Isomorphism classes of elliptic curves

$$\mathbb{Z}\oplus\mathbb{Z}\tau \quad \left\{ \Lambda \subseteq \mathbb{C} \text{ lattices} \right\} / \mathbb{C}^* \xrightarrow{1:1} \left\{ (0, E = \mathbb{C}/\Lambda) \text{ elliptic curve} \right\} / \text{holomorphism}$$

$$E \simeq E' \quad 0 \mapsto 0'$$

$$\uparrow \qquad \updownarrow 1:1$$

$$\bar{\tau} \in \quad \mathbb{H} = \{ \tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0 \} / SL_2(\mathbb{Z}) .$$

def: Let k be an integer. A meromorphic function f on $\mathbb{H}$ is weakly modular of weight $2k$ if

$$(*) \qquad f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

We say that f is modular if it is meromorphic at infinity.

Rmk: $(*)$ is equivalent to say that the "differential form of weight k" $f(z)(dz)^k$ is invariant under $SL_2(\mathbb{Z})$

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad f(gz)\, d(gz)^k = f(z)\, dz^k .$$

Eisenstein series: $\Lambda \subseteq \mathbb{C}$ lattice

$$k \geq 3 \qquad G_k(\Lambda) := \sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{\omega^k} . \qquad G_k = 0 \text{ if } k \text{ is odd}$$

Prop. Let $k \geq 2$ be an integer. Then the function

$$\tau \mapsto G_{2k}(\mathbb{Z}\oplus\mathbb{Z}\tau)$$

is a modular function, holomorphic at infinity with $G_{2k}(\infty) = 2\zeta($

of weight $2k$

Proof: (Invariance) It is equivalent to show that for each $\alpha \in \mathbb{C}^*$,

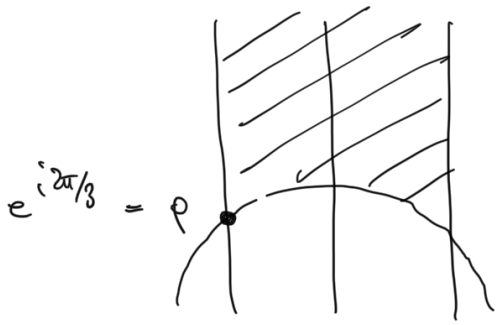
$G_{2k}(\alpha\Lambda) = \frac{1}{\alpha^k} G_{2k}(\Lambda)$.

$$G_{2k}(\alpha\Lambda) = \sum_{\omega \in \Lambda - \{0\}} \frac{1}{(\alpha\omega)^{2k}} = \frac{1}{\alpha^{2k}} \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^{2k}}$$

$$= \frac{1}{\alpha^{2k}} G_{2k}(\Lambda). \quad \checkmark$$

(Convergence) Let D be fundamental domain for the action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$:

$$D = \{ \tau \in \mathbb{H} : |\mathrm{Re}(\tau)| \leq \tfrac{1}{2}, \ |\tau| \geq 1 \}.$$



For $\tau \in \mathbb{H}$:

$$G_{2k}(\mathbb{Z} \oplus \mathbb{Z}\tau) = \sum_{\substack{(m,n) \neq (0,0) \\ \in \mathbb{Z}^2}} \frac{1}{(m\tau + n)^{2k}}.$$

For $\tau \in D$:

$$|m\tau + n|^2 = m^2 \underbrace{|\tau|^2}_{\geq 1} + \underbrace{2\mathrm{Re}(\tau)}_{\geq -\frac{1}{2}} mn + n^2$$

$$\geq m^2 - mn + n^2 = |m\rho - n|^2.$$

$$\Longrightarrow \quad |G_{2k}(\mathbb{Z} \oplus \mathbb{Z}\tau)| \leq \sum_{(m,n) \neq (0,0)} \frac{1}{|m\rho - n|^{2k}} < +\infty.$$

By using the action of $SL_2(\mathbb{Z})$ we see that G_{2k} converges uniformly on the compacts of $\mathbb{H}$.

$\Longrightarrow$ G_{2k} is holomorphic on $\mathbb{H}$.

(Limit) In order to show that G_{2k} is holomorphic

(infinity). In order to ...

at infinity, one has to see that the limit

$$\lim_{\substack{z \in \mathbb{H} \\ \mathrm{Im}(z) \to \infty}} G_{2k}(z) \quad \text{exists.}$$

[To convice yourself:

$$G_{2k}(z+1) = G_{2k}(z)$$

$$\uparrow$$

$$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Consider the function

$$f(e^{2\pi i z}) := G_{2k}(z)$$

well defined and it is a holomorphic function on the punctured unit disc.

