Modular Forms, the Sum of Two Squares, Modular Curves

1. Modular forms

1.1 Def

Def (Automorphic forms)

A function $f: \mathcal{H} \to \mathbb{CP}^1$ is an automorphic form of weight k with respect to $SL_2(\mathbb{Z})$ if

(1) f is mero. (on $\mathcal{H}$)

(2) $\forall\ \gamma \in SL_2(\mathbb{Z})$ $\left(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)$, $f(\gamma\tau) = (c\tau+d)^k f(\tau)$

(3) $\forall\ \gamma \in SL_2(\mathbb{Z})$, $(c\tau+d)^{-k} f(\tau)$ is mero. at ∞.

denoted $f \in \mathcal{A}(SL_2(\mathbb{Z}))$.

Recall, if f is holo. on $\mathcal{H} \cup \{\infty\}$, say f is a modular form, denoted $f \in M(SL_2(\mathbb{Z}))$. Take its Fourier expansion, if $a_0 = 0$ (the constant term), say f is cusp form, denoted $f \in S(SL_2(\mathbb{Z}))$.

Generalization. $\Gamma \subseteq SL_2(\mathbb{Z})$, say Γ is a discrete subgroup.

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N \right\}$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\}$$

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\}$$

Note that τ is implied to be a lattice class or a ell. curve, $\mathcal{H}$ is the space of all the lattice class. $SL_2(\mathbb{Z})$ is the invariant action for lattice class. ($\tau=\infty \leftrightarrow [w_1:0]$)

Rmk. $SL_2(\mathbb{Z}) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$

Checking a function is a modular form (2)
$\Leftrightarrow$ Checking it satisfies $f(\tau+1)=f(\tau)$, $f(-\frac{1}{\tau})=\tau^k f(\tau)$.

1.2 Examples.

Def. (Eisenstein series of order k)

$$E_k(\tau) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(m+n\tau)^k} : \mathcal{H} \to \mathbb{C} \quad (k\geq 3,\ k\in\mathbb{Z},\ \text{fixed})$$

$$= \sum_{\omega\in\Lambda^*} \frac{1}{\omega^k}.$$

Thm. E_k is a modular form of weight k.

Proof. E_k converges uniformly and absolutely in $\{\tau\in\mathbb{C} : \mathrm{Im}(\tau)\geq\delta\}$ for every $\delta>0$. $E_k(\tau+1)=E_k(\tau)$,

$E_k(-\frac{1}{\tau}) = \tau^k E_k(\tau)$. □.

Rmk. When $2\nmid k$, $E_k(\tau)\equiv 0$. □

More Examples.

Def. (Discriminant function)

$$\Delta : \mathcal{H} \longrightarrow \mathbb{C}$$
$$\tau \longmapsto (60 E_4)^3 - 27 (140 E_6)^2$$

$\Delta \in S_{12}(SL_2(\mathbb{Z}))$ □

Thm. $\forall\, \tau \in \mathcal{H}$, $\Delta(\tau) \neq 0$.

Def. (Dedekind eta function)

$$\eta(\tau) = q_{24} \prod_{n=1}^{\infty} (1 - q^n), \text{ where } q_{24} = e^{\frac{2\pi i \tau}{24}}, \quad q = e^{2\pi i \tau},$$

which satisfies the function equation $\eta^{24}\left(-\frac{1}{\tau}\right) = \tau^{12} \cdot \eta^{24}(\tau)$ ($\forall\, \tau \in \mathcal{H}$) and invariant under $\tau \mapsto \tau + 1$. Besides, $\operatorname{Im} \tau \to \infty$, $\eta^{24}(\tau) \to 0$. And $\eta^{24} \in S_{12}(SL_2(\mathbb{Z}))$.

By the dimension formula, computing the leading terms coefficients of Fourier expansions of Δ and η^{24}, we conclude that $\Delta = (2\pi)^{12} \cdot \eta^{24}$.

i.e. $(60 E_4)^3 - 27 (140 E_6)^2 = (2\pi)^{12} \eta^{24}$.

