)}$$

$$f(t) = \sum_{n \geq n_0} a_n q^n$$

$SL_2\mathbb{Z}\cdot\infty = \{\infty\} \cup \mathbb{Q}$

q



$q = \exp(2\pi i t)$

Expansão de Fourier e formas modulares

Forma modular - definição

Definição

Uma forma fracamente modular de peso k para $\mathrm{SL}_2\,\mathbb{Z}$ é uma forma modular se sua expansão de Fourier

$$f(\tau) = \sum_{n \geqslant n_0} a_n q^n, \qquad q = e^{2\pi i \tau},$$

é holomorfa, i.e. $n_0 = 0$.

$f(\text{CUSP}) = 0$

$a_0 = 0$

$\left\{ \begin{array}{l} \text{CUSPIDAL} \\ \text{PARABÓLICA} \end{array} \right.$

Um problema bem pé no chão

$$\# \vee (n = a^2 + b^2 + c^2 + d^2) \subseteq \mathbb{Z}^4$$

Problema

Seja $n \geqslant 1$ inteiro. De quantas maneiras podemos (se é que podemos) escrever n como soma de quatro quadrados?

Um problema bem pé no chão

Problema

Seja $n \geqslant 1$ inteiro. De quantas maneiras podemos (se é que podemos) escrever n como soma de quatro quadrados?

É bem a carinha de pergunta de teoria de números...

Resolvendo o problema

Resolvendo o problema

- Definimos $r(n,k) :=$ número de maneiras de escrever n como k quadrados.

$r(n,4)$

$$\Theta_k(t) = \sum_{n \geq 0} r(n,k) q^n$$

Resolvendo o problema

- Definimos $r(n,k) :=$ número de maneiras de escrever n como k quadrados.
- Definimos uma função $\theta_k(\tau) := \sum_{n \geqslant 0} r(n,k)\, q^n$, $q = e^{2\pi i \tau}$.

Resolvendo o problema

- Definimos $r(n,k) :=$ número de maneiras de escrever n como k quadrados.
- Definimos uma função $\theta_k(\tau) := \sum_{n \geqslant 0} r(n,k)\, q^n$, $q = e^{2\pi i \tau}$.
- $\theta_4(\tau)$ é uma forma modular de peso 2 com respeito ao subgrupo $\Gamma_\theta = \left\langle \pm \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix} \right\rangle$. $\supseteq \Gamma(4)$

$\dim_{\mathbb{C}} \mathcal{M}_2(\Gamma_\theta) = 2$

Resolvendo o problema

- Definimos $r(n,k) :=$ número de maneiras de escrever n como k quadrados.
- Definimos uma função $\theta_k(\tau) := \sum_{n \geqslant 0} r(n,k)\, q^n$, $q = e^{2\pi i \tau}$.
- $\theta_4(\tau)$ é uma forma modular de peso 2 com respeito ao subgrupo $\Gamma_\theta = \left\langle \pm \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix} \right\rangle$.
- O espaço de formas modulares de peso 2 com respeito a Γ_θ tem dimensão 2.

Resolvendo o problema

- Definimos $r(n,k) :=$ número de maneiras de escrever n como k quadrados.
- Definimos uma função $\theta_k(\tau) := \sum_{n \geqslant 0} r(n,k) q^n$, $q = e^{2\pi i \tau}$.
- $\theta_4(\tau)$ é uma forma modular de peso 2 com respeito ao subgrupo $\Gamma_\theta = \left\langle \pm \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix} \right\rangle$.
- O espaço de formas modulares de peso 2 com respeito a Γ_θ tem dimensão 2.
- Podemos definir “correções´´ das séries de Eisenstein que geram esse espaço: $G_{2,2}$, $G_{2,4}$.

$$\theta_4 = \underline{a}\, G_{2,2} + \underline{b}\, G_{2,4}$$

Resolvendo o problema

- Definimos $r(n,k) :=$ número de maneiras de escrever n como k quadrados.
- Definimos uma função $\theta_k(\tau) := \sum_{n\geqslant 0} r(n,k)\, q^n,\ q = e^{2\pi i\tau}$.
- $\theta_4(\tau)$ é uma forma modular de peso 2 com respeito ao subgrupo $\Gamma_\theta = \left\langle \pm \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix} \right\rangle$.
- O espaço de formas modulares de peso 2 com respeito a Γ_θ tem dimensão 2.
- Podemos definir "correções´´ das séries de Eisenstein que geram esse espaço: $G_{2,2}$, $G_{2,4}$.
- Olhando os primeiros coeficientes concluímos que $\theta_4(\tau) = -\frac{1}{\pi^2} G_{2,4}(\tau)$.