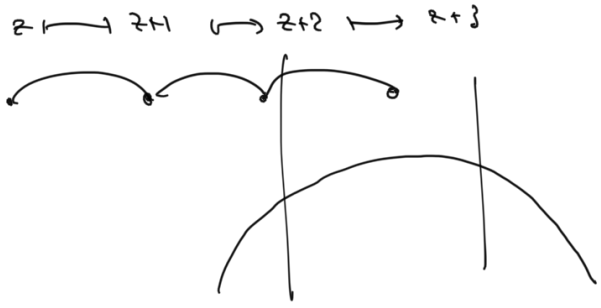
$$\lim_{\substack{z \in \mathbb{H} \\ \mathrm{Im}(z) \to \infty}} G_{2k}(z) = \lim_{q \to 0} f(q). \quad]$$

Let (z_n) be a sequence in $\mathbb{H}$ s.t. $\mathrm{Im}(z_n) \to \infty$.

We may suppose $|z_n| \geq 1$ for each $n \in \mathbb{N}$. Because

$$G_{2k}(z+1) = G_{2k}(z)$$

we may assume that $z_n \in D$ for all $n \in \mathbb{N}$.



Now we know that in D the series $G_{2k}(z)$ converges normally, so we can pass the limit under the sign of sum:

$$\leq \frac{1}{\quad} \qquad \overset{\infty}{\leq} \frac{1}{\quad}$$

$$\lim_{i\to\infty} G_{2k}(z_i) = \sum_{(m,n)\neq(0,0)} \frac{1}{(mz_i+n)^{2k}} = 2\sum_{n=1}^{\infty} \frac{1}{n^{2k}}$$

$i \to \infty$: $(mz_i+n)^{2k} \to \frac{1}{n^{2k}}$

$$= 2\zeta(2k). \qquad \square$$

Some interesting modular forms.

weight 4 $\quad g_2 := 60\, G_4 \qquad g_2(\infty) = 2\zeta(4) = \frac{4}{3}\pi^4$

weight 6 $\quad g_3 := 140\, G_6 \qquad g_3(\infty) = 2\zeta(6) = \frac{8}{27}\pi^6$

$\Delta := g_2^3 - 27 g_3^2$ weight 12 vanishing at infinity, non vanishing anywhere else.

discriminant of the polynomial $4X^3 - g_2 X - g_3$

$$\Delta(\infty) = \left(\tfrac{4}{3}\pi^4\right)^3 - 27\left(\tfrac{8}{27}\pi^6\right)^2 = 0.$$

def: The j-invariant is the weight 0 modular form

$$j = 1728\,\frac{g_2^3}{\Delta}$$

$\uparrow$ $SL_2(\mathbb{Z})$ invariant

$j(g\tau) = j(\tau)$.

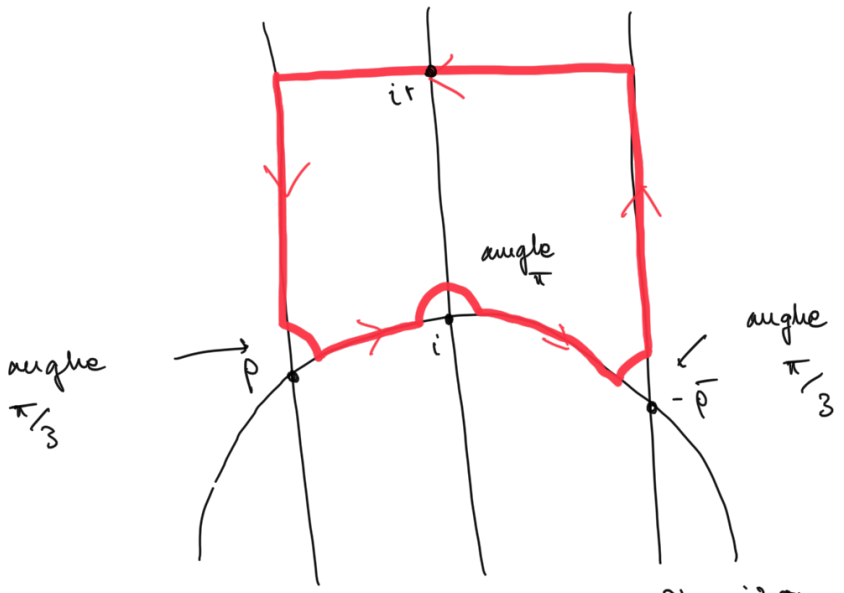
So j is really a function on $\mathcal{H}/SL_2(\mathbb{Z})$.