Def. (the modular function)

$$j : \mathcal{H} \longrightarrow \mathbb{C}$$
$$\tau \longmapsto 1728 \frac{(60 E_4(\tau))^3}{\Delta(\tau)},$$

which is hol. on $\mathcal{H}$ and has a simple at ∞.

We can prove that it is an automorphic form.

Moreover, $j: \mathcal{H} \to \mathbb{C}$.

1.3 Relation of ell. function, ell. curves, ell. integral, modular forms, and complex tori.

Lem. $\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) E_{2k+2} z^{2k}$, (Laurent expansion near $z=0$)

Pf: Notice that $\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2} + \sum_{l=1}^{\infty} \frac{l+1}{\omega^{l+2}} z^l$.

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right] \\
&= \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left(\sum_{l=1}^{\infty} \frac{l+1}{\omega^{l+2}} z^l \right) \\
&= \frac{1}{z^2} + \sum_{l=1}^{\infty} \left(\sum_{\omega \in \Lambda^*} \frac{l+1}{\omega^{l+2}} \right) z^l \\
&= \frac{1}{z^2} + \sum_{l=1}^{\infty} (l+1) E_{l+2} \cdot z^l \\
&= \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) E_{2k+2} z^{2k}.
\end{aligned}$$

□

Thm. $\wp'^2 = 4\wp^3 - 60 E_4 \wp - 140 E_6$.

Proof Take the Laurent expansion of $\wp', \wp^3, \wp$

$$\wp'(z) = \frac{-2}{z^3} + 6E_6 z + 20 E_6 z^3 + \cdots$$

$$\wp^3(z) = \frac{1}{z^6} + \frac{9E_4}{z^2} + 15 E_6 + \cdots$$

$$\wp(z) = \frac{1}{z^2} + 3E_4 z^2 + \cdots$$

$\wp^3 - \frac{60}{4} E_4 \wp - \frac{140}{4} E_6$

$= -4a^3 - 27b^2 = -4\left(\frac{60}{4} E_4\right)^3 - 27\left(-\frac{140}{4} E_6\right)^2$

$= \frac{1}{16}\left(+(60 E_4)^3 - 27 (140 E_6)^2 \right)$

Compute the Laurent expansion of $F(z) = \wp'^2_{(z)} - 4\wp^3_{(z)} - 60E_4\wp_z - 140E_6$. We will find that the primary part and the constant term vanish. It follows that F is hol. at 0, and $F(0)=0$.

Since F is ell., $F \equiv 0$. □

Denote $g_2 = 60E_4$, $g_3 = 140E_6$.

Thm. Suppose $f(w) = \int^w \frac{1}{\sqrt{4t^3 - g_2 t - g_3}}\,dt$, then $\wp(z)$ is the inverse of $f(w)$. Accurately, $z - z_0 = \int_{\wp(z_0)}^{\wp(z)} \frac{dw}{\sqrt{4w^3 - g_2 w - g_3}}$

Proof

Denote $w = \wp(z)$. $\wp'^2(z) = 4\wp^3_{(z)} - g_2\wp_{(z)} - g_3$ implies an ODE $\frac{dw}{dz} = \sqrt{4w^3 - g_2 w - g_3}$, Thus,

$$dz = \frac{1}{\sqrt{4w^3 - g_2 w - g_3}}\,dw \Rightarrow z - z_0 = \int_{\wp'(z_0)}^{\wp(z)} \frac{1}{\sqrt{4w^3 - g_2 w - g_3}}\,dw$$ □

