Modular forms

Josef Svoboda

Charles University, Prague

josefsvobod@gmail.com

Autumn school of algebra
November 19, 2015

Outline

1. Introduction
2. Modular forms
3. Structure of modular forms
4. L-series and elliptic curves

Modular group

Definition

The *modular group* is the group of 2-by-2 integer matrices with determinant 1.

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

Proposition

The group $\mathrm{SL}_2(\mathbb{Z})$ *is generated by the two matrices*

$$\mathrm{T} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \mathrm{S} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Upper half plane

Definition

The *upper half plane* is the set of complex numbers z whose imaginary part $Im(z)$ is > 0.

$$\mathcal{H} = \{z \in \mathbb{C} : Im(z) > 0\}$$

Proposition

Modular group has action on $\mathcal{H}$ as fractional linear transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az+b}{cz+d}, z \in \mathcal{H}$$

Matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ acts trivially on $\mathcal{H}$.

Fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$

Definition

The set D of complex numbers z with $|z| \geq 1$ and $-1/2 \leq Re(z) \leq 1/2$ is called *fundamental domain* for action of $\mathrm{SL}_2(\mathbb{Z})$ on the half plane $\mathcal{H}$.

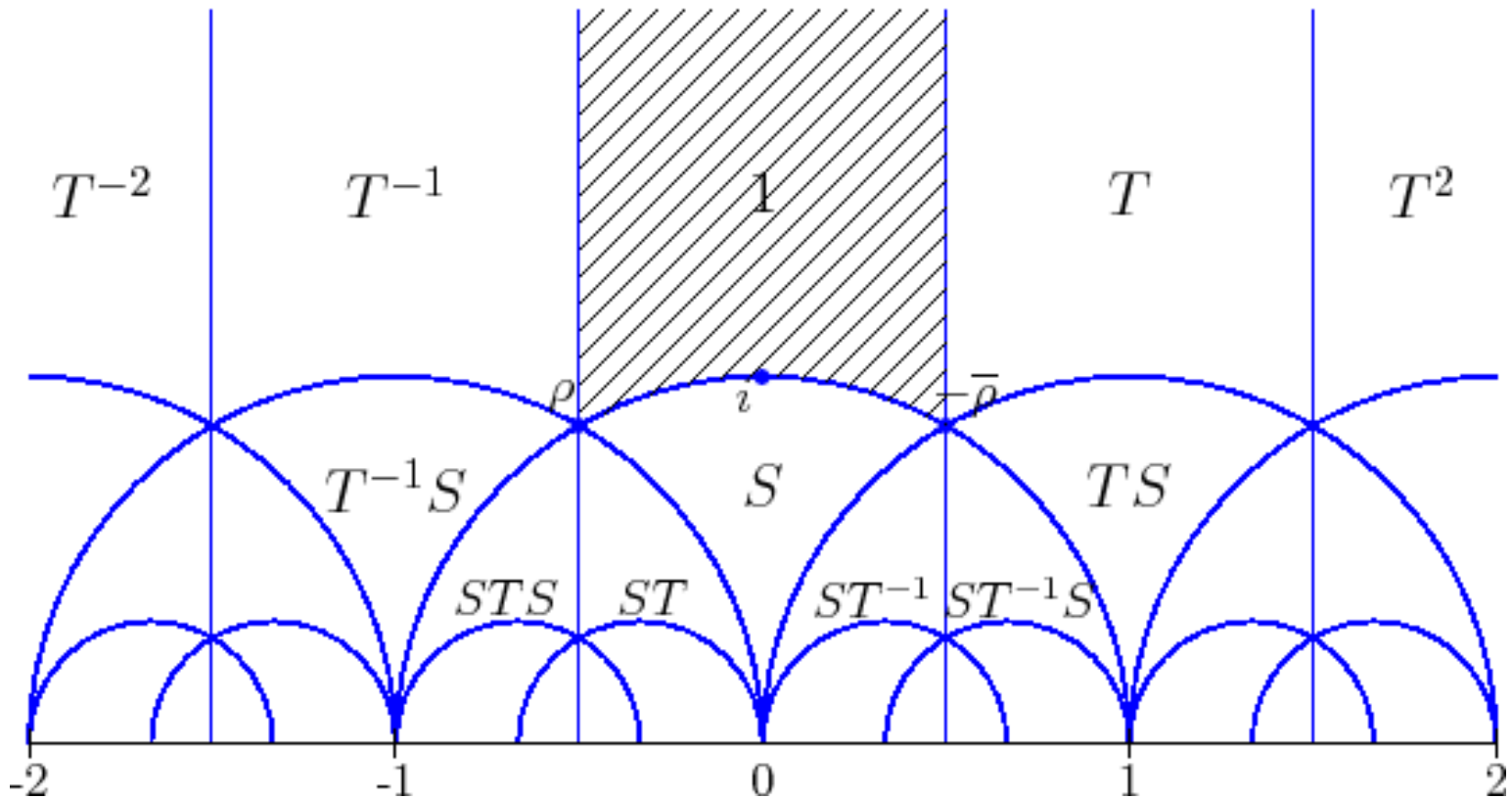

Figure : Fundamental domain

Outline

1. Introduction
2. Modular forms
3. Structure of modular forms
4. L-series and elliptic curves

Definition of modular form

Definition

Function f on $\mathcal{H}$ is called *modular form of weight* $2k$ if it satisfies following conditions:

1) $f(z) = (cz + d)^{-2k} f\left(\frac{az+b}{cz+d}\right)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.