Thm: Let f be a modular form of weight $2k$, not identically zero. Then,

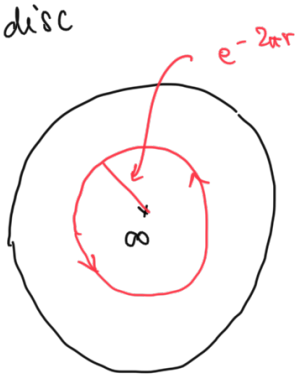
$$\mathrm{ord}_\infty(f) + \tfrac{1}{2}\mathrm{ord}_i(f) + \tfrac{1}{3}\mathrm{ord}_\rho(f) + \sum_{[\tau]\in \mathcal{H}/SL_2(\mathbb{Z}) \setminus \{[i],[\rho]\}} \mathrm{ord}_\tau(f) = \frac{k}{6}$$

Proof: Attend the "Modular forms" course.

[Serre, A course in Arithmetic, Chapter VII, §3, Thm 3].



Since $f(\tau+1) = f(\tau)$, the function $\tilde{f}(e^{i2\pi\tau}) := f(\tau)$ is well-defined and defines a meromorphic function on the unit disc



□

Apply the theorem to Δ: we know that Δ is holomorphic non vanishing away from infinity

$\text{ord}_\infty(\Delta) = \frac{6}{6} = 1$. So Δ has a simple zero at infinity.

In particular

$$j = 1728\,\frac{g_2^3}{\Delta}$$

g_2 does not vanish at ∞.

$\Rightarrow$ j has a simple pole at infinity.

Cor: The function $j: \mathcal{H}/SL_2(\mathbb{Z}) \longrightarrow \mathbb{C}$ is a bijection.

Proof: Apply the theorem for $f(z) = j(z) - a$, $a \in \mathbb{C}$:

$$\underbrace{\mathrm{ord}_\infty(f)}_{=-1} + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \sum_{\substack{\tau \in \mathbb{H}/SL_2(\mathbb{Z}) \\ \tau \neq i,\rho}} \mathrm{ord}_\tau(f) = 0$$

There are only 3 possibilities.

$$-1 + \frac{1}{2}\cdot 2 + 0 + 0 = 0.$$

$$-1 + \frac{1}{2}\cdot 0 + \frac{1}{3}\cdot 3 + 0 = 0$$

$$-1 + \frac{1}{2}\cdot 0 + \frac{1}{3}\cdot 0 + 1 = 0,$$

In any case there is a unique $\tau \in \mathbb{H}/SL_2(\mathbb{Z})$ s.t. $f(\tau) = j(\tau) - a = 0$. Therefore j is bijective. □

Summing up: Two elliptic are isomorphic if and only if they have same j-invariant.

Torsion of an elliptic curve

Let $\Lambda \subseteq \mathbb{C}$ be a lattice, $E = \mathbb{C}/\Lambda$. abelian group

$n \in \mathbb{N} \setminus \{0\}$ $\quad E[n] = \{x \in E : nx = 0\}$

n torsion subgroup

$z \in \mathbb{C}$ $\quad \pi : \mathbb{C} \to \mathbb{C}/\Lambda = E$ projection.

$$n\,\pi(z) = 0 \iff nz \in \Lambda \iff z \in \frac{1}{n}\Lambda.$$

($n\,\pi(z) = \pi(nz)$)

Therefore $E[n] = \frac{1}{n}\Lambda/\Lambda$.

As an abelian group: $\Lambda \simeq \mathbb{Z}^2 \implies \frac{1}{n}\Lambda \cong \frac{1}{n}\mathbb{Z}^2 \subseteq$

$$\frac{1}{n}\Lambda/\Lambda \cong \left(\frac{1}{n}\mathbb{Z}/\mathbb{Z}\right)^2 = \left(\mathbb{Z}/n\mathbb{Z}\right)^2.$$

Lemma: The n torsion subgroup $E[n]$ is isomorphic to $\left(\mathbb{Z}/n\mathbb{Z}\right)^2$.

The group law via the embedding.