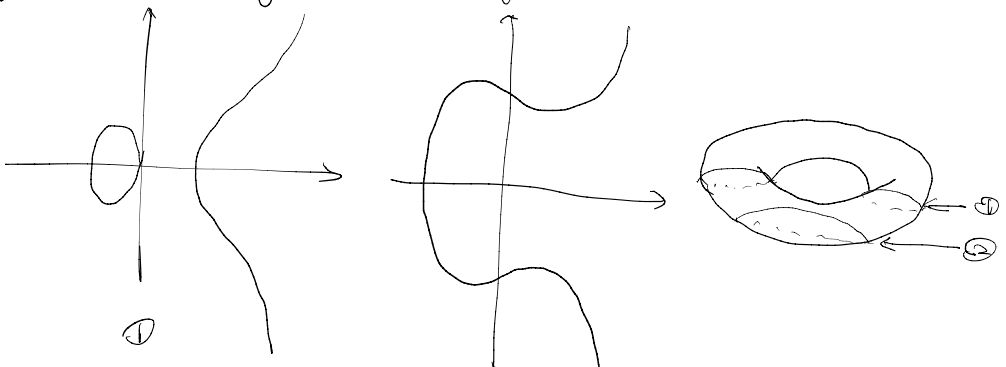
Now consider a map $(\wp, \wp') : \mathbb{C}/\Lambda^* \to \mathbb{C}^2$

$$\tau \longmapsto (\wp(\tau), \wp'(\tau))$$

Then $[1:\wp:\wp'] : \mathbb{C}/\Lambda \hookrightarrow \mathbb{CP}^2$ (embedding)

$$z \longmapsto [1:\wp(z):\wp'(z)]$$

Note that the image of $[1:\wp:\wp']$ in $\mathbb{CP}^2$ is a torus, which satisfies $y^2 = 4x^3 - g_2x - g_3$, denoted E_τ.



- Note that $\wp$ function let the complex torus become an algebraic curve embedded in $\mathbb{CP}^2$.
- Note that ell. function can viewed as function defined on an ell. curve $y^2 = x^3 - g_2(\tau)x - g_3$

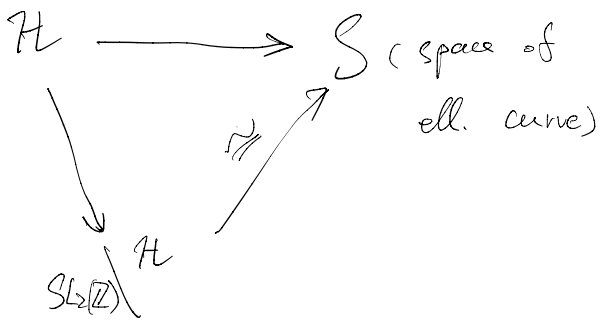
$$\mathbb{C}/\Lambda \longleftrightarrow E_\tau \hookrightarrow \mathbb{CP}^2$$

$$\mathbb{CP}^1$$

- Note that $\tau \in \mathcal{H} \to$ a lattice (nor.) $\to \wp(z)$

$$g_2, g_3 \in \mathbb{C} \qquad [1:\wp:\wp']$$

$$\text{an ell. curve}$$

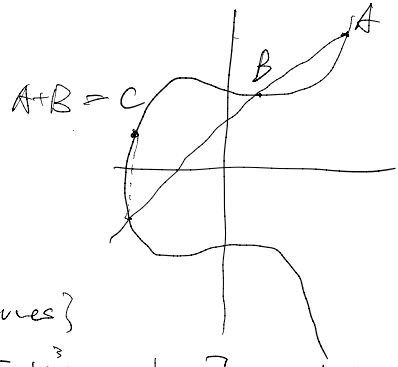


- Note that the ell. curve has a group structure

It is because

$$\mathbb{C}^2 \twoheadrightarrow \mathbb{C}/\Lambda \xleftrightarrow{[1:\wp:\wp']} \text{ell. curve}$$

Abelian gr. $\twoheadrightarrow$ Abelian gr.



Note that $\{\text{lattices}\} \hookrightarrow \{\text{ell. curves}\}$

Thm. Given an ell. curve $y^2 = x^3 + ax + b$, $\exists$ a lattice Λ s.t. $a = g_2(\Lambda)$, $b = g_3(\Lambda)$.

