Elliptic modular forms

Hironori Shiga

Version May 10, 2008

Contents

1 $SL_2(\boldsymbol{Z})$ and elliptic curves

1.1 $SL_2(\boldsymbol{Z})$ and the moduli of complex tori

Definition 1.1. *For $\omega_1, \omega_2 \in \boldsymbol{C} - \{0\}$ with $\tau = \omega_2/\omega_1 \notin \boldsymbol{R}$, we define a lattice in $\boldsymbol{C}$ by*

$$\Lambda = \Lambda(\omega_1, \omega_2) = \{m\omega_1 + n\omega_2 : m, n \in \boldsymbol{Z}\}.$$

Proposition 1.1. *We have*

$$\Lambda(\omega_1, \omega_2) = \Lambda(\omega_1', \omega_2') \Longleftrightarrow \exists M \in GL(2, \boldsymbol{Z}); (\omega_1', \omega_2') = (\omega_1, \omega_2)M.$$

Proposition 1.2. *For $\tau, \tau' \in \boldsymbol{H} = \{z \in \boldsymbol{C} : \text{Im }(z) > 0\}$, we have*

$$\Lambda(1, \tau') = k\Lambda(1, \tau), \quad (k \in \boldsymbol{C} - \{0\}) \Longleftrightarrow \exists M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\boldsymbol{Z}); \tau' = \frac{a\tau + b}{c\tau + d}.$$

Definition 1.2. *We define a complex torus*

$$T(\omega_1, \omega_2) = \boldsymbol{C}/\Lambda(\omega_1, \omega_2), T(\tau) = \boldsymbol{C}/\Lambda(1, \tau).$$

Theorem 1.1.

$$T(\tau) \sim_{biholo} T(\tau') \Longleftrightarrow \exists M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\boldsymbol{Z}); \tau' = \frac{a\tau + b}{c\tau + d}.$$

[proof]. ($\Longleftarrow$) is apparaent from the above Proposition.
We show ($\Longrightarrow$). Let π(resp. π') be the canonical projection from $\boldsymbol{C}$ to $T(\tau)$(resp.$T(\tau')$). And let $f : T(\tau) \to T(\tau')$ be a biholomorphic map. We suppose $f(O) = O'$, with $\pi(0) = O, \pi'(0) = O'$. f has a lifting $f_1 : \boldsymbol{C} \to T(\tau')$ in a natural way. It induces a analytic function $\tilde{f} : U \to \boldsymbol{C}$ defined in a neighborhood U of 0. And $\tilde{f}$ has an analytic continuation on the whole plane $\boldsymbol{C}$ as a possibly multivalued analytic function. Here, by the Monodromy theorem $\tilde{f}$ is single valued.

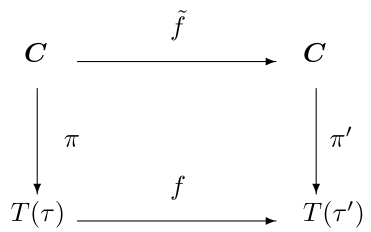


Diagram 1 : Lifting $\tilde{f}$ of f

If we consider $\tilde{f}^{-1}$, by the Monodromy theorem again, we can show $\tilde{f}$ is injective. So $\tilde{f} : \boldsymbol{C} \to \tilde{f}(\boldsymbol{C})$ is a biholomorphic map. By the Riemann uniformization theorem, the image $\tilde{f}(\boldsymbol{C})$ cannot be a proper subdomain. So $\tilde{f} : \boldsymbol{C} \to \boldsymbol{C}$ is a bijective map, and it is biholomorphic. By the Weierstrass singularity theorem we can show that Aut(H) is a group of nontrivial linear functions. Hence we may put

$$\tilde{f}(z) = kz,$$

note that we supposed $f(O) = O'$. So we have $\Lambda(1, \tau') = k\Lambda(1, \tau)$.

q.e.d.

1.2 The Fundamental region and a system of generators

Notations:

$$PSL_2(\boldsymbol{R}) = SL_2(\boldsymbol{R})/\pm I = \mathrm{Aut}(\boldsymbol{H}),$$
$$\Gamma := SL_2(\boldsymbol{Z}), \overline{\Gamma} := SL_2(\boldsymbol{Z})/\pm I,$$
in general, for a subgroup $G \subset \Gamma$, $\overline{G} := G/(< -I > \cap G)$,
$$\Gamma(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma) : a \equiv d \equiv 1 \pmod{N}, b \equiv c \equiv 0 \pmod{N}\} \lhd \Gamma \quad (N \in \boldsymbol{Z}^+).$$

Definition 1.3. $\Gamma(N)$ *is called the principal congruence subgroup of level* N.

Remark 1.1. *Note* $-I \notin \Gamma(N) \quad N > 2$. *So*

$$\overline{\Gamma(2)} = \Gamma(2)/\pm I, \overline{\Gamma(N)} = \Gamma(N) \quad (N > 2).$$

Definition 1.4.

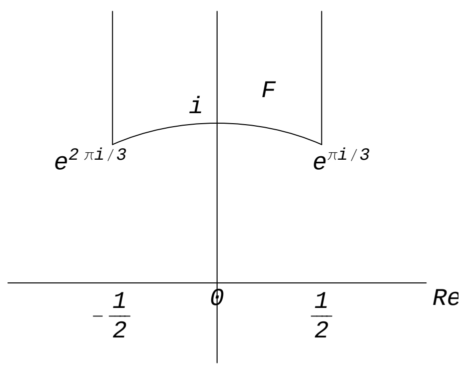
$$\Gamma_0(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \pmod{N}\},$$
$$\Gamma_1(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : a \equiv d \equiv 1 \pmod{N}\}.$$

Definition 1.5. *Let* G *be a subgroup of* Γ. G *acts on* $\boldsymbol{H}$. *Two points* z_1 *and* z_2 *are said to be G-equivalent, if we have* $z_2 = g(z_1)$ *for some* $g \in G$. *A closed region in* $\boldsymbol{H}$ *is said to be a fundamental region of G, if*
(1) *Every point* $z \in \boldsymbol{H}$ *is* G*-equivalent to a point in* F.
(2) *Any two different points in the interior of* F *are not* G*-equivalent.*

Theorem 1.2. *The closed region*

$$F = \{z \in \boldsymbol{H} : |\mathrm{Re}\ z| \le \frac{1}{2} \text{ and } |z| \ge 1\} \tag{1.1}$$

is a fundamental region for Γ.



Fundamental region for Γ

[proof]. (i) F contains all representatives.
Set

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

$G := \langle S, T \rangle \subset \Gamma$. For a fixed $z \in \boldsymbol{H}$ and $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ we have

$$\text{Im } g(z) = \frac{\text{Im } z}{|cz + d|^2}.$$

$\{|cd + d|^2 : c, d \in \boldsymbol{Z}^2 - \{(0,0)\}, \text{coprime}\}$ has the minimum, so Im $g(z)$ has the maximum. Let g_0 realizes the maximum, so do $T^k g_0 \quad (k = 0, \pm 1, \cdots)$. And we can find $g = T^{k_0} g_0 \in G$ such that $|g(z)| \leq \frac{1}{2}$. We have $g(z) \in F$. In fact, if we have $g(z) \notin F$, it holds $|g(z)| < 1$. Take $S(g(z))$. We have

$$\text{Im } S(g(z)) = \frac{\text{Im } g(z)}{|g(z)|^2} > \text{Im } g(z).$$

This is contradicts the maximality. So we could find a $g \in G$ such that $g(z) \in F$.

(ii) Equivalent points.

Suppose z_1, z_2 are equivalent, and we have $z_2 = g(z_1),\ g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma - \{\pm I\}$. Assume Im $z_2 = \frac{\text{Im } z_1}{|cz_1 + d|^2} \geq \text{Im } z_1$. So we have $|c| \cdot \frac{\sqrt{3}}{2} \leq |c| \,\text{Im } z_1 \leq |(c\,\text{Re } z_1 + d) + ic\,\text{Im } z_1| = |cz_1 + d| \leq 1$. We can see that it must hold $|c| \leq 1$. By observing $|cz_1| \leq 1/2$ we have $|d| \leq 1$. So we have only restricted possibilities:

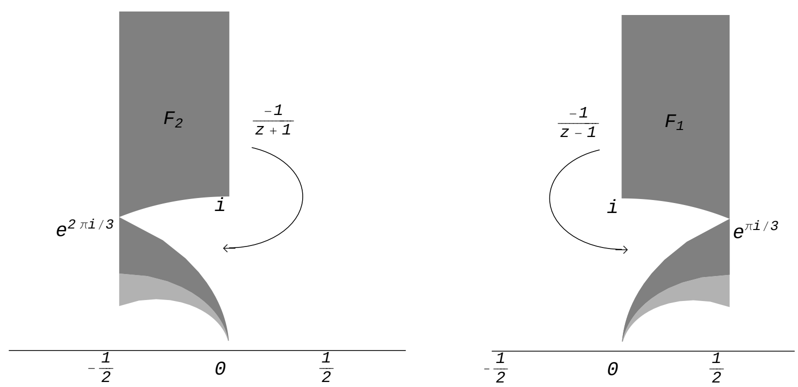
(a) $c = 0, d = \pm 1 \Longrightarrow g : az + b$

(b) $c = \pm 1, d = 0 \Longrightarrow g : a - \frac{1}{z}$

(c) $c = d = \pm 1 \Longrightarrow g : a + \frac{-1}{z+1}$ and $z_1 = e^{2\pi i/3}$

(d) $c = -d = \pm 1 \Longrightarrow g : a + \frac{-1}{z-1}$ and $z_1 = e^{\pi i/3}$.

In any case z_1 and z_2 cannot stay inside F at the same time.



Figures of case (c)(d)

q.e.d.

Proposition 1.3. *Let $z_1, z_2 \in \partial F$. z_1 and z_2 are Γ-equivalent* $\Longleftrightarrow$

(1) $z_2 - z_1 = \pm 1, |\text{Re } z_1| = |\text{Re } z_2| = 1/2$

or

(2) $z_2 = -\dfrac{1}{z_1}, |z_1| = |z_2| = 1.$

We use the notation $G_z = \{g \in G : g(z) = z\}$, the isotropy group for z. Set

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Proposition 1.4. *We have*

$$\begin{aligned}
&\text{(i) } \Gamma_i = \{\pm I, \pm S\} \\
&\text{(ii) } \Gamma_\omega = \{\pm I, \pm ST, \pm (ST)^2\},\ \omega = e^{2\pi i/3} \\
&\text{(iii) } \Gamma_{-\overline{\omega}} = \{\pm I, \pm TS, \pm (TS)^2\},\ -\overline{\omega} = e^{2\pi i/6} \\
&\text{(iv) } \Gamma_z = \pm I,\ \textit{otherwise.}
\end{aligned}$$

[proof]. We can solve

$$cz^2 + (d-a)z - b = 0, ad - bc = 1 \quad (a, b, c, d \in \boldsymbol{Z})$$

for $z = i, \omega, -\omega^2$.

Corollary 1.1. Γ *acts on* $\boldsymbol{H}$ *as a discrete group.*

Theorem 1.3. *We have*

$$\Gamma = \langle S, T. \pm id \rangle.$$

[proof].

Take an element $\gamma \in \Gamma$. According to the part (i) of the proof of Theorem 1.2 we can find $g \in G = \langle S, T \rangle$ so that we have $g\gamma(2i) \in F$. Namely it holds $g\gamma(2i) = 2i$. So $g\gamma \in I_{2i} = \{\pm id\}$. Hence we obtain the required conclusion.

q.e.d.

1.3 The Weierstrass $\wp$ function

Definition 1.6. *Let* $\Lambda = \Lambda(\omega_1, \omega_2)$ *be a lattice in* $\boldsymbol{C}$*. The Weierstrass* $\wp$ *function is defined by*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right). \tag{1.2}$$

Remark 1.2. *For a lattice* Λ,

$$\sum{}' \frac{1}{\omega^k} \quad \left(\sum{}' \textit{ means the sum } \sum_{\omega \in \Lambda - \{0\}}\right)$$

is absolute convergent for $k \geq 3$*, and is conditional convergent for* $k = 2$.

Theorem 1.4. (i) $\wp(z)$ *is meromorphic on* $\boldsymbol{C}$ *and doubly periodic, i.e.*

$$\wp(z + \omega) = \wp(z) \quad (\omega \in \Lambda).$$

(ii) $\wp(z)$ *has double poles at* $z = \omega \in \Lambda$*, and is an even function of order 2.*
(iii) $\wp'$ *is an odd function of order 3. It has zeros at half lattice points* $z = \omega_1/2, \omega_2/2, (\omega_1 + \omega_2)/2$*, and has a triple poles at* $z = \omega \in \Lambda$.

[proof]. (i) We have $\wp'(z + \omega_i) = \wp'(z) \quad (i = 1, 2)$. So $\wp(z + \omega_i) - \wp(z) = c_i \quad (c :$ constant). By putting $z = -\omega_i/2$ we get $c_i = 0$.
(ii)(iii) follows from the following general argument.

Lemma 1.1. (i) *Let* f *be a doubly periodic meromorphic function* $(\neq 0)$ *for a lattice* Λ. f *takes every complex value* α *same times (counting multiplicities) in a period parallelogram* $P_a = \{\lambda\omega_1 + \mu\omega_2 + a : 0 < \lambda < 1, 0 < \mu < 1\}$ *provided* $f \neq \alpha, \infty$ *on* ∂P_a.

(ii) *Let* f *be a doubly periodic meromorphic function.* $a_1, \ldots, a_r$ *be its representatives of zeros, and* $b_1, \ldots, b_r$ *be the representatives of poles. Then we have*

$$a_1 + \ldots + a_r - (b_1 + \ldots + b_r) \in \Lambda.$$

[proof]. (i) By the argument principle

$$\frac{1}{2\pi i}\int_{\partial P_a} \frac{f'}{f-\alpha}dz = \sharp\{z \in P_a : f(z) = \alpha\} - \sharp\{z \in P_a : f(z) = \infty\}.$$

By the periodicity the left hand side is equal to 0.
(ii) By the residue theorem

$$\frac{1}{2\pi i}\int_{\partial P_a} \frac{zf'}{f}dz = \sum_{z\in P_a} \mathrm{Res}(\frac{zf'}{f}, z) = a_1 + \cdots a_r - (b_1 + \cdots b_r).$$

Again by the argument principle we see that the left hand side belongs to Λ.

Theorem 1.5. (i)

$$\wp'(z)^2 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3), \tag{1.3}$$

where $e_1 = \wp(\frac{\omega_1}{2}), e_2 = \wp(\frac{\omega_1+\omega_2}{2}), e_3 = \wp(\frac{\omega_2}{2})$,
(ii)

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3, \tag{1.4}$$

where $g_2 = 60\sum_{\omega\in\Lambda-\{0\}} \frac{1}{\omega^4}, g_3 = 140\sum_{\omega\in\Lambda-\{0\}} \frac{1}{\omega^6}$.

[proof]. Set

$$\varphi(z) = \wp(z) - 1/z^2 = \sum_{\omega\in\Lambda-\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right),$$

and let

$$\varphi(z) = a_0 + a_2z^2 + \ldots + a_{2n}z^{2n} + \ldots$$

be the power series expansion. Obviously $\varphi(0) = 0$, so $a_0 = 0$. And we have

$$a_2 = \frac{\varphi''(0)}{2!} = 3{\sum}' \frac{1}{(m\omega_1 + n\omega_2)^4},\ a_4 = \frac{\varphi''''(0)}{4!} = 5{\sum}' \frac{1}{(m\omega_1 + n\omega_2)^6}.$$

Now we have

$$\wp(z) = \frac{1}{z^2} + a_2z^2 + a_4z^4 + \cdots$$
$$\wp'(z) = -2\frac{1}{z^3} + 2a_2z + 4a_4z^3 + \cdots.$$

So we have

$$\wp(z)^3 = \frac{1}{z^6} + \frac{3a_2}{z^2} + 3a_4 + \cdots$$
$$\wp'(z)^2 = \frac{4}{z^6} - \frac{8a_2}{z^2} - 16a_4 + \cdots.$$

Then it holds

$$\wp'(z)^2 - 4\wp(z)^2 + 20a_2\wp(z) = -28a_4 + c_1z^2 + \cdots.$$

The left hand side is holomorphic and doubly periodic on $\boldsymbol{C}$. So (according to the theorem of Liouville) it is a constant . Namely the right hand side is reduced to $-28a_4$. Then we have the required equality.

q.e.d.

Remark 1.3. *In a natural way* $\wp(z)$ *(resp.* $\wp'(z)$*) becomes to be a function on the torus* $T(\omega_1, \omega_2)$.