Resolvendo o problema

- Definimos $r(n,k) :=$ número de maneiras de escrever n como k quadrados.
- Definimos uma função $\theta_k(\tau) := \sum_{n\geqslant 0} r(n,k)\, q^n$, $q = e^{2\pi i\tau}$.
- $\theta_4(\tau)$ é uma forma modular de peso 2 com respeito ao subgrupo $\Gamma_\theta = \left\langle \pm\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \pm\begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}\right\rangle$.
- O espaço de formas modulares de peso 2 com respeito a Γ_θ tem dimensão 2.
- Podemos definir "correções´´ das séries de Eisenstein que geram esse espaço: $G_{2,2}, G_{2,4}$.
- Olhando os primeiros coeficientes concluímos que $\theta_4(\tau) = -\frac{1}{\pi^2} G_{2,4}(\tau)$.
- E isso nos permite concluir que

$$\boxed{r(n,4) = 8 \sum_{\substack{0<d\mid n \\ 4\nmid d}} d.}$$

Resolvendo o problema

- Definimos $r(n,k) :=$ número de maneiras de escrever n como k quadrados.
- Definimos uma função $\theta_k(\tau) := \sum_{n \geqslant 0} r(n,k)\, q^n,\ q = e^{2\pi i \tau}$.
- $\theta_4(\tau)$ é uma forma modular de peso 2 com respeito ao subgrupo $\Gamma_\theta = \left\langle \pm \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix} \right\rangle$.

$\boxed{\mathcal{M}_k(\Gamma)}$

- O espaço de formas modulares de peso 2 com respeito a Γ_θ tem dimensão 2.
- Podemos definir "correções´´ das séries de Eisenstein que geram esse espaço: $G_{2,2}, G_{2,4}$.
- Olhando os primeiros coeficientes concluímos que $\theta_4(\tau) = -\frac{1}{\pi^2} G_{2,4}(\tau)$.
- E isso nos permite concluir que

$$r(n,4) = 8 \sum_{\substack{0<d\mid n \\ 4\nmid d}} d.$$

- Inclusive generalizamos isso pra $r(n,8)$, $r(n,16)$ bem facilmente!

Curvas modulares

$\Gamma(N) \subseteq \Gamma \subseteq SL_2\mathbb{Z}$

$SL_2\mathbb{Z}\backslash\mathbb{H}$

Retornamos aos $Y(\Gamma) := \Gamma\backslash\mathbb{H}$. $\rightsquigarrow X(\Gamma)$

$\boxed{H^*(Y(\Gamma), \underline{A})}$

Curvas modulares

$\Gamma = SL_2\mathbb{Z}$

Retornamos aos $Y(\Gamma) := \Gamma\backslash\mathbb{H}$. Compactificação: $X(\Gamma) \simeq \Gamma\backslash\mathbb{H}^*$, onde $\mathbb{H}^* := H \cup \mathbb{Q} \cup \{\infty\}$.

Retornamos aos $Y(\Gamma) := \Gamma\backslash\mathbb{H}$. Compactificação: $X(\Gamma) \simeq \Gamma\backslash\mathbb{H}^*$, onde $\mathbb{H}^* := H \cup \mathbb{Q} \cup \{\infty\}$.

Definição

$$\Gamma_1(N) := \left\{ \begin{bmatrix} \overline{1} & * \\ \overline{0} & \overline{1} \end{bmatrix} \in SL_2\mathbb{Z} \right\},\ \Gamma_0(N) := \left\{ \begin{bmatrix} * & * \\ \overline{0} & * \end{bmatrix} \in SL_2\mathbb{Z} \right\}.$$

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq SL_2\mathbb{Z}$$

$$X(N) \to X_1(N) \to X_0(N)$$

$$Y_{\spadesuit}(N)$$

$$\spadesuit \in \{0, 1, \quad \}$$

Curvas modulares

Retornamos aos $Y(\Gamma) := \Gamma \backslash \mathbb{H}$. Compactificação: $X(\Gamma) \simeq \Gamma \backslash \mathbb{H}^*$, onde $\mathbb{H}^* := H \cup \mathbb{Q} \cup \{\infty\}$.