2 The two-squares theorem

Problem. $x^2+y^2=n$ $(x,y \in \mathbb{Z},\ n\in\mathbb{N},\ n \text{ fixed})$.

We wonder when does the equation have solutions and how many solutions the equation has.

For the first reduce n to p since $(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2$

Denote $r_2(n)$ to be the number of solutions for $x^2+y^2=n$. Denote $d_1(n)$ ($d_3(n)$ resp.) to be the number of the divisors of n, who $\equiv 1 \pmod 4$ ($\equiv 3 \pmod 4$ resp.). (Example. 24: 1, 2, 3, 4, 6, 8, 12, 24

$d_1(24)=1$, $d_3(24)=1$).

Thm. $r_2(n) = 4d_1(n) - 4d_3(n)$.

Proof $\vartheta(\tau) = \sum_{n=-\infty}^{+\infty} e^{n^2\cdot\pi\tau} = \sum_{n\in\mathbb{Z}} q^{n^2}$ $\left(q=e^{i\pi\tau},\ \tau\in\mathcal{H}\right)$

$$C(\tau) = 2\sum_{n=-\infty}^{+\infty} \frac{1}{q^n+q^{-n}}.$$

(Step 1. Fourier expansion)

$$\vartheta^2(\tau) = \left(\sum_{n_1\in\mathbb{Z}} q^{n_1^2}\right)\left(\sum_{n_2\in\mathbb{Z}} q^{n_2^2}\right) = \sum_{(n_1,n_2)\in\mathbb{Z}^2} q$$

$$= \sum_{n=0}^{+\infty} r_2(n)\, q^n$$

$$C(\tau) = 2\sum_{n=-\infty}^{+\infty} \frac{1}{q^n+q^{-n}} = 1 + 4\sum_{n=1}^{+\infty} \frac{1}{q^n+q^{-n}}$$

$$= 1 + 4\sum_{n=1}^{+\infty} \frac{q^n}{q^{2n}+1}$$

$$= 1 + 4\sum_{n=1}^{+\infty}\sum_{m=0}^{+\infty} q^{n}\left(-q^{2n}\right)^{m} = 1 + 4\sum_{n=1}^{+\infty}\sum_{m=0}^{+\infty}(-1)^{m} q^{(2m+1)n}$$

$$= 1 + 4\sum_{n=1}^{+\infty}\sum_{k=0}^{+\infty} q^{(4k+1)n} - 4\sum_{n=1}^{+\infty}\sum_{k=0}^{+\infty} q^{(4k+3)n}$$

$$= \sum_{n=0}^{+\infty} 4\left(d_1(n) - d_3(n)\right) q^{n}$$

(Step 2 Modular character)

We are to prove $\theta^2(\tau) = C(\tau)$.

$\theta^2(\tau+2) = \theta^2(\tau)$ $\qquad$ $C(\tau+2) = C(\tau)$

$\theta^2(-\frac{1}{\tau}) = -i\tau\,\theta^2(\tau)$ $\qquad$ $C(-\frac{1}{\tau}) = -i\tau\, C(\tau)$

Poisson Summation $\quad \sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n)$

$\theta^2(\tau) \to 1 \quad (\mathrm{Im}\,\tau \to \infty)$ $\qquad$ $C(\tau) \to 1 \quad (\mathrm{Im}\,\tau \to \infty)$

$\theta^2(-\frac{1}{\tau}) \sim 4\,\frac{i}{\tau}\, e^{\frac{\pi i \tau}{2}}$ $\qquad$ $C(-\frac{1}{\tau}) \sim 4\frac{i}{\tau} e^{\frac{\pi i\tau}{2}}$

Suppose $f = \frac{C}{\theta^2}$, then f is modular form of weight 0, under the discrete subgroup $\Gamma := \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle$. Besides, f is bounded.

We are prove that $f \equiv 1$.

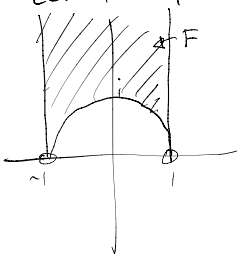
(Step 3 Consider pasting)

$\pi : \mathcal{H} \longrightarrow \Gamma\backslash\mathcal{H}$

$\tau \longmapsto \Gamma\tau$.

