Notes on Modular Forms

Dan Schultz

March 3, 2024

Contents

0.1 Notation

Symbol	Meaning
q	$e^{2\pi i\tau}$
q^a	$e^{2\pi ia\tau}$ (not $(e^{2\pi i\tau})^a$)
q_z^a	$e^{2\pi iaz}$
$e(z)$	$\exp(2\pi iz)$
ζ_b^a	root of unity $e(a/b)$
$\log z$	the logarithm with $-\pi < \operatorname{Im}\log z \le \pi$
a^b	$\exp b \log a$

$(x;q)_n$	$\prod_{k=0}^{n-1}(1-xq^k)$
$(x;q)_\infty$	$\prod_{k=0}^{\infty}(1-xq^k)$, for $\|q\|<1$
$\wp(z\|\omega_1,\omega_2)$	Weierstrass $\wp$ function for the lattice $\omega_1\mathbb{Z}+\omega_2\mathbb{Z}$
$\zeta(z\|\omega_1,\omega_2)$	Weierstrass ζ function
$\sigma(z\|\omega_1,\omega_2)$	Weierstrass σ function
$\wp(z\|\tau)$	$\wp(z\|\tau,1)$
$\eta(\tau)$	Dedekind's η function $q^{1/24}(q,q)_\infty$
$\log\eta(\tau)$	analytic logarithm $\frac{2\pi i\tau}{24}-\sum_{n=1}^{\infty}\frac{q^n}{n(1-q^n)}$
$j(\tau)$	$E_4(\tau)^3\eta(\tau)^{-24}$
$\gamma_2(\tau)$	$j^{1/3}=E_4(\tau)\eta(\tau)^{-8}$
$\gamma_3(\tau)$	$(j-1728)^{1/2}=E_6(\tau)\eta(\tau)^{-12}$
$\Theta[\vec{v}](z\|\tau)$	general elliptic Θ function with characteristic $\vec{v}$
$\Theta_i(z\|\tau)$	Jacobi's four Θ functions with half-integer characteristics
$\Theta_i(z)$	$\Theta_i(z\|\tau)$
$\Theta_i(\tau)$	$\Theta_i(0\|\tau)$
$\Gamma(N)$	$\{M\in\mathrm{SL}_2(\mathbb{Z})\mid M\equiv\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\bmod N\}$
$\Gamma_1(N)$	$\{M\in\mathrm{SL}_2(\mathbb{Z})\mid M\equiv\left(\begin{smallmatrix}1&*\\0&1\end{smallmatrix}\right)\bmod N\}$
$\Gamma^1(N)$	$\{M\in\mathrm{SL}_2(\mathbb{Z})\mid M\equiv\left(\begin{smallmatrix}1&0\\*&1\end{smallmatrix}\right)\bmod N\}$
$\Gamma^0(N)$	$\{M\in\mathrm{SL}_2(\mathbb{Z})\mid M\equiv\left(\begin{smallmatrix}*&0\\*&*\end{smallmatrix}\right)\bmod N\}$
$\Gamma_0(N)$	$\{M\in\mathrm{SL}_2(\mathbb{Z})\mid M\equiv\left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)\bmod N\}$
$\Gamma_0^0(N)$	$\{M\in\mathrm{SL}_2(\mathbb{Z})\mid M\equiv\left(\begin{smallmatrix}*&0\\0&*\end{smallmatrix}\right)\bmod N\}$
$u.v$	dot product of two vectors
$u.M$	product of vector u interpreted as a row vector and the matrix M
$M.v$	product of matrix M and the vector v interpreted as a column vector

Chapter 1

Introduction

The generating functions for many interesting combinatorial objects turn out to be modular forms.

1.1 Partitions and the η function

We have

$$\begin{aligned}\frac{1}{(q;q)_\infty} &= (1+q+q^2+q^3+\cdots)(1+q^2+q^4+q^6+\cdots)(1+q^3+q^6+q^9+\cdots)\cdots \\ &= \sum_{n=0}^{\infty} p(n)q^n,\end{aligned}$$

where $p(n)$ is the number of partitions of n. We have the properties

- $p(5n+4) \equiv 0 \mod 5$
- $p(7n+5) \equiv 0 \mod 7$
- $p(11n+6) \equiv 0 \mod 11$
- $p(5^4 13n + 111247) \equiv 0 \mod 13$ (see [3])

The three primes $5, 7, 11$ are unique in this way. Similar congruences hold at powers of these primes.

1.2 Sums of squares and the θ function

Set

$$\theta(\tau) = \sum_{n\in\mathbb{Z}} q^{n^2}.$$

Then, the generating function for $\#\{(x_1,\ldots,x_k)|n = x_1^2+\cdots+x_k^2\}$, which is the number of representations of n by the sum of k squares, is $\theta(\tau)^k$. If χ_4 is the non-trivial character modulo 4 and $4|c$ and $ad-bc=1$, will we see that θ satisfies the weight $1/2$ relation

$$\theta\left(\frac{a\tau+b}{c\tau+d}\right) = \left(\frac{c}{d}\right)\chi_4(d)^{-1/2}\sqrt{c\tau+d}\,\theta(\tau),$$

and characterize all functions that satisfy even powers of this functional equation. This leads to and easy proof of

$$\{(x,y)\in\mathbb{Z}^2|n = x^2+y^2\} = 4\sum_{d|n}\chi_4(d).$$

Similar formulas exists for other θ functions.

$$\{(x,y)\in\mathbb{Z}^2|n=x^2+xy+y^2\}=6\sum_{d|n}\chi_3(d).$$

1.3 Ramanujan's τ Function

Define $\tau(n)$ by

$$\eta(\tau)^{24}=q(q;q)_\infty^{24}=:\sum_{n=1}^{\infty}\tau(n)q^n.$$

The following properties were observed by Ramanujan.

- $\tau(mn)=\tau(m)\tau(n)$ for $(m,n)=1$
- $\tau(p^{k+1})=\tau(p^k)\tau(p)-p^{11}\tau(p^{k-1})$
- $\tau(p)\le 2p^{11/2}$
- $\tau(n)\equiv\sigma_{11}(n) \mod 691$

The weight 12 relation is satisfied by $\eta(\tau)^{24}$ is

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right)^{24}=(c\tau+d)^{12}\eta(\tau)^{24}.$$

The first two are equivalent to the Euler product

$$f(s)=\sum_{n=1}^{\infty}\frac{\tau(n)}{n^s}=\prod_p\frac{1}{1-\tau(p)p^{-s}+p^{11-2s}},$$

and the weight 12 transformation formula gives the reflection formula

$$\frac{f(s)\Gamma(s)}{(2\pi)^s}=\frac{f(12-s)\Gamma(12-s)}{(2\pi)^{12-s}}.$$

1.4 Mock Modular Forms

By considering the Durfee square, we have

$$\frac{1}{(q;q)_\infty}=\sum_{n=0}^{\infty}\frac{q^{n^2}}{(q;q)_n^2},$$

which is essentially a (weak) modular form of weight $-1/2$. The function

$$f(\tau)=\sum_{n=0}^{\infty}\frac{q^{n^2}}{(-q;q)_n^2}$$

turns out to not be modular, but can be made modular by adding some non-holomorphic function to it. Set

$$F(z)=q_z^{-1}f(24z)+\sqrt{-8}\int_{-\bar{z}}^{i\infty}\frac{\sum_{n\in\mathbb{Z}}\chi_{12}(n)nq^{n^2}}{\sqrt{-i(\tau+z)}}d\tau.$$

If $ad-bc=1$ and $144|c$, we have

$$F\left(\frac{a\tau+b}{c\tau+d}\right)=\left(\frac{12c}{d}\right)\chi_4(d)^{-1/2}\sqrt{c\tau+d}F(\tau).$$

1.5 Special Values of the j Function

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field and let $\mathbb{Z} + \mathbb{Z}\tau$ be its ring of integers. Then, $j(\tau)$ is an algebraic integer of degree $h(-d)$ over $\mathbb{Q}$, and $K(j(\tau))$ is the maximal unramified Abelian extension of K.

Chapter 2

Elliptic Functions and Basic Modular Forms on $\mathrm{SL}_2(\mathbb{Z})$

2.1 Theory of Elliptic Functions

Definition 2.1.1. *Let $\omega_1, \omega_2 \in \mathbb{C}$ with $\mathrm{Im}(\omega_1/\omega_2) > 0$. An elliptic function modulo $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is a meromorphic function $\mathbb{C} \to \mathbb{C}$ satisfying*

$$f(z) = f(z + \omega_1) = f(z + \omega_2).$$

For the order of a non-constant function at a point z_0, we say $\mathrm{ord}_{z_0}(f(z)) = n$ if

$$f(z) = (z - z_0)^n(c + O(z - z_0)), \quad c \neq 0,$$

and $\mathrm{ord}\, f(z)$, the (total) order of the function $f(z)$, is the number of poles of f counted according to multiplitiy (modulo Λ).

Proposition 2.1.2. *Let f be a non-constant elliptic function modulo Λ. Then,*

1. $\sum_{z \in \mathbb{C}/\Lambda} \mathrm{res}_z(f) = 0$
2. $\sum_{z \in \mathbb{C}/\Lambda} \mathrm{ord}_z(f) = 0$
3. $\sum_{z \in \mathbb{C}/\Lambda} z\, \mathrm{ord}_z(f) \in \Lambda$
4. $\mathrm{ord}\, f \geq 2$.

Proof. Let C denote the counterclockwise traversal of the parallelogram with vertices $0, \omega_2, \omega_2 + \omega_1, \omega_1$. Then,

$$\sum_{z \in \mathbb{C}/\Lambda} \mathrm{res}_z(f) = \frac{1}{2\pi i} \int_C f(z)dz = 0$$

$$\sum_{z \in \mathbb{C}/\Lambda} \mathrm{ord}_z(f) = \frac{1}{2\pi i} \int_C \frac{f'(z)}{f(z)}dz = 0$$

since integrals along opposite sides cancel. Next

$$\begin{aligned}
\sum_{z\in\mathbb{C}/\Lambda} z\,\mathrm{ord}_z(f) &= \frac{1}{2\pi i}\int_C \frac{zf'(z)}{f(z)}dz \\
&= \frac{1}{2\pi i}\int_0^{\omega_1} \frac{zf'(z)}{f(z)} - \frac{(\omega_2+z)f'(\omega_2+z)}{f(\omega_2+z)}dz \\
&\quad + \frac{1}{2\pi i}\int_0^{\omega_2} -\frac{zf'(z)}{f(z)} + \frac{(\omega_1+z)f'(\omega_1+z)}{f(\omega_1+z)}dz \\
&= -\omega_2\cdot\frac{1}{2\pi i}\int_0^{\omega_1}\frac{f'(z)}{f(z)}dz \\
&\quad + \omega_1\cdot\frac{1}{2\pi i}\int_0^{\omega_2}\frac{f'(z)}{f(z)}dz \\
&= -\omega_2\left(\frac{1}{2\pi i}\log f(z)\Big]_0^{\omega_1}\right) + \omega_1\left(\frac{1}{2\pi i}\log f(z)\Big]_0^{\omega_2}\right) \\
&\in \Lambda
\end{aligned}$$

since ω_1 (and ω_2) is a period of the function $f(z)$, so the logarithm must change by an integral multiple of $2\pi i$. For (4), if f had order 0, then it has no poles, and is thus bounded so is constant by Liouville's theorem. If f had order 1, then it has a simple pole with non-zero residue, which contradicts (1). □

Later will we see that part (3) of Proposition 2.1.2 has a converse, that is, we can construct an elliptic function with any poles and zeros that satisfy (3).

2.2 The Weierstrass $\wp$ Function

For a lattice Λ, let Λ' denote $\Lambda - 0$. Set

$$\begin{aligned}
\wp(z|\omega_1,\omega_2) &= \frac{1}{z^2} + \sum_{\omega\in\Lambda'}\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}, \\
\wp'(z|\omega_1,\omega_2) &= \sum_{\omega\in\Lambda}\frac{-2}{(z+\omega)^3}, \\
G_k(\omega_1,\omega_2) &= \sum_{\omega\in\Lambda'}\frac{1}{\omega^k}.
\end{aligned}$$

The sum for $\wp(z)$ is arranged so that

$$\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} = O(w^{-3})$$

which makes the sum over Λ absolutely convergent. The series for G_2 is not absolutely convergent, so this is not a proper definition of G_2. Later, when defining E_2, we will fix the order of summation.

Proposition 2.2.1. *Set $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Then, $\wp(z|\omega_1,\omega_2)$ is an elliptic function of order 2 mod Λ, and we have:*

1. *The power series expansion*

$$\wp(z|\omega_1,\omega_2) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}(\omega_1,\omega_2)z^{2k}.$$

2. *For $\lambda \neq 0$ and integers a, b, c, d with $ad - bc = 1$,*

$$\wp(z|\omega_1, \omega_2) = \lambda^2 \wp(\lambda z|\lambda\omega_1, \lambda\omega_2),$$
$$\wp(z|\omega_1, \omega_2) = \wp(z|a\omega_1 + b\omega_2, c\omega_1 + d\omega_2).$$

3. *The differential equation (set $g_2 = 60G_4(\omega_1, \omega_2)$, $g_3 = 140G_6(\omega_1, \omega_2)$)*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

Proof. From the definitions, it is clear that $\wp'(z)$ is elliptic modulo Λ and $\wp(z)$ is an even function. Let $\omega \in \Lambda$. Since $\wp'(z+\omega) = \wp'(z)$, it follows that $\wp(z+\omega) = \wp(z) + \eta$ for some constant η. Setting $z = -\omega/2$ shows that $\eta = 0$. For (2), set $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then,

$$\begin{aligned}
\wp(z|a\omega_1 + b\omega_2, c\omega_1 + d\omega_2) &= \frac{1}{z^2} + \sum_{\vec{n} \in \mathbb{Z}^2 - \{0,0\}} \frac{1}{(z + \vec{n}.M.(\omega_1, \omega_2)^\intercal)^2} - \frac{1}{(\vec{n}.M.(\omega_1, \omega_2)^\intercal)^2} \\
&= \frac{1}{z^2} + \sum_{\vec{m} \in \mathbb{Z}^2 - \{0,0\}} \frac{1}{(z + \vec{m}.(\omega_1, \omega_2)^\intercal)^2} - \frac{1}{(\vec{m}.(\omega_1, \omega_2)^\intercal)^2} \\
&= \wp(z|\omega_1, \omega_2).
\end{aligned}$$

Since $\det(M) = 1$, $\vec{n}.M$ ranges over all of $\mathbb{Z}^2 - \{0, 0\}$ and includes each point once, the change of variables $\vec{m} = \vec{n}.M$ is justified.

For (3),

$$\begin{aligned}
\wp'(z)^2 &= \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + O(z^2) \\
4\wp(z)^3 &= \frac{4}{z^6} + \frac{36G_4}{z^2} + 60G_6 + O(z^2) \\
60\wp(z) &= \frac{60G_4}{z^2} + O(z^2).
\end{aligned}$$

From this it is clear that $\wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z)$ is an entire elliptic function, hence it is a constant. This constant is also easily seen to be $-140G_6$. □

2.3 Eisenstein Series

Due to the homogeneity property in Proposition 2.2.1, without loss of generality we can set $\omega_1 = \tau$ and $\omega_2 = 1$. In this case we have

$$\wp(z|\tau, 1) = (c\tau + d)^{-2} \wp\left(\frac{z}{c\tau + d} \middle| \frac{a\tau + b}{c\tau + d}, 1\right),$$

which shows that the power series coefficients satisfy

$$G_{2k}\left(\frac{a\tau + b}{c\tau + d}, 1\right) = (c\tau + d)^{2k} G_{2k}(\tau, 1), \quad k \geq 2.$$

It will be convenient to have a normalization of these functions $E_{2k}(\tau)$ with $E_{2k}(i\infty) = 1$. For $k \geq 1$, set

$$\begin{aligned}
E_{2k}(\tau) &= \frac{G_{2k}(\tau, 1)}{G_{2k}(i\infty, 1)} \\
&= \frac{1}{2\zeta(2k)} \sum_{m=-\infty}^{\infty} \sum_{\substack{n=-\infty \\ (m,n) \neq (0,0)}}^{\infty} \frac{1}{(m\tau + n)^{2k}}.
\end{aligned}$$

Proposition 2.3.1. *The Eisenstein series E_{2k} have the following properties.*

1. *For $k \geq 1$, we have*
$$E_{2k}(\tau) = 1 + \frac{2}{\zeta(1-2k)} \sum_{n=1}^{\infty} \frac{n^{2k-1}q^k}{1-q^k}.$$

2. *For $k \geq 2$, $E_{2k}(\tau)$ is a holomorphic function $\mathbb{H} \to \mathbb{C}$ satisfying*
$$E_{2k}\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{2k} E_{2k}(\tau).$$

We cannot conclude the last property for $k = 1$ because the series defining $G_2(\tau, 1)$ is not absolutely convergent. It turns out that $E_2(\tau)$ has a similar functional equation with a small "error" term.

Proof. Using Exercise 2.12.3,

$$\begin{aligned}
E_{2k}(\tau) &= \frac{1}{2\zeta(2k)} \left(\sum_{n=1}^{\infty} \frac{2}{(n)^{2k}} + \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(m\tau+n)^{2k}} + \frac{1}{(-m\tau+n)^{2k}} \right) \\
&= 1 + \frac{1}{\zeta(2k)} \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(m\tau+n)^{2k}} \\
&= 1 + \frac{2}{\zeta(1-2k)} \sum_{m=1}^{\infty} \sum_{j=1}^{\infty} j^{2k-1} q^{jm} \\
&= 1 + \frac{2}{\zeta(1-2k)} \sum_{j=1}^{\infty} j^{2k-1} \frac{q^j}{1-q^j}
\end{aligned}$$

□

2.4 Modular Discriminant $\Delta(\tau)$ and Klein's Absolute Invariant $j(\tau)$

Let $e_i(\tau)$ be the roots of the cubic polynomial in the differential equation for $\wp$, that is,

$$\begin{aligned}
(\wp')^2 &= 4\wp^3 - g_2\wp - g_3 \\
&= 4(\wp - e_1)(\wp - e_2)(\wp - e_3).
\end{aligned}$$

The discriminant of the cubic polynomial is therefore

$$\begin{aligned}
\Delta(\tau) :&= 16(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2 \\
&= -64\left(e_1e_2 + e_1e_2 + e_3e_1\right)^3 - 432e_1^2e_2^2e_3^2 \\
&= g_2^3 - 27g_3^2,
\end{aligned}$$

where we have used

$$\begin{aligned}
0 &= e_1 + e_2 + e_3, \\
g_2 &= -4\left(e_1e_2 + e_2e_3 + e_3e_1\right), \\
g_3 &= 4e_1e_2e_3.
\end{aligned}$$

Also, set

$$j(\tau) = \frac{1728 g_2(\tau)^3}{\Delta(\tau)}.$$

This function is known as Klein's absolute invariant, or just the j function.

Proposition 2.4.1. *For $\Delta(\tau)$ and $j(\tau)$ we have*

1. *Representation in E_4 and E_6 and q-series expansions:*

$$\Delta(\tau) = \frac{64\pi^{12}}{27}(E_4^3 - E_6^2) = (2\pi)^{12} q + O(q^2),$$
$$j(\tau) = \frac{1728 E_4^3}{E_4^3 - E_6^2} = \frac{1}{q} + 744 + O(q).$$

2. *For $ad - bc = 1$,*

$$\Delta\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{12}\Delta(\tau),$$
$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau).$$

3. *At $\tau = i\infty$, $\Delta(\tau)$ vanishes and $j(\tau)$ blows up.*

4. *$\Delta(\tau)$ does not vanish (equiviently, $j(\tau)$ has no poles) at any $\tau \in \mathbb{H}$.*

Proof. Exercise 2.12.2. □

2.5 Basic Properties of $\mathrm{SL}_2(\mathbb{Z})$

For the Eisenstein series, we were able to find the transformation formula for any a, b, c, d directly. However, in most cases we will just prove the transformation formula for specific a, b, c, d and hope that the result for general a, b, c, d can be obtained by iterating these special cases. Set

$$\Gamma(1) = \mathrm{SL}_2(\mathbb{Z}),$$

i.e. the "modular group" or "full modular group". A matrix in $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \tau \mapsto \frac{a\tau + b}{c\tau + d}$$

Note that

$$\mathrm{Im}\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{\mathrm{Im}\,\tau}{|c\tau + d|^2} \tag{2.5.1}$$

Two important elements are S and T:

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : \tau \mapsto \frac{-1}{\tau},$$
$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : \tau \mapsto \tau + 1.$$

Also set

$$F = \left\{\tau \in \mathbb{H} \mid -\tfrac{1}{2} \le \mathrm{Re}\,\tau \le \tfrac{1}{2} \text{ and } |\tau| \ge 1\right\}.$$

The left and right edges with $\mathrm{Re}\,\tau = \pm\frac{1}{2}$ are identified via T, and the left and right edges of F on $|\tau| = 1$ are identified via S. We will also formally include $i\infty$ in F as well.