Theorem 1.6. *Let* g_2, g_3 *be the numbers given in Theorem 1.5. We set the corresponding algebraic curve*

$$E = E(g_2, g_3) : y^2 = 4x^3 - g_2 x - g_3$$

in $\boldsymbol{P}^2(\boldsymbol{C})$ *by adding a point at infinity* $[X, Y, Z] = [0, 1, 0]$ *with a homogeneous coordinate* $[X, Y, Z]$ *such that* $x = X/Z, y = Y/Z$. *The map* $\Phi : T(\omega_1, \omega_2) \to E$ *defined by* $z \mapsto (x, y) = (\wp(z), \wp'(z))$ *gives a bijective correspondence between* $T(\omega_1, \omega_2)$ *and* E.

proof]. Denote the point at infinity by P_∞. Take an arbitrary point $(x, y) \in E - \{P_\infty\}$. From $\wp(z) = x$ we obtain at most 2 possibilities z_1, z_2 with $z_2 = -z_1$. These two points are distinguished by the values of $\wp'$. So we can find unique preimage $\Phi^{-1}((x, y))$. Still we have $\lim_{z\to 0} \wp(z) = \infty$. So we have $\lim_{z\to 0} \Phi(z) = P_\infty$.

q.e.d.

Theorem 1.7. (Addition formula for $\wp(z)$)

We have

$$\wp(u + z) = -\wp(u) - \wp(z) + \frac{1}{4}\left(\frac{\wp'(z) - \wp'(u)}{\wp(z) - \wp(u)}\right)^2. \tag{1.5}$$

Corollary 1.2.

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

[proof of the addition formula]

We define

$$\sigma(z) = z {\prod_\omega}' \left\{\left(1 - \frac{z}{\omega}\right) \exp[\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2]\right\} \tag{1.6}$$

and

$$\zeta(z) = \frac{1}{z} + {\sum_\omega}' \left(\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right). \tag{1.7}$$

Proposition 1.5. $\sigma(z)$

(i) *is holomorphic on* $\boldsymbol{C}$,

(ii) *has a simple zero at* $z \in \Lambda$,

(iii) *is an odd function.*

It holds

$$\zeta(z) = \frac{\sigma'(z)}{\sigma(z)} = \frac{d \log \sigma(z)}{dz},$$

and

$$\wp(z) = -\zeta'(z) = \frac{\sigma'(z)^2 - \sigma(z)\sigma''(z)}{\sigma(z)^2}.$$

[proof]. We don't make a precise argument about the absolute convergence of (1.6). Once it is done, the above properties are obvious.

Theorem 1.8. *We have*

$$\zeta(z + \omega_1) - \zeta(z) = \eta_1 \cdots \text{a constant(quasi period)},$$
$$\zeta(z + \omega_2) - \zeta(z) = \eta_2 \cdots \text{a constant(quasi period)},$$
$$\eta_1\omega_2 - \eta_2\omega_1 = 2\pi i \cdots \text{Legendre's formula}.$$

[proof]. We can obtain these properties by the Integral around a parallelogram.

Proposition 1.6. *Set* $\eta = m\eta_1 + n\eta_2$ *for* $\omega = m\omega_1 + n\omega_2$. *It holds*

$$\sigma(z+\omega) = \begin{cases} \exp[\eta(z+\frac{\omega}{2})]\sigma(z) & (\omega \in 2\Lambda) \\ -\exp[\eta(z+\frac{\omega}{2})]\sigma(z) & (\omega \notin 2\Lambda). \end{cases}$$

[proof]. By the relation

$$\frac{d\log\sigma(z+\omega)}{dz} - \frac{d\log\sigma(z)}{dz} = \eta$$

we have $\sigma(z+\omega) = C\exp[\eta z]\sigma(z)$. Determine the constant factor by putting $z = -\frac{\omega}{2}$.

Proposition 1.7. *Let* $f(z)$ *be a doublly periodic meromorphic function* ($\neq 0$). *Let* $a_1, \ldots, a_r$ *and* $b_1, \ldots, b_r$ *be representatives of its zeros and poles with* $a_1 + \cdots + a_r = b_1 + \cdots + b_r$. *Then we have*

$$f(z) = c\frac{\sigma(z-a_1)\cdots\sigma(z-a_r)}{\sigma(z-b_1)\cdots\sigma(z-b_r)}.$$

[proof]. Use the automorphic factor of σ to show the periodicity.

Proposition 1.8.

$$\wp(z) - \wp(u) = -\frac{\sigma(z+u)\sigma(z-u)}{\sigma(z)^2\sigma(u)^2}.$$

[proof]. Use the preceeding proposition for $f(z) = \wp(z) - \wp(u)$ and observe the Laurent expansion at $z = 0$.

Proposition 1.9.

$$\zeta(z+u) = \zeta(z) + \zeta(u) + \frac{1}{2}\frac{\wp'(z) - \wp'(u)}{\wp(z) - \wp(u)}. \quad (1.8)$$

[proof]. Make two logarithmic derivatives of the preceeding formula.
[proof of the addition formula]
z derivative of (1.8):

$$\zeta'(z+u) = \zeta'(z) + \frac{1}{2}\left(\frac{\wp''(z)}{\wp(z)-\wp(u)} - \frac{\wp'(z)(\wp'(z)-\wp'(u))}{(\wp(z)-\wp(u))^2}\right).$$

u derivative of (1.8):

$$\zeta'(z+u) = \zeta'(u) + \frac{1}{2}\left(-\frac{\wp''(u)}{\wp(z)-\wp(u)} - \frac{(-\wp'(u))(\wp'(z)-\wp'(u))}{(\wp(z)-\wp(u))^2}\right).$$

By $\wp(z) = -\zeta'(z)$ we have

$$-2\wp(z+u) = -\wp(z) - \wp(u) + \frac{1}{2}\frac{\wp''(z)-\wp''(u)}{\wp(z)-\wp(u)} - \frac{1}{2}\frac{(\wp'(z)-\wp'(u))^2}{(\wp(z)-\wp(u))^2}.$$

By using $\wp''(z) = 6\wp^2(z) - \frac{1}{2}g_2$ we have

$$\frac{1}{2}\frac{\wp''(z)-\wp''(u)}{\wp(z)-\wp(u)} = 3(\wp(z)+\wp(u)).$$

So we obtain the theorem.

q.e.d.

1.4 Nonsingular cubics and the invariant j

Theorem 1.9. (Hurwitz' formula) *Let R, R_0 be compact Riemann surfaces. Let $\pi : R \to R_0$ be a nonconstant holomorphic map (so necessarily a surjective finite map). $p_1, \ldots, p_r$ be the singular points (or ramification points) on R, namely $d\pi(p_i) = 0$, v_i be its order of zero (ramification index) . Set $n = \sharp\pi^{-1}\pi(p)$ $(\pi(p) \neq \pi(p_i))$. Then we have*

$$2g(R) - 2 = n(2g_0 - 2) + \sum_{i=1}^{r} v_i,$$

where $g(resp.g_0)$ is the genus of $R(resp.R_0)$.

[proof]. Set χ (resp. χ_0) be the Euler characteristic of R (resp. R_0). Make a triangulation of R_0 using $\pi(p_i)$ as its vertices. Obtain a triangulation of R by the lifting. If we don't have any ramification, by counting the numbers of triangles, sides and vertices down and up stairs, we have the relation of Euler characteristics

$$\chi = n\chi_0.$$

When we have ramifications, we loose several vertices by the pinching at the ramification. That is counted by $\sum_i v_i$.

q.e.d.

Example 1.1. (The Fermat curve) *Set a projective algebraic curve*

$$F_n : X^n + Y^n = Z^n$$

with an affine representation $x^n + y^n = 1$ $(x = \frac{X}{Z}, y = \frac{Y}{Z})$. Set $\pi : F_n \to \boldsymbol{P}^1$ by $(x, y) \mapsto x$. The ramification points come from $x = 1, \zeta, \ldots, \zeta^{n-1}, (\zeta^n = 1)$. And at every ramification point ζ^i we have $v_i = n - 1$. So we have

$$2g - 2 = n(2g_0 - 2) + n(n-1), \quad g_0 = 0,$$

namely

$$g(F_n) = \frac{1}{2}(n-1)(n-2).$$

Especially a cubic Fermat curve F_3 is a Riemann surface of genus 1. Note that every nonsingular cubic is diffeomorphic to F_3. That is because a cubic curve

$$a_0X^3 + a_1Y^3 + a_2Z^3 + a_3X^2Y + a_4Y^2Z + a_5Z^2X + a_6XY^2 + a_7YZ^2 + a_8ZX^2 + a_9XYZ = 0 \quad (1.9)$$

is generically nonsingular. (So the family of nonsingular cubic curves makes a locally trivial topological fibre space over the space of parameters.)

By the above argument, we have:

Proposition 1.10. *Every nonsingular cubic curve is a Riemann surface of genus 1, that is homeomorphic to a complex torus.*

Remark 1.4 (Genus Formula)**.** *Let C be an algebraic curve of degree n. Then we have*

$$g(\tilde{C}) = \frac{1}{2}(n-1)(n-2) - \sum_i \delta_i,$$

where $\tilde{C}$ is the nonsingular model of C, $g(\tilde{C})$ is its genus, δ_i is a contribution from every singular point. For example $\delta = 1$ for an ordinary double point.

[Normal forms]

For an arbitrary nonsingular cubic (1.9), we can find a nice homogeneous coordinate with the conditions:
$[X, Y, Z] = [0, 1, 0]$ is a flex with the tangent $Z = 0$,
namely
$[X, Y, Z] = [0, 1, 0]$ is the only intersection with $Z = 0$. (We used here the result that a nonsingular cubic has (9) flex points on it.)

Hence we get $a_1 = a_3 = a_6 = 0$.
So we obtain an affine equation

$$a_4 y'^2 + a_7 y' + a_9 x'y' + a_0 x'^3 + a_2 + a_5 x' + a_7 x'^2 = 0. \tag{1.10}$$

By an affine transformation

$$x = \alpha x' + \beta, y = ay' + bx' + c \tag{1.11}$$

of (1.10) we obtain a normal form

$$E = E(g_2, g_3) : y^2 = 4x^3 - g_2 x - g_3, \text{with } g_2^3 - 27g_3^2 \neq 0, \tag{1.12}$$

here g_2, g_3 are just some constants. $g_2^3 - 27g_3^2 \neq 0$ is the nonsingular condition.

Remark 1.5. *We note that the ambiguity of the transformation (1.11) contains only the proportionality*

$$\tilde{x} = t^2 x, \tilde{y} = t^3 y \quad (t \in \boldsymbol{C} - \{0\}).$$

Definition 1.7. *For an arbitrary given nonsingular cubic, we got an expression (1.12). We call it the Weierstrass normal form. Or we have*

$$y^2 = (x - e_1)(x - e_2)(x - e_3), \textit{with } (e_1 - e_2)(e_2 - e_3)(e_3 - e_1) \neq 0$$

we call it the Legendre normal form.
Together with P_∞ , the point at infinity, the pair (E, P_∞) is called an elliptic curve. Two elliptic curves $(E(g_2, g_3), P_\infty)$ and $(E(g_2', g_3'), P_\infty')$ are said to be projectively equivalent, when there is a projective linear transformation f such that $f(E(g_2, g_3)) = E(g_2', g_3')$ and $f(P_\infty) = P_\infty'$. In some cases we will write only E or $E(g_2, g_3)$ for an elliptic curve. But always we are keeping in mind this "marking" by P_∞.

Definition 1.8. *For an elliptic curve $(E(g_2, g_3), P_\infty)$ we define the j invariant:*

$$j(E(g_2, g_3)) = j = 12^3 \frac{g_2^3}{g_2^3 - 27g_3^2}, \tag{1.13}$$

and we call $\Delta = g_2^3 - 27g_3^2$ the discriminant.

Theorem 1.10. *Two elliptic curves $(E(g_2, g_3), P_\infty)$ and $(E(g_2', g_3'), P_\infty')$ are projectively equivalent if and only if we have*

$$g_2' = t^4 g_2, g_3' = t^6 g_3$$

for some $t \in \boldsymbol{C}^*$. The projective linear transformation is given by

$$\begin{cases} x' = t^2 x \\ y' = t^3 y, \end{cases}$$

and it is equivalent with the condition

$$j(E(g_2, g_3)) = j(E(g_2', g_3')).$$

[proof] The first "if and only" statement is a direct consequence from Remark 1.5. The second condition for the j invariant is equivalent to the proportionality $g_2'^3 : g_2^3 = g_3'^2 : g_3^2$. So it follows our assertion.

q.e.d.

Remark 1.6. *The value λ has more geometric meaning. $\lambda = (e_1, e_2, e_3, \infty)$ is a cross ratio of the 4 tangents from a flex. There is ambiguity of the order. If we take S_3 inavariant*

$$2^8 \frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2},$$

that is the j invariant. We don't speak about the invariant theory $\boldsymbol{C}[X,Y]^{S_3}$.

Definition 1.9. *For an elliptic curve $E : y^2 = 4x^3 - g_2 x - g3, \Delta \neq 0$, we define an addition law $-P(x,y) = P(x,-y)$ and $P_1(x_1,y_1) + P_2(x_2,y_2) = P_3(x_3,y_3)$ by*

$$x_3 = \begin{cases} -x_1 - x_2 + \frac{1}{4}\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 & (P_2 \neq \pm P_1) \\ -2x_1 + \frac{1}{4}\left(\frac{6x_1^2 - g_2/2}{y_1}\right)^2 & (P_1 = P_2 \neq P_\infty) \\ x_2 \quad (P_1 = P_\infty) \end{cases}, y_3 = \begin{cases} -\frac{y_2-y_1}{x_2-x_1} - \frac{y_1x_2-y_2x_1}{x_2-x_1} & (P_2 \neq \pm P_1) \\ y_1 + (x_3 - x_1)(6x_1^2 - g_2/2) & (P_2 = P_1 \neq P_\infty) \\ y_2 \quad (P_1 = P_\infty). \end{cases}$$

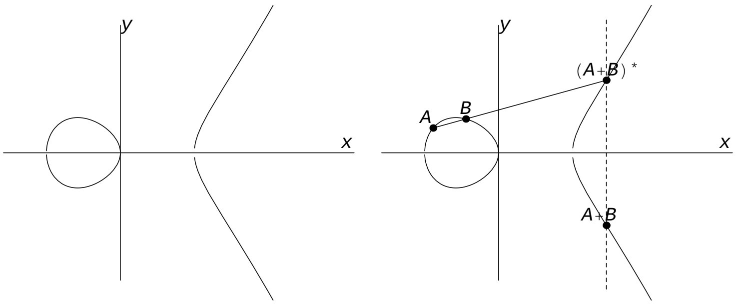


Figure of $A+B$

Remark 1.7. *Here we use the fact that every elliptic curve can be obtained as $\Phi(T(\tau))$ for some complex torus $T(\tau)$ with the marking by O, we shall prove it in the next subsection. So our addition law is just a translation of the group structure of $T(\tau)$. Hence it satisfies the associative law $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ a priori. If we don't use this transcription, it is not easy to get it.*

1.5 Elliptic modular function $j(\tau)$

Definition 1.10. *For $z \in \boldsymbol{H}$, we set*

$$\begin{aligned} g_2(z) &= 60 \sum{}' \frac{1}{(mz+n)^4}, \\ g_3(z) &= 140 \sum{}' \frac{1}{(mz+n)^6}, \quad \left(\sum{}' = \sum_{(m,n)\in \boldsymbol{Z}^2 - \{(0,0)\}}\right) \\ \Delta(z) &= g_2(z)^3 - 27 g_3(z)^2. \end{aligned}$$

The elliptic modular function

$$j(z) := 12^3 \frac{g_2(z)^3}{\Delta(z)} \tag{1.14}$$

is defined on $\boldsymbol{H}$.

For a representaion $\Phi(T(\tau)) = E(\tau)$:

$$y^2 = 4x^3 - g_2(\tau)x - g_3(\tau),$$

we get an invariant $j(\tau)$. As we made an argument, we have

$$(T(\tau), O) \sim_{biholo} (T(\tau'), O') \Longleftrightarrow_{(1)} \tau \sim_{PSL_2(\boldsymbol{Z})} \tau' \Longleftrightarrow_{(2)} \Lambda(\tau) = \exists k \Lambda(\tau') \Longrightarrow_{(3)} j(\tau) = j(\tau').$$

By the argument in the preceeding subsection we have

$$j(\tau) = j(\tau') \Longleftrightarrow_{(a)} (E(\tau), P_\infty) \sim_{projective\ equiv.} (E(\tau'), P'_\infty) \Longrightarrow_{(b)} (T(\tau), O) \sim_{biholo} (T(\tau'), O').$$

In fact (1) is assured by Theorem 1.1, (2) is obtained in Proposition 1.2 and (3) is deduced from the definition of $j(\tau)$. On the other hand (a) is shown in Theorem 1.10 and (b) is a consequence of Theorem . So we have

Theorem 1.11. *0) $j(z)$ is holomorphic on $\boldsymbol{H}$,*
1) $(E(\tau), P_\infty) \sim_{proj.equiv.} (E(\tau'), P'_\infty) \Longleftrightarrow j(\tau) = j(\tau')$,
2) $j(z) = j(z') \Longleftrightarrow z' = g(z) \quad \exists g \in PSL_2(\boldsymbol{Z})$,
3) $j(z)$ gives a biholomorphic equivalence between $\widehat{\Gamma \setminus \boldsymbol{H}}$ and $\boldsymbol{C} \cup \{\infty\} = \boldsymbol{P}^1$, where $\hat{}$ means the one point compactification.
4) We have the Fourier expansion:

$$j(z) = \frac{1}{q} + c_0 + c_1 q + \cdots, \quad q = e^{2\pi i z}.$$

5) Every elliptic curve has a representative in a projective equivalence class given by $(E(\tau), P_\infty)$ coming from a marked complex torus $(T(\tau), O)$.