$\Gamma\backslash\mathcal{H}$ has the quotient topology by π, which is connected, Hausdorff, secondly countable, Local Euclidean and possesses a complex structure. Thus, $\Gamma\backslash\mathcal{H}$ is a Riemann Surface

Let $F = \{\tau \in \mathcal{H} : |\mathrm{Re}(\tau)| \le 1,\ |\tau| \ge 1\}$



Thm. $\forall \tau \in \mathcal{H}$, $\exists \gamma \in \Gamma$, s.t. $\gamma\tau \in F$, say F the fundamental domain.

However, the Riemann surface $\Gamma\backslash\mathcal{H}$ is not compact $(1, \infty)$. Let $X(\Gamma) = \Gamma\backslash\mathcal{H} \amalg \Gamma\cdot 1 \amalg \{\infty\}$ say the modular curve of Γ. Actually we can give a chart at $\Gamma\cdot 1$. Therefore, $X(\Gamma)$ will be a compact Riemann surface. $f : \mathcal{H} \to \mathbb{C}$, which is modular and bounded. can induce $\tilde{f}$: $X(\Gamma) \to \mathbb{C}$, which holo. It follows that f is constant and must equals 1. i.e. $\sigma^2 = C$. the two square theorem holds $\square$

Rmk For a prime number $p \neq 2$

$$r_2(p) = 4\left(d_1(p) - d_3(p)\right) = \begin{cases} 0 & , p \equiv 3 \ (4) \\ 8 & , p \equiv 1 \ (4) \end{cases}$$

3. Modular Curves

3.1 Def. of modular curves

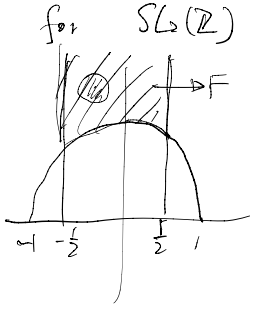
Def. (Open modular curves $Y(\Gamma)$). For a discrete subgroup Γ acting $\mathcal{H}$ on the left, an open modular curve $Y(\Gamma)$ is defined to be the quotient space of orbits under Γ, namely $Y(\Gamma) = \Gamma\backslash\mathcal{H} = \{\Gamma\cdot\tau : \tau\in\mathcal{H}\}$.

(Tology) Quotient topology. $\pi : \mathcal{H} \to Y(\Gamma)$

(Riemann Surface)

- connected ✓
- Hausdorff ✓
- Secondly countable ✓
- Local Euclidean ✓
- transition map holo ✗

fundamental domain for $SL_2(\mathbb{Z})$

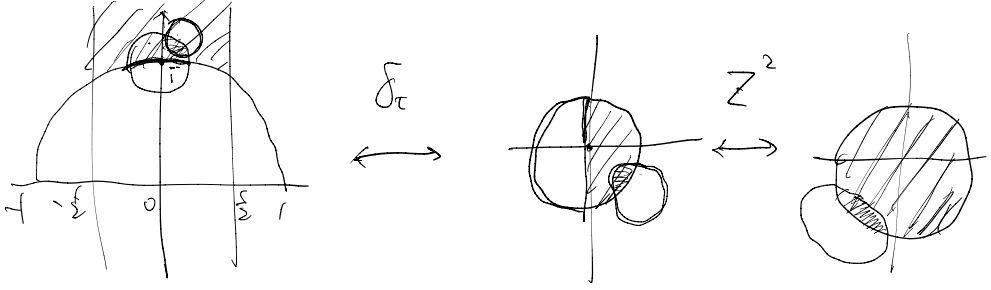


(Ell. points)

Def Suppose $\Gamma_\tau = \{\gamma\in\Gamma : \gamma\tau = \tau\}$ to be the τ-fixing subgroup of Γ. A point $\tau\in\mathcal{H}$ is called an ell. point if Γ_τ is not trivial.