Proposition 2.5.1. *For $\Gamma(1)$, we have*

1. *F is a fundamental for $\mathbb{H}/\Gamma(1)$ with the appropriate edges identitfied.*
2. *S and T generate $\Gamma(1)/\pm I$.*
3. *For any $\tau \in F$ the isotropy subgroup $\Gamma(1)_\tau := \{g \in \Gamma(1) | g\tau = \tau\}$ is $\pm I$ except in the cases*
   - $\tau = i\infty$, $\Gamma(1)_\tau := \pm\{T^k\}_{k\in\mathbb{Z}}$
   - $\tau = i$, $\Gamma(1)_\tau := \pm\{I, S\}$
   - $\tau = e(1/3)$, $\Gamma(1)_\tau := \pm\{I, ST, (ST)^2\}$
   - $\tau = e(1/6)$, $\Gamma(1)_\tau := \pm\{I, TS, (TS)^2\}$

Proof. Sketch of (1) and (3): Given $\tau \in H$, we can apply T and S to get a point in F by repeating the following steps. Apply T^k to get τ inside $-\frac{1}{2} \le \operatorname{Re}\tau \le \frac{1}{2}$. If $|\tau| < 1$ apply S. This must terminate with a point in F because $\operatorname{Im}\tau$ only increases throughout the process. Now suppose $\tau_1, \tau_2 \in F$ with $\operatorname{Im}\tau_2 \ge \operatorname{Im}\tau_1$ are related by $\tau_2 = (a\tau_1 + b)/(c\tau_1 + d)$. From (2.5.1), this means that $|c\tau_1 + d| \le 1$. Since τ_1 is in F this restricts c to $c = 0, 1, -1$.

(2). Given $g \in \Gamma(1)$ take any τ in the interior of F. Use S and T to get $g\tau$ back into F and use (1) to conclude that g is a product of T and S (modulo $\pm I$). □

2.6 The η function and E_2

The logarithmic derivative of

$$\eta(\tau) := q^{1/24}(q;q)_\infty$$

is simply related to $E_2(\tau)$.

$$\begin{aligned}
\frac{1}{2\pi i}\frac{d}{d\tau}\log\eta(\tau) &= \frac{1}{2\pi i}\frac{d}{d\tau}\left(\frac{2\pi i\tau}{24} + \sum_{n=1}^{\infty}\log(1-q^n)\right)\\
&= \frac{1}{24} + q\frac{d}{dq}\sum_{n=1}^{\infty}\log(1-q^n)\\
&= \frac{1}{24} - \sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}\\
&= \frac{1}{24}E_2(\tau).
\end{aligned}$$

Lemma 2.6.1 (Poisson Summation Formula for Cosine)**.** *Under suitable restrictions of the function f, if*

$$f_c(y) = \int_{-\infty}^{\infty} f(x)\cos(2\pi xy)dx,$$

then

$$\sum_{n=-\infty}^{\infty} f_c(n) = \frac{f(0)}{2} + \sum_{n=1}^{\infty} f(n).$$

Proposition 2.6.2. *For $\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \Gamma(1)$, we have*

1. E_2 transformation:

$$\begin{aligned} E_2(\tau+1) &= E_2(\tau), \\ \tau^{-2}E_2\left(-\frac{1}{\tau}\right) &= E_2(\tau)+\frac{12}{2\pi i\tau}, \\ (c\tau+d)^{-2}E_2\left(\frac{a\tau+b}{c\tau+d}\right) &= E_2(\tau)+\frac{12c}{2\pi i(c\tau+d)}. \end{aligned}$$

2. η transformation:

$$\begin{aligned} \eta(\tau+1) &= e\left(\frac{1}{24}\right)\eta(\tau), \\ \eta\left(-\frac{1}{\tau}\right) &= \sqrt{-i\tau}\eta(\tau), \\ \eta\left(\frac{a\tau+b}{c\tau+d}\right) &= \epsilon_\eta\begin{pmatrix} a & b \\ c & d \end{pmatrix}\sqrt{-i(c\tau+d)}\eta(\tau), \end{aligned}$$

where $\epsilon_\eta\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is some 24^{th} root of unity.

Proof. The first parts of (1) and (2) are trivial, so we start with the second part of (1). In Lemma 2.6.1 set

$$\begin{aligned} f(x) &= -24\sum_{n=1}^{\infty} xe(n\tau x) = \frac{-24xq^x}{1-q^x}, \\ f(0) &= \frac{24}{2\pi i\tau}. \end{aligned}$$

The result

$$\begin{aligned} f_c(y) &= \frac{1}{2\zeta(2)}\sum_{n=1}^{\infty}\frac{1}{(n\tau+y)^2}+\frac{1}{(-n\tau+y)^2} \\ &= \frac{1}{2\zeta(2)}\sum_{\substack{n\in\mathbb{Z}\\ n\neq 0}}\frac{1}{(n\tau+y)^2} \end{aligned}$$

is elementary, so the assertion of Lemma 2.6.1 gives

$$\frac{1}{2\zeta(2)}\sum_{m=-\infty}^{\infty}\sum_{\substack{n=-\infty\\ n\neq 0}}^{\infty}\frac{1}{(n\tau+m)^2} = \frac{12}{2\pi i\tau}-24\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n},$$

or,

$$\frac{1}{2\zeta(2)}\left(-2\zeta(2)+\tau^{-2}G_2\left(-\frac{1}{\tau}\right)\right) = \frac{12}{2\pi i\tau}-1+E_2(\tau),$$

which is the second part of (1). The second part of (2) follows from integrating the second part of (1) and using $\tau = i$ to evaluate the constant of integration. The third parts of each follow from the first two since S and T generate $\Gamma(1)$. □

Note that the η function is non-vanishing on $\mathbb{H}$ so we may define a logarithm

$$\log \eta(\tau) := \frac{2\pi i \tau}{24} + \sum_{n=1}^{\infty} \log\left(1 - q^n\right).$$

This also entails that we may define a logarithm of the corresponding multiplier system

$$\log \epsilon_\eta\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) := \log \eta\left(\frac{a\tau + b}{c\tau + d}\right) - \frac{1}{2}\log(\sqrt{-i(c\tau + d)}) - \log \eta(\tau).$$

Now we give a formula for $\log \epsilon_\eta\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in terms of Dedekind sums and a slightly simpler formula for its exponential $\epsilon_\eta\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. For odd primes p let $\left(\frac{c}{p}\right)$ be the usual Legendre symbol. Extend this to all positive odd d by means of the prime factorization $d = p_1^{e_1} \cdots p_n^{e_n}$ via

$$\left(\frac{c}{d}\right) = \left(\frac{c}{p_1}\right)^{e_1} \cdots \left(\frac{c}{p_n}\right)^{e_n}.$$

Then, extend to negative odd d by

$$\left(\frac{c}{d}\right) = (-1)^{\frac{\operatorname{sign}(d)-1}{2}\frac{\operatorname{sign}(c)-1}{2}} \left(\frac{c}{|d|}\right).$$

Note we have the generalized quadratic reciprocity and periodicity

$$\begin{aligned}
\left(\frac{c}{d}\right) &= (-1)^{\frac{d-1}{2}\frac{c-1}{2}} \left(\frac{d}{|c|}\right), \text{ for } c, d \text{ odd} \\
\left(\frac{c+d}{d}\right) &= \begin{cases} -\left(\frac{c}{d}\right) & , d < 0 \text{ and } \operatorname{sign}(c) \neq \operatorname{sign}(c+d) \\ +\left(\frac{c}{d}\right) & , \text{otherwise} \end{cases}, \\
\left(\frac{d}{c+2d}\right) &= \begin{cases} -\left(\frac{d}{c}\right) & , d \equiv 2, 3 \mod 4 \\ +\left(\frac{d}{c}\right) & , d \equiv 0, 1 \mod 4 \end{cases},
\end{aligned}$$

which are useful in evaluating the Jacobi symbol.

Proposition 2.6.3. *For $c > 0$, the multiplier system of $\eta(\tau)$ satisfies*

$$\begin{aligned}
\epsilon_\eta\begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{cases} \left(\frac{d}{c}\right)\zeta_{24}^{3(1-c)+bd(1-c^2)+c(a+d)} & , c \text{ odd} \\ \left(\frac{c}{|d|}\right)\zeta_{24}^{3d+ac(1-d^2)+d(b-c)} & , d \text{ odd} \end{cases}, \\
\log \epsilon_\eta\begin{pmatrix} a & b \\ c & d \end{pmatrix} &= 2\pi i\left(\frac{a+d}{24c} + \frac{S(-d,c)}{2}\right),
\end{aligned}$$

where S is the Dedekind sum $S(h,k) = \sum_{r=1}^{k-1} \frac{r}{k}\bar{B}_1\left(\frac{hr}{k}\right)$ and $\bar{B}_1(x)$ is the periodic Bernoulli polynomial

$$\bar{B}_1(x) = \sum_{n=1}^{\infty} -\frac{\sin(2\pi n x)}{\pi n} = \operatorname{FracPart}(x) - \frac{1}{2}.$$

Proof. The first formula can be found in [10, pg. 51]. The second formula can be found in [2, sec. 3.4]. The first formula can also be deduced directly from the main result of Section 2.11. □

2.7 Recursions for the Eisenstein Series

The main result of this section is that the Eisenstein series $E_8, E_{10}, \ldots$ can be expressed as polynomials in just E_4 and E_6. In the next chapter we will see that this is no accident and that the representation is unique.

Proposition 2.7.1. *For $n \geq 0$*

$$E_{2n+8}(\tau) = \sum_{\substack{0 \leq k,l \leq n \\ k+l=n}} \frac{6(2k+3)(2l+3)\zeta(2k+4)\zeta(2l+4)}{(n+1)(2n+7)(2n+9)\zeta(2n+8)} E_{2k+4}(\tau)E_{2l+4}(\tau).$$

Proof. We have

$$\begin{aligned}
\wp''(z) &= \frac{6}{z^4} + 6G_4 + 60G_6 z^2 + 210G_8 z^4 + 504G_{10} z^6 + O(z^8), \\
6\wp(z)^2 &= \frac{6}{z^4} + 36G_4 + 60G_6 z^2 + \left(54G_4^2 + 84G_8\right) z^4 + \left(180G_4G_6 + 108G_{10}\right) z^6 + O(z^8),
\end{aligned}$$

so $\wp''(z) - 6\wp(z)^2$ must be a constant. The assertion follows by equating the coefficients of $z^4, z^6, \ldots$ to zero in the difference $\wp''(z) - 6\wp(z)^2$. Recall that $E_{2k} = \frac{1}{2\zeta(2k)} G_{2k}$. □

2.8 Elliptic Θ Functions

Besides the Eisenstein series, there are other ways of constructing modular forms. The main ingredient is the Poisson summation formula applied to the Gaussian distribution. For arbitrary $\alpha, \beta \in \mathbb{R}$, define the Θ function with characteristics α, β as

$$\Theta \left[\begin{array}{c} \alpha \\ \beta \end{array} \right] (z|\tau) = \sum_{n \in \mathbb{Z}} e\left((z+\beta)(n+\alpha) + \tau (n+\alpha)^2 / 2 \right)$$

The variable z may take any value in $\mathbb{C}$, but τ is constrained to $\mathbb{H}$, where the sum absolutely convergent. Jacobi's four Θ functions are then

$$\begin{aligned}
\Theta_1(z|\tau) &= \Theta \left[\begin{array}{c} 1/2 \\ 1/2 \end{array} \right] (z|\tau) = -2\sin(\pi z) q^{1/8} + 2\sin(3\pi z) q^{9/8} + O(q^{17/8}), \\
\Theta_2(z|\tau) &= \Theta \left[\begin{array}{c} 1/2 \\ 0/2 \end{array} \right] (z|\tau) = 2\cos(\pi z) q^{1/8} + 2\cos(3\pi z) q^{9/8} + O(q^{17/8}), \\
\Theta_3(z|\tau) &= \Theta \left[\begin{array}{c} 0/2 \\ 0/2 \end{array} \right] (z|\tau) = 1 + 2\cos(2\pi z) q^{1/2} + 2\cos(4\pi z) q^{2} + O(q^{5/2}), \\
\Theta_4(z|\tau) &= \Theta \left[\begin{array}{c} 0/2 \\ 1/2 \end{array} \right] (z|\tau) = 1 - 2\cos(2\pi z) q^{1/2} + 2\cos(4\pi z) q^{2} + O(q^{5/2}).
\end{aligned}$$

Proposition 2.8.1. *For integers A and B, we have*

1. *Quasi-periodicity relation:*

$$\Theta \left[\begin{array}{c} \alpha \\ \beta \end{array} \right] (z + A\tau + B|\tau) = e\left(B\alpha - A\beta - Az - \frac{A^2\tau}{2} \right) \Theta \left[\begin{array}{c} \alpha \\ \beta \end{array} \right] (z|\tau).$$

2. *Shift of characteristics:*

$$\Theta \left[\begin{array}{c} \alpha + A \\ \beta + B \end{array} \right] (z|\tau) = e(\alpha B) \Theta \left[\begin{array}{c} \alpha \\ \beta \end{array} \right] (z|\tau)$$

Proof. For (1), let

$$s_n(z) = e\left((z+\beta)(n+\alpha) + \tau(n+\alpha)^2/2\right).$$

We have

$$\begin{aligned}
\Theta\left[\begin{array}{c}\alpha\\ \beta\end{array}\right](z+A\tau+B|\tau) &= \sum_{n\in\mathbb{Z}} s_n(z+A\tau+B)\\
&= e\left(-AB-A\beta-Az-\frac{A^2\tau}{2}\right)\sum_{n\in\mathbb{Z}} s_{n+A}(z+B)\\
&= e\left(-A\beta-Az-\frac{A^2\tau}{2}\right)\sum_{n\in\mathbb{Z}} s_n(z+B)\\
&= e\left(-A\beta-Az-\frac{A^2\tau}{2}\right)e(B\alpha+Bn)\sum_{n\in\mathbb{Z}} s_n(z)\\
&= e\left(B\alpha-A\beta-Az-\frac{A^2\tau}{2}\right)\Theta\left[\begin{array}{c}\alpha\\ \beta\end{array}\right](z|\tau).
\end{aligned}$$

(2) says that Θ doesn't change much when the characteristics are changed by integers and follows by shifting $n \to n-A$ in the series definition of $\Theta\left[\begin{array}{c}\alpha+A\\ \beta+B\end{array}\right](z|\tau)$. □

Lemma 2.8.2 (Poisson Summation Formula)**.** *Under suitable restrictions of the function f, if*

$$\hat{f}(y) = \int_{-\infty}^{\infty} f(x)\exp(-2\pi xy)dy,$$

then

$$\sum_{n=-\infty}^{\infty}\hat{f}(n) = \sum_{n=-\infty}^{\infty} f(n).$$

Proposition 2.8.3. *For $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma(1)$, we have*

1. *Transformation under T:*

$$\begin{aligned}
\Theta_1(z|\tau+1) &= \sqrt{i}\Theta_1(z|\tau),\\
\Theta_2(z|\tau+1) &= \sqrt{i}\Theta_2(z|\tau),\\
\Theta_3(z|\tau+1) &= \Theta_4(z|\tau),\\
\Theta_4(z|\tau+1) &= \Theta_3(z|\tau).
\end{aligned}$$

2. *Transformation under S:*

$$\begin{aligned}
\Theta_1\left(\frac{z}{\tau}\middle|-\frac{1}{\tau}\right) &= -i\sqrt{-i\tau}e\left(\frac{z^2}{2\tau}\right)\Theta_1(z|\tau),\\
\Theta_2\left(\frac{z}{\tau}\middle|-\frac{1}{\tau}\right) &= \sqrt{-i\tau}e\left(\frac{z^2}{2\tau}\right)\Theta_4(z|\tau),\\
\Theta_3\left(\frac{z}{\tau}\middle|-\frac{1}{\tau}\right) &= \sqrt{-i\tau}e\left(\frac{z^2}{2\tau}\right)\Theta_3(z|\tau),\\
\Theta_4\left(\frac{z}{\tau}\middle|-\frac{1}{\tau}\right) &= \sqrt{-i\tau}e\left(\frac{z^2}{2\tau}\right)\Theta_2(z|\tau).
\end{aligned}$$

3. *General transformation for Θ_1:*

$$\Theta_1\left(\frac{z}{c\tau+d}\Big|\frac{a\tau+b}{c\tau+d}\right)=\epsilon_{\Theta_1}\sqrt{-i(c\tau+d)}e\left(\frac{cz^2}{2(c\tau+d)}\right)\Theta_1(z|\tau)$$

where $\epsilon_{\Theta_1}\left(\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\right)$ is some 8^{th} root of unity.

4. *General transformation for arbitrary characteristics:*

$$\Theta\left[\begin{array}{c}\frac{1}{2}+\alpha\\ \frac{1}{2}+\beta\end{array}\right]\left(\frac{z}{c\tau+d}\Big|\frac{a\tau+b}{c\tau+d}\right)=\epsilon_{\Theta_1}\sqrt{-i(c\tau+d)}e\left(\frac{cz^2}{2(c\tau+d)}\right)\Theta\left[\begin{array}{c}\frac{1}{2}+a\alpha+c\beta\\ \frac{1}{2}+b\alpha+d\beta\end{array}\right](z|\tau)$$
$$\times e\left(-\frac{ab\alpha^2}{2}-bc\alpha\beta-\frac{cd\beta^2}{2}\right)e\left(-\frac{(a-1)\alpha+c\beta}{2}\right)$$

Proof. The transformations in (1) are straightforward, so we concentrate on (2), where the proof for Θ_3 will give the idea of the proof of the others. In Lemma 2.8.2 set

$$f(x)=e\left(zx+\tau x^2/2\right)$$

It is easy to compute

$$\hat{f}(y)=\frac{e\left(\frac{zy}{\tau}-\frac{y^2}{2\tau}\right)}{\sqrt{-i\tau}e\left(\frac{z^2}{2\tau}\right)},$$

so the transformation for Θ_3 follows. (3) follows by iterating (1) and (2).

The assertion (4) is equivalent to (3) since the Θ function with an arbitrary characteristic is no more general than $\Theta_1(z|\tau)$. We can write Θ_1 as a shift of the Θ function with general characteristics as

$$\Theta_1(z|\tau)=e\left(\frac{\alpha(\alpha\tau-2z-1)}{2}\right)\Theta\left[\begin{array}{c}\frac{1}{2}+\alpha\\ \frac{1}{2}+\beta\end{array}\right](z-\alpha\tau-\beta|\tau)$$

and then transform part (3) of Proposition 2.8.3 . The details are messy but straightforward. □

Proposition 2.8.4. *We have*

1. *$\Theta_1(z)$ is an odd function of z*
2. *The zero set of $\Theta_1(z)$ is exactly $\mathbb{Z}+\mathbb{Z}\tau$*
3. *Jacobi Triple Product:*

$$\Theta_1(z|\tau)=-iq_z^{-1/2}q^{1/8}(q_z;q)_\infty(q/q_z;q)_\infty(q;q)_\infty.$$

4. *As $z\to 0$*

$$\Theta_1(z|\tau)=-2\pi\eta(\tau)^3z+O(z^3).$$

5. $\epsilon_{\Theta_1}\left(\begin{array}{cc}a&b\\c&d\end{array}\right)=-i\epsilon_\eta\left(\left(\begin{array}{cc}a&b\\c&d\end{array}\right)\right)^3$.

Proof. (1) follows by replacing $n\to -1-n$ in the series definition of Θ_1.

$$\Theta_1(z|\tau)=\sum_{n\in\mathbb{Z}}q^{\frac{1}{2}(n+\frac{1}{2})^2}i(-1)^ne\left(z\left(n+\frac{1}{2}\right)\right)$$

For (2), we integrate around a fundamental parallelogram to get the number of zeros of Θ_1 modulo the lattice as

$$\frac{1}{2\pi i}\left(\int_w^{w+1} + \int_{w+1}^{w+1+\tau} + \int_{w+1+\tau}^{w+\tau} + \int_{w+\tau}^{w}\right) d\log\Theta_1(z).$$

By Proposition 2.8.1, we have

$$\begin{aligned} d\log\Theta_1(z+1) &= d\log\Theta_1(z) \\ d\log\Theta_1(z+\tau) &= d\log\Theta_1(z) - 2\pi i dz \end{aligned}$$

This first equation says that the second and fourth integrals cancel completely. This second equation says that the first and third integrals combine to give a total of

$$\frac{1}{2\pi i}\int_w^{w+1} 2\pi i dz = 1$$

zero in a fundamental parallelogram.

(3) is a well-known identity, and (4) follows from rewriting (3) as

$$\frac{\Theta_1(z|\tau)}{i(q_z^{1/2} - q_z^{-1/2})} = q^{1/8}(qq_z;q)_\infty(q/q_z;q)_\infty(q;q)_\infty,$$

and letting $z \to 0$.

(5) follows from differentiating part (3) of Proposition 2.8.3 and substituting part (4) here. □

Proposition 2.8.5. *We have*

1. *Relation between $\wp(z)$ and $\Theta_1(z)$:*

$$\wp(z|\tau) = -\frac{\partial^2}{\partial z^2}\log\Theta_1(z|\tau) - \frac{\pi^2}{3}E_2(\tau).$$

2. *If $p_1 + \cdots + p_r = q_1 + \cdots + q_r$, then*

$$\frac{\Theta_1(z-q_1|\tau)\cdots\Theta_1(z-q_r|\tau)}{\Theta_1(z-p_1|\tau)\cdots\Theta_1(z-p_r|\tau)}$$

   is an elliptic function modulo $\mathbb{Z}+\mathbb{Z}\tau$ with poles $p_1,\ldots,p_r$ and zeros $q_1,\ldots,q_r$.