2) f is holomorphic on $\mathcal{H}$.
3) f is holomorphic at ∞.

Modular form is called *cusp form* if it satisfies also

4) $f(\infty) = 0$.

Fourier expansion

Proposition

First condition in the definition of modular form is equivalent to

$$f(z+1) = f(z)$$

$$f\left(\frac{-1}{z}\right) = z^{2k} f(z)$$

Lemma

Let $q = e^{2\pi i z}$. Every modular form f can be written as a series $f(z) = \sum_{n=0}^{\infty} a_n q^n$ which converges for $|q| < 1$ (i.e. for $Im(z) > 0$). It is a cusp form iff $a_0 = 0$.

Eisenstein series

Definition

Eisenstein series is defined by

$$E_k(z) = \dot{\sum_{(m,n)\in\mathbb{Z}^2}} \frac{1}{(mz+n)^{2k}}$$

where $\dot{\sum}$ is sum over all pairs $\neq (0,0)$

Proposition

Let k be an integer ≥ 2. The Eisenstein series $E_k(z)$ converges absolutely and it is a modular form of weight $2k$.

$$\dot{\sum_{(m,n)\in\mathbb{Z}^2}} \frac{1}{(m\frac{az+b}{cz+d}+n)^{2k}} = \frac{1}{(cz+d)^{2k}} \dot{\sum_{(m,n)\in\mathbb{Z}^2}} \frac{1}{(m(az+b)+n(cz+d))^{2k}}$$

Outline

1. Introduction
2. Modular forms
3. Structure of modular forms
4. L-series and elliptic curves

Spaces of modular forms

Definition

Define Δ function as

$$\Delta(z) = (60E_2(z))^3 - 27(140E_3(z))^2$$

It is a cusp form of weight 12.

Definition

Modular forms (resp. cusp forms) of weight $2k$ form a $\mathbb{C}-$vector space, which we denote by M_k (resp. S_k).

Proposition

$$\dim(S_k) = \begin{cases} \dim(M_k) \\ \dim(M_k) - 1 \end{cases}$$

Dimension

Theorem

1. *We have* $M_k = 0$ *for* $k < 0$ *and* $k = 1$.
2. *For* $k = 0, 2, 3, 4, 5$, M_k *is a vector space of dimension 1 with basis* $1, E_2, E_3, E_4, E_5$; *we have* $S_k = 0$.
3. *Multiplication by* Δ *defines an isomorphism of* M_{k-6} *onto* S_k.