Definição

$\Gamma_1(N) := \left\{ \begin{bmatrix} \overline{1} & * \\ \overline{0} & \overline{1} \end{bmatrix} \in \mathrm{SL}_2 \mathbb{Z} \right\}$, $\Gamma_0(N) := \left\{ \begin{bmatrix} * & * \\ \overline{0} & * \end{bmatrix} \in \mathrm{SL}_2 \mathbb{Z} \right\}$.

$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N)$.

Curvas modulares

$$Y(1) \longleftrightarrow \{E/\sim\}$$

Retornamos aos $Y(\Gamma) := \Gamma\backslash\mathbb{H}$. Compactificação: $X(\Gamma) \simeq \Gamma\backslash\mathbb{H}^*$, onde $\mathbb{H}^* := H \cup \mathbb{Q} \cup \{\infty\}$.

Definição

$$\Gamma_1(N) := \left\{ \begin{bmatrix} \overline{1} & * \\ \overline{0} & \overline{1} \end{bmatrix} \in \mathrm{SL}_2\,\mathbb{Z} \right\},\ \Gamma_0(N) := \left\{ \begin{bmatrix} * & * \\ \overline{0} & * \end{bmatrix} \in \mathrm{SL}_2\,\mathbb{Z} \right\}.$$

$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N)$.

As curvas modulares $X_0(N)$ e $X_1(N)$ são importantes!

$Y_1(N)$ $Y_0(N)$

Curvas modulares como espaços de moduli

Curvas modulares como espaços de moduli

- $Y(1) \longleftrightarrow \{\text{Classes de isomorfismo de curvas elípticas}\}$;

Curvas modulares como espaços de moduli

$N \cdot P = 0$ $\quad \langle P, Q \rangle$

- $Y(1) \longleftrightarrow$ {Classes de isomorfismo de curvas elípticas};
- $Y(N) \longleftrightarrow$ {Curvas elípticas munidas de dois pontos em $\underline{E[N]}$ tais que $\underline{e_N(P,Q)} = \underline{\exp(2\pi i/N)}$}/ $\sim$;

Curvas modulares como espaços de moduli

- $Y(1) \longleftrightarrow \{\text{Classes de isomorfismo de curvas elípticas}\}$;
- $Y(N) \longleftrightarrow \{\text{Curvas elípticas munidas de dois pontos em } E[N] \text{ tais que } e_N(P,Q) = \exp(2\pi i/N)\}/\sim$;
- $Y_1(N) \longleftrightarrow \{\text{Curvas elípticas munidas de um ponto em } E[N]\}/\sim$;

$X(1)$ $\mathbb{Q}$ $\mathbb{F}_q(t)$

- $Y(1) \longleftrightarrow$ {Classes de isomorfismo de curvas elípticas};
- $Y(N) \longleftrightarrow$ {Curvas elípticas munidas de dois pontos em $E[N]$ tais que $e_N(P, Q) = \exp(2\pi i/N)$}$/\sim$;
- $Y_1(N) \longleftrightarrow$ {Curvas elípticas munidas de um ponto em $E[N]$}$/\sim$; $\langle P \rangle$
- $Y_0(N) \longleftrightarrow$ {Curvas elípticas munidas de um subgrupo cíclico de ordem N}$/\sim$.

Variedades de Shimura $H^*(X, \overline{\mathbb{Q}}_\ell)$

Shtukas

Teorema (modularidade)

① SEMISTÁVEL ③ $j(F) \in \mathbb{Q}$ (FLT | $a^p = b^p + c^p$ — curva de Frey (ELÍPTICA)

② NÃO-MODULAR SEMISTÁVEIS

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

Seja $E/\mathbb{C}$ uma curva elíptica e suponha que $j(E) \in \mathbb{Q}$. Então existe sobrejeção

$$X_0(N) \to E,$$

$J_0(N)$

para algum N.

Teorema (modularidade)

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

Seja $E/\mathbb{C}$ uma curva elíptica e suponha que $j(E) \in \mathbb{Q}$. Então existe sobrejeção

$$X_0(N) \to E,$$

para algum N.