3. *Factorization of $\wp(z_1) - \wp(z_2)$:*

$$\wp(z_1) - \wp(z_2) = (2\pi i)^2\eta(\tau)^6\frac{\Theta_1(z_1-z_2)\Theta_1(z_1+z_2)}{\Theta_1(z_1)^2\Theta_1(z_2)^2}.$$

Proof. From Propositions 2.8.1 and 2.8.4, we see that

$$\wp(z|\tau) + \frac{\partial^2}{\partial z^2}\log\Theta_1(z,\tau)$$

is an entire elliptic function, hence it is some constant C. In order to evaluate this constant we need to get the next coefficient in the expansion of $\Theta_1(z)$, i.e.

$$\Theta_1(z) = -2\pi\eta(\tau)^3(z + \frac{C}{2}z^3 + O(z^5)).$$

To this end, note that

$$\begin{aligned}\frac{\partial^3}{\partial z^3}\Theta_1(z|\tau) &= (2\pi i)^3 \sum_{n\in\mathbb{Z}} \left(n+\frac{1}{2}\right)^3 e\left(\left(z+\frac{1}{2}\right)\left(n+\frac{1}{2}\right)+\frac{\tau}{2}\left(n+\frac{1}{2}\right)^2\right)\\ &= 4\pi i \frac{\partial^2}{\partial\tau\partial z}\Theta_1(z|\tau).\end{aligned}$$

Therefore,

$$\begin{aligned}-2\pi\eta(\tau)^3\frac{C}{2}\cdot 6 &= \frac{\partial^3}{\partial z^3}\Theta_1(z|\tau)\Big|_{z=0}\\ &= 4\pi i\frac{\partial^2}{\partial\tau\partial z}\Theta_1(z|\tau)\Big|_{z=0}\\ &= -8\pi^2 i\frac{\partial}{\partial\tau}\eta(\tau)^3\\ &= 2\pi^3\eta(\tau)^3E_2(\tau),\end{aligned}$$

and so $C = -\frac{\pi^2}{3}E_2(\tau)$.

(2) Follows immediately from Proposition 2.8.1, which says that

$$\begin{aligned}\Theta_1((z+1)-a|\tau) &= -\Theta_1(z-a|\tau),\\ \Theta_1((z+\tau)-a|\tau) &= -e(a-z-\tau/2)\Theta_1(z-a|\tau).\end{aligned}$$

As long as $e(q_1+\cdots+q_r-p_1-\cdots-p_r)=1$, the displayed quotient will be an elliptic function modulo $\mathbb{Z}+\mathbb{Z}\tau$.

For (3), note that there is a constant A, depending only on τ, such that

$$\wp(z_1)-\wp(z_2) = A\frac{\Theta_1(z_1-z_2)\Theta_1(z_1+z_2)}{\Theta_1(z_1)^2\Theta_1(z_2)^2},$$

since both sides have the same poles and zeros as functions of either z_1 or z_2. To evaluate this constant, multiply both sides by z_1^2 and let $z_1\to 0$. This gives

$$\begin{aligned}1 &= A\frac{\Theta_1(-z_2)\Theta_1(z_2)}{\Theta_1(z_2)^2}\lim_{z_1\to 0}\frac{z_1^2}{\Theta_1(z_1)^2}\\ &= -A\lim_{z_1\to 0}\frac{z_1^2}{\Theta_1(z_1)^2}\\ &= -A(-2\pi\eta(\tau)^3)^{-2}.\end{aligned}$$

□

2.9 $\Gamma(2)$ and the Asymptotic of Θ Near the Cusps

According to Proposition 2.8.3, we have a surjective homomorphism $\Gamma(1)\to S_3$, where S_3 the the group of permutations on the Θ functions $\Theta_2,\Theta_3,\Theta_4$. One might wonder what the kernel and stabilizer of, say, Θ_3 is, that is, what the groups

$$\begin{aligned}G_1 &= \left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma(1)\mid \Theta_i\left(0\Big|\frac{a\tau+b}{c\tau+d}\right)^8 = (c\tau+d)^4\Theta_i(0|\tau)^8 \text{ for all } i\in\{2,3,4\}\right\},\\ G_2 &= \left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma(1)\mid \Theta_3\left(0\Big|\frac{a\tau+b}{c\tau+d}\right)^8 = (c\tau+d)^4\Theta_3(0|\tau)^8\right\}\end{aligned}$$

are. To answer this question we can apply part (4) of Proposition 2.8.3 to see that the kernel of the homomorphism $\Gamma(1) \to S_3$ consists of those $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$ for which

$$\begin{aligned} a\alpha + c\beta &= \alpha \mod 1, \\ b\alpha + d\beta &= \beta \mod 1, \end{aligned}$$

for all half-integers α and β. Clearly this is the group

$$G_1 = \Gamma(2) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2 \right\}.$$

By the first isomorphism theorem, we have

$$\Gamma(1)/\Gamma(2) \simeq S_3 = \{\Gamma(2), (ST)\Gamma(2), (ST)^2\Gamma(2), (S)\Gamma(2), (T)\Gamma(2), (TST)\Gamma(2)\}.$$

The following groups between $\Gamma(1)$ and $\Gamma(2)$ have important names:

$$\begin{aligned} \Gamma_0(2) &= \{\Gamma(2), (T)\Gamma(2)\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid c \equiv 0 \bmod 2 \right\}, \\ \Gamma_\vartheta &= \{\Gamma(2), (S)\Gamma(2)\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid ab \equiv cd \equiv 0 \bmod 2 \right\}. \end{aligned}$$

Note that $G_2 = \Gamma_\vartheta$, which is known as the theta subgroup of $\Gamma(1)$ while $\Gamma_0(2)$ is know as the principal Hecke subgroup of level 2.

The main goal of this section is to establish asymptotic formulas for the Θ functions near the cusps in order to obtain explicit formulas for the roots of unity involved in the multiplier systems for these functions. When the function vanishes at a cusp, it seems that we need to use the modular inverse symbol

$$x^{-1}_{\bmod y} = z \text{ whenever there is a } z \text{ such that } zx \equiv 1 \bmod y \text{ and } 0 \le z/y < 1.$$

Note that we always have a reciprocity property given by

$$\frac{x^{-1}_{\bmod y}}{y} + \frac{y^{-1}_{\bmod x}}{x} = 1 + \frac{1}{xy}.$$

When it is clear, we will set $\Theta(\tau) = \Theta(0|\tau)$.

Proposition 2.9.1. *Let c and d be any integers with $(c,d) = 1$ and $c \neq 0$. Then, as $t \to 0^+$,*

1. *Relation to exponential sums*

$$\begin{aligned} \sqrt{ict}\Theta_3\left(it - \frac{d}{c}\right) &\sim \frac{1}{\sqrt{-ic}} \sum_{n=1}^{|c|} \zeta_{2c}^{-dn^2} && \text{, } cd \text{ even} \\ \frac{e^{\frac{\pi}{4c^2t}}}{2}\sqrt{ict}\Theta_3\left(it - \frac{d}{c}\right) &\sim \frac{1}{\sqrt{-4ic}} \sum_{n=1}^{|c|} \left(\zeta_{2c}^{n} + \zeta_{2c}^{-n}\right)\zeta_{2c}^{-dn^2} && \text{, } cd \text{ odd} \end{aligned}$$

2. Θ_3*:*

$$\begin{aligned} \sqrt{ict}\Theta_3\left(it - \frac{d}{c}\right) &\sim \left(\frac{c}{d}\right)\zeta_8^{1-d} && \text{, } c \text{ even } d \text{ odd} \\ \frac{e^{\frac{\pi}{4c^2t}}}{2}\sqrt{ict}\Theta_3\left(it - \frac{d}{c}\right) &\sim \left(\frac{d}{|c|}\right)\zeta_8^{c}\zeta_c^{(8d)^{-1}_{\bmod c}} && \text{, } c \text{ odd } d \text{ odd} \\ \sqrt{ict}\Theta_3\left(it - \frac{d}{c}\right) &\sim \left(\frac{d}{|c|}\right)\zeta_8^{c} && \text{, } c \text{ odd } d \text{ even} \end{aligned}$$

3. Θ_4*:*

$$\begin{aligned}
\sqrt{ict}\Theta_4\left(it-\frac{d}{c}\right) &\sim \left(\frac{c}{d}\right)\zeta_8^{1+2c-d-cd} && ,\ c \text{ even } d \text{ odd}\\
\sqrt{ict}\Theta_4\left(it-\frac{d}{c}\right) &\sim \left(\frac{d}{|c|}\right)\zeta_8^{c} && ,\ c \text{ odd } d \text{ odd}\\
\frac{e^{\frac{\pi}{4c^2t}}}{2}\sqrt{ict}\Theta_4\left(it-\frac{d}{c}\right) &\sim \left(\frac{d}{|c|}\right)\zeta_8^{c}\zeta_c^{(8d)^{-1}\bmod c} && ,\ c \text{ odd } d \text{ even}
\end{aligned}$$

4. Θ_2*:*

$$\begin{aligned}
\frac{e^{\frac{\pi}{4c^2t}}}{2}\sqrt{ict}\Theta_2\left(it-\frac{d}{c}\right) &\sim \left(\frac{c}{d}\right)\zeta_8^{3d-3}\zeta_{8c}^{d^{-1}\bmod 8c} && ,\ c \text{ even } d \text{ odd}\\
\sqrt{ict}\Theta_2\left(it-\frac{d}{c}\right) &\sim \left(\frac{d}{|c|}\right)\zeta_8^{cd+3c+2d+2} && ,\ c \text{ odd } d \text{ odd}\\
\sqrt{ict}\Theta_2\left(it-\frac{d}{c}\right) &\sim \left(\frac{d}{|c|}\right)\zeta_8^{cd+c-2d} && ,\ c \text{ odd } d \text{ even}
\end{aligned}$$

Proof. To avoid complications, the factor $\sqrt{-ict}$ is handled like $\sqrt{|c|t}$. This results in a $\zeta_8^{\operatorname{sgn}(c)}$ canceling in the formulas, since

$$\sqrt{ict} = \sqrt{|c|t}\zeta_8^{\operatorname{sgn}(c)}.$$

For (1), if cd is even then the function of n given by $e\left(\frac{-dn^2}{2c}\right)$ has c as a period. Therefore,

$$\begin{aligned}
\Theta_3\left(it-\frac{d}{c}\right) &= \sum_{n\in\mathbb{Z}} e\left(\frac{-dn^2}{2c}\right)e^{-\pi n^2 t}\\
&= \sum_{n=1}^{|c|} e\left(\frac{-dn^2}{2c}\right)\sum_{\substack{m\in\mathbb{Z}\\ m\equiv n \bmod c}} e^{-\pi m^2 t}\\
&= \sum_{n=1}^{|c|} e\left(\frac{-dn^2}{2c}\right)e^{-\pi c^2 t}\Theta_3\left(icnt|ic^2t\right)\\
&= \sum_{n=1}^{|c|} e\left(\frac{-dn^2}{2c}\right)\frac{1}{|c|\sqrt{t}}\Theta_3\left(\frac{n}{c}\Big|\frac{i}{c^2t}\right)\\
&\sim \frac{1}{\sqrt{|c|}}\sum_{n=1}^{|c|}\zeta_{2c}^{-dn^2}\times\frac{1}{\sqrt{|c|t}}.
\end{aligned}$$

If cd is odd, then Θ_3 vanishes at this cusp, so the evaluation is slightly more difficult. In this case $e\left(\frac{dn^2}{2c}\right)$

changes sign when n is incremented by c, so temporarily setting $q = e^{-\frac{\pi}{4c^2t}}$,

$$\begin{aligned}
\Theta_3\left(it - \frac{d}{c}\right) &= \sum_{n=1}^{|c|} e\left(\frac{dn^2}{2c}\right) \sum_{\substack{m\in\mathbb{Z} \\ m\equiv n \bmod 2|c|}} e^{-\pi m^2 t} - e^{-\pi(m+c)^2 t} \\
&= \sum_{n=1}^{|c|} e\left(\frac{dn^2}{2c}\right) \frac{\Theta_3\left(\frac{n}{2c}\middle|\frac{i}{4c^2t}\right) - \Theta_3\left(\frac{c+n}{2c}\middle|\frac{i}{4c^2t}\right)}{2|c|\sqrt{t}} \\
&= \sum_{n=1}^{|c|} e\left(\frac{-dn^2}{2c}\right) \frac{\left(1 + 2q\cos\left(\frac{\pi n}{c}\right) + \cdots\right) - \left(1 + 2q\cos\left(\frac{\pi(n+c)}{c}\right) + \cdots\right)}{2|c|\sqrt{t}} \\
&\sim \frac{1}{\sqrt{|c|}} \sum_{n=1}^{|c|} e\left(\frac{-dn^2}{2c}\right) \cos\left(\frac{2n\pi}{c}\right) \times \frac{2q}{\sqrt{|c|t}}.
\end{aligned}$$

For (2), let $T(d,c)$ denote $\lim_{t\to 0}\sqrt{|c|t}\Theta_3\left(it - \frac{d}{c}\right)$. By (1),

$$T(d,c) = \frac{1}{\sqrt{|c|}} \sum_{n=1}^{|c|} \zeta_{2c}^{-dn^2} = \begin{cases} \left(\frac{d}{|c|}\right)\zeta_8^{c-\mathrm{sgn}(c)} & , c \text{ odd } d \text{ even} \\ \left(\frac{c}{d}\right)\zeta_8^{1-d-\mathrm{sgn}(c)} & , c \text{ even } d \text{ odd} \end{cases},$$

where we have used the classical evaluation of quadratic Gauss sums (for any integers p and q with $q > 0$ and $(p,q) = 1$

$$\frac{1}{\sqrt{q}} \sum_{n=1}^{q} \zeta_q^{pn^2} = \begin{cases} \left(\frac{p}{q}\right)\frac{1+i}{1+i^q} & , q \text{ odd} \\ \left(\frac{q}{p}\right)\frac{1+i^p}{1+i}\frac{1+i^q}{1-i} & , p \text{ odd} \end{cases}$$

) in the case c odd d even for in this cases it becomes a sum over $|c|^{\text{th}}$ roots of unity. The c odd and d even case follows from $\Theta_3(-1/\tau) = \sqrt{-i\tau}\Theta_3(\tau)$. The second part of (2) can be obtained by completing the square in the sum $\sum_{n=1}^{|c|}\left(\zeta_{2c}^{n} + \zeta_{2c}^{-n}\right)\zeta_{2c}^{-dn^2}$, but here will use the easy identity

$$\Theta_3(\tau + 1) = 2\Theta_3(4\tau) - \Theta_3(\tau).$$

to give an alternate derivation. First, we need to obtain the next term in the expansion of $\Theta_3\left(it - \frac{d}{c}\right)$ for c odd and d even. In this cases find integers a and b so that $ad - bc = 1$ and a is even. The transformation formula for Θ_3 is

$$\Theta_3(\tau) = \frac{\epsilon}{\sqrt{-i(c\tau + d)}}\Theta_3\left(\frac{a\tau + b}{c\tau + d}\right),$$

where ϵ is some 8^{th} root of unity. Setting $\tau = it - d/c$ in this formula produces

$$\begin{aligned}
\Theta_3\left(\frac{-d}{c} + it\right) &= \frac{\epsilon}{\sqrt{ct}}\Theta_3\left(\frac{a}{c} + \frac{i}{c^2t}\right) \\
&= \frac{\epsilon}{\sqrt{ct}}\left(1 + 2e\left(\frac{a}{2c}\right)e^{-\frac{\pi}{c^2t}} + \cdots\right) \\
&= \frac{T(d,c)}{\sqrt{|c|t}}\left(1 + 2e\left(\frac{(2d)^{-1} \bmod c}{c}\right)e^{-\frac{\pi}{c^2t}} + \cdots\right).
\end{aligned}$$

Now let c and d both be odd. Setting $\tau = \frac{-c-d}{c} + it$ in the identity produces

$$\begin{aligned}\Theta_3\left(-\frac{d}{c}+it\right) &= 2\Theta_3\left(\frac{-4c-4d}{c}+4it\right) - \Theta_3\left(\frac{-c-d}{c}+it\right)\\ &= 2\frac{T(4d+4c,c)}{\sqrt{4|c|t}}\left(1+2e\left(\frac{(8d+8c)^{-1}_{\bmod c}}{c}\right)e^{-\frac{\pi}{4c^2t}}+\cdots\right)\\ &\quad - \frac{T(d+c,c)}{\sqrt{|c|t}}\left(1+2e\left(\frac{(2d+2c)^{-1}_{\bmod c}}{c}\right)e^{-\frac{\pi}{c^2t}}+\cdots\right)\\ &= \frac{T(d+c,c)}{\sqrt{|c|t}}e\left(\frac{(8d)^{-1}_{\bmod c}}{c}\right)2e^{-\frac{\pi}{4c^2t}}+\cdots,\end{aligned}$$

which gives the second part of (2). Parts (3) and (4) follow from the identities

$$\begin{aligned}\Theta_4(\tau+1) &= \Theta_3(\tau),\\ \Theta_2(-1/\tau) &= \sqrt{-i\tau}\Theta_4(\tau).\end{aligned}$$

Care has been taken to ensure that the formulas are valid for negative c as well. □

2.10 Addition Formulas

Theorem 2.10.1 (Weierstrass)**.** *A meromorphic function $f : \mathbb{C} \to \mathbb{C}$ possesses an algebraic addition theorem, that is, a non-trivial relation of the form*

$$P(f(x), f(y), f(x+y)) = 0,$$

for some polynomial P with coefficients independent of x and y if and only if $f(z)$ is one of the three possibilities:

1. *rational function of z*
2. *rational function of $e(z/\omega)$ for some period ω*
3. *rational function of $\wp(z|\omega_1,\omega_2)$ and $\wp'(z|\omega_1,\omega_2)$ for some periods ω_1, ω_2*

The third part of this theorem is usually stated with "an elliptic function of z modulo $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$". These are equivalent because any elliptic function is a rational function of $\wp(z)$ and $\wp'(z)$. First suppose that $f(z)$ is an even elliptic function with zeros $\pm q_n, ..., \pm q_n$ and poles $\pm p_n, ..., \pm q_n$. Then, there must be a constant c such that

$$f(z) = c\prod_{i=1}^{n}\frac{\wp(z)-\wp(q_i)}{\wp(z)-\wp(p_i)},$$

and so $f(z)$ is a rational function of $\wp(z)$. Next, for an elliptic function that is not necessarily even, use

$$f(z) = \frac{f(z)+f(-z)}{2} + \wp'(z)\cdot\frac{f(z)-f(-z)}{2\wp'(z)},$$

where $\frac{f(z)+f(-z)}{2}$ and $\frac{f(z)-f(-z)}{2\wp'(z)}$ are even elliptic functions.

Proposition 2.10.2.

1. *The map* $z \to (\wp(z|\omega_1,\omega_2), \wp'(z|\omega_1,\omega_2))$ *defines a bijection between the points of* $\mathbb{C}/(\omega_1\mathbb{Z}+\omega_2\mathbb{Z})$ *and the points on the curve* $y^2 = 4x^3 - g_2x - g_3$ *(with* ∞ *included).*

2. *For any* $g_2, g_3 \in \mathbb{C}$ *such that* $g_2^3 - 27g^2 \neq 0$*, the system*

$$\begin{aligned} g_2 &= 40G_4(\omega_1,\omega_2) \\ g_3 &= 140G_6(\omega_1,\omega_2) \end{aligned}$$

   is solvable for some periods ω_1, ω_2*.*

3. *If* $u+v+w \equiv 0 \mod \omega_1\mathbb{Z}+\omega_2\mathbb{Z}$*, then* $(\wp(u),\wp'(u))$*,* $(\wp(v),\wp'(v))$*, and* $(\wp(w),\wp'(w))$ *are colinear, that is*

$$\det \begin{pmatrix} 1 & \wp(u) & \wp'(u) \\ 1 & \wp(v) & \wp'(v) \\ 1 & \wp(w) & \wp'(w) \end{pmatrix} = 0$$

4. *Explicit addition formula for* $\wp(z)$*:*

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

Proof. (4) is left as an exercise. (2) will be established later when it is shown that $j(\tau)$ is a univalent function $\mathbb{H}/\Gamma(1) \to \mathbb{C}$.

For (1), suppose that $(\wp(z_1),\wp'(z_1)) = (\wp(z_2),\wp'(z_2))$. Since $\wp(z)$ is an elliptic function of order 2, we must have $z_1 + z_2 \equiv 0$. This implies that $\wp'(z_1) = \wp'(-z_2) = -\wp'(z_2) = -\wp'(z_1)$ which means that $\wp'(z_1) = 0$ and $\wp'(z_2) = 0$. If it were true that $z_1 \not\equiv z_2$ this would mean that the function $f(z) = \wp(z) - \wp(z_1)$ would have at least double zeros at the two distinct locations z_1 and z_2. This contradicts the fact the $f(z)$ has order 2.

For (3), determine the line $l(x,y) = 0$ through the points $(\wp(u),\wp'(u))$ and $(\wp(v),\wp'(v))$. Assume that this line is not vertical, so $l(x,y) = A + Bx + y$ for some constants A and B. The elliptic function $l(\wp(z),\wp'(z))$ has order 3 in this case so its zeros u, v and w_1, say, satisfy $u+v+w_1 \equiv 0$. This implies that $w_1 \equiv w$, so the assertion follows. If line is vertical, then it follows that $u+v \equiv 0$, and so $w \equiv 0$, which is consistent with the third point $(\wp(w),\wp'(w))$ being located at ∞.

□

2.11 $\Gamma(3)$ and the Asymptotic of η Near the Cusps

The η function vanishes at every cusp and is modular with respect to $\Gamma(1)$. It turns out that there is quite a magical formula for the asymptotics near the cusps. We simply state this first and devote this section to understanding this formula.