Thm (Summation formula for $\wp$): Let $z_1, z_2 \in \mathbb{C}\setminus\Lambda$ be such that $\wp(z_1) \neq \wp(z_2)$. Then,

$$\wp(z_1+z_2) + \wp(z_1) + \wp(z_2) = \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2.$$

slope of the line containing $(\wp(z_1), \wp'(z_1))$ and $(\wp(z_2), \wp'(z_2))$

Proof: Consider the line passing through

$$(\wp(z_i), \wp'(z_i)), \quad i=1,2.$$

$$y - \wp'(z_i) = \left(\frac{\wp'(z_2) - \wp'(z_1)}{\wp(z_2) - \wp(z_1)}\right)(x - \wp(z_i)) \rightarrow y = ax+b$$

$$\longrightarrow \quad \wp'(z_i) = a\,\wp(z_i) + b \quad \text{for } i=1,2.$$

Consider the elliptic function

$$f(z) = \wp'(z) - (a\wp(z) + b)$$

elliptic function with a pole of order 3 in 0 and holomorphic everywhere else

Therefore f has three zeros:

$$z_1, z_2, z_3.$$

We saw: for an elliptic function g

$$\left(\sum \operatorname{ord}_a(g)\cdot a \in \Lambda\right)$$

$\sum_{x \in E} \operatorname{ord}_x(g) \cdot x \equiv 0$ ($\sum_{x \in D}$ ...)

sum on $E = \mathbb{C}/\Lambda$

D: fundamental domain

In our case

$$3 \cdot 0_E + z_1 + z_2 + z_3 \equiv 0 \quad \text{in } E.$$

(0_E: zero of the elliptic curve)

$$\Longrightarrow \quad z_3 \equiv -(z_1 + z_2) \quad \text{in } E.$$

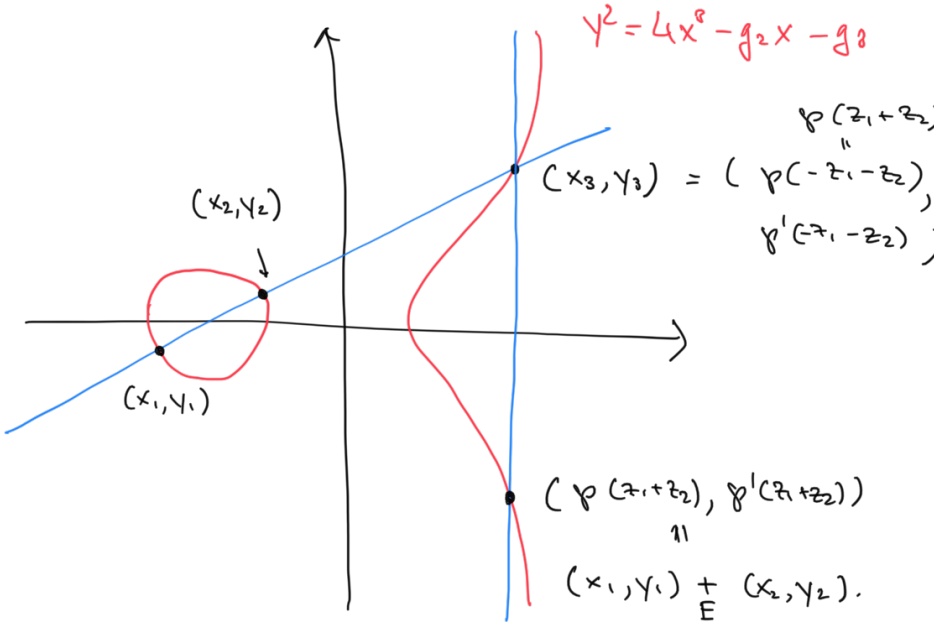
$$\Longrightarrow \quad \wp(z_3) = \wp(-(z_1+z_2)) = \wp(z_1+z_2)$$

($\wp$ elliptic; $\wp$ even.)

Rmk: Given $(x_i, y_i) = (\wp(z_i), \wp'(z_i))$ $i = 1, 2$

the line passing throug (x_i, y_i) for $i=1,2$ intersects the curve $E \hookrightarrow \mathbb{P}^2(\mathbb{C})$ in the point

$$(\wp(-(z_1+z_2)), \wp'(-z_1-z_2))$$



In the group law of the elliptic curve, we have

$$(x_1, y_1) \overset{+}{_E} (x_2, y_2) \overset{+}{_E} (x_3, y_3) = 0_E.$$

The proof does not end here. I let you to show that the intersection of

$$\begin{cases} y = ax + b \\ y^2 = 4x^3 - g_2 - g_3 \end{cases}$$

gives the summation. Anyway we will come back at this.

Automorphisms and endomorphisms of elliptic curves.