O enunciado também é válido com Jacobiano de $X_0(N)$: $J_0(N) \to E$.

Funções L

Se E é uma curva elíptica, podemos definir uma função L a ela associada

$$L(E,s) := \sum_{n\geqslant 2} \left(\underbrace{n+1}_{\#\mathbb{P}^1_{\mathbb{Z}/n\mathbb{Z}}} - \#E\,(n)\right) n^{-s}.$$

$\#E(\mathbb{Z}/n\mathbb{Z})$

Funções L

Se E é uma curva elíptica, podemos definir uma função L a ela associada $\mathbb{Z}/n\mathbb{Z}$ $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

$$L(E,s) := \sum_{n \geqslant 2} (n + 1 - \#E(n))\, n^{-s}.$$

Se $f(\tau) = \sum_{n \geqslant 1} a_n q^n$ é uma forma modular, podemos também definir uma função L a ela associada:

$$L(f,s) := \sum_{n \geqslant 1} a_n n^{-s}.$$

$\zeta(s) = \sum_{n \geqslant 1} n^{-s}$

$E \to j(E)$ $\mathbb{C}$

$y^2 = 4x^3 + ax + b$ $j(a,b) \in \mathbb{C}$

$j(E) = j(E') \Rightarrow E \simeq E'$ $\forall j \in \mathbb{C}\ \exists E$ tq $j(E) = j$

$\prod_{p \text{ primo}} X_p$ PRODUTO DE EULER

Se E é uma curva elíptica, podemos definir uma função L a ela associada

$$L(E, s) := \sum_{n \geqslant 2} (n + 1 - \#E(n)) n^{-s}.$$

Se $f(\tau) = \sum_{n \geqslant 1} a_n q^n$ é uma forma modular, podemos também definir uma função L a ela associada:

$$L(f, s) := \sum_{n \geqslant 1} a_n n^{-s}.$$

thm: $j(E) \in \mathbb{Q}$, sim!

$f \in S_k(\Gamma_0(N))$ ~~new~~

Pergunta

Dada uma curva elíptica E, quando existe uma forma modular f tal que $L(E, s) = L(f, s)$?

BSD $\mathrm{ord}_{s=1} L(E,s) = \mathrm{rk}_{\mathbb{Z}} E$

Representações de Galois

$$\mathrm{Gal}(L/K) \longrightarrow GL(V) \quad \mathbb{Q}_\ell$$

$$\boxed{\mathrm{Gal}(L/K) \circlearrowright V}$$

Em curvas elípticas, o módulo de Tate nos permite criar facilmente representações de Galois.

$$G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$$

$$G_{\mathbb{Q}} \circlearrowright E[p^n]_{n}$$

$$G \circlearrowright X \rightsquigarrow \boxed{G \circlearrowright H^i(X, \overline{\mathbb{Q}_\ell})}$$

$$G_{\mathbb{Q}} \circlearrowright T_pE \quad \otimes \mathbb{Q}_p \quad \mathbb{Z}_p \quad V_pE$$

$$X_1(N) \rightsquigarrow \mathrm{Jac}(X_1(N)) = J_1(N)$$

$$\boxed{\int f(t)\,dt}$$

Em curvas elípticas, o módulo de Tate nos permite criar facilmente representações de Galois. Para curvas modulares num geral (especialmente $X_1(N)$), fazemos isso com seu jacobiano.

Por que peso 2?

"MODULO DE TATE" $\longleftrightarrow$ "H_2"

$$\Omega^2(X(\Gamma))^\vee \xrightarrow{\int} \mathbb{C}$$

$$\mathrm{Jac}(X(\Gamma)) \cong \frac{\Omega^2(X(\Gamma))^\vee}{H_2} \cong S_2(\Gamma)^\vee$$

Representações de Galois

Em curvas elípticas, o módulo de Tate nos permite criar facilmente representações de Galois. Para curvas modulares num geral (especialmente $X_1(N)$), fazemos isso com seu jacobiano.

Por que peso 2?

$S_2(\Gamma) \simeq \Omega^1(Y(\Gamma))$.

Representações de Galois

Em curvas elípticas, o módulo de Tate nos permite criar facilmente representações de Galois. Para curvas modulares num geral (especialmente $X_1(N)$), fazemos isso com seu jacobiano.

Por que peso 2?