Remark 1.8. *We know that $j(\tau)$ has a simple pole at $q = 0$ i.e. $\tau = i\infty$. But to get the exact value of the residue, we need some more argument. We shall show it in the later section.*

Proposition 1.11. (i) We have

$$j(\omega) = 0, \; j(i) = 1728.$$

(ii) For a pure imaginary z, it holds $j(z) \in \boldsymbol{R}$.

[proof]. (i) We have

$$\sum_{m,n}{}' \frac{1}{(mi+n)^6} = \sum_{m,n}{}' \frac{1}{i^6} \frac{1}{(m+(-i)n)^6} = -\sum_{m,n}{}' \frac{1}{(mi+n)^6}.$$

It means $g_3(i) = 0$. So we have $j(i) = 1728$. Also we have

$$\sum_{m,n}{}' \frac{1}{(m\omega+n)^4} = \sum_{m,n}{}' \frac{1}{\omega^8} \frac{1}{(m+n\omega^2)^4} = \sum_{m,n}{}' \frac{1}{\omega^8} \frac{1}{(m+n\omega^2)^4} = \omega \sum_{m,n}{}' \frac{1}{((m-n)-n\omega)^4} = \omega \sum_{m,n}{}' \frac{1}{(m\omega+n)^4}.$$

It means $g_2(\omega) = 0$. So we have $j(\omega) = 0$
(ii) Set $z = it \quad (t > 0)$. It holds

$$\overline{\sum_{m,n}{}' \frac{1}{(m(it)+n)^4}} = \sum_{m,n}{}' \frac{1}{\overline{(m(it)+n)}^4} = \sum_{m,n}{}' \frac{1}{(-m(it)+n)^4} = \sum_{m,n}{}' \frac{1}{(m(it)+n)^4}.$$

Hence $g_2(it)$ is always real valued. It is the same for $g_3(it)$. So $j(z)$ takes a real value for every $z = it$.

q.e.d.

Remark 1.9. *There is no general formula for the Fourier coefficients of $j(\tau)$. But they are always integers and have deep arithmetic meaning:*

$$j(\tau) = \frac{1}{q} + 744 + 196884\, q + 21493760\, q^2 + 864299970\, q^3 + \cdots .$$

What does 196884 means ?

Setting $J(z) = j(z) - 744 = \frac{1}{q} + \sum_{n\geq 1} c(n) q^n$

$$J(z) = \frac{\Theta(\Lambda_L, z)}{\Delta(z)} - 24,$$

where Λ_L means the Leech lattice, that is an even unimodular selfdual lattice with length 24 and minimum distance 2, and

$$\Theta(\Lambda_L, z) = \sum_{\alpha\in\Lambda_L} \exp[\pi\langle\alpha,\alpha\rangle z] = \sum_{n\geq 0} |\Lambda_{2n}| q^n \quad (\Lambda_{2n} = \{\alpha \in \Lambda_L : \langle\alpha,\alpha\rangle = 2n\}),$$

where $\langle\alpha,\alpha\rangle$ is the inner product of Λ_L. This is the starting point of the Monster theory. And the Leech lattice has many nice properties.

Example 1.2. (The oldest example of an elliptic curve found in " Diophantus "Number theory".)

$$E : y^2 = x^3 - x + 9.$$

We have integer points $(0, \pm 3)$ on E. Find other integer points as far as possible.
(See also, E. Brawn and B. Myers, " Elliptic curves from Mordell to Diophantus and back ", Mathematics Monthly, August-September 2002,639-649)

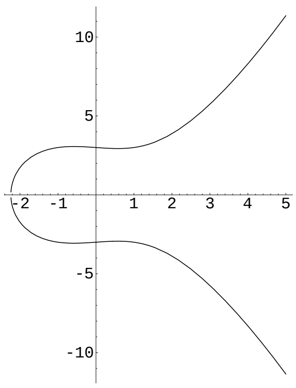


Figure of the Diophantus elliptic curve

2 Modular forms for $SL_2(\boldsymbol{Z})$

2.1 Cusps

We obtain the quotient space $\Gamma \setminus \boldsymbol{H}$ for Γ. How to make it complete ? We set

$$\overline{\boldsymbol{H}} = \boldsymbol{H} \cup \{i\infty\} \cup \boldsymbol{Q}.$$

A point of $\overline{\boldsymbol{H}} - \boldsymbol{H}$ is called a cusp. Γ acts on the set of cusps transitively. In other words cusps belong to only one Γ equivalence class. For a subgroup Γ' it acts on the cusps but in general not transitively. [Topology of $\overline{\boldsymbol{H}}$.]

For a positive number C set

$$N_C = \{z \in \boldsymbol{H} : \mathrm{Im}\ z > C\} \cup \{i\infty\}.$$

We define the fundamental system of open neighborhood of $i\infty$ by $\{N_C : C > 0\}$. Let $a/c \in \boldsymbol{Q}$ and take a matrix $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Then it holds $\alpha(i\infty) = \frac{a}{c}$. We define $\{\alpha N_C : C > 0\}$ to be the fundamental system of open neighborhood of $\frac{a}{c}$. Together with a usual system of open neighborhood for $z \in \boldsymbol{H}$, we define a topology of $\overline{\boldsymbol{H}} = \boldsymbol{H} \cup \{i\infty\} \cup \boldsymbol{Q}$.

This topology induces a one point compactification $\widehat{\Gamma \setminus \boldsymbol{H}} = \Gamma \setminus (F \cup \{i\infty\})$ of $\Gamma \setminus \boldsymbol{H}$.

Under the map

$$q(z) : z \mapsto q := e^{2\pi i z}$$

we have

$$\boldsymbol{H} \cup \{i\infty\} \to D = \{|q| < 1\}, \tag{2.1}$$

and N_C is mapped to a disc $\{|q| < e^{-2\pi C}\}$. The topology of $\boldsymbol{H} \cup \{i\infty\}$ is the weakest topology that makes $q(z)$ to be continuous.

Let $f(z)$ be a holomorphic function on $\boldsymbol{H}$ with a period $f(z+1) = f(z)$. Then we have a Fourier expansion (that is a Laurent series in q)

$$f(z) = \sum_{n \in \boldsymbol{Z}} a_n e^{2\pi i n z} = \sum_{n \in \boldsymbol{Z}} a_n q^n. \tag{2.2}$$

We say $f(z)$ is meromorphic (resp. holomorphic, 0)at $i\infty$, if it has only finite negative power terms (resp. no negative term, neither negative term nor constant term).

If $f(z)$ is holomorphic on $\boldsymbol{H}$ and has a periodicity

$$f(z+N) = f(z)$$

for a fixed positive integer N, we consider a map

$$z \mapsto e^{2\pi i z/N},$$

and we may have an analogous argument.

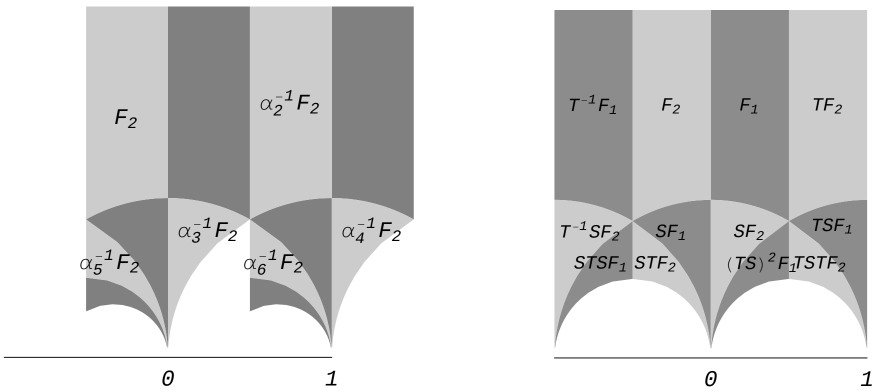
Proposition 2.1. *Let Γ' be a index finite subgroup of Γ. Set $[\overline{\Gamma} : \overline{\Gamma'}] = n$. We have a coset decomposition*

$$\overline{\Gamma} = \bigsqcup_{i=1}^{n} \alpha_i \overline{\Gamma'}$$

with a complete set $\{a_1, \ldots, a_n\}$ of coset representatives. Then $F' = \bigcup_{i=1}^{n} \alpha_i^{-1} F$ is a fundamental region of Γ'.

Example 2.1. $\Gamma' = \Gamma(2)$. *Because we have* $SL_2(\boldsymbol{Z}/2\boldsymbol{Z}) \cong S_3$, *we have* $[\Gamma, \Gamma(2)] = [\overline{\Gamma}, \overline{\Gamma(2)}] = 6$. *We have the following representatives of the cosets:*

$$\alpha_1 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^{-1}, \ \alpha_2 = T^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1}$$
$$\alpha_3 = S^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1}, \ \alpha_4 = (TS)^{-1} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}^{-1}$$
$$\alpha_5 = (ST)^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^{-1}, \quad \alpha_6 = (TST)^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1}.$$



Fundamental region for $\Gamma(2)$

[proof of the proposition]. Take an arbitrary point $z \in \boldsymbol{H}$. Find $\gamma \in \overline{\Gamma}; \gamma(z) \in F$. We have unique $\alpha_i; \gamma \in \alpha_i\overline{\Gamma'}$. So we have $g_i = \alpha_i^{-1}\gamma \in \overline{\Gamma'}$, and $g_i(z) \in \alpha_i^{-1}F$.
Suppose $z \in \alpha_i^{-1}F^\circ, z' \in \alpha_j^{-1}F^\circ$ with $z' = gz, \quad \exists g \in \overline{\Gamma'} - \{\text{id}\}$. We have $\alpha_i z \in F^\circ, \alpha_j z' = \alpha_j gz \in F^\circ$, and they are Γ equivalent. So $\alpha_j g(z) = \alpha_i(z)$. Namely

$$\alpha_j g \alpha_i^{-1}(\alpha_i z) = \alpha_i z \in F^\circ.$$

According to the triviality of the isometry subgroup (see Prop 1.4), we have $\alpha_j g \alpha_i^{-1} = \text{id}$. So we have $\alpha_i\overline{\Gamma'} = \alpha_j\overline{\Gamma'}$. This is a contradiction.
For the case $z \in \partial(\alpha_i^{-1}F)$ or $z' \in \partial(\alpha_j^{-1}F)$, we can shift a little bit them to some interior points all together. It is possible because $g' \in \Gamma'$ is a homeomorphism that sends a small neighborfood of z to that of z'. So we may reduce the argument to the above case.

q.e.d.

2.2 Concept of modular forms

Definition 2.1. *Let* $f(z)$ *be a holomorphic function on* $\boldsymbol{H}$. *And let* k *be a non-negative integer.* $f(z)$ *is said to be* <u>*a modular form of weight* k *for* Γ</u> *if the following conditions are satisfied:*
(i) $f(z)$ *is holomorphic at* $z = i\infty$,
(ii)

$$f(\gamma(z)) = (cz+d)^k f(z) \quad \textit{for} \ \ \forall\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma. \tag{2.3}$$

The $\boldsymbol{C}$ *vector space of modular forms of weight* k *for* Γ *is denoted by* $M_k(\Gamma)$.

In addition if we have
(iii) *$f(z)$ is 0 at $z = i\infty$,*
$f(z)$ is said to be <u>*a cusp form of weight k for Γ*</u>*. The $\boldsymbol{C}$ vector space of cusp forms of weight k for Γ is denoted by $S_k(\Gamma)$.*

Remark 2.1. *Some times we use the term "meromorphic modular form". It means a meromorphic function $f(z)$ on $\boldsymbol{H}$ that satisfies* (i') *$f(z)$ is meromorphic at $z = i\infty$ together with the automorphic property* (ii).

Remark 2.2. *By putting $\gamma = T, S$ we have*

$$f(z+1) = f(z), \tag{2.4}$$
$$f\left(-\frac{1}{z}\right) = (-z)^k f(z) \tag{2.5}$$

for a modular form $f(z)$ of weight k.

For a modular form for Γ with any weight k has a "q-expansion":

$$f(z) = \sum_{n=0}^{\infty} a_n q^n \qquad (q = e^{2\pi i z}). \tag{2.6}$$

Remark 2.3. (1) *Putting $\gamma = -I$ we have $M_k(\Gamma) = 0$ for an odd integer k. So we consider only the case k is even.*
(2) *We have*

$$\frac{d\gamma(z)}{dz} = \frac{1}{(cz+d)^2}. \tag{2.7}$$

So we may rewrite the condition (2.3) by

$$f(\gamma(z))(d\gamma(z))^{k/2} = f(z)(dz)^{k/2}. \tag{2.8}$$

By this equality we know that if (2.3) holds for γ_1 and γ_2 then it holds for $\gamma_1\gamma_2$ also. Then two equalities (2.4) and (2.5) guarantee (2.3) for any $\gamma \in \Gamma$.

Remark 2.4. *Observing (2.8) one may regard that a modular form is nothing but a multi differential form on $\Gamma \setminus \overline{\boldsymbol{H}}$. A modular form is very near to it. But they are not exactly the same thing . We should note that z does not necessarily give a local coordinate on it. We shall study this point in detail later.*

2.3 Eisenstein series

Definition 2.2. *Suppose k is an even integer with $k \geq 3$. We define* <u>*the Eisenstein series of weight k:*</u>

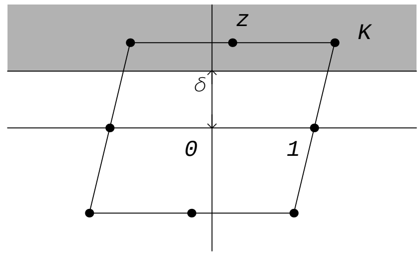
$$G_k(z) = \sum{}' \frac{1}{(mz+n)^k}. \tag{2.9}$$

Lemma 2.1. *The righthand side of (2.9) is absolutely uniform convergent on the compact set in $\boldsymbol{H}$.*

proof]. Suppose a positive real number $\delta(<1)$. Let $K \subset \{\text{Im } z \geq \delta\} \subset \boldsymbol{H}$ be a compact set.

$$\sum_{(m,n)\in \boldsymbol{Z}^2 - \{(0,0)\}} \left|\frac{1}{(mz+n)^k}\right| = \sum_{L=1}^{\infty} \sum_{\max\{|m|,|n|\}=L} \left|\frac{1}{(mz+n)^k}\right| \leq \sum_{L=1}^{\infty} 8L\frac{1}{(L\delta)^k} = \frac{8}{\delta^k}\sum_{L=1}^{\infty}\frac{1}{L^{k-1}}.$$

So we obtain the conclusion.



δ evaluates the distance

q.e.d.

Proposition 2.2. *We have $G_k(z) \in M_k(\Gamma)$.*

[proof]. According to Lema 2.1, $G_k(z)$ is holomorphic on $\boldsymbol{H}$. And obviously it holds $G_k(z+1) = G_k(z)$. Still we have

$$G_k(-\frac{1}{z}) = \sum{}' \frac{1}{(-m/z+n)^k} = (-z)^k \sum{}' \frac{1}{(m-nz)^k} = (-z)^k G_k(z).$$

It holds

$$\lim_{z\to i\infty} G_k(z) = 2\sum_{n=1}^{\infty} = 2\zeta(k).$$

It means $G_k(z)$ is bounded at $z = i\infty$, namely it is holomorphic there.

q.e.d.

Proposition 2.3. (Fourier expansion of the Eisenstein series)
Suppose k is an even integer greater than 2. We have

$$G_k(z) = 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n \quad \textit{with} \quad \sigma_k(n) = \sum_{d|n} d^k,$$

$$G_k(z) = 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\right). \tag{2.10}$$

Here we define the Bernoulli numbers by

$$\frac{x}{e^x-1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}. \tag{2.11}$$

Several beginning numbers are given by

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, \cdots .$$

Lemma 2.2. (Due to Euler)

$$\zeta(2k) = -\frac{1}{2}\frac{(2\pi i)^{2k}}{(2k)!}B_{2k} \quad (k = 1, 2, 3, \ldots). \tag{2.12}$$

[proof]. Note that $B_0 = 1, B_1 = -\frac{1}{2}, B_{2k+1} = 0 \quad (k \geq 1)$. In fact we have the following argument. By putting $\varphi(x) = \frac{x}{e^x-1} + \frac{1}{2}x$, we have

$$\varphi(-x) = \frac{-x}{e^{-x}-1} - \frac{1}{2}x = \frac{xe^x}{e^x-1} - \frac{1}{2}x.$$

So it holds

$$\varphi(x)-\varphi(-x)=\frac{x}{e^x-1}-\frac{xe^x}{e^x-1}+x=0.$$

It means that $\varphi(x)$ is an even function. Hence it's power series expansion does not contain any odd power term. Namely $B_{2k+1}=0$ for $k=1,2,\cdots$. We get $B_0=1, B_1=-\frac{1}{2}$ by direct calculation.