Proposition 2.11.1. *Let* c *and* d *be any integers with* $(c,d) = 1$ *and* $c \neq 0$*. Then, as* $t \to 0^+$*,*

$$\begin{aligned} \sqrt{ict}\; e^{\frac{\pi}{12c^2t}}\; \eta\left(-\frac{d}{c}+it\right) &\sim \frac{1}{\sqrt{-3ic}} \sum_{n=0}^{|c|} (-1)^n \left(\zeta_{24c}^{-2(6n-1)} + \zeta_{24c}^{2(6n-1)}\right) \zeta_{24c}^{-d(6n-1)^2} \\ &= \zeta_{24c}^{d+(c^2-1)(d^2-1)d^{-1}_{\bmod c}} \times \begin{cases} \left(\frac{c}{d}\right)\zeta_{24}^{15+9d+cd} & , \; d \text{ odd} \\ \left(\frac{d}{|c|}\right)\zeta_{24}^{3c-2cd} & , \; c \text{ odd} \end{cases} \end{aligned}$$

Proof. Let us first check that the final expression on the right hand side is well-defined. This entails showing that $(c^2-1)(d^2-1) \equiv 0 \bmod 24$, which is indeed true for relatively prime integers c and d. As a consequence of the Jacobi's triple product identity, we have the representation

$$\eta(\tau) = q^{1/24}(q,q^3)_\infty(q^2,q^3)_\infty(q^3,q^3)_\infty = \sum_{m\in\mathbb{Z}}(-1)^m e\left(\frac{(6m-1)^2\tau}{24}\right),$$

hence the representation as a sum over roots of unity follows along the same lines as the calculations in Proposition 2.9.1. The explicit evaluation will be deduced below. □

Since the exponential sum in Proposition 2.11.1 seems difficult to evaluate directly, we will use an indirect approach based properties of the modular group. Recall that we have the subgroup of $\Gamma(1)$ given by

$$\Gamma(2) = \{M \in \Gamma(1) | M \equiv I \bmod 2\}.$$

We had $\Gamma(1)/\Gamma(2) \simeq S_3$ with the elements of the quotient realized as the six permutations of the three functions $\Theta_2(\tau)^8$, $\Theta_3(\tau)^8$ and $\Theta_4(\tau)^8$. We can also define

$$\Gamma(3) = \{M \in \Gamma(1) | M \equiv I \bmod 3\}.$$

The full modular group $\Gamma(1)$ acts on the four functions

$$f_\infty(\tau) = 3^{12}\eta(3\tau)^{24}, \quad f_0(\tau) = \eta\left(\frac{\tau}{3}\right)^{24}, \quad f_1(\tau) = \eta\left(\frac{\tau+1}{3}\right)^{24}, \quad f_2(\tau) = \eta\left(\frac{\tau+2}{3}\right)^{24}$$

by permuting them according to A_4 since the two permutations

$$\begin{aligned}
f_\infty(-1/\tau) &= \tau^{12} f_0(\tau), & f_\infty(\tau+1) &= f_\infty(\tau),\\
f_0(-1/\tau) &= \tau^{12} f_\infty(\tau), & f_0(\tau+1) &= f_1(\tau),\\
f_1(-1/\tau) &= \tau^{12} f_2(\tau), & f_1(\tau+1) &= f_2(\tau),\\
f_2(-1/\tau) &= \tau^{12} f_1(\tau), & f_2(\tau+1) &= f_0(\tau)
\end{aligned}$$

generate all of A_4. It is not hard to show that the kernel of this homomorphism $\Gamma(1) \to A_4$ is exactly $\pm\Gamma(3)$. Suppose f_∞ and f_0 are fixed by some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$. Thse two conditions are equivalent to

$$\begin{aligned}
\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} a & 3b \\ c/3 & d \end{pmatrix} \in \Gamma(1),\\
\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}^{-1} &= \begin{pmatrix} a & b/3 \\ 3c & d \end{pmatrix} \in \Gamma(1).
\end{aligned}$$

Therefore, we must have $b \equiv c \equiv 0 \bmod 3$, which is exactly the defining congruences for $\pm\Gamma(3)$. Now, any permutation in A_4 that fixes f_∞ and f_0 necessarily fixes f_1 and f_2, so we have shown that the kernel is exactly $\pm\Gamma(3)$.

Since S_3 has a normal subgroup whose factor group is $\mathbb{Z}_2$, there is a group Γ^2 with $\Gamma(1)/\Gamma^2 \simeq \mathbb{Z}_2$. Similarly, A_4 has a normal subgroup $(\mathbb{Z}_2 \times \mathbb{Z}_2)$ whose factor group is $\mathbb{Z}_3$, so there is a group Γ^3 with $\Gamma(1)/\Gamma^3 \simeq \mathbb{Z}_3$. In summary,

$$\begin{aligned}
\Gamma(2) \trianglelefteq \Gamma^2 \trianglelefteq \Gamma(1) \quad &\text{with} \quad \Gamma(1)/\Gamma^2 \simeq \mathbb{Z}_2,\\
\pm\Gamma(3) \trianglelefteq \Gamma^3 \trianglelefteq \Gamma(1) \quad &\text{with} \quad \Gamma(1)/\Gamma^3 \simeq \mathbb{Z}_3.
\end{aligned}$$

For a given subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, let $\bar{\Gamma}$ denote $\Gamma/\pm I$, that is, the equivalent classes of matrices up to sign. Sometimes, if we are very careful, we will denote these elements with a bar over them. Note that

$$\begin{aligned}\bar{\Gamma}(1)/\bar{\Gamma}(2) &\simeq S_3, \quad \bar{\Gamma}(1)/\bar{\Gamma}^2 \simeq \mathbb{Z}_2,\\ \bar{\Gamma}(1)/\bar{\Gamma}(3) &\simeq A_4, \quad \bar{\Gamma}(1)/\bar{\Gamma}^3 \simeq \mathbb{Z}_3.\end{aligned}$$

Also, let G^{ab} denote the Abelianization of G, the quotient of G and its commutator subgroup. We have the following universal property of the Abelianization: if $\phi : G \to \mathrm{im}(\phi)$ is a homomorphism to an Abelian group, then there is a unique homomorphism $h : G^{\mathrm{ab}} \to \mathrm{im}(\phi)$ so that the diagram

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G^{\mathrm{ab}} \\ & \searrow^{\phi} & \downarrow h \\ & & \mathrm{im}(\phi) \end{array}$$

commutes. Since $\bar{\Gamma}(1)$ is generated by $\bar{S}$ and $\bar{S}\bar{T}$ and these elements have orders two and three, respectively, it follows that

$$\bar{\Gamma}(1)^{\mathrm{ab}} \subset \{\bar{S}^i(\bar{S}\bar{T})^j \mid i \in \{0,1\}, j \in \{0,1,2\}\} \simeq \mathbb{Z}_6.$$

Now define $\pi : \bar{\Gamma}(1) \to \mathbb{Z}_6$ by

$$\pi\left(\left(\begin{array}{cc} a & b \\ c & d \end{array}\right)\right) = \frac{\eta\left(\frac{a\tau+b}{c\tau+d}\right)^4}{(c\tau+d)^2\eta(\tau)^4},$$

where we have identified $\mathbb{Z}_6$ with the sixth roots of unity. Since $\pi(\bar{S}) = -1$ and $\pi(\bar{T}) = \zeta_6$, we see that π is a surjection, and so

$$\bar{\Gamma}(1)^{\mathrm{ab}} \simeq \mathbb{Z}_6.$$

Proposition 2.11.2. *The function $\eta(\tau)^4$ is modular in weight 2 with respect to $\Gamma(2) \cap \Gamma(3)$, i.e.*

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right)^4 = (c\tau+d)^2\eta\left(\tau\right)^4, \text{ for } \left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \in \Gamma(2) \cap \Gamma(3).$$

Proof. The natural projection map $\phi : \overline{\Gamma}(1) \to \overline{\Gamma}(1)/\overline{\Gamma}^2 \times \overline{\Gamma}(1)/\overline{\Gamma}^3$ has image $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$, which is Abelian. By the universal property of the Abelianization, we have $\phi = h \circ \pi$, where, in this case, h must be an isomorphism. Therefore, $\ker(\pi) = \ker(\phi) = \overline{\Gamma}^2 \cap \overline{\Gamma}^3 \subset \overline{\Gamma}(2) \cap \overline{\Gamma}(3)$. □

According to Proposition 2.11.2, if we want to find the sixth root of unity $\epsilon(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$ so that

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right)^4 = \epsilon\left(\left(\begin{array}{cc} a & b \\ c & d \end{array}\right)\right)(c\tau+d)^2\eta\left(\tau\right)^4, \text{ for } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1),$$

it suffices to find a formula for $\epsilon(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))$ that satsifies

$$\begin{aligned}\eta\left(\frac{a\tau+b}{c\tau+d}\right)^{12} &= \epsilon\left(\left(\begin{array}{cc} a & b \\ c & d \end{array}\right)\right)^3(c\tau+d)^6\eta\left(\tau\right)^{12}, \text{ for } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1),\\ \eta\left(\frac{a\tau+b}{c\tau+d}\right)^{8} &= \epsilon\left(\left(\begin{array}{cc} a & b \\ c & d \end{array}\right)\right)^2(c\tau+d)^4\eta\left(\tau\right)^{8}, \text{ for } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1).\end{aligned}$$

for just the *finite* number of elements in $\Gamma(1)/\Gamma(2)$ for the first formula and $\Gamma(1)/\pm\Gamma(3)$ for the second formula. For $\Gamma(1)/\Gamma(2)$, we have,

$$\begin{aligned}
&\epsilon\left(\begin{pmatrix}1&0\\0&1\end{pmatrix}\right)^3=1 \qquad \epsilon\left(\begin{pmatrix}0&1\\1&0\end{pmatrix}\right)^3=-1,\\
&\epsilon\left(\begin{pmatrix}1&1\\1&0\end{pmatrix}\right)^3=1 \qquad \epsilon\left(\begin{pmatrix}1&0\\1&1\end{pmatrix}\right)^3=-1,\\
&\epsilon\left(\begin{pmatrix}0&1\\1&1\end{pmatrix}\right)^3=1 \qquad \epsilon\left(\begin{pmatrix}1&1\\0&1\end{pmatrix}\right)^3=-1.
\end{aligned} \tag{2.11.1}$$

For $\Gamma(1)/\pm\Gamma(3)$, we have

$$\begin{aligned}
&\epsilon\left(\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}\right)^2=\zeta_3^0 \quad \epsilon\left(\pm\begin{pmatrix}0&1\\2&2\end{pmatrix}\right)^2=\zeta_3^1 \quad \epsilon\left(\pm\begin{pmatrix}0&1\\2&1\end{pmatrix}\right)^2=\zeta_3^2,\\
&\epsilon\left(\pm\begin{pmatrix}0&1\\2&0\end{pmatrix}\right)^2=\zeta_3^0 \quad \epsilon\left(\pm\begin{pmatrix}1&0\\2&1\end{pmatrix}\right)^2=\zeta_3^1 \quad \epsilon\left(\pm\begin{pmatrix}1&0\\1&1\end{pmatrix}\right)^2=\zeta_3^2,\\
&\epsilon\left(\pm\begin{pmatrix}1&1\\1&2\end{pmatrix}\right)^2=\zeta_3^0 \quad \epsilon\left(\pm\begin{pmatrix}1&1\\0&1\end{pmatrix}\right)^2=\zeta_3^1 \quad \epsilon\left(\pm\begin{pmatrix}1&1\\2&0\end{pmatrix}\right)^2=\zeta_3^2,\\
&\epsilon\left(\pm\begin{pmatrix}1&2\\2&2\end{pmatrix}\right)^2=\zeta_3^0 \quad \epsilon\left(\pm\begin{pmatrix}1&2\\1&0\end{pmatrix}\right)^2=\zeta_3^1 \quad \epsilon\left(\pm\begin{pmatrix}1&2\\0&1\end{pmatrix}\right)^2=\zeta_3^2.
\end{aligned} \tag{2.11.2}$$

In order to complete these calculations, we write each matrix in $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ (resp. $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$) as a word in S and T modulo 2 (resp. 3) and apply the homomorphism $(T\mapsto\zeta_2,\ S\mapsto\zeta_2)$ (resp. $(T\mapsto\zeta_3,\ S\mapsto 1)$). Noticing that $1-c^2$ is congruent to 0 mod 2 (resp. 3) only when c is not congruent to 0 mod 2 (resp. 3), we split the evaluations into the two cases $c\equiv 0 \bmod 2$ (resp. 3) and $c\not\equiv 0 \bmod 2$ (resp. 3). By inspection of (2.11.1) and (2.11.2), we see that

$$\begin{aligned}
\epsilon\left(\begin{pmatrix}a&b\\c&d\end{pmatrix}\right)^3&=\begin{cases}\zeta_2^{bd} & ,\ c\equiv 0 \bmod 2\\ \zeta_2^{a+d+1} & ,\ c\not\equiv 0 \bmod 2\end{cases},\\
\epsilon\left(\pm\begin{pmatrix}a&b\\c&d\end{pmatrix}\right)^2&=\begin{cases}\zeta_3^{bd} & ,\ c\equiv 0 \bmod 3\\ \zeta_3^{(a+d)c} & ,\ c\not\equiv 0 \bmod 3\end{cases}.
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
\epsilon\left(\begin{pmatrix}a&b\\c&d\end{pmatrix}\right)^3&=\zeta_2^{bd(1-c^2)+(a+d+1)c},\\
\epsilon\left(\begin{pmatrix}a&b\\c&d\end{pmatrix}\right)^2&=\zeta_3^{bd(1-c^2)+(a+d)c},
\end{aligned}$$

and so,

$$\begin{aligned}
\epsilon\left(\begin{pmatrix}a&b\\c&d\end{pmatrix}\right)&=\epsilon_6\left(\begin{pmatrix}a&b\\c&d\end{pmatrix}\right)^3/\epsilon_6\left(\begin{pmatrix}a&b\\c&d\end{pmatrix}\right)^2\\
&=\zeta_6^{bd(1-c^2)+(a+d+3)c}.
\end{aligned}$$

Finally, setting $\tau=it-d/c$ in the transformation formula

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right)^4=\zeta_6^{bd(1-c^2)+(a+d+3)c}(c\tau+d)^2\eta(\tau)^4,$$

and keeping in mind that $ad - bc = 1$, we derive

$$(ict)^2\ e^{\frac{\pi}{3c^2t}}\ \eta\left(\frac{-d}{c} + it\right)^4 \sim e\left(-\frac{ac}{6} + \frac{a}{6c} + \frac{bc^2d}{6} - \frac{bd}{6} - \frac{cd}{6} - \frac{c}{2}\right).$$

In order to determine the correct fourth root, we need a formula for an odd power of the η function. Fortunately, the relation

$$\eta(\tau)^3 = \frac{1}{2}\Theta_2(\tau)\Theta_3(\tau)\Theta_4(\tau) \tag{2.11.3}$$

is a consequence of Jacobi's triple product identity (see Exercise 2.12.4). Let us now assume that c is odd and apply the asymptotic for the Θ functions derived in Section 2.9. These formulas give

$$\begin{aligned}(ict)^{3/2}\ e^{\frac{\pi}{4c^2t}}\ \eta\left(it - \frac{d}{c}\right)^3 &\sim \begin{cases}\left(\frac{d}{|c|}\right)\zeta_c^{(8d)^{-1}_{\bmod c}}\zeta_8^{5c+2d+cd+2}, & d \text{ odd}\\ \left(\frac{d}{|c|}\right)\zeta_c^{(8d)^{-1}_{\bmod c}}\zeta_8^{3c-2d+cd}, & d \text{ even}\end{cases}\\ &= \left(\frac{d}{|c|}\right)\zeta_c^{(8d)^{-1}_{\bmod c}}\zeta_8^{c(3-d)},\\ &= \left(\frac{d}{|c|}\right)e\left(\frac{a(1-c^2)}{8c} - \frac{cd}{8} + \frac{3c}{8}\right),\end{aligned}$$

where we have cleverly combined the two cases into one that holds for all d and used the elementary observation that

$$\frac{(8d)^{-1}_{\bmod c}}{c} \equiv \frac{(1-c^2)a}{8c} \mod 1$$

for odd c (recall that $ad - bc = 1$ so $a = d^{-1}_{\bmod c}$). Also, this is well-defined because $c^2 - 1 \equiv 0 \bmod 8$. Finally, since $c^2 - 1 \equiv 0 \bmod 8$,

$$\begin{aligned}\sqrt{ict}\ e^{\frac{\pi}{12c^2t}}\ \eta\left(\frac{-d}{c} + it\right) &= e\left(c - \frac{bd(c^2-1)}{8}\right)\frac{(ict)^2\ e^{\frac{\pi}{3c^2t}}\ \eta\left(it - \frac{d}{c}\right)^4}{(ict)^{3/2}\ e^{\frac{\pi}{4c^2t}}\ \eta\left(it - \frac{d}{c}\right)^3}\\ &\sim \left(\frac{d}{|c|}\right)e\left(-\frac{ac}{24} + \frac{a}{24c} + \frac{bc^2d}{24} - \frac{bd}{24} - \frac{cd}{24} + \frac{c}{8}\right).\end{aligned}$$

After eliminating b via $ad-bc = 1$ and replacing a by $d^{-1}_{\bmod c}$, this becomes the assertion of the proposition for c odd. The case d odd can be dealt with similarly, but we can also use $\eta(-1/\tau) = \sqrt{-i\tau}\eta(\tau)$, and, when relating d_c^{-1} to c_d^{-1}, we can use

$$\frac{d_c^{-1}}{c} + \frac{c_d^{-1}}{d} \equiv \frac{1}{cd} \mod 1.$$

2.12 Exercises

Exercise 2.12.1. *Prove part (4) of Proposition 2.10.2. You will have to actually work out the third intersection point of a line with the curve $y^2 = 4x^3 - g_2x - g_3$.*

Exercise 2.12.2. *Prove all parts of Proposition 2.4.1*

Exercise 2.12.3 (Lipschitz summation formula)**.** *For integers $k \geq 1$, show*

$$\frac{1}{\zeta(2k)}\sum_{n=-\infty}^{\infty}\frac{1}{(z+n)^{2k}} = \frac{2}{\zeta(1-2k)}\sum_{j=1}^{\infty}j^{2k-1}q_z^j.$$

You might need the functional equation for ζ in the form

$$\frac{2}{\zeta(1-2k)} = \frac{(2\pi i)^{2k}}{(2k-1)!}\frac{1}{\zeta(2k)}.$$

Exercise 2.12.4. *Via Jacobi's triple product identity, show that*

$$\Theta_2(0|\tau) = 2\frac{\eta(2\tau)^2}{\eta(\tau)} = 2q^{1/8} + \cdots,$$
$$\Theta_3(0|\tau) = \frac{\eta(\tau)^5}{\eta(2\tau)^2\eta(\tau/2)^2} = 1 + 2q^{1/2} + \cdots,$$
$$\Theta_4(0|\tau) = \frac{\eta(\tau/2)^2}{\eta(\tau)} = 1 - 2q^{1/2} + \cdots.$$

Exercise 2.12.5. *This exercise deals with the theta subgroup*

$$\Gamma_\vartheta = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid ab \equiv cd \equiv 0 \mod 2 \right\}.$$

1. *Show that S and T^2 generate $\Gamma_\vartheta/\pm I$. Possible hint: first show that every rational number is Γ_ϑ-equivalent to either $1(= 1/1)$ or $i\infty(= 1/0)$ and deduce a fundamental domain that has $3 = [\Gamma(1) : \Gamma_\vartheta]$ translates of the fundamental domain for $\Gamma(1)$.*

2. *Deduce that the multiplier system for Θ_3 satisfies*

$$\Theta_3\left(0\Big|\frac{a\tau+b}{c\tau+d}\right) = \Theta_3(0|\tau) \times \begin{cases} \left(\frac{d}{c}\right) e\left(\frac{1-c}{8}\right)\sqrt{-i(c\tau+d)} & , c \text{ odd} \\ \left(\frac{c}{d}\right) e\left(\frac{d-1}{8}\right)\sqrt{c\tau+d} & , d \text{ odd} \end{cases}$$

for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_\vartheta$. Hint: Let $\tau = it - d/c$ and use the asymptotics at the cusps and be careful with the branches of the square root: $-\pi/2 < \operatorname{Arg}(\sqrt{z}) \leq \pi/2$ and the properties of the Jacobi symbol.

Exercise 2.12.6. *Show that for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$*

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right) = \sqrt{-i(c\tau+d)}\eta(\tau) \times \begin{cases} \left(\frac{d}{c}\right)\zeta_{24}^{3(1-c)+c(a+d)+bd(1-c^2)} & , c \text{ odd} \\ \left(\frac{c}{|d|}\right)\zeta_{24}^{3d+d(b-c)+ac(1-d^2)} & , d \text{ odd} \end{cases}.$$

Exercise 2.12.7. *Investigate*

$$\frac{\log|\Theta_3\left(it + \frac{1+\sqrt{5}}{2}\right)|}{\log(t)}$$

as $t \to 0^+$.

Exercise 2.12.8. *The Weierstrass σ function for the lattice $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$ is the entire function defined as*

$$\sigma(z|\tau) = z\prod_{\omega\in\Lambda'}\left(1 - \frac{z}{\omega}\right)e^{\frac{z}{\omega}+\frac{z^2}{2\omega^2}}.$$

The product is absolutely convergent. For $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$ and integers A, B with $\omega = A\tau + B$, show that

$$\wp(z|\tau) = -\frac{\partial^2}{\partial z^2}\sigma(z|\tau)$$
$$\sigma(z|\tau) = \frac{-e^{\frac{\pi^2}{6}E_2(\tau)z^2}}{2\pi\eta(\tau)^3}\Theta_1(z|\tau)$$
$$\sigma\left(\frac{z}{c\tau+d}\Big|\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{-1}\sigma(z|\tau)$$
$$\frac{\sigma(z+\omega|\tau)}{\sigma(z|\tau)} = (-1)^{A+B+AB}e\left(-\frac{(6A+\pi iE_2(\tau)\omega)(2z+\omega)}{12}\right)$$

Exercise 2.12.9. *Use Proposition 2.7.1 to get*

$$E_8 = E_4^2$$
$$E_{10} = E_4 E_6$$

Chapter 3

Theory of Modular Forms on $\mathrm{SL}_2(\mathbb{Z})$

3.1 Definition of a Modular Form

Define the slash operator $|_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right),k}$ in weight k (an integer) for a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with positive determinant as

$$f|_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right),k}(\tau) = \frac{(ad-bc)^{k-1}}{(c\tau+d)^k} f\left(\frac{a\tau+b}{c\tau+d}\right).$$

One can easily check that this operation is compatible with matrix multiplication, that is,

$$f|_{M_1,k}|_{M_2,k}(\tau) = f|_{M_1M_2,k}(\tau).$$

Here, $|_{M_1,k}|_{M_2,k}$ means the result of applying $|_{M_1,k}$ followed by $|_{M_2,k}$.