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

$$\mathrm{End}(E) = \{ f : E \to E \text{ holomorphic} : f(0_E) = 0_E \}.$$

$$= \{ \mu \in \mathbb{C} : \mu\Lambda \subseteq \Lambda \}$$

So let $\mu \in \mathbb{C}$ be such that

$$\begin{array}{ccc} z & \longmapsto & \mu z \\ \mathbb{C} & \longrightarrow & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{Z} \oplus \mathbb{Z}\tau & \longrightarrow & \mathbb{Z} \oplus \mathbb{Z}\tau \end{array}$$

$$1 \longmapsto \mu = a + b\tau$$

$$\tau \longmapsto \mu\tau = c + d\tau.$$

$$(a + b\tau)\tau = c + d\tau. \qquad a, b, c, d \in \mathbb{Z}.$$

$$\Longrightarrow \quad b\tau^2 + (a - d)\tau - c = 0.$$

Two possibilities:

- $\underline{b = 0}$: $\underbrace{(a - d)}_{\in \mathbb{Z}}\tau - c = 0$ $\quad \tau \notin \mathbb{H}$ $\quad c \in \mathbb{Z}$

$$\Rightarrow \begin{cases} a=d \\ c=0 \end{cases} \Longrightarrow \quad \mu = a$$

So the induced map $E \to E$, $x \mapsto ax$, $a \in \mathbb{Z}$

It is the multiplication by a.

- $\underline{b \neq 0}$. $\quad b\tau^2 + (a-d)\tau + c = 0$.

  Therefore τ satisfies a degree 2 equation with rational coefficient. Since $\mathrm{Im}(\tau) > 0$, τ lies in a purely imaginary quadratic extension of $\mathbb{Q}$.

  So, when τ lies in a purely imaginary quadratic extension of $\mathbb{Q}$, the elliptic curve has extra endomorphisms.

  def: In this case we say that E has complex multiplication.

$$\mathrm{End}(E) = \begin{cases} \mathbb{Z} & \text{if } E \text{ has no complex multiplication} \\ R & \text{if } E \text{ has complex multiplication.} \end{cases}$$

$\mathbb{C} \supseteq K/\mathbb{Q}$ purely imaginary quadratic extension

$\tau \in K \cap \mathcal{H}$.

$\mathcal{O}_K \subseteq K$ ring of integers

$\mathrm{End}\left(\mathbb{C}/\mathbb{Z}\oplus\mathbb{Z}\tau\right) =$ order in $\mathcal{O}_K$.

Automorphisms. $\mu \in \mathbb{C}$ s.t. $\mu\Lambda = \Lambda$.

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\mu} & \mathbb{C} \\ \cup & & \cup \\ \mathbb{Z}\oplus\mathbb{Z}\tau & \xrightarrow{\mu} & \mathbb{Z}\oplus\mathbb{Z}\tau \\ 1 & \longmapsto & \mu = a+b\tau \\ \tau & \longmapsto & \mu\tau = c+d\tau. \end{array}$$

Now I assume that $\mu : \mathbb{Z}\oplus\mathbb{Z}\tau \to \mathbb{Z}\oplus\mathbb{Z}\tau$ is an isomorphism. I identify $\mathbb{Z}\oplus\mathbb{Z}\tau$ with $\mathbb{Z}^2$ via $(1,\tau)$:

$$\begin{array}{rccc} \mu : & \mathbb{Z}^2 & \to & \mathbb{Z}^2 \\ & (1,0) & \mapsto & (a,b) \\ & (0,1) & \mapsto & (c,d) \end{array} \qquad \begin{pmatrix} a & c \\ b & d \end{pmatrix} = M$$

matrix of μ.

We are asking that $\det M = \pm 1$. One can see that $\det M = 1$ because $\mathrm{Im}(\tau) > 0$. $1, \tau$ is a $\mathbb{R}$-basis of $\mathbb{C}$.

So the eigenvalues of the multiplication by μ on $\mathbb{C}$ (seen as a $\mathbb{R}$-linear map) are $\mu, \bar{\mu}$. These are the roots of the characteristic polynomial of M.

So $\mu, \bar{\mu}$ satisfy the equation

$$X^2 - \underbrace{(a+d)}_{\in \mathbb{Z}} X + 1 = 0.$$

I would like to conclude that the only possibilities are

$$X^2 - X + 1 = 0 \iff \tau = -\bar{\rho}$$

$$X^2 + X + 1 = 0 \iff \tau = \rho$$

$$X^2 + 1 = 0. \iff \tau = i.$$

(Exercise!)