Now we have

$$\pi z\cot\pi z=\pi zi\cdot\frac{e^{\pi iz}+e^{-\pi iz}}{e^{\pi iz}-e^{-\pi iz}}=\pi iz+\frac{2\pi iz}{e^{2\pi iz}-1}=1+\sum_{k=1}^{\infty}(-1)^k B_{2k}\frac{2^{2k}\pi^{2k}z^{2k}}{(2k)!}.$$

On the other hand, from

$$\left(\pi i-\frac{2\pi i}{1-e^{2\pi iz}}\right)=\pi\cot\pi z=\frac{1}{z}+\sum_{n\neq 0}^{\infty}\left(\frac{1}{z+n}+\frac{1}{z-n}\right)$$

we have

$$\pi z\cot\pi z=1+2\sum_{n=1}^{\infty}\left(1-\frac{n^2}{n^2-z^2}\right)=1-2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty}\left(\frac{z}{n}\right)^{2k}=1-2\sum_{k=1}^{\infty}\left(\sum_{n=1}^{\infty}\frac{1}{n^{2k}}\right)z^{2k}.$$

So by tem by term observation we obtain (2.12).

q.e.d.

Lemma 2.3. *For an integer $k(\geq 2)$, we have*

$$\sum_{n\in\boldsymbol{Z}}\frac{1}{(t+n)^k}=\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}n^{k-1}e^{2\pi int}\quad(\mathrm{Im}\ t>0)\tag{2.13}$$

[proof]. We have

$$\varphi(t):=\frac{1}{t}+\sum_{n\neq 0}\left(\frac{1}{t+n}+\frac{1}{t-n}\right)=\pi\cot\pi t=\pi i\left(1+\frac{2}{e^{2\pi it}-1}\right)=\pi i-2\pi i\sum_{n=0}^{\infty}e^{2\pi int}.$$

Making derivative we get

$$\varphi'(t)=-\sum_{n\in\boldsymbol{Z}}\frac{1}{(t+n)^2}=-2\pi i\sum_{n=0}^{\infty}2\pi in\cdot e^{2\pi int}.$$

This is the case $k=2$. Taking higher derivatives we get equalities for all even k.

q.e.d.

[proof of the proposition]

We have

$$G_k(z)=2\zeta(k)+2\sum_{m=1}^{\infty}\sum_{n\in\boldsymbol{Z}}\frac{1}{(mz+n)^k}=2\zeta(k)+2\sum_{m=1}^{\infty}\left[\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}n^{k-1}e^{2\pi in(mz)}\right]$$
$$=2\zeta(k)+2\frac{(2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}\left[\sum_{n=1}^{\infty}n^{k-1}e^{2\pi inmz}\right]=2\zeta(k)+2\frac{(2\pi i)^k}{(k-1)!}\sum_{N=1}^{\infty}\left[\sum_{n|N}n^{k-1}e^{2\pi iNz}\right].$$

So we obtain the required first equality. The second formula follows from Lemma 2.2.

q.e.d.

Definition 2.3. *Let k be an even integer greater than 2. A* <u>*normalized Eisenstein series*</u> *is defined by:*

$$E_k(z):=\frac{1}{2\zeta(k)}G_k(z)=1-\frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n=\frac{1}{2}\sum_{m,n\in\boldsymbol{Z},(m,n)=1}\frac{1}{(mz+n)^k}.\tag{2.14}$$

We have

$$\begin{cases} E_4(z) = 1 + 240(q + 9q^2 + \dots), \\ \\ E_6(z) = 1 - 504(q + 33q^2 + \dots), \end{cases} \tag{2.15}$$

here we used $B_4 = -\frac{1}{60},\ B_6 = \frac{1}{42}$ to get the equalities.

2.4 Discriminant form

For the torus $\boldsymbol{C}/\boldsymbol{Z} + z\boldsymbol{Z}$ and its realization as an elliptic curve $y^2 = 4x^3 - g_2(z)x - g_3(z)$. We have

$$g_2(z) = 60G_4(z),\ g_3(z) = 140G_6(z).$$

Note that, due to Euler,

$$\zeta(4) = \frac{\pi^4}{90}, \zeta(6) = \frac{\pi^6}{945}.$$

So we have

$$g_2(z) = \frac{4}{3}\pi^4 E_4(z),\ g_3(z) = \frac{8}{27}\pi^6 E_6(z).$$

These are modular forms of weight 4 and 6. The discriminant is expressed via Eisenstein series:

$$\Delta(z) = g_2(z)^3 - 27g_3(z)^2 = \frac{(2\pi)^{12}}{1728}(E_4(z)^3 - E_6(z)^2). \tag{2.16}$$

By observing (2.14) we know that this is a cusp form of weight 12. By substituting (2.15) we get

$$g_2^3(z) = \frac{4^3}{3^3}\pi^{12}(1 + \dots), \Delta(z) = (2\pi)^{12}(q + \dots).$$

So it holds $12^3 q \cdot \frac{4^3}{3^3}\pi^{12}(1 + \dots)\frac{1}{(2\pi)^{12}(q+\dots)}{}_{|q=0} = 1$. We can determine several other leading terms of $j(z)$, also. Hence we obtain the q expansion of $j(z)$ as we stated in Theorem 1.11 (4) and mentioned in Remark 1.9:

$$j(z) = \frac{1}{q} + 744 + 196884 \cdot q + \dots.$$

2.5 Eisenstein series $E_2(z)$

Definition 2.4.

$$\begin{cases} E_2(z) = \frac{1}{2\zeta(2)} \sum_{m=-\infty}^{\infty} {\sum_{n=-\infty}^{\infty}}' \frac{1}{(mz+n)^2} \\ \\ = 1 + \frac{3}{\pi^2} \sum_{m\neq 0} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^2} \\ \\ = 1 + \frac{6}{\pi^2} \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^2}. \end{cases} \tag{2.17}$$

Here the sum is not absolutely convergent. So the order of the smmations is very important.

According to (2.13) we have

$$\sum_{n=-\infty}^{\infty} \frac{1}{(z+n)^2} = -4\pi^2 \sum_{n=1}^{\infty} nq^n. \tag{2.18}$$

Substitute mz for z, and take the summation for m.

So we have

$$E_2(z) = 1 - 24 \sum_{m=1}^{\infty} \sum_{d=1}^{\infty} dq^{md}.$$

This double sum is absolutely convergent on $|q| < 1$. For example: for $\forall K > 0$,

$$\sum_{m\geq 1}^{K}\sum_{d\geq 1}^{K} d|q|^{md} \leq \sum_{d} \frac{d|q|^d}{1-|q|^d} \leq \int_1^\infty \frac{xr^x}{1-r^x}dx \sim -\log(1-r), \quad r = |q| < 1.$$

Hence we can rewrite

$$E_2(z) = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n)q^n. \tag{2.19}$$

How it behaves under the invertion $S(z) = -1/z$?

$$\frac{1}{z^2}E_2\left(-\frac{1}{z}\right) = \frac{1}{2\zeta(2)}\sum_{m=\infty}^{\infty}\sum_{n}{}'' \frac{1}{(-m+nz)^2} = 1 + \frac{3}{\pi^2}\sum_{n=-\infty}^{\infty}\sum_{m}{}' \frac{1}{(mz+n)^2}. \tag{2.20}$$

(2.20) is not equal to (2.17), because our double sum is not absolutely convergent.

Proposition 2.4.

$$\frac{1}{z^2}E_2\left(-\frac{1}{z}\right) = E_2(z) + \frac{12}{2\pi i z}. \tag{2.21}$$

[proof]. Set

$$a_{m.n}(z) = \frac{1}{(mz+n-1)(mz+n)} = \frac{1}{mz+n-1} - \frac{1}{mz+n}$$

and set

$$\tilde{E}_2(z) = 1 + \frac{3}{\pi^2}\sum_{m\neq 0}\sum_{n=-\infty}^{\infty}\left(\frac{1}{(mz+n)^2} - a_{m,n}(z)\right).$$

Note that

$$\frac{1}{(mz+n)^2} - a_{m,n}(z) = \frac{1}{(mz+n)^2(mz+n-1)} \sim \frac{1}{(mz+n)^3}$$

is absolutely convergent. So we have

$$\tilde{E}_2(z) = 1 + \frac{3}{\pi^2}\sum_{m\neq 0}\sum_{n=-\infty}^{\infty}\frac{1}{(mz+n)^2} + \frac{3}{\pi^2}\sum_{m\neq 0}\sum_{n=-\infty}^{\infty}\left(\frac{1}{mz+n} - \frac{1}{mz+n-1}\right).$$

But the third term is equal to 0. Hence it holds

$$\tilde{E}_2(z) = E_2(z).$$

Because the double sum of $\tilde{E}_2(z)$ is absolutely convergent, we have

$$E_2(z) = 1 + \frac{3}{\pi^2}\sum_{n=-\infty}^{\infty}\sum_{m\neq 0}\left(\frac{1}{(mz+n)^2} - a_{m,n}(z)\right) = \frac{1}{z^2}E_2(-\frac{1}{z}) - \frac{3}{\pi^2}\sum_{n=-\infty}^{\infty}\sum_{m\neq 0} a_{m,n}(z).$$

So we are asked to evaluate the last term. We claim

$$\sum_{n=-\infty}^{\infty}\left|\sum_{m\neq 0} a_{m,n}(z)\right|$$

is convergent. This is assured by the same way as the convergence

$$\sum_{n=-\infty}^{\infty}\left|\sum_{m\neq 0}\frac{1}{(mz+n)^2}\right|.$$

And it is derived as the following: by using (2.18) it holds

$$\sum_{m\neq 0}\frac{1}{(-mz-n)^2}=\frac{1}{z^2}\sum_{m\neq 0}\frac{1}{(-m-n/z)^2}=-\frac{1}{n^2}-\frac{(2\pi)^2}{z^2}\sum_{d=1}^{\infty}de^{-2\pi idn/z}\quad (n>0).$$

Set $-\frac{1}{z}=s+it \quad (t>0)$. So

$$\left|\sum_{m\neq 0}\frac{1}{(mz+n)^2}\right|\leq\frac{1}{n^2}+4\pi^2|s+it|^2\sum_{d=1}^{\infty}de^{-2\pi dnt}\quad (n>0).$$

And we have

$$\sum_{n=-\infty}^{\infty}\left|\sum_{m\neq 0}\frac{1}{(mz+n)^2}\right|\leq\sum_{n=-\infty}^{\infty}\frac{1}{n^2}+|s+it|^2\zeta(2)+8\pi^2|s+it|^2\sum_{n=1}^{\infty}\sum_{d=1}^{\infty}de^{-2\pi dnt}$$
$$=(2+|s+it|^2)\zeta(2)+8\pi^2|s+it|^2\sum_{n=1}^{\infty}\sum_{d=1}^{\infty}de^{-2\pi dnt}=(2+|s+it|^2)\zeta(2)+8\pi^2|s+it|^2\sum_{N=1}^{\infty}\sigma_1(N)(e^{-2\pi t})^N.$$

Hence we are allowed to write

$$\sum_{n=-\infty}^{\infty}\sum_{m\neq 0}a_{m,n}(z)=\lim_{N\to\infty}\sum_{n=-N+1}^{N}\sum_{m\neq 0}a_{m,n}(z)=\lim_{N\to\infty}\sum_{m\neq 0}\sum_{n=-N+1}^{N}a_{m,n}(z)$$
$$=\lim_{N\to\infty}\sum_{m\neq 0}\left(\frac{1}{mz-N}-\frac{1}{mz+N}\right).$$

Now we have

$$\sum_{m\neq 0}\left(\frac{1}{mz-N}-\frac{1}{mz+N}\right)=\frac{2}{z}\sum_{m\neq 0}\left(\frac{1}{m-N/z}-\frac{1}{m+N/z}\right)=\frac{2}{z}\left[\pi\cot\left(-\frac{\pi N}{z}\right)+\frac{z}{N}\right].$$

Here we have

$$\lim_{N\to\infty}\frac{2}{z}\pi\cot\left(-\frac{\pi N}{z}\right)=\frac{2\pi}{z}\lim_{N\to\infty}i\frac{e^{-2\pi iN/z}+1}{e^{-2\pi iN/z}-1}=-\frac{2\pi i}{z}.$$

Hence

$$E_2(z)=\frac{1}{z^2}E_2(-\frac{1}{z})+\frac{6i}{\pi z}=\frac{1}{z^2}E_2(-\frac{1}{z})-\frac{12}{2\pi iz}.$$

q.e.d.

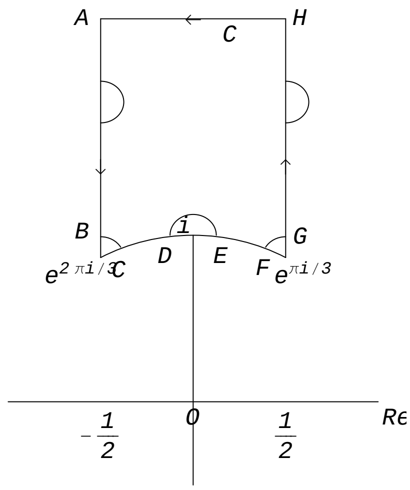
2.6 Algebra $M(\Gamma)$

Theorem 2.1. *For a nonzero meromorphic modular form $f(z)$ of weight k, we have*

$$v_\infty(f)+\frac{1}{2}v_i(f)+\frac{1}{3}v_\omega(f)+\sum_{a\in F-\{i,\omega\}}v_a(f)=\frac{k}{12}. \tag{2.22}$$

Where $v_a(f)$ means the order of $f(z)$ at $z=a$.

[proof]. Let C be a closed arc indicated by the figure with possibly additional deviation around the zeros on ∂F.



the path of integration C

According to the residue theorem

$$\frac{1}{2\pi i}\int_C \frac{f'(z)}{f(z)}dz = \sum_{P\in F-\partial F} v_P(f). \tag{2.23}$$

The right hand side is nothing but the term $\sum_{a\in F-\{i\omega\}} v_a(f)$.

Let us evaluate the left hand side as the sum of piece-wise integration.

(i) Because of the periodicity of f

$$\int_{AB}\frac{f'(z)}{f(z)}dz + \int_{GH}\frac{f'(z)}{f(z)}dz = 0.$$

(ii) Set $\tilde{f}(q) = f(z) = \sum a_n q^n \quad (q = e^{2\pi i z})$. Note that $f'(z) = \frac{d}{dq}\tilde{f}(q)\frac{dq}{dz}$. So

$$\frac{1}{2\pi i}\int_{HA}\frac{f'(z)}{f(z)}dz = -\frac{1}{2\pi i}\int_{|q|=e^{-2\pi T}}\frac{d\tilde{f}/dq}{\tilde{f}(q)}dq$$

Hence

$$\frac{1}{2\pi i}\int_{HA}\frac{f'(z)}{f(z)}dz = -v_\infty(f).$$

(iii)

$$\frac{1}{2\pi i}\int_{BC}\frac{f'(z)}{f(z)}dz = \frac{1}{2\pi i}\int_{FG}\frac{f'(z)}{f(z)}dz \to -\frac{1}{6}v_\omega(f)$$

as $\varepsilon \to 0$.

(iv)

$$\frac{1}{2\pi i}\int_{DE}\frac{f'(z)}{f(z)}dz \to -\frac{1}{2}v_i(f)$$

as $\varepsilon \to 0$.

(v) We claim

$$\frac{1}{2\pi i}\int_{CD}\frac{f'(z)}{f(z)}dz + \frac{1}{2\pi i}\int_{EF}\frac{f'(z)}{f(z)}dz \to \frac{k}{12}$$

as $\varepsilon \to 0$.

Lemma 2.4. *For $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ with $c \neq 0$ and a closed arc r on $\boldsymbol{H}$ we have*

$$\int_r \frac{f'(z)}{f(z)}dz - \int_{g(r)}\frac{f'(z)}{f(z)}dz = -k\int_r \frac{dz}{z+d/c} \tag{2.24}$$

According to this lemma, setting $g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, we have

$$\lim_{\varepsilon \to 0} \frac{1}{2\pi i} \int_{CD} \frac{dz}{z} = \lim_{\varepsilon \to 0} \frac{1}{2\pi i} \int_{CD} d \log z = \frac{1}{2\pi i} [\arg z]_{z=\omega}^{z=i} = -\frac{1}{12}.$$

So we have (v) and we complete the proof of the theorem.

[proof of the lemma].