Now suppose that $f(\tau)$ has period 1 ($f|_T = f$) so that it has a Fourier series expansion in the form

$$f(\tau) = \sum_{k=-\infty}^{\infty} a_k q^k. \tag{3.1.1}$$

We say:

1. $f(\tau)$ is meromorphic at ∞ if only finitely many negative powers of q appear in (3.1.1).
2. $f(\tau)$ is holomorphic at ∞ if only no (strictly) negative powers of q appear in (3.1.1).
3. $f(\tau)$ is vanishes at ∞ if only (strictly) powers of q appear in (3.1.1).

Since $T \in \Gamma(1)$, the following definition makes sense.

Definition 3.1.1. *Suppose that*

$$f|_{g,k}(\tau) = f(\tau), \text{ for all } g \in \Gamma(1) \text{ and almost all } \tau \in \mathbb{H}.$$

Define the various spaces A_k, $M_k^!$, M_k, S_k for any integer k as

1. *Automorphic forms of weight k:*
$$A_k(\Gamma(1)) = \{f(\tau) \mid f \text{ meromorphic on } \mathbb{H} \text{ and meromorphic at } \infty\}.$$
2. *Weakly-modular forms of weight k:*
$$M_k^!(\Gamma(1)) = \{f(\tau) \mid f \text{ holomorphic on } \mathbb{H} \text{ and meromorphic at } \infty\}.$$
3. *Modular forms of weight k:*
$$M_k(\Gamma(1)) = \{f(\tau) \mid f \text{ holomorphic on } \mathbb{H} \text{ and holomorhpic at } \infty\}.$$
4. *Cusp forms of weight k:*
$$S_k(\Gamma(1)) = \{f(\tau) \mid f \text{ holomorphic on } \mathbb{H} \text{ and vanishes at } \infty\}.$$

3.2 Valence Formula

For any $\tau_0 \in \mathbb{H} \cup \{\infty\}$, define the order of a meromorphic function as

$$\mathrm{ord}_{\tau_0}(f) = \begin{cases} \text{smallest power of } (\tau - \tau_0) \text{ in the Laurent series expansion of } f \text{ at } \tau_0 & , \tau_0 \in \mathbb{H} \\ \text{smallest power of } q \text{ in the } q\text{-series expansion of } f & , \tau_0 = \infty \end{cases}.$$

Proposition 3.2.1. *If $f \in A_k(\Gamma(1))$ is not a constant, then*

$$\mathrm{ord}_\infty(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_{e(\frac{1}{3})}(f) + \sum_{\substack{\tau \in \mathbb{H}/\Gamma(1) \\ \tau \neq i, e(\frac{1}{3})}} \mathrm{ord}_\tau(f) = \frac{k}{12}.$$

Proposition 3.2.2. *If $f \in A_k(\Gamma(1))$ is not a constant, then*

1. *k is even*
2. *Set $\zeta = e(\frac{1}{3})$ and $n = \mathrm{ord}_\zeta(f)$. Then, $n \equiv -k/2 \bmod 3$, and f has an expansion in the local variable at ζ of the form*
$$\left(\frac{\tau - \bar{\zeta}}{\zeta - \bar{\zeta}}\right)^k f(\tau) = \sum_{j=0}^{\infty} c_j \left(\frac{\tau - \zeta}{\tau - \bar{\zeta}}\right)^{n+3j}, \quad c_0 \neq 0.$$
3. *Set $\zeta = i$ and $n = \mathrm{ord}_\zeta(f)$. Then, $n \equiv -k/2 \bmod 2$, and f has an expansion in the local variable at ζ of the form*
$$\left(\frac{\tau - \bar{\zeta}}{\zeta - \bar{\zeta}}\right)^k f(\tau) = \sum_{j=0}^{\infty} c_j \left(\frac{\tau - \zeta}{\tau - \bar{\zeta}}\right)^{n+2j}, \quad c_0 \neq 0.$$

Proof. Since $-I \in \Gamma(1)$, (1) follows.

For (2), set $\zeta = e(\frac{1}{3})$ and $t = \frac{\tau - \zeta}{\tau - \bar{\zeta}}$. The fact that $n \equiv -k/2 \bmod 3$ follows easily from the valence formula. Next with $g(t)$ defined for $|t| < 1$ by

$$\left(\frac{\tau - \bar{\zeta}}{\zeta - \bar{\zeta}}\right)^k f(\tau) = t^n g(t)$$

Note that $g(t)$ is holomorphic at $t = 0$. One checks that the relation $f(-1 - 1/\tau) = \tau^k f(\tau)$ is equivlant to $g(\zeta t) = \zeta^{k-n} g(t)$. Since $g(0) \neq 0$, this provides another proof of the fact that $n \equiv k \bmod 3$. Also, $g(t)$ has a expansion in non-negative powers of t that are all multiples of 3 since $g(\zeta t) = g(t)$.

A similar argument establishes (3).

□

3.3 Dimension Formulas and Generators

Proposition 3.3.1. *We have*

1. *$A_{k_1} \cap A_{k_2} = \{0\}$ for $k_1 \neq k_2$.*
2. *$A_{k_1} \cdot A_{k_2} \subset A_{k_1+k_2}$.*
3. *$M_0^!(\Gamma(1)) = \mathbb{C}[j(\tau)]$.*
4. *$A_0(\Gamma(1)) = \mathbb{C}(j(\tau))$.*

5. $S_k(\Gamma(1)) = \Delta(\tau) M_{k-12}(\Gamma(1))$.

6. $M_k(\Gamma(1)) = \bigoplus_{\substack{4a+6b=k \\ a,b\geq 0}} \mathbb{C} E_4^a E_6^b$. *Also,*

$$\sum_{k=-\infty}^{\infty} \dim M_k(\Gamma(1)) t^k = \frac{1}{(1-t^4)(1-t^6)} = \frac{1+t^4+t^6+t^8+t^{10}+t^{14}}{(1-t^{12})^2}$$
$$= 1 + t^4 + t^6 + t^8 + t^{10} + 2t^{12} + t^{14} + 2t^{16} + 2t^{18} + 2t^{20} + \cdots.$$

Proof. (3). By subtracting powers of the j function ($j = \frac{1}{q} + \cdots$), for any $f \in M_0^!(\Gamma(1))$ we can write

$$f(\tau) - P(j(\tau)) = O(q)$$

where P is a polynomial. The valence formula implies that $f(\tau) - P(j(\tau))$ vanishes identically because it is a function of weight 0 without any poles and a zero at ∞.

(4). Given any $f(\tau) \in A_0(\Gamma(1))$, we can multiply it by a suitable polynoimal in $j(\tau)$ to obtain a function in $M_0^!(\Gamma(1))$. By (3), $f(\tau)$ must be a rational function of $j(\tau)$.

(5). If $f(\tau) \in S_k(\Gamma(1))$ then $f(\tau)/\Delta(\tau) \in M_{k-12}(\Gamma(1))$ since $\Delta(\tau)$ has no zeros on $\mathbb{H}$ (Proposition 2.4.1) and a simple zero at ∞.

(6). The valence formula implies that $\dim(M_k(\Gamma(1))) = 0$ for $k = 2$ or $k < 0$ (or k odd) and that $\dim(M_0(\Gamma(1))) = 1$. Suppose that k is even and $f(\tau) = c + O(q) \in M_k(\Gamma(1))$. Then,

$$f(\tau) = cE_k(\tau) + (E_4(\tau)^3 - E_6(\tau)^2) g(\tau)$$

where $g(\tau) \in M_{k-12}(\tau)$. Since we have already shown that E_k is a polynomial in E_4 and E_6, by induction we obtain that f is of the form

$$f(\tau) = \sum_{\substack{4a+6b=k \\ a,b\geq 0}} c_{a,b} E_4^a E_6^b.$$

This representation is unique because if

$$0 = \sum_{\substack{4a+6b=k \\ a,b\geq 0}} c_{a,b} E_4^a E_6^b$$

for some k and some choice of $c_{a,b}$ then muliplying by $E_4^{-k/4}$ shows that E_6^2/E_4^3 is constant, which it is not. □

Proposition 3.3.2. *The map $\tau \mapsto j(\tau)$ defines a bijection between $\mathbb{H}/\Gamma(1)$ and $\mathbb{C}$.*

Proof. The function $j(\tau) - c \in A_0(\Gamma(1))$ has exactly pole (at ∞) so has exactly one zero. □

3.4 Applications to Identities

Proposition 3.4.1.

$$\Delta(\tau) = (2\pi)^{12} \eta(\tau)^{24}.$$

Proof. $\dim S_{12}(\Gamma(1)) = 1$ and the first term in the q-series expansion of Δ is given in Proposition 2.4.1. □

Proposition 3.4.2. *Let f_i be a non-constant element of $M_{k_i}(\Gamma(1))$ for $i = 1, 2, 3$. Then, there is a nontrivial algebraic relation of the form*

$$P(f_1, f_2, f_3) = 0,$$

for some polynomial P.

Proof. Consider the set

$$F_k = \left\{ f_1^a f_2^b f_3^c \right\}_{\substack{a,b,c \geq 0 \\ ak_1 + bk_2 + ck_3 = k}}.$$

We have (as $k \to \infty$)

$$\begin{aligned} |F_0| + |F_1| + \cdots + |F_k| &= |\{(a, b, c) \in \mathbb{Z}_{\geq 0}^3 \mid ak_1 + bk_2 + ck_3 \leq k\}| \\ &\sim \frac{1}{3!} \frac{k^3}{k_1 k_2 k_3}. \end{aligned}$$

If f_1, f_2, f_3 were algebraically independent, F_k would be a set of linearly independent elements of M_k for any k. Therefore, $|F_k| \leq \dim M_k$ and

$$\begin{aligned} |F_0| + |F_1| + \cdots + |F_k| &\leq \dim M_0 + \dim M_1 + \cdots + \dim M_k \\ &\sim \frac{1}{2!} \frac{k^2}{4 \cdot 6}, \end{aligned}$$

which is a contradition for large k. □

One should note that Propostion 3.4.2 applies not only to $\Gamma(1)$ but to any finite index subgroup Γ of $\Gamma(1)$, as later we will show that

$$\dim M_k(\Gamma) \sim \frac{k}{12} [\Gamma(1) : \Gamma],$$

where this formula is restricted to even k when $-I \in \Gamma$.

Proposition 3.4.3. *The three Θ constants $\Theta_2(\tau), \Theta_3(\tau), \Theta_4(\tau)$ are algebraically dependent, and*

$$\Theta_3(\tau)^4 = \Theta_2(\tau)^4 + \Theta_4(\tau)^4.$$

Proof. We can obtain the algebraic dependence from Propostion 3.4.2 with $f_i = \Theta_2^{8i} + \Theta_3^{8i} + \Theta_4^{8i}$. In order to actually obtain the relation, we compute that

$$\begin{aligned} 2E_4 &= \Theta_2^8 + \Theta_3^8 + \Theta_4^8, \\ 2E_4^2 &= \Theta_2^{16} + \Theta_3^{16} + \Theta_4^{16}, \\ E_4^2 &= \Theta_2^8 \Theta_3^8 + \Theta_3^8 \Theta_4^8 + \Theta_4^8 \Theta_2^8, \\ 2^8 \eta^{24} &= \Theta_2^8 \Theta_3^8 \Theta_4^8, \end{aligned}$$

since M_4, M_8 and S_{12} are all one-dimensional. Therefore,

$$\begin{aligned} 0 &= \Theta_2^{16} + \Theta_3^{16} + \Theta_4^{16} - 2\left(\Theta_2^8 \Theta_3^8 + \Theta_4^8 \Theta_3^8 + \Theta_2^8 \Theta_4^8\right) \\ &= \left(\Theta_2^4 - \Theta_3^4 - \Theta_4^4\right)\left(\Theta_2^4 + \Theta_3^4 - \Theta_4^4\right)\left(\Theta_2^4 - \Theta_3^4 + \Theta_4^4\right)\left(\Theta_2^4 + \Theta_3^4 + \Theta_4^4\right). \end{aligned}$$

By examining the q-series expansions, we see that it must be the third term that vanishes identically. □

We will frequently use Ramanujan's differential operator θ defined by

$$\theta f(\tau) = \frac{1}{2\pi i} \frac{d}{d\tau} f(\tau) = q \frac{d}{dq} f(\tau).$$

Lemma 3.4.4. *The operator*

$$f(\tau) \mapsto \theta f(\tau) - \frac{k}{12} E_2(\tau) f(\tau)$$

maps $M_k(\Gamma(1))$ to $M_{k+2}(\Gamma(1))$ (and $A_k(\Gamma(1))$ to $A_{k+2}(\Gamma(1))$).

Proof. Exercise. □

Proposition 3.4.5.

$$\theta j(\tau) = -\frac{E_6(\tau)}{E_4(\tau)} j(\tau).$$

Proof. Exercise. □

3.5 Exercises

Exercise 3.5.1. *Show that*

$$f(\tau) \mapsto \theta f(\tau) - \frac{k}{12} E_2(\tau) f(\tau)$$

maps $A_k \to A_{k+2}$, $M_k \to M_{k+2}$, and $S_k \to S_{k+2}$.

Exercise 3.5.2. *Show that*

$$\theta j(\tau) = -\frac{E_6(\tau)}{E_4(\tau)} j(\tau).$$

Hint: $j = E_4^3/\eta^{24}$ and $M_{14}(\Gamma(1)) = \mathbb{C} E_4^2 E_6$.

Exercise 3.5.3. *Express $j(\tau)$ as a rational function of the elliptic λ function, which is defined by*

$$\lambda(\tau) = \frac{\Theta_2(\tau)^4}{\Theta_3(\tau)^4} = 1 - \frac{\Theta_4(\tau)^4}{\Theta_3(\tau)^4}.$$

Exercise 3.5.4. *Show that $E_4(\frac{-1+\sqrt{-3}}{2}) = 0$ and $E_6(\sqrt{-1}) = 0$ and deduce the following values of the j function at quadratic irrationals:*

$$j(\tfrac{-1+\sqrt{-3}}{2}) = 0,$$
$$j(\sqrt{-1}) = 12^3.$$

Chapter 4

Theory of Modular Forms on Congruence Subgroups of $\mathrm{SL}_2(\mathbb{Z})$

In this chapter several ways of building modular forms on conruence subgroups of $\Gamma(1)$ are presented. Although there certainly are other methods, we will contruct functions by means of

- Klein forms and Eisenstein series. These turn out to be specializations of the functions $\sigma(z)$ and $\zeta(z), \wp(z), \wp'(z), \wp''(z), \ldots$ functions to points $z \in \frac{1}{N}\mathbb{Z} + \frac{1}{N}\mathbb{Z}\tau$. These produce modular functions and forms on $\Gamma(N)$.
- Θ functions from any positive definite qudratic form. If the quadratic form takes values in the even integers and its dual takes values in $\frac{1}{N}\mathbb{Z}$, then the resulting Θ function is modular with respect to $\Gamma_0(N)$.
- The η function $q^{-1/24}\prod_{n=1}^{\infty}(1-q^n)$ can be generalized, leading to a function that is invariant under a subgroup of $\Gamma_0(N)$ of index 2.

Using the theory developed in this chapter, many identities involving these functions can be easily obtained.

4.1 Definition of modular forms on Γ with $[\Gamma(1) : \Gamma] < \infty$

Extend the action of $\mathrm{SL}_2(\mathbb{Z})$ to include $\mathbb{Q} \cup \{\infty\}$ by setting

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\frac{p}{q}\right) = \frac{ap+bq}{cp+dq},$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(-\frac{d}{c}\right) = \infty,$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\infty) = \frac{a}{c}.$$

We will also set $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$.

We need to make sense of the order of vanishing of a function on the quotient $\overline{\mathbb{H}}/\Gamma$

Definition 4.1.1. *Let $[\Gamma(1) : \Gamma] < \infty$ and let f be a non-constant function such that $f|_{M,k} = f$ for all $M \in \Gamma$. We define the invariant order of the function f at a point $\tau_0 \in \overline{\mathbb{H}}$ with respect to Γ as follows. (Note: $c_n \neq 0$.)*

1. *For any* $\tau_0 \in \mathbb{H}$,
$$\mathrm{ord}_{\tau_0}(f,\Gamma) = \frac{n}{|\overline{\Gamma}_{\tau_0}|} \text{ where } f = \sum_{m\geq n} c_m(\tau-\tau_0)^m.$$
Points where $|\overline{\Gamma}_{\tau_0}| = 2$ *are called elliptic points of order two, and these only occur at points in* $\Gamma(1)(i)$. *The size of the* Γ*-equivalence class of elliptic points of order two is denoted by* ϵ_2.
Points where $|\overline{\Gamma}_{\tau_0}| = 3$ *are called elliptic points of order three, and these only occur at points in* $\Gamma(1)(e(\frac{1}{3}))$. *The size of the* Γ*-equivalence class of elliptic points of order three is denoted by* ϵ_3.

2. *For* $\tau_0 \in \overline{\mathbb{Q}}$, *let* $\alpha \in \Gamma(1)$ *be such that* $\tau_0 = \alpha(\infty)$, *and let* $h \in \mathbb{Z}_{>0}$, *the width of the cusp* τ_0, *be defined by*
$$(\alpha^{-1}\overline{\Gamma}\alpha)_\infty = \left\langle \overline{\left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right)} \right\rangle.$$
Then,
$$\mathrm{ord}_{\tau_0}(f,\Gamma) = \begin{cases} n & \text{if } (\alpha^{-1}\Gamma\alpha)_\infty = \pm\left\langle \left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right)\right\rangle \text{ and } f|_\alpha = \sum_{m\geq n} c_m q^{\frac{m}{h}} \\ n & \text{if } (\alpha^{-1}\Gamma\alpha)_\infty = \left\langle +\left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right)\right\rangle \text{ and } f|_\alpha = \sum_{m\geq n} c_m q^{\frac{m}{h}} \\ n & \text{if } (\alpha^{-1}\Gamma\alpha)_\infty = \left\langle -\left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right)\right\rangle \text{ and } f|_\alpha = \sum_{m\geq n} c_m q^{\frac{m}{h}} \text{ and } k \text{ even} \\ \frac{n}{2} & \text{if } (\alpha^{-1}\Gamma\alpha)_\infty = \left\langle -\left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right)\right\rangle \text{ and } f|_\alpha = \sum_{m\geq n} c_m q^{\frac{m}{2h}} \text{ and } k \text{ odd} \end{cases}$$
These points are called cusps. The size of the Γ*-equivalence class of cusps is denoted by* ϵ_∞. *When the last condition is satisfied, the cusp is called irregular, otherwise it is called regular, the sizes of the* Γ*-equivalence classes of theses sets are denoted by* $\epsilon_\infty^{\mathrm{irr}}$ *and* $\epsilon_\infty^{\mathrm{reg}}$.

Definition 4.1.2. *If* $[\Gamma(1):\Gamma] < \infty$ *and* $\alpha \in \overline{\mathbb{Q}}$, *let* $h_\Gamma(\alpha)$ *be the width of the cusp* α *for* Γ. *The level of* Γ *is the least common multiple of all cusp widths. That is,*
$$\mathrm{level}(\Gamma) = \mathrm{lcm}(\{h_\Gamma(\alpha)\}_{\alpha\in\overline{\mathbb{Q}}}).$$

Definition 4.1.3. *Suppose that* $f|M, k = f$ *for all* $M \in \Gamma$.
$$\begin{aligned} A_k(\Gamma) &= \{f \mid \forall_{\tau\in\mathbb{H}}\, \mathrm{ord}_\tau(f,\Gamma) > -\infty \text{ and } \forall_{\tau\in\overline{\mathbb{Q}}}\, \mathrm{ord}_\tau(f,\Gamma) > -\infty\},\\ M_k^!(\Gamma) &= \{f \mid \forall_{\tau\in\mathbb{H}}\, \mathrm{ord}_\tau(f,\Gamma) \geq 0 \text{ and } \forall_{\tau\in\overline{\mathbb{Q}}}\, \mathrm{ord}_\tau(f,\Gamma) > -\infty\},\\ M_k(\Gamma) &= \{f \mid \forall_{\tau\in\mathbb{H}}\, \mathrm{ord}_\tau(f,\Gamma) \geq 0 \text{ and } \forall_{\tau\in\overline{\mathbb{Q}}}\, \mathrm{ord}_\tau(f,\Gamma) \geq 0\},\\ S_k(\Gamma) &= \{f \mid \forall_{\tau\in\mathbb{H}}\, \mathrm{ord}_\tau(f,\Gamma) \geq 0 \text{ and } \forall_{\tau\in\overline{\mathbb{Q}}}\, \mathrm{ord}_\tau(f,\Gamma) > 0\},\\ E_k(\Gamma) &= M_k(\Gamma)/S_k(\Gamma). \end{aligned}$$

For an example of an irregular cusp, take $\Gamma = \Gamma_1(4)$. The cusp $\frac{1}{2}$ is irregular. In this case $\frac{1}{2} = \left(\begin{smallmatrix}1 & 0\\ 2 & 1\end{smallmatrix}\right)(\infty)$, so $\alpha = \left(\begin{smallmatrix}1 & 0\\ 2 & 1\end{smallmatrix}\right)$, and
$$\begin{aligned} +\alpha\begin{pmatrix}1 & h\\ 0 & 1\end{pmatrix}\alpha^{-1} &= \begin{pmatrix}+1-2h & +h\\ -4h & +1+2h\end{pmatrix},\\ -\alpha\begin{pmatrix}1 & h\\ 0 & 1\end{pmatrix}\alpha^{-1} &= \begin{pmatrix}-1+2h & -h\\ +4h & -1-2h\end{pmatrix}. \end{aligned}$$
Thus, we see that $(\alpha^{-1}\Gamma_1(4)\alpha)_\infty$ is generated by $-\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$, which means that $\frac{1}{2}$ is an irregular cusp of width 1 for $\Gamma_1(4)$. Furthermore, for the cusp $0 = \alpha(\infty)$ where $\alpha = S$, the computation
$$\alpha\begin{pmatrix}1 & h\\ 0 & 1\end{pmatrix}\alpha^{-1} = \begin{pmatrix}1 & 0\\ -h & 1\end{pmatrix}$$
shows that $\frac{0}{1}$ is a regular cusp of width 4 for $\Gamma_1(4)$.