$S_2(\Gamma) \simeq \Omega^1(Y(\Gamma))$. Daí pro módulo de Tate do Jacobiano é dois toque!

Representações de Galois

Se $f(\tau) = \sum_{n \geqslant 1} a_n q^n$ é uma forma modular, denotemos $\mathbb{Q}(f) := \mathbb{Q}(\{a_n | \, n \geqslant 1\})$.

Representações de Galois

Se $f(\tau) = \sum_{n \geqslant 1} a_n q^n$ é uma forma modular, denotemos $\mathbb{Q}(f) := \mathbb{Q}(\{a_n \mid n \geqslant 1\})$. Se ℓ é um primo e $\lambda | \ell$ é uma valorização de $\mathbb{Q}(f)$,

$$V_{f,\lambda} := V_\ell(J_1(N)) \otimes \mathbb{Q}(f)_\lambda .$$

Representações de Galois

Se $f(\tau) = \sum\limits_{n \geqslant 1} a_n q^n$ é uma forma modular, denotemos $\mathbb{Q}(f) := \mathbb{Q}(\{a_n \mid n \geqslant 1\})$. Se ℓ é um primo e $\lambda | \ell$ é uma valorização de $\mathbb{Q}(f)$,

$$V_{f,\lambda} := V_\ell(J_1(N)) \otimes \mathbb{Q}(f)_\lambda .$$

Trata-se de uma representação de Galois ℓ-ádica, de dimensão 2, e não-ramificada em todo $p \nmid N\ell$.

Se $f(\tau) = \sum_{n \geqslant 1} a_n q^n$ é uma forma modular, denotemos $\mathbb{Q}(f) := \mathbb{Q}(\{a_n | \, n \geqslant 1\})$. Se ℓ é um primo e $\lambda | \ell$ é uma valorização de $\mathbb{Q}(f)$,

$$V_{f,\lambda} := V_\ell(J_1(N)) \otimes \mathbb{Q}(f)_\lambda \,.$$

Trata-se de uma representação de Galois ℓ-ádica, de dimensão 2, e não-ramificada em todo $p \nmid N\ell$.

Melhor ainda!

Se φ_p é um elemento de Frobenius de $G_{\mathbb{Q}}$, então $\det(1 - t\varphi_p) = 1 - a_p(f)\,t + \chi(p)\,t^2$, em que χ é um caracter ciclotômico de $G_{\mathbb{Q}}$.

$= (1-\alpha t)(1-\beta t)$

$E/\mathbb{F}_q \sim \#E(\mathbb{F}_{q^n}) = \frac{\alpha^n + \beta^n}{\alpha + \beta}$

Algumas Referências

- Daniel Bump: Automorphic Forms and Representations.
- Pierre Deligne: Formes modulaires et représentations ℓ-adiques. Séminaire Bourbaki, 1971.
- Fred Diamond/Jerry Schurman: A First Course in Modular Forms.
- Takeshi Saito: Galois Representations and Modular Forms. Escola de Verão IHÉS, 2006.
- Benjamin Schraen: Modular Curves (poly).
- Goro Shimura: Introduction to the Arithmetic Theory of Automorphic Functions.
- Goro Shimura: Automorphic Functions and Number Theory.

CFT $\leftrightarrow$ jugendtraum $\leftrightarrow$ th. KW automorphic forms $\xrightarrow{H^*}$ Galois reps

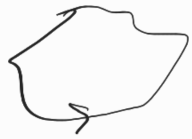
Irr
$n=1$

$$\begin{tikzcd} G_{\mathbb{Q}} \arrow[r] \arrow[d] & \mathbb{C}^\times \\ G_{\mathbb{Q}}^{ab} \arrow[ur] & \end{tikzcd}$$

The End

$$\boxed{\mathbb{Q}^{ab} = \mathbb{Q}(\{\zeta_n \mid n \geq 1\})}$$

FM $\boxed{\text{}}$  $\cancel{y^2 = 4x^3 + \cdots}$

$\boxed{\mathcal{M}_{1,1}}$ $\int$ 

$\mathcal{M}_g$

$$\boxed{T_p E \;\text{"}\!\underset{\simeq}{\longleftrightarrow}\!\text{"}\; H_1(E, \mathbb{Z}_p)}$$

$G_{\mathbb{Q}}$