Thm. Γ_τ is finite and cyclic.

Give a chart at an ell. point.



$Y(\Gamma)$ $\left(\delta_\tau = \begin{pmatrix} 1 & -\tau \\ 1 & -\bar{\tau} \end{pmatrix}\right)$

$\psi = z^2 \circ \delta_\tau$

$h = h_\tau = \begin{cases} \frac{1}{2}|\Gamma_\tau| & -I \in \Gamma_\tau \\ |\Gamma_\tau| & -I \notin \Gamma_\tau \end{cases}$

Let $\psi = z^h \circ \delta_\tau$

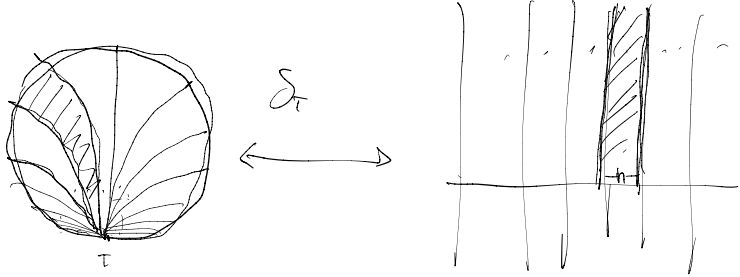
Open modular curves are Riemann surfaces

$\Gamma\backslash\mathcal{H} \subset \Gamma\backslash\mathbb{QP}^1$ Γ is transitive on $\mathbb{QP}^1$.

Thus, $\Gamma\backslash\mathbb{QP}^1$ is actually one point

$X(\Gamma) := \Gamma\backslash\mathcal{H} \subset \Gamma\backslash\mathbb{QP}^1$

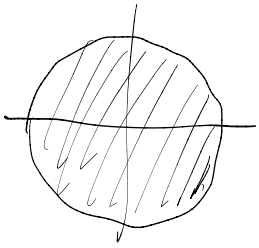
Charts should be given on $\Gamma\backslash\mathbb{QP}^1$.



$e^{2\pi i \frac{z}{h}}$

$\psi = e^{2\pi i \frac{z}{h}} \circ \delta_\tau$ is bijective

which gives a chart at $\mathbb{Q}\mathbb{P}^1$



$X(\Gamma)$ is called a modular curve.

3.2 Holomorphic differentials

Consider $f(\tau)(d\tau)^{\frac{k}{2}}$ $\left(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})\right)$

$$f(\gamma\tau)\left(d(\gamma\tau)\right)^{\frac{k}{2}} = (c\tau+d)^k f(\tau)\left(d\frac{a\tau+b}{c\tau+d}\right)^{\frac{k}{2}}$$

$$= (c\tau+d)^k f(\tau)\left(\frac{ad-bc}{(c\tau+d)^2}\, d\tau\right)^{\frac{k}{2}}$$

$$= (c\tau+d)^k f(\tau) \frac{1}{(c\tau+d)^k} (d\tau)^{\frac{k}{2}}$$

$$= f(\tau)(d\tau)^{\frac{k}{2}}$$

Rmk Modular forms are holo. forms on the modular curves.

Apply the Riemann-Roch theorem by computing the ell. points we obtain the dimension for modular forms.

Thm. $M(SL_2(\mathbb{Z})) = \mathbb{C}[E_4, E_6]$

$M_k(SL_2(\mathbb{Z}))$	basis
$k=4$	E_4
$k=6$	E_6
$k=8$	E_4^2
$k=10$	E_4E_6
$k=12$	E_4^3, E_6^2
⋮	⋮

Modularity theorem (Taniyama-Shimura conjecture)

(one version)

Let E be an ell. curve with $j(E) \in \mathbb{Q}$. Then for some positive integer N, $\exists$ a surjection which is holo. of compact Riemann surface : $X_0(N) \longrightarrow E$.

The function is called the modular parametrization of E.