4.2 Dimension formulas

Proposition 4.2.1 (Valence Formula)**.** *If $f \in A_k(\Gamma)$ is not constant, then*

$$\sum_{\tau \in \overline{\mathbb{H}}/\Gamma} \operatorname{ord}_\tau(f, \Gamma) = \frac{k[\overline{\Gamma}(1) : \overline{\Gamma}]}{12}.$$

Proof. Let $d = [\overline{\Gamma}(1) : \overline{\Gamma}]$ and let $M_1, \ldots, M_d$ be a list of representatives of $\overline{\Gamma}\ \overline{\Gamma}(1)$. First assume that k is even and define

$$g(\tau) = \prod_j f|_{M_j,k}(\tau),$$

and note that $g \in M_{kd}(\Gamma(1))$. The valence formula for $\Gamma(1)$ now reads as

$$\operatorname{ord}_\infty(g, \Gamma(1)) + \sum_{\tau \in \mathbb{H}/\Gamma(1)} \operatorname{ord}_\tau(g, \Gamma(1)) = \frac{k[\overline{\Gamma}(1) : \overline{\Gamma}]}{12}.$$

We will deal with the points of finite order first.

$$\begin{aligned}
\operatorname{ord}_\tau(g) &= \sum_{j=1}^{i} \operatorname{ord}_\tau(f|_{M_j}) \\
&= \sum_{j=1}^{i} \operatorname{ord}_{M_j\tau}(f) \\
&= \sum_{z \in (\Gamma(1)\tau)/\Gamma} \frac{|\overline{\Gamma}(1)_\tau|}{|\overline{\Gamma}_z|} \operatorname{ord}_z(f)
\end{aligned}$$

Dividing this equality by $|\overline{\Gamma}(1)_\tau|$ and summing over all τ in the fundamental domain for $\Gamma(1)$ gives

$$\begin{aligned}
\sum_{\tau \in \mathbb{H}/\Gamma(1)} \operatorname{ord}_\tau(g, \Gamma(1)) &= \sum_{\tau \in \mathbb{H}/\Gamma(1)} \frac{\operatorname{ord}_\tau(g)}{|\overline{\Gamma}(1)_\tau|} \\
&= \sum_{z \in \mathbb{H}/\Gamma} \frac{\operatorname{ord}_\tau(g)}{|\overline{\Gamma}_\tau|} \\
&= \sum_{z \in \mathbb{H}/\Gamma} \operatorname{ord}_\tau(g, \Gamma).
\end{aligned}$$

For the cusps, we have the easy equality

$$\operatorname{ord}_\infty(g) = \sum_{\tau \in \overline{\mathbb{Q}}/\Gamma} \operatorname{ord}_\tau(f, \Gamma).$$

For odd k, we can apply the formula to g^2, and using

$$\operatorname{ord}_\tau(f^2, \Gamma) = 2 \operatorname{ord}_\tau(f, \Gamma),$$

we see that the formula is valid for odd k as well. □

Proposition 4.2.2 (Genus Formula)**.**

$$g = 1 + \frac{[\overline{\Gamma}(1) : \overline{\Gamma}]}{12} - \frac{\epsilon_2}{4} - \frac{\epsilon_3}{3} - \frac{\epsilon_\infty}{2}$$

Proof. Set $d = [\overline{\Gamma}(1) : \overline{\Gamma}]$. Define $f : \mathbb{H}/\Gamma \to \mathbb{H}/\Gamma(1)$ via the natural projection to the fundamental domain for $\Gamma(1)$. Triangulate the domain for $\Gamma(1)$ with

$$\begin{aligned} |F'| &= 2 \\ |E'| &= 3 \\ |V'| &= 3 \end{aligned}$$

with a vertex at i, $e(\frac{1}{3})$ and ∞. Pull back this trangulation via f^{-1}. For the triangulation of a fundamental domain for Γ, we have

$$\begin{aligned} |F| &= 2d \\ |E| &= 3d \\ |V| &= \epsilon_\infty + d - \sum_{z \in f^{-1}(i)} \begin{cases} 0, \text{ if } z \text{ is an elliptic point of order 2} \\ 1, \text{ if } z \text{ is not an elliptic point of order 2} \end{cases} \\ &\quad + d - \sum_{z \in f^{-1}(e(\frac{1}{3}))} \begin{cases} 0, \text{ if } z \text{ is an elliptic point of order 2} \\ 2, \text{ if } z \text{ is not an elliptic point of order 3} \end{cases} . \end{aligned}$$

Therefore, $|V| = \epsilon_\infty + d - \frac{1}{2}(d - \epsilon_2) + d - \frac{2}{3}(d - \epsilon_3)$ and the formula for the genus follows from $2 - 2g = |F| - |E| + |V|$. □

We next simply quote the dimension formulas from [6, Ch. 3], as the derivation requires the Riemann-Roch Theorem from the theory of Riemann surfaces. If we need the dimension of any specific one of these spaces in the future, hopefully we can give a self-contained argument.

Theorem 4.2.3. *We have*

1. *Dimension formulas for k even:*

$$\dim M_k(\Gamma) = \begin{cases} (k-1)(g-1) + \lfloor \frac{k}{4} \rfloor \epsilon_2 + \lfloor \frac{k}{3} \rfloor \epsilon_3 + \frac{k}{2} \epsilon_\infty & , k \geq 2 \\ 1 & , k = 0 \\ 0 & , k < 0 \end{cases},$$

$$\dim S_k(\Gamma) = \begin{cases} (k-1)(g-1) + \lfloor \frac{k}{4} \rfloor \epsilon_2 + \lfloor \frac{k}{3} \rfloor \epsilon_3 + \left(\frac{k}{2} - 1\right) \epsilon_\infty & , k \geq 4 \\ g & , k = 2 \\ 0 & , k \leq 0 \end{cases},$$

$$\dim E_k(\Gamma) = \begin{cases} \epsilon_\infty & , k \geq 4 \\ \epsilon_\infty - 1 & , k = 2 \\ 1 & , k = 0 \\ 0 & , k < 0 \end{cases}.$$

2. *Dimension formulas for k odd and $-I \notin \Gamma$ ($\epsilon_2 = 0$ in this case):*

$$\dim M_k(\Gamma) = \begin{cases} (k-1)(g-1) + \lfloor \frac{k}{4} \rfloor \epsilon_2 + \lfloor \frac{k}{3} \rfloor \epsilon_3 + \frac{k}{2}\epsilon_\infty^{\text{reg}} + \frac{k-1}{2}\epsilon_\infty^{\text{irr}} & , k \geq 3 \\ \geq \frac{1}{2}\epsilon_\infty^{\text{reg}} \text{ (equality if } \epsilon_\infty^{\text{reg}} > 2g-2) & , k = 1 \\ 0 & , k < 0 \end{cases},$$

$$\dim S_k(\Gamma) = \begin{cases} (k-1)(g-1) + \lfloor \frac{k}{4} \rfloor \epsilon_2 + \lfloor \frac{k}{3} \rfloor \epsilon_3 + \frac{k-2}{2}\epsilon_\infty^{\text{reg}} + \frac{k-1}{2}\epsilon_\infty^{\text{irr}} & , k \geq 3 \\ \dim M_1(\Gamma) - \frac{1}{2}\epsilon_\infty^{\text{reg}} & , k = 1 \\ 0 & , k < 0 \end{cases},$$

$$\dim E_k(\Gamma) = \begin{cases} \epsilon_\infty^{\text{reg}} & , k \geq 3 \\ \frac{1}{2}\epsilon_\infty^{\text{reg}} & , k = 1 \\ 0 & , k < 0 \end{cases}.$$

4.3 Counting ϵ_i for $\Gamma(N)$ and $\Gamma_1(N)$ and $\Gamma_0(N)$

Set

$$\begin{aligned} \Gamma(N) &= \{M \in \Gamma(1) \mid M \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod N\}, \\ \Gamma_1(N) &= \{M \in \Gamma(1) \mid M \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \bmod N\}, \\ \Gamma_0(N) &= \{M \in \Gamma(1) \mid M \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod N\}. \end{aligned}$$

Proposition 4.3.1. *For $\Gamma(N)$, we have*

1. $[\Gamma(1) : \Gamma(N)] = |\operatorname{SL}_2(\mathbb{Z}/N\mathbb{Z})| = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$.

$$[\overline{\Gamma}(1) : \overline{\Gamma}(N)] = \begin{cases} \frac{1}{2}N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right) & , N \geq 3 \\ 6 & , N = 2 \end{cases}.$$

2. *Two cusps a_1/c_1 and a_2/c_2 ($\gcd(a_i, c_i) = 1$) of $\Gamma(N)$ are equivalent when.*

$$(a_1, c_1) \equiv \pm(a_2, c_2) \bmod (\mathbb{Z}/N\mathbb{Z})^2.$$

The total number of cusps is

$$\epsilon_\infty = \begin{cases} \frac{1}{2}N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right) & , N \geq 3 \\ 3 & , N = 2 \end{cases}.$$

3. *There are no elliptic points.*

$$\epsilon_2 = \epsilon_3 = 0.$$

Proposition 4.3.2. *For $\Gamma_1(N)$, we have*

1. $[\Gamma_1(N) : \Gamma(N)] = N$.

$$[\overline{\Gamma}(1) : \overline{\Gamma}_1(N)] = N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right).$$

2. *The number of cusps is given by*

$$\epsilon_\infty = \begin{cases} \frac{1}{2}\sum_{d|N}\phi(d)\phi(N/d) & , N > 4 \\ 3 & , N = 4 \\ 2 & , N = 2, 3 \end{cases}.$$

3. *The number of elliptic points of order* 2 *is given by*

$$\epsilon_2 = \begin{cases} 1 & , N = 2 \\ 0 & , N \neq 2 \end{cases}.$$

4. *The number of elliptic points of order* 3 *is given by*

$$\epsilon_3 = \begin{cases} 1 & , N = 3 \\ 0 & , N \neq 2 \end{cases}.$$

Proposition 4.3.3. *For* $\Gamma_0(N)$*, we have*

1. $[\Gamma_0(N) : \Gamma_1(N)] = \phi(N)$.

$$[\Gamma(1) : \Gamma_0(N)] = N\prod_{p|N}\left(1 + \frac{1}{p}\right).$$

2. *The cusps are enumerated by* $\frac{a}{c}$ *with* $\gcd(a, c) = 1$ *and* $c|N$ *and where the* a*'s are chosen in the interval* $1 \leq a \leq c$ *to be inequivalent modulo* $\gcd(c, N/c)$*. Since for* $d|c$ *the reduction map* $(\mathbb{Z}/c\mathbb{Z})^* \to (\mathbb{Z}/d\mathbb{Z})^*$ *surjects, the number of choices for* a *is* $\phi(\gcd(c, N/c))$*. The number of cusps is*

$$\epsilon_\infty = \sum_{c|N}\phi(\gcd(c, N/c)).$$

The width of the cusps with denominator c *is* $N/(c\gcd(c, N/c))$*.*

3. *The elliptic points of order* 2 *are enumerated by* $\left(\begin{smallmatrix} 0 & -1 \\ 1 & k \end{smallmatrix}\right)(i)$ *where* k *(taken modulo* N*) ranges over the solutions to* $k^2 + 1 = 0 \bmod N$*.*

$$\epsilon_2 = \begin{cases} \prod_{p|N}\left(1 + \left(\frac{-1}{p}\right)\right) & , 4 \nmid N \\ 0 & , 4 \mid N \end{cases}.$$

4. *The elliptic points of order* 3 *are enumerated by* $\left(\begin{smallmatrix} 0 & -1 \\ 1 & k \end{smallmatrix}\right)(e(\frac{1}{6}))$ *where* k *(taken modulo* N*) ranges over the solutions to* $k^2 + k + 1 = 0 \bmod N$*.*

$$\epsilon_3 = \begin{cases} \prod_{p|N}\left(1 + \left(\frac{-3}{p}\right)\right) & , 9 \nmid N \\ 0 & , 9 \mid N \end{cases}.$$

Proof. We will show (1) and (2) just for prime $N = p$. The full discussion for any N can be found in [6, Ch. 3]. Since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\frac{1}{0}\right) = \frac{a}{c},$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\left(\frac{0}{1}\right) = \frac{b}{d},$$

any rational number with denominator divisible by p is equivalent to $\frac{1}{0}$ while the other rational numbers are equivalent to $\frac{0}{1}$. Thus, since $\frac{0}{1}$ has width p and $\frac{1}{0}$ has width 1,

$$[\Gamma(1) : \Gamma_0(p)] = p + 1.$$

(3). Let us first show that, with $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$, the points $g(i)$ with non-trivial stabilizers in $\Gamma_0(N)$ are all $\Gamma_0(N)$-equivalent to $M_k(i)$ with $M_k = \left(\begin{smallmatrix} 0 & -1 \\ 1 & k \end{smallmatrix}\right)$. We can compute that

$$gSg^{-1} = \begin{pmatrix} ac + bd & -a^2 - b^2 \\ c^2 + d^2 & -ac - bd \end{pmatrix},$$

so any $g(i)$ with non-trivial stabilizer in $\Gamma_0(N)$ must have $c^2 + d^2 \equiv 0 \bmod N$. Since c and d are relatively prime, this means that c and N are also relatively prime. Now,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ak - b & a \\ ck - d & c \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}.$$

Since c and N are relatively prime, we can find an integer k so that $ck - d \equiv 0 \bmod N$, thus showing that $g(i)$ and $M_k(i)$ are $\Gamma_0(N)$-equivalent.

If $M_k(i)$ has a non-trivial stabilizer in $\Gamma_0(N)$, we need $k^2+1 \equiv 0 \bmod N$. Let us show that when k is as such and is taken modulo N, these points are inequivalent under $\Gamma_0(N)$. Suppose that $M_{k_1}(i) = hM_{k_2}(i)$ for some $h \in \Gamma_0(N)$ with $k_1^2 + 1 \equiv k_2^2 + 1 \equiv 0 \bmod N$. This means that $M_{k_1} S^i M_{k_2}^{-1} \in \Gamma_0(N)$ for $i = 0$ or 1. As

$$M_{k_1} S^0 M_{k_2}^{-1} = \begin{pmatrix} 1 & 0 \\ k_2 - k_1 & 1 \end{pmatrix},$$
$$M_{k_1} S^1 M_{k_2}^{-1} = \begin{pmatrix} -k_2 & -1 \\ k_1 k_2 + 1 & k_1 \end{pmatrix},$$

we see that $k_1 \equiv k_2 \bmod N$ since $k_1 k_2 \equiv -1 \mod N$ is equivalent to $k_1 \equiv k_2 \mod N$ because $k_2^2 \equiv -1 \bmod N$.

□

4.4 General properties of $A_k(\Gamma)$

The proof of the follow proposition follows exactly along the same lines as the proof of Proposition 3.2.2.

Proposition 4.4.1. *Suppose k is even and $f \in A_k(\Gamma)$.*

1. *If ζ is an elliptic point of order 2 then*

$$\frac{k}{2} + 2 \operatorname{ord}_\zeta(f, \Gamma) \equiv 0 \bmod 2.$$

2. *If ζ is an elliptic point of order 3 then*

$$\frac{k}{2} + 3 \operatorname{ord}_\zeta(f, \Gamma) \equiv 0 \bmod 3.$$

It follows that for functions in $A_0(\Gamma)$ the order should be measured in the variable

$$t = \begin{cases} \left(\frac{\tau - z}{\tau - \bar{z}}\right)^{|\overline{\Gamma}_z|} & , z \in \mathbb{H} \\ \exp \frac{2\pi i}{h} \alpha^{-1}(\tau) & , z = \alpha(\infty), \ h \text{ is cusp width} \end{cases},$$

called the local variable at $z \in \overline{\mathbb{H}}$, and all function will have expansions in integral powers of this variable. In the case of the cusp ∞, this variable is also $q^{1/h}$.

As with elliptic functions, we usually refer to the number of poles of a function as its order, but according to the following definition this number is also the number of times the function takes any complex value.

Definition 4.4.2. *If $f \in A_0(\Gamma)$ then the number of solution to $f(\tau) = c$ counted according to multiplicity for any $c \in \mathbb{C}_\infty$ is independent of c and is called the order of the function f, also denoted by $\operatorname{ord}_\Gamma(f)$.*

Proof. The number of zeros of $f(\tau) - c$ is equal to the number of poles of $f(\tau)$ by the valence formula, so $\operatorname{ord}_\Gamma(f)$ is well-defined. □

Definition 4.4.3. *If $f \in A_0(\Gamma)$, define the ramification index $\operatorname{ram}_z(f, \Gamma) \in \mathbb{Z}_{>0}$ by*

$$\operatorname{ram}_z(f, \Gamma) = \begin{cases} \operatorname{ord}_z(f - f(z)) & , f(z) \neq \infty \\ -\operatorname{ord}_z(f) & , f(z) = \infty \end{cases}$$

Proposition 4.4.4. *If $f \in A_0(\Gamma)$ and g is the genus of $\overline{\mathbb{H}}/\Gamma$, then*

$$\sum_{z \in \overline{\mathbb{H}}/\Gamma} (\operatorname{ram}_z(f, \Gamma) - 1) = 2(g - 1 + \operatorname{ord}_\Gamma(f)).$$

Proof. The is a special case of the Riemann-Hurwitz Formula where the target space is $\mathbb{C}_\infty$. It may be proven exactly as the genus formula was obtained (in fact the genus formula is this with $f = j$ so that $\operatorname{ord}_\Gamma(j) = [\overline{\Gamma}(1) : \overline{\Gamma}]$). One triangulates $\overline{\mathbb{H}}/\Gamma$ with vertices at the finite number of points z where $\operatorname{ram}_z(f, \Gamma) > 1$. □

Proposition 4.4.5. *$S_0(\Gamma) = \{0\}$ and $M_0(\Gamma) = \mathbb{C}$.*

Proof. The first assertion follows from the valence formula. For the second, if $f(\tau) = c + O(q^{1/h})$ where h is the width of the cusp ∞, then $f(\tau) - c$ has a zero at ∞ and is still an element of $M_0(\Gamma)$. The valence formula then implies that $f(\tau)$ is constant. □

Proposition 4.4.6. *If R is a rational function of degree d and $x \in A_0(\Gamma)$, then*

$$\operatorname{ord}_\Gamma(R(x)) = d \operatorname{ord}_\Gamma(x).$$

The function x in the following proposition, if it exists, is called a Hauptmodul for Γ, and all Hauptmoduln for a given Γ differ by a Möbius transformation.

Proposition 4.4.7. *Suppose that $x \in A_0(\Gamma)$ with $\operatorname{ord}_\Gamma(x) = 1$.*

1. *$x : \overline{\mathbb{H}}/\Gamma \to \mathbb{C}_\infty$ is a bijection and $g = 0$.*
2. *If y is another non-constant function in $A_0(\Gamma)$, then there are polynomials $p_i(x)$ such that $p_0(x) + p_1(x)y = 0$. Specifically, there is a constant c such that $cy = \prod_{z \in \overline{\mathbb{H}}/\Gamma} (x - x(z))^{\operatorname{ord}_z(y, \Gamma)}$ where the possible term from the pole z of x is omitted.*
3. *$A_0(\Gamma) = \mathbb{C}(x)$.*
4. *$S_1(\Gamma) = S_2(\Gamma) = \{0\}$.*

Proof. (1). $x(\tau) - c$ has one pole so it has exactly one zero by the valence formula. The proves that x defines a bijection. Suppose that $g > 0$. Then there is a loop on $\overline{\mathbb{H}}/\Gamma$ that may not be contracted to a point. However, the image of this loop on $\mathbb{C}_\infty$ is contractible. This is a contradiction because the contraction of the loop on $\mathbb{C}_\infty$ may be pulled back (via x^{-1}) to a contraction on $\overline{\mathbb{H}}/\Gamma$.

(2). Define

$$g(\tau) = \frac{1}{y(\tau)} \prod_{\substack{z \in \overline{\mathbb{H}}/\Gamma \\ x(z) \neq \infty}} (x(\tau) - x(z))^{\mathrm{ord}_z(y,\Gamma)}.$$

Since $x(\tau) - x(z)$ has a simple zero at $\tau = z$ (as measured in the local variable at z), for all $z = \overline{\mathbb{H}}/\Gamma$ we have $\mathrm{ord}_z(g, \Gamma) = 0$ expect possibly at the unique pole of the function x. However, if z is this pole, the valence formula implies that $\mathrm{ord}_z(g, \Gamma) = 0$ as well. Thus, $g \in M_0(\Gamma)$ which consists entirely of constants.

(3) is then a direct consequence of (2).