From

$$f(g(z)) = (cz+d)^k f(z)$$

we have

$$f'(g(z)) \frac{dg(z)}{dz} = (cz+d)^k f'(z) + kc(cz+d)^{k-1} f(z).$$

Then

$$\frac{f'(g(z))}{f(g(z))} dg(z) = \frac{f'(z)}{f(z)} dz + k \frac{cdz}{cz+d}.$$

So

$$\int_C \frac{f'(z)}{f(z)} dz - \frac{f'(g(z))}{f(g(z))} dg(z) = -k \int_C \frac{cdz}{cz+d}.$$

Hence we have the Lemma.

q.e.d.

Theorem 2.2. *We have the following.*
(a) *For* $k < 0$, $M_0(\Gamma) = 0$.
(b) $M_0(\Gamma) = \boldsymbol{C}$.
(c) $M_2(\Gamma) = 0$.
(d) $M_k(\Gamma) = \boldsymbol{C} E_k \cong \boldsymbol{C}$ *for* $k = 4, 6, 8, 10, 14$.
(e)

$$S_k(\Gamma) = \begin{cases} 0 & (k < 12, k = 14) \\ \boldsymbol{C}\Delta & k = 12 \\ \Delta M_{k-12}(\Gamma) & k \geq 14. \end{cases}$$

(f) $M_k(\Gamma) = S_k(\Gamma) \oplus \boldsymbol{C} E_k$ *for* $k > 2$.

[proof]. (a) The left hand side of (2.22) is a nongegative number. So k can not be negative.
(b) When $k = 0$, $f(z)$ becomes to be a holomorphic function on $\Gamma \setminus \overline{\boldsymbol{H}} \cong \boldsymbol{P}^1$. The left hand side of (2.22) is zero only if all the terms are zero. That means f does not have zero. Hence $f(z)$ must be a constant.
(c) $\frac{1}{6}$ cannot be attained in the left hand side of (2.22). So $M_2(\Gamma)$ contains only 0.
(d) For example the case $k = 4$ is realized only if $\nu_\rho = 1$ and other terms in LHS are all zero. So $f \in M_4(\Gamma)$ is determined up to a constant multiple factor. According to Proposition 2.2 $E_4(z) \in M_4(\Gamma)$. So we have $M_4(\Gamma) = \boldsymbol{C} E_4(z)$. We can make a similar argument for other cases.
(e) For $f \in S_{12}(\Gamma)$ we have only possibility $\nu_\infty = 1$ and all other terms in LHS of (2.22) are zero. Hence it is determined up to a constant multiple factor. In subsection 2.4 we discussed that $\Delta(z) \in S_{12}(\Gamma)$. Hence we have $S_{12}(\Gamma) = \boldsymbol{C}\Delta(z)$. When $k \geq 14$ we know that $\Delta M_{k-12}(\Gamma) \subset S_k(\Gamma)$. Take an arbitrary $f \in S_k(\Gamma)$. Then f/Δ is holomorphic on $\boldsymbol{H} \cup \{i\infty\}$. Namely $f \in \Delta M_{k-12}(\Gamma)$.
(f) When $k < 12$ the assertion is reduced to (c). When $k \geq 12$, take an element $f \in M_k(\Gamma)$, and suppose $f(i\infty) = c$. Then $f - cE_k \in S_k(\Gamma)$. So $f \in S_k \oplus \boldsymbol{C} E_k$.

q.e.d.

Theorem 2.3. (1) $M_k(\Gamma) = \oplus_{4i+6j=k} \boldsymbol{C} E_4^i E_6^j$,
(2) $M(\Gamma) = \oplus_{k=0}^{\infty} M_k(\Gamma) = \oplus_{k:\text{even}} M_k(\Gamma) = \boldsymbol{C}[E_4, E_6]$. Moreover E_4 and E_6 does not have any algebraic relation, namely $M(\Gamma)$ is isomorphic to the polynomial algebra $\boldsymbol{C}[X, Y]$.

[proof]. (1) The assertion is true for $k \leq 12$. For $k \geq 14$, we have a solution i, j such that $k = 4i + 6j$. Take $E_4^i E_6^j$. It belongs to $M_k(\Gamma)$. So by the same argument as in the proof of the preceeding theorem we have $M_k = \Delta M_{k-12} \oplus \boldsymbol{C} E_4^i E_6^j$. By induction we obtain the required assertion.

(2) The first statement is a direct consequence of (1). Suppose that we have an algebraic relation between E_4 and E_6. There should exists a weighted homogeneous polynomial $P(X,Y)$ with weight 4 for X and weight 6 for Y such that $P(E_4, E_6) = 0$. Namely we have a homogeneous polynomial Q with $Q(E_4^3, E_6^2) = 0$. That means $j(z)$ satisfies an algebraic equation. According to Theorem 1.11 $j(z)$ takes every complex value. Hence we have a contradiction.

q.e.d.

2.7 The Dedekind η function

Definition 2.5. *The Dedekind η function is defined by*

$$\eta(z) = e^{2\pi iz/24} \prod_{n=1}^{\infty} \left(1 - e^{2\pi inz}\right) \qquad z \in \boldsymbol{H}. \tag{2.25}$$

The absolute convergence of the infinte product follows from that of $\sum_{n\geq 1} |e^{2\pi inz}|$.

Proposition 2.5.

$$\eta\left(-\frac{1}{z}\right) = \sqrt{-iz}\,\eta(z), \tag{2.26}$$

where we choose the branch so that we have $\mathrm{Re}\,\sqrt{-iz} > 0$.

[proof]. Put

$$h(z) = \frac{1}{\sqrt{-iz}}\eta(-1/z).$$

We claim that

$$\frac{\eta'(z)}{\eta(z)} = \frac{h'(z)}{h(z)}. \tag{2.27}$$

Then we have $h(z) = c\eta(z)$ for some constant c. Observing $h(i) = \eta(i)$ we obtain the required equality. So we concentrate ourselves to show (2.27).

$$\begin{aligned}
\frac{\eta'}{\eta} &= \frac{2\pi i}{24} + \sum_{n\geq 1} \frac{-2\pi ine^{2\pi inz}}{1 - e^{2\pi inz}} = \frac{2\pi i}{24}\left(1 - 24\sum_{n\geq 1} \frac{ne^{2\pi inz}}{1 - e^{2\pi inz}}\right) \\
&= \frac{2\pi i}{24}\left(1 - 24\sum_{n\geq 1} ne^{2\pi inz}\left(\sum_{m\geq 0} e^{2\pi im(nz)}\right)\right) = \frac{2\pi i}{24}\left(1 - 24\sum_{n\geq 1}\sum_{m\geq 1} ne^{2\pi im(nz)}\right) \\
&= \frac{2\pi i}{24}\left(1 - 24\sum_{n} \sigma_1(n) q^n\right).
\end{aligned}$$

According to (2.19) we have

$$\frac{\eta'(z)}{\eta(z)} = \frac{2\pi i}{24} E_2(z). \tag{2.28}$$

On the other hand, it holds

$$\frac{h'(z)}{h(z)} = (\left(\frac{1}{\sqrt{-iz}}\eta\left(-\frac{1}{z}\right)\right)')/h(z) = \frac{1}{z^2}\frac{\eta'(-\frac{1}{z})}{\eta(-\frac{1}{z})} - \frac{1}{2z}.$$

Using (2.28) we have

$$\frac{h'(z)}{h(z)} = \frac{2\pi i}{24}\left(\frac{1}{z^2}E_2\left(-\frac{1}{z}\right) - \frac{12}{2\pi i z}\right).$$

Due to the quasi automorphic property of E_2 (Proposition 2.4), we obtain the required equality.

q.e.d.

Proposition 2.6.

$$\frac{1}{(2\pi)^{12}}\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \eta(z)^{24}, \quad q = e^{2\pi i z}. \tag{2.29}$$

(*Note that* $E_4^3 - E_6^2 = 1728q + \cdots, \Delta = (2\pi)^{12}q + \cdots .$)

Remark 2.5. (a) *Note that we used the automorphic propertiy of* $E_2(z)$ *to get that of* $\eta(z)$.
(b) *For the* q*- expansion*

$$\eta(z)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n,$$

$\tau(n)$ *is called the Ramanujan* τ *function. There are many nice arithmetic properties for it.*
(i) $\tau(mn) = \tau(m)\tau(n)$ *for* $(m,n) = 1$ (We shall show it in the later section).
(ii) $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$.
(iii) (Deligne 1973 from Weil conjecture)

$$|\tau(p)| < 2p^{\frac{11}{2}} \quad (p : prime).$$

3 Modular form for congruence subgroups

In this section we use the following notation:

$\Gamma = SL(2, \boldsymbol{Z})$,

for a positive interger N,

$\Gamma(N) = \{g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : g \equiv id \ (\mathrm{mod} N)\}$,

$\Gamma_0(N) = \{g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : g \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \ (\mathrm{mod} N)\}$,

$\Gamma_1(N) = \{g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : g \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \ (\mathrm{mod} N)\}$,

Γ' : a congruence subgroup i.e. it holds $\Gamma(N) \subset \Gamma' \subset \Gamma$, for some positive integer N,

$F(\Gamma')$: fundamental region for Γ',

$F = F(\Gamma) = F_1 \cup F_2$: fundamental region for Γ $\quad (F_1 = F \cap \{\mathrm{Re}\ z \geq 0\}, F_2 = F \cap \{\mathrm{Re}\ z \leq 0\})$,

$\mu = [\overline{\Gamma} : \overline{\Gamma'}]$,

ν_ρ : number of non multiple vertices of $\Gamma(\rho)$ on $F(\Gamma')$, where, $\rho = e^{\pi i/3}$,

ν_i : number of non multiple vertices of $\Gamma(i)$ on $F(\Gamma')$,

t : number of equivalence classes of cusps for Γ',

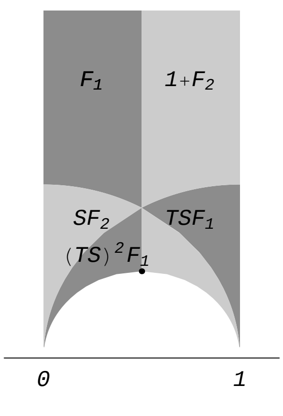
g : genus of $\Gamma' \backslash \overline{\boldsymbol{H}}$.

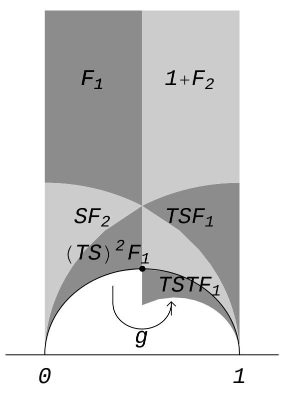
Remark 3.1. *Recall that in Proposition 2.1 we obtained*

$$F(\Gamma') = \cup_{i=1}^{\mu} \alpha_i^{-1} F$$

for a cosets decomposition $\overline{\Gamma} = \bigsqcup_{i=1}^{\mu} \alpha_i \overline{\Gamma'}$*. For* $a \in \Gamma(\rho) \cap F(\Gamma')$ *we have the following two cases. First, the case* a *is a common vertex of* $\alpha_i(F_1), \alpha_j(F_1)$ *and* $\alpha_k(F_1)$ *for different three indices* i, j, k*. Second, the case* a *is a vertex of unique triangle* $\alpha_i(F_1)$*.* ν_ρ *is the number of* $\alpha_i(\rho)$*'s of the second case. We define* ν_i *by the same manner.*

We find an example of non multiple vertex for $\Gamma(i)$ *in the configuration of* $F(\Gamma_0(2))$*. Here* $(TS)^2 F_1$ *is mapped to* $TSTF_1$ *by* $g = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \in \Gamma_0(2)$*. Together with the matrix* T*,* g *determines the gluing of the edges of* $F(\Gamma_0(2))$*.*





Fundamental region for $\overline{\Gamma_0(2)}$ $\qquad$ non multiple vertex $\frac{1+i}{2}$.

3.1 Geometry of congruence subgroups

Theorem 3.1. (genus formula) *We have*

$$g = 1 + \frac{\mu}{12} - \frac{\nu_i}{4} - \frac{\nu_\rho}{3} - \frac{t}{2}. \tag{3.1}$$

[proof of the theorem]. Let us consider the triangulation of $\overline{\Gamma} \setminus \overline{\boldsymbol{H}}$ obtained by the Γ orbits of F_1 and F_2. Set a_0, a_1, a_2 be the number of vertices, sides and triangles in it. We have

$$\begin{cases} a_2 = 2\mu, \\ a_1 = 3\mu, \\ a_0 = t + (\nu_i + \frac{\mu-\nu_i}{2}) + (\nu_\rho + \frac{\mu-\nu_\rho}{3}). \end{cases}$$

We are requested to show

$$2 - 2g = t + \frac{\nu_i}{2} + \frac{2\nu_\rho}{3} - \frac{\mu}{6}.$$

By the above counting we have the Euler characteristic of $\overline{\Gamma} \setminus \overline{\boldsymbol{H}}$:

$$2 - 2g = a_0 - a_1 + a_2 = (t + (\nu_i + \frac{\mu - \nu_i}{2}) + (\nu_\rho + \frac{\mu - \nu_\rho}{3})) - 3\mu + 2\mu.$$

So we obtain the assertion.

q.e.d.

3.2 Principal congruence subgroup $\Gamma(N)$

Theorem 3.2. (1)

$$\Gamma/\Gamma(N) \cong SL(2, \boldsymbol{Z}/N\boldsymbol{Z}).$$

(2)

$$[\overline{\Gamma} : \overline{\Gamma(N)}] = \mu(N) = \frac{1}{2}N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right) \qquad (N \geq 3).$$

[proof]. (1) We observe the reduction map

$$f_N : SL_2(\boldsymbol{Z}) \to SL_2(\boldsymbol{Z}/N\boldsymbol{Z}).$$

So it holds

$$\Gamma(N) = \ker(f_N).$$

Because we have $f_N(\Gamma) \cong \Gamma/\ker f_N$, the assertion follows from the surjectivity of f_N. So we show that f_N is surjective. Take an arbitrary element $g \in SL_2(\boldsymbol{Z}/N\boldsymbol{Z})$. It is expressed by an integer matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\boldsymbol{Z})$ satisfying $ad - bc \equiv 1 \pmod N$. We can find an interger t such that $(a, b + Nt) = 1$. (Put $t = \prod_{p|a,(p,b)=1} p \quad (p : \text{prime})$. Let us examine a common prime factor of a and $b + Nt$. We may consider only a prime factor p of a. If we don't have $p|b$, it holds $p|Nt$ so we don't have $p|(b + Nt)$. If $p|b$, from the condition $ad - bc \equiv 1 \pmod N$ and the fact that p is not contained in t, we know that p does not devide $b + Nt$.)
We exchange b with $b' = b + Nt$. So we have

$$ad - b'c = 1 + uN$$

with some integer u. Because $(a, b') = 1$, we can find integers x, y so that we have $-ax + b'y = u$. Put

$$c' = c + Ny, \; d' = d + Nx.$$

Then we have $ad' - b'c' = 1$. Namely we found a representative $\begin{pmatrix} a & b' \\ c' & d' \end{pmatrix} \in SL_2(\boldsymbol{Z})$ of g.
(2) Suppose $(N_1, N_2) = 1$ for $N_1, N_2 \in \boldsymbol{Z}$. We have

$$SL_2(\boldsymbol{Z}/N\boldsymbol{Z}) \cong SL_2(\boldsymbol{Z}/N_1\boldsymbol{Z}) \times SL_2(\boldsymbol{Z}/N_2\boldsymbol{Z}).$$

In fact. Take an element $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\boldsymbol{Z}/N\boldsymbol{Z}),\ ad - bc \equiv 1 \pmod{N}$, and observe the homomorphism

$$g : SL_2(\boldsymbol{Z}/N\boldsymbol{Z}) \to SL_2(\boldsymbol{Z}/N_1\boldsymbol{Z}) \times SL_2(\boldsymbol{Z}/N_2\boldsymbol{Z})$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (\begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{N_1}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{N_2}).$$

According to the Chinese Remainder Theorem it is a bijective homomorphism. So in this case, we obtain

$$\mu(\Gamma(N)) = \mu(\Gamma(N_1)) \cdot \mu(\Gamma(N_2)).$$

Hence it is enough to show

$$\mu(\Gamma(p^n)) = \sharp SL_2(\boldsymbol{Z}/p^n\boldsymbol{Z}) = p^{3n}(1 - \frac{1}{p^2}) = p^{3n} - p^{3n-2}, \quad p : \text{prime}.$$

Let us count the possible choices of an element $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\boldsymbol{Z}/p^n\boldsymbol{Z})$.

The case we have $(a, p) = 1$. For arbitrarily given b, y we have unique solution x for $ax - by \equiv 1 \pmod{p^n}$. We have $p^n - p^{n-1}$ possibilities for a. Hence we have $p^{3n} - p^{3n-1}$ elements here.