Corollary

We have

$$\dim(M_k) = \begin{cases} \lfloor \frac{k}{6} \rfloor & \text{if } k \equiv 1 \pmod 6, k \geq 0 \\ \lfloor \frac{k}{6} \rfloor + 1 & \text{if } k \not\equiv 1 \pmod 6, k \geq 0 \end{cases}$$

Corollary

Space M_k *has for basis the family of monomials* $E_2^\alpha E_3^\beta$ *with* $\alpha, \beta \in \mathbb{N}_0$ *and* $2\alpha + 3\beta = k$.

Application - sums of divisors

Theorem

Let $\sigma_k(n) = \sum_{d|n} d^k$. Then the Fourier expansion of Eisenstein series is

- $G_2(z) = (2\zeta(4))^{-1} E_2(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n$
- $G_3(z) = (2\zeta(6))^{-1} E_3(z) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n$
- $G_4(z) = (2\zeta(8))^{-1} E_4(z) = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n$

Corollary

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{k=1}^{n-1} \sigma_3(k)\sigma_3(n-k)$$

Proof.

We have (up to constant) only one modular form of weight 8 so

$$G_4 = G_2^2$$

Outline

1. Introduction
2. Modular forms
3. Structure of modular forms
4. L-series and elliptic curves

L-series for modular form

Definition

Modular form is called *Hecke form* if the coefficients of expansion $f = \sum_{n=0}^{\infty} a(n)q^n$ satisfy the following conditions

1. $a(n)a(m) = a(nm)$ if $(m, n) = 1$
2. $a(p)a(p^n) = a(p^{n+1}) + p^{2k-1}a(p^{n-1})$

Definition

Let $f(z) = \sum_{n=0}^{\infty} a_n q^n$ is a modular form. L-function for f is defined by

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

Properties of L-series

Theorem

Let f be modular form of weight k, which is Hecke form. Then function $L(s, f)$ satisfies the following conditions:

1. *$L(s, f)$ is absolutely convergent for $\mathbf{Re}(s) > 2k, k \in \mathbb{N}$*
2. *$L(s, f)$ has analytic continuation to $\mathbb{C}$*
3. $$L(s, f) = \prod_{p \in \mathbb{P}} \frac{1}{1 - a_p p^{-s} + p^{2k+1-2s}}$$
4. *Let $\widetilde{L}(s, f) = (2\pi)^{-s}\Gamma(s)L(s, f)$. Then*
$$\widetilde{L}(s, f) = (-1)^k \widetilde{L}(2k - s, f)$$

Generalization

Definition

Modular group $\Gamma_0(n)$ is the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of matrices

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathrm{SL}_2(\mathbb{Z}), c \equiv 0 \pmod{n} \right\}$$

Definition

Function f on $\mathcal{H}$ is called *modular form of weight* $2k$ *and level* N if it satisfies following conditions:

1) $f(z) = (cz + d)^{-2k} f\left(\frac{az+b}{cz+d}\right)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(n)$.
2) f is holomorphic on $\mathcal{H}$.
3) f is holomorphic at ∞.

Elliptic curves

Definition

Elliptic curve is given by a cubic equation

$$y^2 = x^3 + ax + b \tag{1}$$

such that $a, b \in \mathbb{Z}$ and $\Delta = -16(4a^3 + 27b^2) \neq 0$.

Let E be an elliptic curve.

1. We can solve equation (1) over different fields.
2. Specially, we are interested in the number of solutions of (1) over $\mathbb{Q}$ or $\mathbb{F}_p$.
3. To an elliptic curve E we can associate an L-function $L(s, E)$ whose coefficients are $a_p = p + 1 -$(number of solutions mod p).

Modularity theorem

Theorem (Taniyama - Shimura conjecture = Wiles - Taylor theorem)

Let E be an elliptic curve and $L(s, E) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ its L-function. Then there exist $\sum_{n=1}^{\infty} a_n q^n$ is a cusp Hecke form of weight 2 and level N where N is modulus of E such that $L(s, E) = L(s, f)$.

Corollary

L-functions of elliptic curves satisfy product formula and functional equation.

Corollary

Equation $x^n + y^n = z^n$ has no solutions for $x, y, z, n \in \mathbb{N}$ for $n > 2$.

Thanks

Thanks for your attention!

josefsvobod@gmail.com