(4) If $f \in S_2(\Gamma)$ then define

$$g(\tau) = \frac{f(\tau)}{dx/d\tau}.$$

That $g(\tau) \in A_0(\Gamma)$ is essentially Lemma 3.4.4. Let $z \in \mathbb{H}$ not be a pole of x and $p = |\overline{\Gamma}_z|$ and let t be the local variable at z. Let c_i denote certain non-zero constants (that could depend on z). Recalling that $x(\tau) - x(z)$ has a simple zero at $\tau = z$, we see that $dx = (c_1 + O(t))dt$. Since $d\tau = t^{\frac{1}{p}-1}(c_2 + O(t))dt$, we have

$$g(\tau) = \frac{f(\tau)}{dx/d\tau} = t^{\mathrm{ord}_z(f,\Gamma)+\frac{1}{p}-1}(c_3 + O(t)).$$

Since, by definition of $S_2(\Gamma)$, $\mathrm{ord}_z(f, \Gamma) \geq 0$, and we have $\mathrm{ord}_z(f, \Gamma) \equiv 1 - \frac{1}{p} \bmod 1$ by Proposition 4.4.1, $g(\tau)$ does not have a pole at z. If z is a pole of x then the only thing that needs to be changed in this discussion is that $dx = t^{-2}(c_3 + O(t))dt$, and so we see that $g(\tau)$ has a zero at z in this case.

Next, if $z = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(\infty) \in \overline{\mathbb{Q}}$, let t be the local variable at this cusp z. We have

$$\begin{aligned} f(\tau) &= (a - c\tau)^2 t^{\mathrm{ord}_z(f,\Gamma)}(c_4 + O(t)) \\ d\tau &= (a - c\tau)^{-2} t^{-1} c_5 dt \\ dx &= \begin{cases} (c_6 + O(q))dt & , z \text{ is not a pole of } x \\ t^{-2}(c_7 + O(q))dt & , z \text{ is a pole of } x \end{cases}. \end{aligned}$$

Thus we see that g does not have a pole and actually vanishes at the pole of x. Since g was an element of $A_0(\Gamma)$, this means that g mush be identically 0. Therefore, $S_2(\Gamma) = \{0\}$. The square of any element of $S_1(\Gamma)$ is in $S_2(\Gamma)$, so $S_1(\Gamma) = \{0\}$ as well. □

Proposition 4.4.8. *Suppose that $x \in A_0(\Gamma)$ with $\mathrm{ord}_\Gamma(x) = 2$.*

1. *Any three functions in $A_0(\Gamma)$ are linearly dependent over $\mathbb{C}(x)$.*
2. *If y is a function of odd order, then there is a unique irreducible polynomial $P(x, y)$ of degree 2 in y with $P(x(\tau), y(\tau)) = 0$, and we have $A_0(\Gamma) = \mathbb{C}(x, y)/(P(x, y))$.*

Proof. (1). By Proposition 4.4.4 there is a ramification point of the function x because

$$\sum_{z \in \overline{\mathbb{H}}/\Gamma} (\mathrm{ram}_z(x, \Gamma) - 1) = 2(g + 1) > 0.$$

Since none of the assertions of the proposition are affected by applying a Möbius transformation to x, if necessary, we can let z be such a ramification point and replace x by $1/(x - x(z))$ to *assume that x has a single double pole at some point z.*

Let $L(m)$ denote the vector space of functions that have poles only at z and the order of this pole is $\leq m$. Clearly,

$$\dim L(m) \leq 1 + m.$$

Let $f_1, f_2, f_3 \in A_0(\Gamma)$ and assume that they are linearly independent over $\mathbb{C}(x)$. We can find polynomials $p_i(x)$ so that $p_i(x)f_i$ has no poles outside z. This means that there is an integer m_0 such that, for $i = 1, 2, 3$,

$$p_i(x)f_i \in L(2m_0).$$

For any integer $m \geq m_0$, the set

$$\{x^j p_i(x) f_i\}_{\substack{i=1,2,3 \\ 0 \leq j \leq m - m_0}}$$

consists of $3(m-m_0+1)$ linearly independent functions in $L(2m)$. This contradicts the bound $\dim L(2m) \leq 1 + 2m$ for large m and shows that f_1, f_2, f_3 are linearly dependent over $\mathbb{C}(x)$.

(2). Let y be a function of odd order. By multiplying by a suitable polynomial in x, we may assume that y has no poles outside of z and that y has a pole of odd order at z because multiplying by a polynomial in x changes the order of y by an even integer. Then, it is easy to see that 1 and y are linearly independent over $\mathbb{C}(x)$, for suppose that there were polynomials $p_0(x)$ and $p_1(x)$ with

$$p_0(x) + p_1(x)y = 0.$$

If $p_1(x) \neq 0$, then the Laurent series expansion of $p_0(x)$ begins with t to a negative even power and $p_1(x)y$ begins with a negative odd power. Thus $p_1(x) = p_0(x) = 0$ and 1 and y are linearly independent over $\mathbb{C}(x)$. We can get the quadratic relation by applying (1) to the three functions $1, y, y^2$. Finally, if $f \in A_0(\Gamma)$, apply (1) to the three functions $1, y, f$. □

Proposition 4.4.9. *If $x \in A_0(\Gamma)$ with $l = \mathrm{ord}_\Gamma(x)$, then any $l + 1$ functions in $A_0(\Gamma)$ are linearly dependent over $\mathbb{C}(x)$.*

Proof. Suppose x has poles at $q_1, \ldots, q_r$ and that the orders of these poles are $n_1, \ldots, n_r$. Assume that there are $l+1$ functions $f_1, \ldots, f_{l+1}$ that are linearly independent over $\mathbb{C}(x)$. Let $L(m)$ denote the vector space of functions that have no poles outside $q_1, \ldots, q_r$ and having a pole of order not worse than mn_i at each q_i. Clearly, $\dim(L(m)) \leq 1 + mn_1 + \cdots + mn_r = 1 + ml$. We can find polynomials $p_1, \ldots, p_r$ with $p_1(x)f_1, \ldots, p_r(x)f_r$ each having no poles outisde of $q_1, \ldots, q_r$. Therefore, for some fixed m_0, we have $p_i(x)f_i \in L(m_0)$ for every $i = 1, \ldots, l + 1$. It follows that

$$\{x^j p_i(x) f_i\}_{\substack{i=1,\ldots,l+1 \\ 0 \leq j \leq m - m_0}}$$

consists of $(m - m_0 + 1)(l + 1)$ linearly independent functions in $L(m)$, which contradicts the bound $\dim(L(m)) \leq 1 + ml$ for large m. □

4.5 Working with finite index subgroups of $\Gamma(1)$

This section discusses several of the representations of a finite index subgroup, Γ, of $\Gamma(1)$. The first and most intuitive way is via the combination of a fundamental domain for Γ and edge-pairing matrices, as given in the following theorem.

Theorem 4.5.1 (Siegel)**.** *If $[\Gamma(1) : \Gamma] < \infty$, there is a connected fundamental domain D for Γ in which the sides of D can be paired up by elements of Γ, and the elements of Γ that the pair up all of the sides generate $\overline{\Gamma}$.*

Unfortunately, the generators in this theorem are not guaranteed to be independent. For example S and T pair up the edges in the usual fundamental domain for $\Gamma(1)$, but S and T are not independent generators. We will describe the so called Farey symbol for subgroup Γ of $\Gamma(1)$ of finite index, which allows a list of independent generators to be easily computed (see [13] and [12]). We will also describe the bicuboid graph for Γ as well, and find the following correspondences:

1. fundamental domains with side pairings $\Rightarrow$ subgroups (onto, many-to-one)
2. Farey symbols $\Rightarrow$ subgroups (onto, many-to-one)
3. bicuboid graphs $\Leftrightarrow$ conjugacy classes of subgroups (bijection)
4. marked bicuboid graphs $\Leftrightarrow$ subgroups (bijection)
5. marked bicuboid graphs with cuts $\Leftrightarrow$ Farey symbols (bijection)

We will first define all of these terms appears in these correspondences.

Definition 4.5.2.

1. *Label the following points in* $\overline{\mathbb{H}}$*:*
   (a) *An even point is the image of* i *under some element of* $\Gamma(1)$*.*
   (b) *An odd point is the image of* $e(\frac{1}{6})$ *under some element of* $\Gamma(1)$*.*
   (c) *An cusp is the image of* ∞ *under some element of* $\Gamma(1)$*.*
2. *Label the following half arcs in* $\overline{\mathbb{H}}$*:*
   (a) *An even edge is the image the set* $\{e(\frac{1}{4}) + it \mid t > 0\}$ *under some element of* $\Gamma(1)$*.*
   (b) *An odd edge is the image the set* $\{e(\frac{1}{6}) + it \mid t > 0\}$ *under some element of* $\Gamma(1)$*.*
   (c) *A free edge is the image the set* $\{e(t) \mid \frac{1}{6} < t < \frac{1}{4}\}$ *under some element of* $\Gamma(1)$*.*
3. *A special polygon for* Γ *is a convex hyperbolic polygon* P *satisfying:*
   (a) *The boundary of* P *consists of even and odd edges.*
   (b) *The even edges come in pairs, each pair forming an arc connecting two elements of* $\mathbb{Q}$*. Each arc is either paired with itself under* Γ *(in which case it contains an elliptic point of order* 2*) or is paired with another such arc under* Γ*.*
   (c) *The odd edges come in pairs, each pair meeting at a vertex with angle* $2\pi/3$*, which is an elliptic point of order* 3 *for* Γ*.*

Definition 4.5.3.

1. *A bipartite cuboid graph (or bicuboid graph) is a finite connected graph such that*
   (a) *Every vertex is marked by either* $\bullet$ *or* $\circ$*. These are called odd and even vertices, respectively.*
   (b) *Every odd vertex has valence 1 or 3.*
   (c) *Every even vertex has valence 1 or 2.*
   (d) *There is a set cyclic order on the edges originating at each vertex of valence three.*
   (e) *Every edge joins an even and odd vertex.*

2. A marked bicuboid graph is a bicuboid graph with a distiguished edge.

Definition 4.5.4. *A Farey symbol is a symbol of the form*

$$\frac{-1}{0} \underset{p_{-1}}{\longleftrightarrow} \frac{a_0}{c_0} \underset{p_0}{\longleftrightarrow} \frac{a_1}{c_1} \underset{p_1}{\longleftrightarrow} \cdots \underset{p_{n-1}}{\longleftrightarrow} \frac{a_n}{c_n} \underset{p_n}{\longleftrightarrow} \frac{1}{0},$$

where one of the $\frac{a_n}{c_n}$ *is* 0*. The pairing symbols* p_i *are allowed to be natural numbers or one of symbols* $\bullet$ *or* $\circ$ *and we always have* $a_{i+1}c_i - a_i c_{i+1} = 1$*.*

A natural number n*, if it appears among the* p_i*, appears exactly twice at two edges, say,* p_i *and* p_k*. In this cases, the edges* p_i *and* p_k *are said to the paired by a free pairing.*

If $p_i = \circ$*, the edge is said to be paired with itself by an even pairing.*

If $p_i = \bullet$*, the edge is said to be paired with itself by an odd pairing.*

Define the pairing matrix for even pairings, odd pairings, and free pairings, respectively, as

$$G_i\left(\frac{a_i}{c_i} \underset{\circ}{\longleftrightarrow} \frac{a_{i+1}}{c_{i+1}}\right) = \begin{pmatrix} a_{i+1} & a_i \\ c_{i+1} & c_i \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{i+1} & a_i \\ c_{i+1} & c_i \end{pmatrix}^{-1},$$

$$G_i\left(\frac{a_i}{c_i} \underset{\bullet}{\longleftrightarrow} \frac{a_{i+1}}{c_{i+1}}\right) = \begin{pmatrix} a_{i+1} & a_i \\ c_{i+1} & c_i \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} a_{i+1} & a_i \\ c_{i+1} & c_i \end{pmatrix}^{-1},$$

$$G_{i,k}\left(\frac{a_i}{c_i} \underset{n}{\longleftrightarrow} \frac{a_{i+1}}{c_{i+1}}, \frac{a_k}{c_k} \underset{n}{\longleftrightarrow} \frac{a_{k+1}}{c_{k+1}}\right) = \begin{pmatrix} a_{k+1} & a_k \\ c_{k+1} & c_k \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{i+1} & a_i \\ c_{i+1} & c_i \end{pmatrix}^{-1}.$$

In this section will we assume that all matrices are taken modulo $\pm I$ since we are concerned with their action on $\overline{\mathbb{H}}$ and mercifully suppress the lines on the groups. In addition to the matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, the matrices

$$O = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

will be useful. The main result which is useful for studying subgroups of $\Gamma(1)$ is the result that $\Gamma(1) = \mathbb{Z}_2 * \mathbb{Z}_3$.

Proposition 4.5.5. *For* $\Gamma(1)$*, the matrices* S *and* O *are independent generators of orders* 2 *and* 3*, that is, each element of* $\Gamma(1)$ *can be written uniquely as a word in* S *and* O *with no two consecutive* S*'s and no three consecutive* O*'s.*

Proof. Exercise. Hint: $OS = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $OOS = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. □

Exercise 4.5.6. *Show that* S *and* T^n *generate a subgroup of finite index in* $\Gamma(1)$ *only when* $|n| = 1, 2$*. Hint: for* $n > 3$ *assume the opposite and consider* $(OS)^m OOSO$ *for large* m*.*

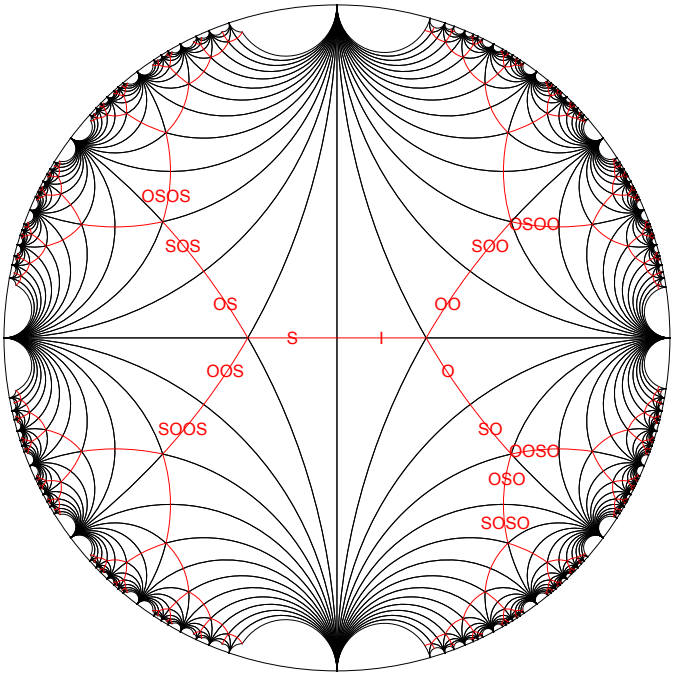
Remark 4.5.7. *Let* $xy'(x)/y(x) = x + x^2 + 4x^3 + 8x^4 + 5x^5 + \cdots$ *be the formal generating function for subgroups of* $\Gamma(1)$ *of a given index. It is possible to show ([14]) that* $y(x)$ *satisfies the differential equation*

$$x^7(x^3-1)y''(x) + (4x^9 + 2x^7 - 4x^6 - 2x^4 - 4x^3 + 1)y'(x)$$
$$+(2x^8 + 2x^6 - 4x^5 + x^4 - 4x^3 - 4x^2 - x - 1)y(x) = 0.$$

It is possible to give an explicit algorithm for writing a given $M \in \Gamma(1)$ as a word in S and O. If $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then the even point $M(i)$ is part of an arc that connects the two cusps $\frac{a}{c}$ and $\frac{b}{d}$. Let M_0 be the matrix we wish to write in terms of S and O. At each step of the following algorithm, a, b, c, and d denote the entries of M_k.

$$\text{if } M_k = I \text{ or } S, \text{ then terminate}$$
$$\text{if } -\infty \leq \tfrac{a}{c}, \tfrac{b}{d} \leq 0, \text{ then } M_{k+1} = SM_k$$
$$\text{if } 0 \leq \tfrac{a}{c}, \tfrac{b}{d} \leq 1, \text{ then } M_{k+1} = OM_k$$
$$\text{if } 1 \leq \tfrac{a}{c}, \tfrac{b}{d} \leq \infty, \text{ then } M_{k+1} = OOM_k$$

This will terminate, in which case M_0^{-1} is expressed as a word in S and O and so M_0 is as well. In the following diagram, $\mathbb{H}$ has been mapped into the unit disk, and the free edges E have been marked with the matrix that sends E to the free edge between i and $e(\frac{1}{6})$.



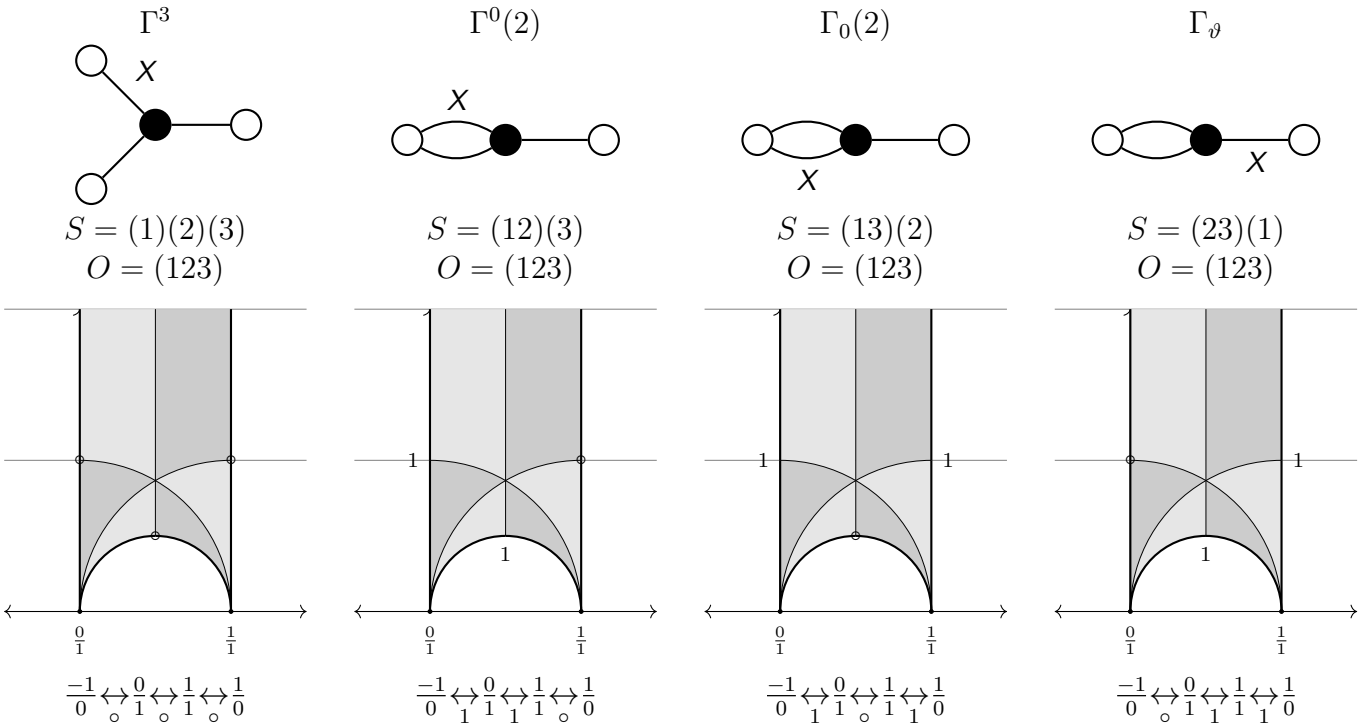
Proposition 4.5.8. *Let* $[\Gamma(1) : \Gamma] = \mu$ *and* ϕ *denote the homomorphism* $\Gamma(1) \to \mathrm{Sym}_\mu$ *obtained by the permutation action of* $g \in \Gamma(1)$ *on the left cosets* $\Gamma(1)\backslash\Gamma$.

1. Γ *is completely determined by* $\phi(S)$ *and* $\phi(O)$ *up to a relabeling of the non-trivial cosets as long as* $\phi(S)$ *and* $\phi(O)$ *have order* 2 *and* 3, *respectively, and generate a transitive subgroup of* Sym_μ.
2. *The number of fixed points of* $\phi(S)$ *is* ϵ_2.
3. *The number of fixed points of* $\phi(O)$ *is* ϵ_3.
4. *The number of cycles in* $\phi(T)$ *is* ϵ_∞. *The lengths of these cycles are the widths of the inequivalent cusps of* Γ.
5. *The order of the permutation* $\phi(T)$ *is* $\mathrm{level}(\Gamma)$.

As an example of this correspondence, we list the subgroups of Γ of index 3.

Example 4.5.9. *For the* 4 *groups of index* 3 *in* $\Gamma(1)$, *namely* Γ^3, $\Gamma^0(2)$, $\Gamma_0(2)$, Γ_ϑ *the corresponding*

marked bicuboid graph, special polygon and Farey Symbol are shown below.

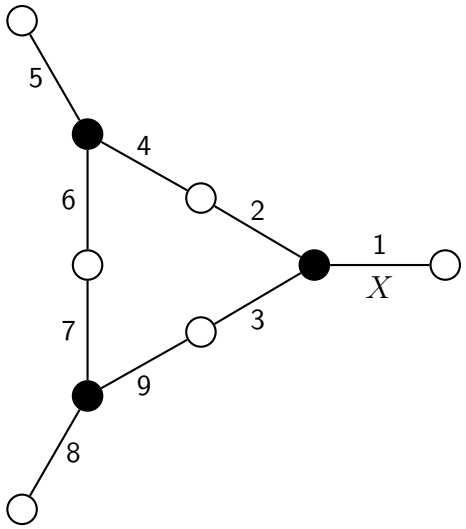


Any relabeling of the edges for Γ^3 *produces isomorphic graphs because* Γ^3 *is a normal subgroup of* $\Gamma(1)$*. The remaining three graphs are distinct because the position of the marked edge, the edge marked "X", is distinguished by the orientation on the odd vertex. This marked ege is placed by default along the free edge from* i *to* $e(\frac{1}{6})$ *in the special polygon.*

From Proposition 4.5.8 we can construct the correspondence between bicuboid graphs and subgroups Γ of $\Gamma(1)$, which we illustrate for a group of index 9. Let $\phi : \Gamma(1) \to \mathrm{Sym}_9$ be defined by

$$\phi(O) = (123)(456)(789),$$
$$\phi(S) = (24)(39)(67).$$

The group Γ is then defined as the set of all $g \in \Gamma(1)$ such that $\phi(g)(1) = 1$. This marks "1" as the coset Γ in $\Gamma(1)\backslash\Gamma$. The corresponding graph (whose ordering on the trivalent vertices is counter-clockwise) is

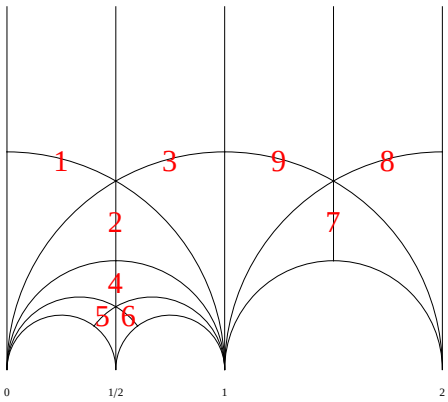


This bicuboid graph has one edge marked with an "X", making it into a marked bicuboid graph. Note that marking any of the other 8 vertices gives rise to a total of only 3 distinct marked graphs, hence there are two other subgroups of $\Gamma(1)$ that are conjugate to this Γ.