The case $p|a$. We have p^{n-1} possibilities for a. For $ad - bc \equiv 1 \pmod{p^n}$ we need $(b, p) = 1$. If this is the case, for an arbitrary d we have unique solution c. For b we have $p^n - p^{n-1}$ possibilities, and p^n choices for d. Then we have $p^{n-1}p^n(p^n - p^{n-1}) = p^{3n-1} - p^{3n-2}$ elements here.

So we get the assertion.

q.e.d.

Proposition 3.1. *We have*

$$t = \frac{\mu(N)}{N} \quad \text{for } \Gamma' = \Gamma(N).$$

[proof]. Consider the reduction map

$$\varphi : \overline{\Gamma'} \setminus (\overline{\boldsymbol{H}} - \boldsymbol{H}) \to \overline{\Gamma} \setminus (\overline{\boldsymbol{H}} - \boldsymbol{H}).$$

It holds

$$t = \sharp \left(\overline{\Gamma'} \setminus (\overline{\boldsymbol{H}} - \boldsymbol{H})\right),\ \sharp \left(\overline{\Gamma} \setminus (\overline{\boldsymbol{H}} - \boldsymbol{H})\right) = 1.$$

Note that

$$\overline{\Gamma}_{i\infty} = \left\{ \begin{pmatrix} a & k \\ 0 & 1 \end{pmatrix} : k = 0, \pm 1, \cdots \right\} / \pm I,\ \overline{\Gamma'}_{i\infty} = \left\{ \begin{pmatrix} a & Nk \\ 0 & 1 \end{pmatrix} : k = 0, \pm 1, \cdots \right\} / \pm I.$$

We can regard $\overline{\boldsymbol{H}} - \boldsymbol{H}$ as a homogeneous space $\overline{\Gamma}/\overline{\Gamma}_{i\infty}$, where the quotient means the set of right cosets. So we have

$$t = \sharp \left(\overline{\Gamma'} \setminus (\overline{\boldsymbol{H}} - \boldsymbol{H})\right) = \sharp \left(\overline{\Gamma'}/(\overline{\Gamma}_{i\infty} \cap \overline{\Gamma'}) \setminus \overline{\Gamma}/\overline{\Gamma}_{i\infty}\right) = \sharp \left(\overline{\Gamma'}/\overline{\Gamma'}_{i\infty} \setminus \overline{\Gamma}/\overline{\Gamma}_{i\infty}\right),$$

and

$$\sharp \left(\overline{\Gamma} \setminus (\overline{\boldsymbol{H}} - \boldsymbol{H})\right) = \sharp \left(\overline{\Gamma}/\overline{\Gamma}_{i\infty} \setminus \overline{\Gamma}/\overline{\Gamma}_{i\infty}\right) = 1.$$

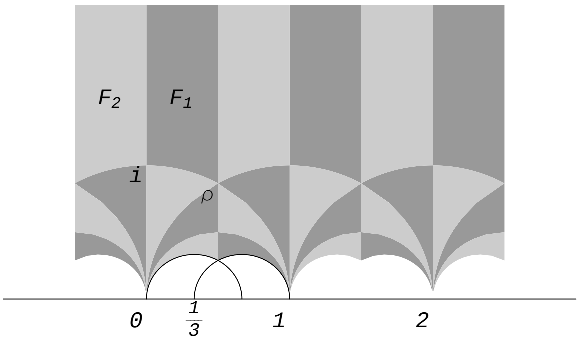
So we obtain

$$t = \frac{\sharp(\overline{\Gamma}/\overline{\Gamma'})}{\sharp(\overline{\Gamma}_{i\infty}/\overline{\Gamma'}_{i\infty})} = \frac{\mu(N)}{N}.$$

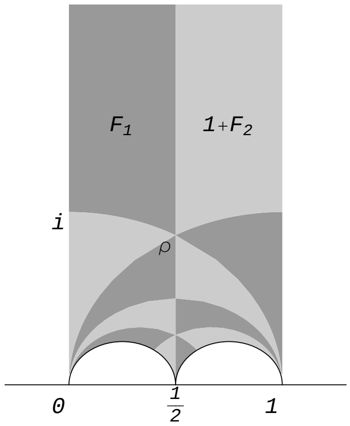
q.e.d.

name	μ	genus	ν_i	ν_ρ	t	isomorphic
$\overline{\Gamma(2)}$	6	0	0	0	3	$\mathfrak{S}_3$
$\Gamma(3)$	12	0	0	0	4	$\mathfrak{A}_4$: tetrahedral group
$\Gamma(4)$	24	0	0	0	6	$\mathfrak{S}_4$: octahedral group
$\Gamma(5)$	60	0	0	0	12	$\mathfrak{A}_5$: icosahedral group
$\Gamma(6)$	72	1	0	0	12	
$\Gamma(7)$	168	3	0	0	24	Klein's max. aut. gr.
.	.	.	.			
.						

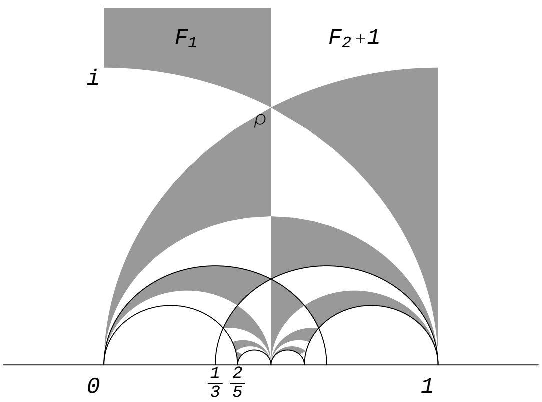
Table for $\Gamma(N)$



Fundamental region for $\overline{\Gamma(3)}$



Fundamental region for $\overline{\Gamma_0(4)} = \overline{\Gamma_1(4)}$



Fundamental region for $\overline{\Gamma_1(5)}$

By

$$IF_1, TSF_1, (TS)^2F_1, TSTF_1, TF_2, SF_2, TSTF_2, ST^{-1}F_2$$

we get a fundamental region of $\Gamma_1(3) = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -2 & 1 \\ -3 & 1 \end{pmatrix} \rangle = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \rangle$.

By

$$IF_1, TSF_1, (TS)^2F_1, TSTF_1, TST(TS)F_1, TST(TS)^2F_1,$$
$$TF_2, SF_2, TSTF_2, ST^{-1}F_2, ST^{-1}(ST)F_2, ST^{-1}(ST)^2F_2$$

we get a fundamental region of $\Gamma_1(4) = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -3 & 1 \\ -4 & 1 \end{pmatrix} \rangle == \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \rangle$.

3.3 Recalling the Riemann-Roch theorem

In the next subsection we use the Riemann-Roch Theorem for a compact Riemann surface. Here we recall it. Let X be a compact Riemann surface of genus g.

Definition 3.1. *Let $P_1, \dots, P_r$ be points on it, and let $n_1, \dots, n_r$ be integers. The formal sum $\sum_{i=1}^r n_i P_i$ is said to be a divisor on X. We define a divisor with coefficient in $\boldsymbol{Q}$ by the same manner. We say a divisor D is effective if all the coefficient are non negative, and we denote this by $D \geq 0$. For $D = \sum_{i=1}^r n_i P_i$, $\sum_{i=1}^r n_i$ is called the degree of D and is denoted by $\deg D$.*
For a meromorphic function f on X, by (f) we denote the divisor $\sum_P n_P(f)$. For a multi-differential ω on X, we define a divisor (ω) by the same way. Let K be the divisor of a meromorphic differential on X, that is called a canonical divisor. Any two canonical divisors are linearly equivalent, so we don't distinguish such a difference.

Theorem 3.3. *Let X be a compact Riemann surface of genus g. Let D be a divisor on it. Then we have*

$$\dim H^0(X, \mathcal{O}(D)) - \dim H^1(X, \mathcal{O}(D)) = 1 - g + \deg D. \tag{3.2}$$

Here we note that $H^1(X, \mathcal{O}(D)) \cong H^0(X, \mathcal{O}(K - D)) = H^0(X, \Omega(D))$.

Remark 3.2. *$H^0(X, \mathcal{O}(D))$ is the vector space of meromorphic functions on X with $(f) + D \geq 0$. $H^0(X, \mathcal{O}(K - D))$ is the vector space of meromorphic 1-forms with $(\omega) - D \geq 0$. $H^0(X, \mathcal{O}(mK + D))$ is the vector space of meromorphic multi-differentials of order m with $(\omega) + D \geq 0$.*

Remark 3.3. *Note that we have $H^0(X, \mathcal{O}(D)) = 0$ for $\deg D < 0$. It is an easy consequence from the fact $\deg(f) = 0$ for any meromorphic function f on X.*

Example 3.1. *By putting $D = 0$ we get*

$$\dim H^0(X, \mathcal{O}) = g.$$

By putting $D = K$ and using the above equality, we get

$$\deg K = 2g - 2.$$

3.4 Dimension formula for congruence subgroups

We fix a cogruence subgroup Γ' of Γ. For an even integer k we set

$$d_k = \dim M_k(\Gamma'),$$
$$e_k = \dim S_k(\Gamma').$$

Theorem 3.4. (Dimension formula 1) *For a congruence subgroup Γ', we have:*

$$\begin{cases} d_k = 0 \quad (k < 0) \\ d_0 = 1 \\ d_2 = \begin{cases} g \quad (t = 0) \\ g + t - 1 \quad (t \geq 1) \end{cases} \\ d_k = (k-1)(g-1) + \sum_{j=1}^s [\frac{k}{2}(1 - \frac{1}{n_j})] + \frac{k}{2} t \end{cases},$$

where $[a]$ *means the integer part of* a, $s = \nu_i + \nu_\rho$, *and for a non multiple vertex* P_j *we set*

$$n_j = \begin{cases} 2 & P_j \in \pi'(\Gamma(i)) \\ 3 & P_j \in \pi'(\Gamma(\rho)) \end{cases} .$$

[proof]. We denote the Riemann surface $\overline{\Gamma'} \setminus \overline{\boldsymbol{H}}$ by X. We shall speak about the system of local coordinates later. Take a meromorphic modular form $f(z)$ of weight k for Γ'. If we consider $f(z)(dz)^{k/2}$, it seems to be something like a multidifferential form on X. But it is not the case. Because z does not necessarily give a local coordinate on X, it comes out a difference from an usual multidifferential form. We examine this difference in an exact way.

Let

$$\pi : \overline{\boldsymbol{H}} \to \overline{\Gamma} \setminus \overline{\boldsymbol{H}}, \pi' : \overline{\boldsymbol{H}} \to \overline{\Gamma'} \setminus \overline{\boldsymbol{H}}$$

be the natural projection. And set the natural covering map

$$\varphi : \overline{\Gamma'} \setminus \overline{\boldsymbol{H}} \to \overline{\Gamma} \setminus \overline{\boldsymbol{H}}.$$

According to Theorem 1.10 we know that $j(z)$ gives a global coordinate of $\overline{\Gamma} \setminus \overline{\boldsymbol{H}}$ as $\boldsymbol{P}^1(\boldsymbol{C})$.

(0) For any point $p = \pi'(a) \in \pi'(\boldsymbol{H} - \Gamma(i) \cup \Gamma(\rho))$, z gives a local coordinate at p. So we are safe. Namely, $f(z)(dz)^{k/2}$ itself is locally a multidifferential form there.
Suppose $p = \pi'(a) \in \pi'(\Gamma(i) \cup \Gamma(\rho))$ and a is a multivertex of $F(\Gamma')$. In this case π' is locally biholomorphic, and z gives a local coordinate there. So we are safe here, also.

(i) The case when $p = \pi'(a) \in \pi'(\Gamma(i))$ and a is a non-multiple vertex of $F(\Gamma')$. The map φ is locally biholomorphic there. So $j(z) - j(\pi(a)) = j(z) - 1728$ gives a local coordinate at p, recall $j(i) = 1728$. Note that $j(z)$ gives a $2:1$ map in a neighborhood of $z = i$. So $j(z) - 1728$ has a double zero at $z = a$. So we can take a local coordinate t at p such that $t = (z - a)^2$. Hence we have

$$dz = \frac{1}{2} t^{-1/2} dt.$$

(ii) For a non-multiple vertex $a \in \Gamma(\rho) \cap F(\Gamma')$, by the same consideration as above we get a local coordinate $t = (z - a)^3$ at $p = \pi'(a)$. Hence we have

$$dz = \frac{1}{3} t^{-2/3} dt.$$

(iii) Finally, the case when $p = \pi'(a)$ with $a \in \Gamma(i\infty)$. We have $t = e^{2\pi i/N}$ for some positive integer N. Hence we have

$$dz = \frac{2\pi i}{N} t^{-1} dt,$$

recall that at a cusp $r = \frac{a}{c} \in \boldsymbol{Q}$, always we observe the behavior of $f(z)$ by that of $f(\alpha(z))$ with $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

According to this argument $f(z)$ is a (holomorphic) modular form, if and only if the multi-differential form

$$\omega = f(z)(dz)^{k/2}$$

on X has some poles those arising at $p = P_j (j = 1, \ldots, s)$ or $p = Q_\ell (\ell = 1, \ldots, t)$ with the condition

$$(\omega) \geq -\frac{k}{2} \cdot \left(\sum_{j=1}^{s} (1 - \frac{1}{n_j}) P_j + \sum_{\ell=1}^{t} Q_\ell \right). \tag{3.3}$$

Remark 3.4. *Note that we have the paraphrase of this argument for a cusp form. $f(z)$ is a cusp form, if and only if the multi-differential form ω satisfies*

$$(\omega) \geq -\frac{k}{2} \cdot \left(\sum_{j=1}^{s} (1 - \frac{1}{n_j}) P_j + \sum_{\ell=1}^{t} Q_\ell \right) + \sum_{\ell=1}^{t} Q_\ell. \tag{3.4}$$

Set $D = \sum_{j=1}^{s}(1 - \frac{1}{n_j})P_j + \sum_{\ell=1}^{t} Q_\ell$, and set $D_1 = \sum_{j=1}^{s}(1 - \frac{1}{n_j})P_j, D_2 = \sum_{\ell=1}^{t} Q_\ell$. Via this correspondence between f and ω we have an isomorphism of vector spaces:

$$M_k(\Gamma') \cong H^0(X, \mathcal{O}(\frac{k}{2}(K + D))).$$

Naturally we have

$$H^0(X, \mathcal{O}(\frac{k}{2}(K + D))) \cong H^0(X, \mathcal{O}(\frac{k}{2}K + \sum_{j=1}^{s}[\frac{k}{2}(1 - \frac{1}{n_j})]P_j + \frac{k}{2}\sum_{\ell=1}^{t} Q_\ell)).$$

and

$$\dim H^0(X, \mathcal{O}(\frac{k}{2}(K + D))) = \dim H^0(X, \mathcal{O}(\frac{k}{2}K + \sum_{j=1}^{s}[\frac{k}{2}(1 - \frac{1}{n_j})]P_j + \frac{k}{2}\sum_{\ell=1}^{t} Q_\ell)).$$

By using Riemann-Roch theorem, let us count the right hand side. We use an abbreviation

$$\frac{k}{2}K + \sum_{j=1}^{s}[\frac{k}{2}(1 - \frac{1}{n_j})]P_j + \frac{k}{2}\sum_{\ell=1}^{t} Q_\ell = \frac{k}{2}K + [\frac{k}{2}D_1] + \frac{k}{2}D_2.$$

At first we have

$$\deg(K + D) > 0.$$

In fact, by R-R theorem $\deg K = 2g - 2$. And $\deg D = \frac{\nu_i}{2} + \frac{2\nu_\rho}{3} + t$. By the genus formula Theorem 3.1 we have $2g - 2 + \frac{\nu_i}{2} + \frac{2\nu_\rho}{3} + t = \frac{\mu}{6} > 0$.

(a) For the case $k < 0$, we have $H^0(X, \mathcal{O}(\frac{k}{2}(K + D))) = 0$ because $\deg \frac{k}{2}(K + D) < 0$.

(b) For the case $k = 0$, we have $H^0(X, \mathcal{O}(\frac{k}{2}(K + D))) = H^0(X, \mathcal{O}) = \boldsymbol{C}$. This is trivial.

(c) Let us consider the case $k \geq 4$. By the R-R theorem we have

$$\dim H^0(X, \mathcal{O}(\frac{k}{2}K + [\frac{k}{2}D_1] + \frac{k}{2}D_2) = 1 - g + \deg(\frac{k}{2}K + [\frac{k}{2}D_1] + \frac{k}{2}D_2) + \dim H^0(X, \mathcal{O}((1 - \frac{k}{2})K - [\frac{k}{2}D_1] - \frac{k}{2}D_2)$$

Note that we have

$$-[\frac{k}{2} \cdot \frac{1}{2}] = [(1 - \frac{k}{2}) \cdot \frac{1}{2}], \ -[\frac{k}{2} \cdot \frac{2}{3}] = [(1 - \frac{k}{2}) \cdot \frac{2}{3}].$$

It means that we have always

$$(1 - \frac{k}{2})K - [\frac{k}{2}D_1] - \frac{k}{2}D_2 = (1 - \frac{k}{2})K + [(1 - \frac{k}{2})D_1] + (1 - \frac{k}{2})D_2 - D_2 < (1 - \frac{k}{2})(K + D) < 0.$$

Hence $\dim H^0(X, \mathcal{O}((1 - \frac{k}{2})K - [\frac{k}{2}D_1] - \frac{k}{2}D_2)) = 0$. So, using $\deg K = 2g - 2$ again we have

$$H^0(X, \mathcal{O}(\frac{k}{2}(K + D))) = 1 - g + \deg(\frac{k}{2}K + [\frac{k}{2}D_1] + \frac{k}{2}D_2) = (k - 1)(g - 1) + \sum_{j=1}^{s}[\frac{k}{2}(1 - \frac{1}{n_j})] + \frac{k}{2}t.$$

(d) For the case $k = 2$, the cohomologcal term on the right hand side becomes to be

$$H^0(X, \mathcal{O}(-[D1] - D2)) = H^0(X, \mathcal{O}(-D2)).$$

So we have

$$\dim H^0(X, \mathcal{O}(-[D1] - D2)) = \begin{cases} 0 & t > 0 \\ 1 & t = 0 \end{cases}.$$

By using $\deg K = 2g-2$, in case $t>0$ we have (note that $\deg[D_1]=0$)

$$\dim M_2(\Gamma') = 1 - g + \deg(K + [D_1] + D_2) = g - 1 + t.$$

In case $t=0$ we have $\dim M_2(\Gamma') = g$ by the same way. Hence we obtain the assertion.

q.e.d.

Theorem 3.5. (Dimension formula 2) *For a congruence subgroup* Γ'*, we have:*

$$\begin{cases} e_k = 0 \quad (k<0) \\ e_0 = \begin{cases} 1 & (t=0) \\ 0 & (t>0) \end{cases} \\ e_2 = g \\ e_k = d_k - t \quad (k \geq 4). \end{cases}$$

[proof]. We can prove this formula by the same method just using the condition mentioned in Remark 3.4.

Remark 3.5. *For the principal congruence subgroup* $\Gamma(N)$*, we don't have any nonmultiple vertex. So we get the genus* g *for by an easy calculation. But, for general cases we need to know the glueing of the* $\partial F(\Gamma')$ *by using the list of cosets representatives.*

name	μ	genus	t	isomorphic	$d_k(k\geq 2)$	$e_2(=g)$	$e_k(=d_k-t), k\geq 4$
$\Gamma(2)$	6	0	3	$\mathfrak{S}_3$	$k/2+1$	0	$k/2-2$
$\Gamma(3)$	12	0	4	$\mathfrak{A}_4$	$k+1$	0	$k-3$
$\Gamma(4)$	24	0	6	$\mathfrak{S}_4$	$2k+1$	0	$2k-5$
$\Gamma(5)$	60	0	12	$\mathfrak{A}_5$	$5k+1$	0	$5k-11$
$\Gamma(6)$	72	1	12		$6k$	1	$6k-12$
$\Gamma(7)$	168	3	24		$14k-2$	3	$14k-26$
.	.	.	.				
.							

Table for $\Gamma(N)$

name	μ	(ν_i, ν_ρ, t)	genus	coinsidence	d_2	$d_k(k\geq 4)$	$e_1(=g)$	$e_k(=d_k-t)$
$\overline{\Gamma_1(2)}$	3	(1,0,2)	0	$\overline{\Gamma_0(2)}$		$k/2+1$	0	
$\overline{\Gamma_1(3)}$	4	(0,1,2)	0	$\overline{\Gamma_0(3)}$		$[2k/3]+1$	0	
$\overline{\Gamma_1(4)}$	6	(0,0,3)	0	$\overline{\Gamma_0(4)}$		$k+1$	0	
$\overline{\Gamma_1(5)}$	12	(0,0,4)	0			$2k+1$	0	
$\overline{\Gamma_1(6)}$	12	(0,0,4)	0	$\overline{\Gamma_0(6)}$		$2k+1$	0	
.	.	.	.					
.								

Table for $\Gamma_1(N)$

4 Hecke operators and Hecke eigen forms

4.1 Preparatory consideration

Definition 4.1. *Let $\mathcal{R}$ be the set of all lattices in $\boldsymbol{C}$, and let $X_{\mathcal{R}}$ be the free $\boldsymbol{Z}$ module generated by $\mathcal{R}$. We define an operator*

$$T(n)\Lambda = \sum_{[\Lambda:\Lambda']=n} \Lambda'$$

for $\Lambda \in \mathcal{R}$ and make a natural extension on $X_{\mathcal{R}}$. We call it a Hecke correspondence. Set

$$\mathcal{K}_\alpha \Lambda = \alpha\Lambda.$$

Remark 4.1. *For a lattice $\Lambda(\omega_1, \omega_2)$ in $\boldsymbol{C}$, denote the volume of the parallelogram $\{z = k\omega_1 + \ell\omega_2 : 0 \le k \le 1, 0 \le \ell \le 1\}$ by $\mathrm{vol}(\Lambda)$. For a sublattice $\Lambda' \subset \Lambda$ it holds*

$$[\Lambda : \Lambda'] = \mathrm{vol}(\Lambda')/\mathrm{vol}(\Lambda).$$

When $n = p$: prime, we have $p + 1$ sublattices with $[\Lambda : \Lambda'] = p$. In fact, for $\Lambda =< 1, \tau >$ we have the choices (see Figure 4.1):

$$< 1, p\tau >, < p, \tau >, < p, 1 + \tau >, \ldots, < p, p - 1 + \tau > .$$

Note that always it holds $p\Lambda \subset \Lambda'$.

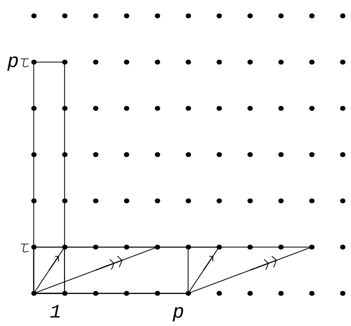


Figure 4.1 Sublattices with index p

Proposition 4.1. *We have*

(1) $\mathcal{K}_\alpha \mathcal{K}_\beta = \mathcal{K}_{\alpha\beta}$,

(2) $\mathcal{K}_\alpha T(n) = T(n)\mathcal{K}_\alpha$,

(3) $T(m)T(n) = T(mn) \quad ((m, n) = 1)$,

(4) $T(p^n)T(p) = T(p^{n+1}) + pT(p^{n-1})\mathcal{K}_p \quad (p : \textit{prime})$.

[proof]. We can obtain (1)(2) easily.

(3) Suppose $\Lambda'' \subset \Lambda, [\Lambda : \Lambda''] = mn$. According to the isomorphism $\boldsymbol{Z}/mn\boldsymbol{Z} \cong \boldsymbol{Z}/m\boldsymbol{Z} \times \boldsymbol{Z}/n\boldsymbol{Z}$ we can find a intermediate sublattice Λ' such that $\Lambda'' \subset \Lambda' \subset \Lambda$ with $[\Lambda : \Lambda'] = n, [\Lambda' : \Lambda''] = m$ in a unique way. It shows the property.

(4) We consider $T(p^n)T(p)\Lambda, T(p^{n+1})\Lambda, T(p^{n-1})\mathcal{K}_p\Lambda$. They are elements in $X_{\mathcal{R}}$ composed of sublattices of index p^{n+1}. Set

$$\begin{cases} T(p^n)T(p)\Lambda = \sum a(\Lambda'')\Lambda'' \\ T(p^{n+1})\Lambda = \sum b(\Lambda'')\Lambda'' = \sum_{[\Lambda:\Lambda'']=p^{n+1}} \Lambda'' \\ T(p^{n-1})\mathcal{K}_p\Lambda = \sum c(\Lambda'')\Lambda'', \end{cases}$$

where Λ'' be a sublattice with $[\Lambda : \Lambda''] = p^{n+1}$. We are requested to show $a = b + pc (= 1 + pc)$.
(i) The case Λ'' is not a sublattice of $p\Lambda$. By definition we have $c(\Lambda'') = 0$. On the other hand we have

$$a(\Lambda'') = \sharp\{\Lambda' : [\Lambda : \Lambda'] = p, \Lambda'' \subset \Lambda' \subset \Lambda\}.$$

As we observed in Figure 4.1, this Λ' necessarily contains $p\Lambda$. Note that $\Lambda'/p\Lambda$ is a index p subgroup of $\Lambda/p\Lambda \cong \boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/p\boldsymbol{Z}$. It is determined by an element of order p in it. Here take an element $\lambda \in \Lambda'' - p\Lambda$. It is regarded as an element of $\Lambda'/p\Lambda$ with order p. So it determines Λ' in a unique way. It means $a = 1$.
(ii) The case Λ'' is a sublattice of $p\Lambda$. By definition $T(p^{n-1})\mathcal{K}_p\Lambda = T(p^{n-1})(p\Lambda)$, so $c = 1$. And we have $b + pc = 1 + p$. As we already saw, $[\Lambda : \Lambda'] = p$ implies $p\Lambda \subset \Lambda'$. So especially $\Lambda'' \subset \Lambda'$. Namely we have $a = p + 1$.
By the above argument we obtained the required equality.

q.e.d.

Corollary 4.1. *For prime number p, $T(p^n)$ is a polynomial of $T(p)$ and $\mathcal{K}_p$.*

Corollary 4.2. *For prime number p, the algebra $\boldsymbol{Z}(T(p), \mathcal{K}_p)$ is commutative and contains every $T(p^n)$*

[proof of the corollaries]. These are direct consequence of (3)(4) in the proposition.

q.e.d.

We consider a function F on $X_{\mathcal{R}}$ satisfying the following condition:

$$\begin{aligned} &F(\alpha\Lambda) = \alpha^{-k}F(\Lambda) \\ &F(\sum_i \Lambda_i) = \sum_i F(\Lambda_i) \\ &F(\Lambda(1,z)) \text{is a meromorphic function on } \boldsymbol{H}. \end{aligned}$$

We call this function a meromorphic function of weight k defined on $X_{\mathcal{R}}$. For such a function we define

$$\begin{aligned} \mathcal{K}_\alpha F(\Lambda) &:= F(\mathcal{K}_\alpha \Lambda) = F(\alpha\Lambda), \\ T(n)F(\Lambda) &:= F(T(n)\Lambda) = \sum_{[\Lambda:\Lambda']=n} F(\Lambda'), \end{aligned}$$

and by the natural extension we define these operations for every element of $X_{\mathcal{R}}$. We have

$$\mathcal{K}_\alpha(T(n)F) = T(n)(\mathcal{K}_\alpha F) = \alpha^{-k}T(n)F.$$

So we obtain a meromorphic function $T(n)F$ of weight k again.

Proposition 4.2. *For a meromorphic function F of weight k on $X_{\mathcal{R}}$ we have*

$$\begin{cases} T(m)T(n)F = T(mn)F \quad ((m,n) = 1), \\ T(p)T(p^n)F = T(p^{n+1})F + p^{1-k}T(p^{n-1})F \quad (p : \textit{prime}) \end{cases}$$

[proof]. This is only a paraphrase of Proposition 4.1 .

4.2 Hecke operator $T(n)$

Lemma 4.1. *Let $\Lambda =< \omega_1, \omega_2 >$ be a lattice in $\boldsymbol{C}$. Set*

$$S_n = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\boldsymbol{Z}) : ad = n, a \geq 1, 0 \leq b < d\}.$$

For $\sigma \in S_n$, we set $\Lambda_\sigma = \langle \omega_1', \omega_2' \rangle = \langle a\omega_1 + b\omega_2, d\omega_2 \rangle$. Then the map $\sigma : S_n \to \Lambda(n) = \{\Lambda' \subset \Lambda : [\Lambda : \Lambda'] = n\}$ defined by $\sigma(\Lambda) = \Lambda_\sigma$ is bijective.

[proof]. By Remark 4.1 we know $[\Lambda, \Lambda_\sigma] = n$. If we consider the right cosets $\Gamma\sigma_1, \Gamma\sigma_2$ for $\sigma_1, \sigma_2 \in S_n$, the injectivity follows. So let us suppose a sublattice Λ' with $[\Lambda : \Lambda'] = n$. Set

$$Y_1 = \Lambda/(\Lambda' + \boldsymbol{Z}\omega_2), Y_2 = \boldsymbol{Z}\omega_2/(\Lambda' \cap \boldsymbol{Z}\omega_2).$$

These are cyclic groups generated by the mages of ω_1, ω_2, respectively. Set a and d be thier orders, respectively. By the exact sequence

$$0 \to Y_2 \to \Lambda/\Lambda' \to Y_1 \to 0$$

we have $ad = n$. We have $d\omega_2 \in \Lambda'$. So, put $\omega_2' = d\omega_2$. On the other hand we have $a\omega_1 \in \Lambda' + \boldsymbol{Z}\omega_2$. So we can find $\omega_1' = a\omega_1 + b\omega_2 \in \Lambda'$. Considering the indices, the lattice $< \omega_1', \omega_2' >$ should coincides with Λ'.

q.e.d.

Let F be a meromorphic function of weight k on $X_{\mathcal{R}}$.Then

$$f(z) := F(\Lambda(1, z))$$

is a meromorphic modular form of weight k for Γ, and vice versa. For it, note that

$$f(\frac{-1}{z}) = F(\Lambda(1, \frac{-1}{z})) = F(\frac{-1}{z})\Lambda(-z, 1)) = (-z)^k F(\Lambda(1, z)) = (-z)^k f(z).$$

Definition 4.2. *For a meromorphic modular form $f(z)$ of weight k we define*

$$T(n)f(z) := n^{k-1}T(n)F(\Lambda(1, z)).$$

So we have

$$T(n)f(z) = n^{k-1} \sum_{a \geq 1, ad=n, 0 \leq b < d} d^{-k} f(\frac{az+b}{d}).$$

$T(n)$ is said to be a Hecke operator.

Proposition 4.3. *Let f be a meromorphic modular form of weight k.*

(1) *$T(n)f$ is a meromorphic modular form of weight k also,*

(2) *$T(m)T(n)f = T(mn)f \quad ((m, n) = 1)$,*

(3) *$T(p)T(p^n)f = T(p^{n+1})f + p^{k-1}T(p^{n-1})f$.*

[proof]. To make clear our argument, we denote $\tilde{T}(n)$ the operator $T(n)$ to the functions on $X_{\mathcal{R}}$.
(1) is apparent.
(2) Using Proposition 4.2 we have

$$\text{LHS} = T(m)(n^{k-1}\tilde{T}(n)F(\Lambda(1, z)) = n^{k-1}m^{k-1}\tilde{T}(m)\tilde{T}(n)F(\Lambda(1, z)) = (mn)^{k-1}\tilde{T}(mn)F(\Lambda(1, z)).$$

By definition $(mn)^{k-1}\tilde{T}(mn)F(\Lambda(1, z)) = T(mn)f(z)$. So we obtain the assertion.
(3) We have

$$\begin{aligned}\text{LHS} &= T(p)((p^n)^{k-1}\tilde{T}(p^n)F(\Lambda(1, z)) = (p^n)^{k-1}p^{k-1}\tilde{T}(p)\tilde{T}(p^n)F(\lambda(1, z)) \\ &= (p^{n+1})^{k-1}(\tilde{T}(p^{n+1})F(\Lambda(1, z)) + p^{1-k}\tilde{T}(p^{n-1})F(\Lambda(1, z)) \\ &= (p^{n+1})^{k-1}\tilde{T}(p^{n+1})F(\Lambda(1, z)) + (p^n)^{k-1}\tilde{T}(p^{n-1})F(\Lambda(1, z))\end{aligned}$$

On the other hand

$$\begin{aligned}\text{RHS} &= (p^{n+1})^{k+1}\tilde{T}(p^{n+1})F(\Lambda(1, z)) + p^{k-1}(p^{n-1})^{k-1}\tilde{T}(p^{n-1})F(\Lambda(1, z)) \\ &= (p^{n+1})^{k+1}\tilde{T}(p^{n+1})F(\Lambda(1, z)) + (p^n)^{k-1}\tilde{T}(p^{n-1})F(\Lambda(1, z)).\end{aligned}$$

So we obtain the assertion.

q.e.d.

Proposition 4.4. *(Explicit description of $T(n)$)*

Let f be a meromorphic modular form of weight k. Suppose we have a "q" expansion

$$f(z) = \sum_{m \in \boldsymbol{Z}} c(m) q^m.$$

Then we have

$$\begin{cases} T(n)f(z) = \sum_{m \in \boldsymbol{Z}} \gamma(m) q^m \\ \\ \gamma(m) = \sum_{a|(m,n), a \geq 1} a^{k-1} c(\frac{mn}{a^2}). \end{cases} \tag{4.1}$$

[proof]. By definition we have

$$T(n)f(z) = n^{k-1} \sum_{ad=n, a \geq 1, 0 \leq b < d} d^{-k} \sum_{m \in \boldsymbol{Z}} c(m) e^{2\pi i m(az+b)/d}.$$

Here we have

$$\sum_{0 \leq b < d} e^{2\pi i b m/d} = \begin{cases} d & d|m \\ 0 & \text{otherwise.} \end{cases}$$

Put $m' = \frac{m}{d}$. Then it holds

$$T(n)f(z) = n^{k-1} \sum_{ad=n, a \geq 1, m' \in \boldsymbol{Z}} d^{-k+1} c(m'd) q^{am'}.$$

Re arrange the sum following the power of q:

$$= \sum_{\mu \in \boldsymbol{Z}} q^{\mu} \sum_{a|(n,\mu), a \geq 1} \left(\frac{n}{d}\right)^{k-1} c\left(\frac{\mu d}{a}\right)$$

So we obtain the assertion.

q.e.d.

Corollary 4.3.

$$\gamma(0) = \sigma_{k-1}(n) c(0), \ \gamma(1) = c(n).$$

Corollary 4.4. *For $n = p$: prime, we have*

$$\gamma(m) = \begin{cases} c(pm) & (p, m) = 1 \\ c(pm) + p^{k-1} c(\frac{m}{p}) & p|m. \end{cases}$$

Corollary 4.5. *$T(n)$ is a linear operator on $M_k(\Gamma)$ and $S_k(\Gamma)$.*

4.3 Hecke eigen form

Definition 4.3. *$f \in M_k(\Gamma)$ is said to be a Hecke eigen form if it is a eigen form for every $T(n)$ $(n = 1, 2, \cdots)$. It is called a normalized Hecke eigen form if its Fourier expansion has the form $f(z) = c(0) + q + c(2)q^2 + \cdots$.*

Theorem 4.1. *Let $f(z) = \sum_{n \geq 0} c(n) q^n$ be amodular form of weight k $(k > 0)$. Suppose f is an eigen function for every $T(n)$, and put $T(n)f = \lambda(n) f$ $(n = 1, 2, \ldots)$. Then*
(a) $c(1) \neq 0$,
(b)

$$c(n) = \lambda(n) c(1) \quad (n = 2, 3, \ldots).$$

[proof]. Consider

$$T(n)f = \lambda(n)c(0) + \lambda(n)c(1)q + \cdots .$$

By Corollary 4.3 to Proposition 4.4we have

$$T(n)f = \sigma_{k-1}(n)c(0) + c(n)q + \cdots .$$

Hence $c(n) = \lambda(n)c(1) \quad (n = 2, 3, \ldots)$. If $c(1) = 0$, we have $c(n) = 0 \quad (n = 1, 2, \ldots)$. It means that f is a constant. But a constant function is not a modular form of positive weight. So we obtain the assertion (a)(b) at the same time.

q.e.d.

Corollary 4.6. *If f, g are eigen forms of weight k with same eigen values $\{\lambda(n)\}$, then differs at most with a constant factor.*

Corollary 4.7. *Let $f = \sum_{n\geq 0} c(n)q^n$ be a normalized Hecke eigen form. Then we have*
(1) $c(m)c(n) = c(mn) \quad ((m, n) = 1)$
(2) $c(p)c(p^n) = c(p^{n+1}) + p^{k-1}c(p^{n-1})$

[proof]. Direct consequence of Proposition 4.3.

q.e.d.

Set

$$\Phi_f(s) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s}.$$

This is convergent on the region $\{s \in \boldsymbol{C} : \mathrm{Re}\ (s) > k\}$.
[Theorem according to Hecke]
(1) For a cusp form $f(z) = \sum c(n)q^n$ of weight k, we have

$$c(n) = O(n^k).$$

(2) For a modular form $f(z)$ that is not a cusp form, we have

$$c(n) = O(n^{k-1}).$$

For example see the case $f(z) = E_k(z)$.

[Convergence of $\Phi_f(s)$]
For some positive number A, it holds

$$\left|\frac{c(n)}{n^{k+\varepsilon}}\right| \leq \frac{A}{n^{k+\varepsilon-(k-1)}} = \frac{A}{n^{1+\varepsilon}}.$$

So $\Phi_f(s)$ converges on Re $s > k$.

Corollary 4.8. *For a normalized Hecke eigen form $f(z)$, it holds*

$$\Phi_f(s) = \prod_p \frac{1}{1 - c(p)p^{-s} + p^{k-1} \cdot p^{-2s}}.$$

[proof]. By We have

$$\sum_{n\geq 1} \frac{c(n)}{n^s} = \prod_p (1 + c(p)p^{-s} + \cdots + c(p^m)p^{-ms} + \cdots).$$

Putting

$$\Phi_{f,p}(T) = 1 - c(p)T + p^{k-1}T^2,$$

we may show

$$\sum_{n=0}^{\infty} c(p^n)T^n = \frac{1}{\Phi_{f,p}(T)}.$$

4.4 Examples

(a)

Proposition 4.5. *The Eisenstein series $G_k(z)$ $(k \geq 4, even)$ is a Hecke eigen form. The normalized eigen form is given by*

$$\left(-\frac{B_k}{2k}\right) E_k(z) = \left(-\frac{B_k}{2k}\right) + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

So $T(n)$ has the eigen value $\lambda(n) = \sigma_{k-1}(n)$, and the corresponding Dirichlet series is given by $\zeta(s)\zeta(s-k+1)$.

[proof]. Because of Proposition 4.3 we may consider only for the case $n = p$: prime. We can regard $G_k(z)$ as a function $F(\Lambda(1,z))$ on $X_{\mathcal{R}}$. Namely

$$F(\Lambda) = F(\Lambda(1,z)) = G_k(\Lambda) = \sum_{\gamma \in \Lambda}' \frac{1}{\gamma^k}.$$

We have

$$\tilde{T}(p) F(\Lambda) = \sum_{[\Lambda:\Lambda']=p} \sum_{\gamma \in \Lambda'} \frac{1}{\gamma^k}.$$

In case $\gamma \in p\Lambda$ it belongs to all $p+1$ sublattices with $[\Lambda : \Lambda'] = p$, and in case $\gamma \notin p\Lambda$ it belongs to only one index p sublattice. So

$$= F(\Lambda) + p \sum_{\gamma \in p\Lambda} \frac{1}{\gamma^k} = F(\Lambda) + pF(p\Lambda) = (1 + p^{1-k}) F(\Lambda)$$

Because $T(p) G_k(z) := p^{k-1} \tilde{T}(p) F(\Lambda(1,z))$, we have

$$T(p) G_k(z) = \sigma_{k-1}(p) G_k(z).$$

For the Dirichlet series, we have

$$\sum_{n=1}^{\infty} \frac{\sigma_{k-1}(n)}{n^s} = \sum_{a,d \geq 1} \frac{a^{k-1}}{a^s d^s} = \left(\sum_{d \geq 1} \frac{1}{d^s}\right) \left(\sum_{a \geq 1} \frac{1}{a^{s+1-k}}\right) = \zeta(s)\zeta(s-k+1).$$

5 Theta functions

Definition 5.1. *Let $a, b \in \{0,1\}$. The infinte series*

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (\tau) = \sum_{n \in \boldsymbol{Z}} \exp[\pi i (n + \frac{a}{2})^2 \tau + 2\pi i (n + \frac{a}{2}) \frac{b}{2}], \ a, b \in \{0,1\}$$

converges on $\boldsymbol{H}$ as a function of τ, and it becomes to be holomorphic there. It is called a <u>*Jacobi theta constant*</u>. *Note that $\vartheta \begin{bmatrix} 1 \\ 1 \end{bmatrix} (\tau)$ becomes to be constant zero, and others are non constant function.*

Put $\tilde{q} = \exp[\pi i \tau]$. We can rewrite the definition in the form of Fourier series:

$$\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\tau) = \sum_{n \in \boldsymbol{Z}} \tilde{q}^{n^2}, \vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (\tau) = \sum_{n \in \boldsymbol{Z}} (-1)^n \tilde{q}^{n^2}, \vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix} (\tau) = \sum_{n \in \boldsymbol{Z}} \tilde{q}^{(n+\frac{1}{2})^2}.$$

Theorem 5.1. (Jacobi's identity)

$$\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix}^4 (\tau) = \vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix}^4 (\tau) + \vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix}^4 (\tau).$$

The Jacobi theta constants have the following automorphic behavior:

Theorem 5.2.

$$\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\tau+1) = \vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (\tau),\ \vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (\tau+1) = \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\tau),\ \vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix} (\tau+1) = \exp[\frac{\pi i}{4}]\vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix} (\tau),$$
$$\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\frac{-1}{\tau}) = \exp[\frac{-\pi i}{4}]\sqrt{\tau}\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (\tau),$$
$$\vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (\frac{-1}{\tau}) = \exp[\frac{-\pi i}{4}]\sqrt{\tau}\vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix} (\tau),$$
$$\vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix} (\frac{-1}{\tau}) = \exp[\frac{-\pi i}{4}]\sqrt{\tau}\vartheta \begin{bmatrix} 0 \\ 1 \end{bmatrix} (\tau) \quad (\sqrt{\tau} \in \boldsymbol{H}).$$

We note here the above inversion formula is equivalent to the reflection formula of the Riemann *zeta* function via "Mellin transformation". By this theorem we have

Proposition 5.1. $\vartheta \begin{bmatrix} a \\ b \end{bmatrix}^4 (\tau) \in M_2(\Gamma(2)),\ (a, b \in \{0, 1\}).$

For the Legendre normal form

$$y^2 = x(x-1)(x-\lambda)$$

of a complex torus $T(\tau) = \boldsymbol{C}/(\boldsymbol{Z} + \boldsymbol{Z}\tau)$, by the same argument as for $j(\tau)$ we have

Theorem 5.3.

$$\lambda(\tau) = \frac{\vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix}^4 (\tau)}{\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix}^4 (\tau)}.$$

According to this theorem we can obtain:

Theorem 5.4.

$$M(\Gamma(2)) = \boldsymbol{C}[\vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix}^4 (\tau), \vartheta \begin{bmatrix} 1 \\ 0 \end{bmatrix}^4 (\tau)].$$

You can see precise descriptions of the modular function for some other congruence subgroups in [5] and [4](Klein).

6 An example: how it works the theory applied to number theoretic problems

As an example of application of the theory of modular form, here we show the following classical theorem due to Legendre and Jacobi:

Theorem 6.1. *For a positive integer n, let $a(n)$ be the number of integer solutions for*

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n.$$

We have

$$a(n) = \begin{cases} 8\sigma_1(n), & (n: odd) \\ 24\sigma_1(n_0), & (n = 2^r n_0, (2, n_0) = 1). \end{cases}$$

Especially every positive integer can be expressed as a sum of 4 *squares.*

The theorem itself is very classical, but the method is very suggestive. We have various applications with the same philosophy. You can see one enlarged application for the congruence number problem in [3] (Koblitz).

At first we note:
[Fact 1]
Set $\Theta(z) = \vartheta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (2z)$. Then we have

$$\Theta(z)^4 = 1 + \sum_{n=1}^{\infty} a(n) q^n \quad (q = e^{2piiz}).$$

We shall work in the space $M_2(\overline{\Gamma_0(4)}) = M_2(\overline{\Gamma_1(4)})$. Recall
[Fact 2]
(1) $\overline{\Gamma_1(4)} = \langle T, \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \rangle$. (2) $\dim M_2(\overline{\Gamma_1(4)}) = 2$.

By using the automorphic property of the Dedekind η function we can show
[Fact 3]
(1)

$$F(z) = \frac{\eta^8(4z)}{\eta^4(2z)} \in M_2(\overline{\Gamma_1(4)}).$$

(2)

$$F(z) = \frac{\eta^8(4z)}{\eta^4(2z)} = q \prod_{n=1}^{\infty} (1 - q^{4n})^4 (1 + q^{2n})^4 = \sum_{\text{odd } n>0} \sigma_1(n) q^n = q + 4q^3 + 6q^5 + \cdots .$$

By the automorphic property of $\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z)$ (and the behavior at the cusps) we can show
[Fact 4]

$$\Theta(z)^4 \in M_2(\overline{\Gamma_1(4)}).$$

[Hecke operator on $M_k(\overline{\Gamma_0(N)})$]
We can define Hecke operators acting on $M_k(\overline{\Gamma_0(N)})$ (k : even), and we have similar properties as those acting on $M_k(\overline{\Gamma})$.

Proposition 6.1. *Let k be an even integer. Let p be a prime number. For $f(z) = \sum_{n=0}^{\infty} a(n) q^n \in M_k(\overline{\Gamma_0(N)})$ $(q = e^{2\pi iz})$, we have*

$$T(p)f(z) = \sum_{n=0}^{\infty} b(n) q^n, \ b(n) = \begin{cases} a(pn) & (p|N) \, or \, (p, n) = 1 \\ a(pn) + p^{k-1} a(\frac{n}{p}) & otherwise \end{cases}$$

We obtain the same properties as Prop. 4.3,

Proposition 6.2. *Let f be a meromorphic modular form of weight k for $\overline{\Gamma_0(N)}$.*
(1) $T(m)T(n)f = T(mn)f \quad ((m, n) = 1)$,
(2) $T(p^{n+1})f = \begin{cases} T(p)T(p^n)f - p^{k-1} T(p^{n-1})f & ((p, N) = 1), \\ T(p)^{n+1} f & (p|N). \end{cases}$

So we can use those two propositions as a definition of $T(n)$ for $M_k(\overline{\Gamma_0(N)})$. As for Hecke eigen forms we have the paraphrase of Theorem 4.1 :

Theorem 6.2. *Let $f(z) = \sum_{n\geq 0} c(n)q^n \in M_k(\overline{\Gamma_0(N)})$. Suppose f is an eigen form for every $T(n)$, and put $T(n)f = \lambda(n)f \quad (n = 1, 2, \ldots)$. Then*
(a) $c(1) \neq 0$,
(b) $c(n) = \lambda(n)c(1) \quad (n = 2, 3, \ldots)$.

We consider a complementary operator on $M_k(\overline{\Gamma_0(N)})$:

$$[\gamma]_k : f(z) \mapsto (\det \gamma)^{k/2}(cz + d)^{-k} f(\gamma(z)), \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\boldsymbol{Q}).$$

Especially we use

$$[\alpha_4]_k : f(z) \mapsto 4^{k/2}(4z)^{-k} f(\frac{-1}{4z}), \quad \alpha_4 = \begin{pmatrix} 0 & -1 \\ 4 & 0 \end{pmatrix}.$$

[Fact 5]
(1) $[\alpha_4]_2$ is a linear transformation of the vector space (of dimension 2) $M_2(\overline{\Gamma_0(4)})$ of order 2.
(2) We have $[\alpha_4]_2(\Theta^4(z)) = -\Theta^4(z)$, and $F(z)$ is not an eigen form of $[\alpha_4]_2$. So $[\alpha_4]_2$ has different eigen values $+1$ and -1.
[Fact 6]
(0) $T(2)F(z) = 0,\ T(2)\Theta^4(z) = \Theta^4(z) + 16F(z)$,
(1) For an odd positive integer n, $[\alpha_4]_2 T(n) = T(n)[\alpha_4]_2$ and $T(2)T(n) = T(n)T(2)$.
(2) An eigen form for $[\alpha_4]_2$ is an eigen form of every $T(n)$ for every odd positive integer n, and for an eigen form for $T(2)$, also.
By Fact 6, we have three eigenforms $F, \Theta^4 + 16F, \Theta^4$ of $T(n)$ for every odd positive integer n. That means $T(n)$ acts on $M_2(\overline{\Gamma_0(4)})$ as a constant map.
[Conclusion]
Apply Theorem 6.2 to $F(z) = 1 + \sum_{\text{odd } n>0} \sigma_1(n)q^n$. Then we know $T(n)$ is a constant map $\lambda(n)\mathrm{id} = \sigma_1(n)\mathrm{id}$. Again apply Theorem 6.2 to $\Theta^4(z) = 1 + \sum_{n=1}^{\infty} a(n)q^n$. Then we obtain

$$a(n) = a(1)\lambda(n) = 8\sigma_1(n), \quad n : \text{odd}.$$

To obtain the result for even n, we need some more detailed argument, but the method is quite the same.

[References]

1. D. Mumford, Tata Lectures on Theta I, (II, III,) Birkhäuser.

2. J.P. Serre, Cours d'arithmetiques, PUF.

3. N. Koblitz, Introduction to Elliptic Curves and Modular Forms, Springer GTM.

4. F. Klein, Gesammelte Mathematische Abhandlungen, III, Springer 1923.

5. F. Klein and R. Fricke, Vorlesungen über die Theorie der Elliptischen Modulfunctionen, Zweiter Band, Especially "Fünfter Abschnitt, Viertes Kapitel", Teubner, 1892.

6. Y. Kawada, Theory of modular functions of one variable, Seminary Note, Univ. Tokyo,1964(in Japanese)