We can read much of the data for Γ directly from this marked graph. First, we see that $\phi(O) = (123)(456)(789)$ has no fixed points, so $\epsilon_3 = 0$. Next, $\phi(S) = (24)(39)(67)$ has three fixed points, so $\epsilon_2 = 3$. By multiplying the permutations, we have $\phi(T) = \phi(OS) = (145783)(296)$, so $\epsilon_\infty = 2$ and the width of these two cusps are 6 and 3. To find generators, first note that the graph has a cycle, but that if the vertex between edges 6 and 7 is cut, the cycle is broken the the resulting cut graph is a tree. There is now a unique path from the marked edge to any edge that does not cross over from edge 6 to edge 7. The path from the marked edge to the edge labeled i corresponds to a matrix, and we have

$$\begin{array}{lll} M_1 = I, & M_4 = SO, & M_9 = SOO, \\ M_2 = O, & M_5 = OSO, & M_7 = OSOO, \\ M_3 = OO, & M_6 = OOSO, & M_8 = OOSOO. \end{array}$$

Free generators for Γ are then $M_7^{-1}SM_6$, $M_1^{-1}SM_1$, $M_5^{-1}SM_5$, and $M_8^{-1}SM_8$, and so $\Gamma \simeq \mathbb{Z} * \mathbb{Z}_2 * \mathbb{Z}_2 * \mathbb{Z}_2$. In order to construct a special polygon and Farey symbol for this Γ, we first agree to make a cut between edges 6 and 7, as before, so that the resulting graph is a tree. Next, we place the marked edge on the free edge from i to $e(\frac{1}{6})$ in $\mathbb{H}$, and let the remaining edges fall naturally onto their respective free edges in $\mathbb{H}$. The result is



Therefore, the cusps in the Farey symbol are $\infty \leftrightarrow \frac{0}{1} \leftrightarrow \frac{1}{2} \leftrightarrow \frac{1}{1} \leftrightarrow \frac{2}{1} \leftrightarrow \infty$. In order to fill in the pairing information, note that the even points in the arcs $\infty \leftrightarrow \frac{0}{1}$, $\frac{0}{1} \leftrightarrow \frac{1}{2}$, and $\frac{2}{1} \leftrightarrow \infty$ are all elliptic points of order 2 for Γ since $\phi(S)$ fixes each of the cosets labeled 1, 5 and 8. This means that each of these three arcs is paired with itself. Finally the arc $\frac{1}{2} \leftrightarrow \frac{1}{1}$ is paired with the arc $\frac{1}{1} \leftrightarrow \frac{2}{1}$ in order to glue back together the cut that was made between the edges 6 and 7. In summary, a Farey symbol for Γ is given by

$$\infty \underset{\circ}{\longleftrightarrow} \frac{0}{1} \underset{\circ}{\longleftrightarrow} \frac{1}{2} \underset{1}{\longleftrightarrow} \frac{1}{1} \underset{1}{\longleftrightarrow} \frac{2}{1} \underset{\circ}{\longleftrightarrow} \infty.$$

We could have made one cut between edges 2 and 4 or 3 and 9, so there are in total two more Farey symbols corresponding to this subgroup Γ.

Algorithm 4.5.10. *Input: a finite index subgroup* Γ *of* $\Gamma(1)$. *Output: a Farey symbol for* Γ.
Step 1: If $[\Gamma(1) : \Gamma] \leq 2$

$$\text{return} \begin{cases} \frac{-1}{0} \underset{\circ}{\longleftrightarrow} \frac{0}{1} \underset{\bullet}{\longleftrightarrow} \frac{1}{0} & , \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma \qquad (i.e.\ \Gamma = \Gamma(1)) \\ \frac{-1}{0} \underset{\bullet}{\longleftrightarrow} \frac{0}{1} \underset{\bullet}{\longleftrightarrow} \frac{1}{0} & , \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma \quad (i.e.\ \Gamma = \Gamma^2) \end{cases}.$$

Step 2: Let F be the partial Farey symbol

$$F = \begin{cases} \frac{-1}{0} \longleftrightarrow \frac{0}{1} \longleftrightarrow \frac{1}{1} \longleftrightarrow \frac{1}{0} & , \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right) \notin \Gamma \\ \frac{-1}{0} \longleftrightarrow \frac{-1}{1} \longleftrightarrow \frac{0}{1} \longleftrightarrow \frac{1}{0} & , \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \Gamma \end{cases}.$$

Step 3: For each unpaired edge in F, check if it can be paired with itself by an even or odd pairing ($G_i \in \Gamma$) or if it can be paired with another unpaired edge (free pairing $G_{i,k} \in \Gamma$) and fill in all of the possible pairings.
Step 4: If all edges are paired, then return F.
Step 5: If there is still an unpaired edge in F between, say, a_i/c_i and a_{i+1}/c_{i+1}, place an new vertex $(a_i + a_{i+1})/(c_i + c_{i+1})$ in between with no pairing information on the two adjacent edges and goto Step 3.

Given a special polygon P, we may convert P to a Farey symbol F and vice-versa. If P is a special polygon, we assume that that ∞ is included as a vertex and that there are certain rational vertices $\frac{a_0}{c_0} < \cdots < \frac{a_n}{c_n}$. These are put into F in the obvious way with the corresponding pairing information. Note that we have $a_{i+1}c_i - a_ic_{i+1} = 1$ because the quantity $a_{i+1}c_i - a_ic_{i+1}$ is unchanged when $\frac{a_i}{c_i}$ and $\frac{a_{i+1}}{c_{i+1}}$ are simultaneously acted upon by some element of $\Gamma(1)$ and $a_{i+1}c_i - a_ic_{i+1} = 1$ for the basic choices $\frac{a_i}{c_i} = \frac{-1}{0}$ and $\frac{a_{i+1}}{c_{i+1}} = \frac{0}{1}$.

Now given F, we can convert to edges of P in the following way (set $g = \left(\begin{smallmatrix} a_{i+1} & a_i \\ c_{i+1} & c_i \end{smallmatrix}\right)$).

$$\left.\begin{array}{l} \frac{a_i}{c_i} \underset{\circ}{\longleftrightarrow} \frac{a_{i+1}}{c_{i+1}} \\ \frac{a_i}{c_i} \underset{n}{\longleftrightarrow} \frac{a_{i+1}}{c_{i+1}} \end{array}\right\} \Longleftrightarrow g(E \cup \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)(l)), \quad E = \{e(\tfrac{1}{4}) + it \mid t > 0\}$$

$$\frac{a_i}{c_i} \underset{\bullet}{\longleftrightarrow} \frac{a_{i+1}}{c_{i+1}} \Longleftrightarrow g(E \cup \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)(E)), \quad E = \{e(\tfrac{1}{6}) + it \mid t > 0\}$$

Theorem 4.5.11.

1. *If P is a special polygon, then the edge pairing matrices $\{g_i\}$ generate some Γ and P is a fundamental domain for Γ.*
   There are ϵ_2 generators of order 2.
   There are ϵ_3 generators of order 3.
   There are $2g + \epsilon_\infty - 1$ free generators (order ∞).

2. *The g_i are an independent set of generators for Γ. This means that any element of Γ can be written uniquely as $\prod_{g_k \in \{g_i\}} g_k^{e_k}$ where $e_k \neq 0$ and e_k is further restricted to $1 \leq e_k < p$ if g_k is a generator of finite order p. In symbols,*
   $$\Gamma \simeq \mathbb{Z}_2^{*\epsilon_2} * \mathbb{Z}_3^{*\epsilon_3} * \mathbb{Z}^{*(2g-1+\epsilon_\infty)}.$$

Proof. See [12]. □

4.6 $\Gamma(2)$

The main function for the group $\Gamma(2)$, which play the same role as $j(\tau)$ plays for $\Gamma(1)$ (the so-called Hauptmodul), is the modular λ function defined by

$$\lambda(\tau) = \left(\frac{\Theta_2(\tau)}{\Theta_3(\tau)}\right)^4.$$

Proposition 4.6.1. *Let $\lambda(\tau)$ be the modular λ function. Then,*

1. $\lambda(\tau) \in M_0^!(\Gamma(2))$, $\Theta_2^4, \Theta_3^4, \Theta_4^4 \in M_2(\Gamma(2))$
2. $\lambda(\tau)$ *has a simple pole at* $\frac{1}{1}$, *a simple zero at* $\frac{1}{0}$, *and takes the value* 1 *at* $\frac{0}{1}$.
3. $A_0(\Gamma(2)) = \mathbb{C}(\lambda)$.
4. $S_k(\Gamma(2)) = \Theta_2^4\Theta_3^4\Theta_4^4 M_{k-6}(\Gamma(2))$.
5. $\Theta_3^4 = \Theta_2^4 + \Theta_4^4$.
6. $M_k(\Gamma(2)) = \bigoplus_{\substack{2a+2b=k \\ a,b\geq 0}} \mathbb{C}\Theta_2^{4a}\Theta_3^{4b}$.

Proof. (1). The fundamental domain $\{\tau \mid |\mathrm{Re}(\tau)| \leq 1 \text{ and } |2\tau \pm 1| \geq 1\}$ for $\Gamma(2)$ shows that $\overline{\Gamma}(2)$ is generated by T^2 and ST^2S. From Proposition 2.8.3, we have

$$(\Theta_2, \Theta_3, \Theta_4)|_T = (\zeta_8^1\Theta_2, \Theta_3, \Theta_4),$$
$$(\Theta_2, \Theta_3, \Theta_4)|_S = \zeta_8^{-1}(\Theta_4, \Theta_3, \Theta_2).$$

Therefore,

$$(\Theta_2, \Theta_3, \Theta_4)|_{T^2} = (\zeta_4\Theta_2, \Theta_3, \Theta_4),$$
$$(\Theta_2, \Theta_3, \Theta_4)|_{ST^2S} = (\zeta_4^3\Theta_2, \zeta_4^3\Theta_3, \Theta_4).$$

and we see that $\Theta_2^4/\Theta_3^4 \in M_0^!(\Gamma(2))$ because Exercise 2.12.4 shows that λ has no poles or zeros in $\mathbb{H}$.

(2). For the values at the cusps, we have the table

cusp	function	q-series
$\frac{1}{0}$	$\lambda\|_I$	$\frac{\Theta_2^4}{\Theta_3^4} = 2q^{1/2} + \cdots$
$\frac{0}{1}$	$\lambda\|_S$	$\frac{\Theta_4^4}{\Theta_3^4} = 1 + \cdots$
$\frac{1}{1}$	$\lambda\|_{TS}$	$-\frac{\Theta_4^4}{\Theta_2^4} = -\frac{1}{2}q^{-1/2} + \cdots$

(3). Since $\mathrm{ord}_{\Gamma(2)}(\lambda) = 1$ all of the assertions of Proposition 4.4.7 apply.

(4). Since $\Theta_2^4\Theta_3^4\Theta_4^4$ has a simple zero at each cusp, we must obtain S_k in this way.

(5). The form $\Theta_2^4+\Theta_4^4-\Theta_3^4 = O(q^{2/2})$ in $M_2(\Gamma(2))$ has a zero of order at least 2 at ∞ which contradicts the valence formula unless this function vanishes identically.

(6). First note Θ_2 and Θ_3 are algebraically independent. If $f \in M_k(\Gamma(2))$ with $k \geq 0$ and even, then $g := f/\Theta_3^{2k} \in A_0(\Gamma(2))$ with the only possible pole of g located at the pole of λ. Therefore, part 2 of Prop 4.4.7 shows that g is a polynomial in λ of degree no more than $k/2$ since the valence formula says that f has $k/2$ zeros (hence g has no more than $k/2$ zeros). □

4.7 Building congruence modular forms N from Klein Forms

A subgroup Γ of $\Gamma(1)$ is called a congruence subgroup if Γ contains $\Gamma(N)$ for some N. The smallest such N turns out to be the level of Γ in this case (see Proposition 4.13.4 below). Similarly, a modular function f is said to have level N if it is invariant under $\Gamma(N)$. Most subgroups of $\Gamma(1)$ are not congruence; let a_n denote the number of subgroups of $\Gamma(1)$ of index n and let b_n denote the number of congruence subgroups of $\Gamma(1)$ of index at most n. Then it is known ([14], [15], [19]) that

$$a_n \sim \exp\left(\frac{1}{6}n\log n - \frac{1}{6}n + n^{1/2} + n^{1/3} + \frac{1}{2}\log n - \frac{1}{4} - \frac{1}{2}\log 2\pi\right),$$
$$\log(b_n) \sim \left(\frac{\sqrt{2}-1}{2}\right)^2 \frac{\log^2 n}{\log\log n}.$$

One of the building blocks of modular forms of higher levels is the Klein form $\mathfrak{k}_{\vec{r}}(\tau)$, which is defined for $\vec{r} \in \mathbb{Q}^2, \tau \in \mathbb{H}$ and has weight -1 and generalizes $\eta(\tau)^{-2}$. We will also introduce a form of positive integral weight k by $\mathfrak{e}^k_{\vec{r}}(\tau)$ which generalizes the Eisenstein series $E_{2k}(\tau)$. Set

$$\begin{aligned}
\mathfrak{k}_{\vec{r}}(\tau) &= -2\pi i z e^{\pi i r_1 z} \prod_{\omega \in \Lambda'} \left(1 + \frac{z}{\omega}\right) e^{-\frac{z}{\omega}}, \\
\mathfrak{e}^1_{\vec{r}}(\tau) &= \frac{1}{2\pi i}\left(\frac{1}{z} + \sum_{\Omega \in \Lambda'} \frac{1}{z+\omega} - \frac{1}{\omega}\right), \\
\mathfrak{e}^k_{\vec{r}}(\tau) &= \frac{(k-1)!}{(2\pi i)^k} \sum_{\omega \in \Lambda} \frac{1}{(z+\omega)^k}, \quad k \geq 2,
\end{aligned}$$

where $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$ and $z = r_1\tau + r_2$ and the sums or products over $\omega = m\tau + n$ are performed over n first and then m. These sums are not defined if $\vec{r} \in \mathbb{Z}^2$, in which we take out the undefined term and obtain the definitions

$$\mathfrak{e}^k_{\vec{r}}(\tau) = \begin{cases} \zeta(1-k)E_k(\tau) & , k \text{ even} \\ 0 & , k \text{ odd} \end{cases}, \text{ for } \vec{r} \in \mathbb{Z}^2.$$

The function $\mathfrak{k}_{\vec{r}}(\tau)$ is a specialization of the Weierstrass σ function for the lattice $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$, which is defined as

$$\sigma(z|\tau) = z \prod_{\omega \in \Lambda'} \left(1 - \frac{z}{\omega}\right) e^{\frac{z}{\omega} + \frac{z^2}{2\omega^2}}.$$

The product is absolutely convergent. In Exercise 2.12.8 we had, for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$ and integers A, B with $\omega = A\tau + B$

$$\begin{aligned}
\sigma(z|\tau) &= \frac{-e^{\frac{\pi^2}{6}E_2(\tau)z^2}}{2\pi\eta(\tau)^3}\Theta_1(z|\tau), \\
\sigma\left(\frac{z}{c\tau+d}\middle|\frac{a\tau+b}{c\tau+d}\right) &= (c\tau+d)^{-1}\sigma(z|\tau), \\
\frac{\sigma(z+\omega|\tau)}{\sigma(z|\tau)} &= (-1)^{A+B+AB} e\left(-\frac{(6A + \pi i E_2(\tau)\omega)(2z+\omega)}{12}\right).
\end{aligned}$$

Thus the following relations are clear (when $z = r_1\tau + r_2$).

$$\begin{aligned}
\mathfrak{k}_{\vec{r}}(\tau) &= -2\pi i e^{\pi i r_1 z} e^{-\frac{\pi^2 z^2}{6}E_2(\tau)}\sigma(z|\tau), \\
2\pi i \mathfrak{e}^1_{\vec{r}}(\tau) &= -\frac{\pi^2}{3}E_2(\tau)z + \frac{d}{dz}\log\sigma(z|\tau), \\
(2\pi i)^2 \mathfrak{e}^2_{\vec{r}}(\tau) &= \frac{\pi^2}{3}E_2(\tau) - \frac{d^2}{dz^2}\log\sigma(z|\tau).
\end{aligned}$$

Using the Jacobi triple product identity in these relations give the following proposition.

Proposition 4.7.1. *Set $z = r_1\tau + r_2$. The Klein forms have the series expansions,*

$$\begin{aligned}
\mathfrak{k}_{\vec{r}}(\tau) &= q_z^{(r_1-1)/2}\frac{(q_z;q)_\infty(q/q_z;q)_\infty}{(q;q)_\infty^2},\\
\mathfrak{e}^1_{\vec{r}}(\tau) &= \frac{q_z+1}{2(q_z-1)} - \sum_{n=1}^{\infty}(q_z^n - q_z^{-n})\frac{q^n}{1-q^n},\ \textit{for } |r_1|<1,\\
\mathfrak{e}^2_{\vec{r}}(\tau) &= \frac{q_z}{(q_z-1)^2} + \sum_{n=1}^{\infty}(q_z^n + q_z^{-n})\frac{nq^n}{1-q^n},\ \textit{for } |r_1|<1,\\
\mathfrak{e}^3_{\vec{r}}(\tau) &= \frac{q_z(q_z+1)}{(q_z-1)^3} - \sum_{n=1}^{\infty}(q_z^n - q_z^{-n})\frac{n^2q^n}{1-q^n},\ \textit{for } |r_1|<1,
\end{aligned}$$

where $\mathfrak{e}^{k+1}_{\vec{r}}(\tau)$ is formally obtained from $\mathfrak{e}^k_{\vec{r}}(\tau)$ by applying $\frac{-1}{2\pi i}\frac{\partial}{\partial z}$.

Note that the classical identity [1, Entry 3.2.1],

$$\frac{(q;q)_\infty^2}{(x;q)_\infty(q/x;q)_\infty} = \sum_{n=-\infty}^{\infty}\frac{(-1)^n q^{n(n+1)/2}}{1-xq^n},$$

allows us to recognize the transformation properties of the sums of the type on the right hand side of this identity, since it is essentially the reciprocal of a Klein form.

Proposition 4.7.2. *For $N > 1$,*

$$\begin{aligned}
\prod_{j=0}^{N-1}\mathfrak{k}_{\frac{i}{N},\frac{j}{N}}(\tau) &= \zeta_{4N}^{(N-1)(i-N)}\frac{\eta(N\tau)^2}{\eta(\tau)^{2N}}\mathfrak{k}_{\frac{i}{N},\frac{0}{N}}(N\tau),\\
\prod_{j=1}^{N-1}\mathfrak{k}_{\frac{0}{N},\frac{j}{N}}(\tau) &= N\zeta_4^{1-N}\frac{\eta(N\tau)^2}{\eta(\tau)^{2N}}.
\end{aligned}$$

Proof. Using the q-product representation of the Klein forms, we see that these follows from the identity

$$\prod_{j=0}^{N-1}(1-\zeta_N^j x^i) = 1 - x^{iN}.$$

□

The modular transformation and quasi-periodicity relations for the σ function give the following.

Proposition 4.7.3. *For $\vec{r} = (r_1, r_2)$ and $g = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \Gamma(1)$,*

$$\begin{aligned}
\mathfrak{k}_{\vec{r}}|_g(\tau) &= \mathfrak{k}_{\vec{r}.g}(\tau),\\
\mathfrak{e}^1_{\vec{r}}|_g(\tau) &= \mathfrak{e}^1_{\vec{r}.g}(\tau) + c(a\tau+b)r_1 + c(c\tau+d)r_2,\\
\mathfrak{e}^2_{\vec{r}}|_g(\tau) &= \mathfrak{e}^2_{\vec{r}.g}(\tau) - \frac{c}{2\pi i(c\tau+d)},\\
\mathfrak{e}^k_{\vec{r}}|_g(\tau) &= \mathfrak{e}^k_{\vec{r}.g}(\tau), \quad k \geq 3.
\end{aligned}$$

If $(n_1, n_2) \in \mathbb{Z}^2$,

$$\begin{aligned}
\mathfrak{k}_{\vec{r}+(n_1,n_2)}(\tau) &= (-1)^{n_1+n_2+n_1n_2}e(\tfrac{1}{2}(r_1n_2 - r_2n_1))\mathfrak{k}_{\vec{r}}(\tau),\\
\mathfrak{e}^1_{\vec{r}+(n_1,n_2)}(\tau) &= \mathfrak{e}^1_{\vec{r}}(\tau) - n_1,\\
\mathfrak{e}^k_{\vec{r}+(n_1,n_2)}(\tau) &= \mathfrak{e}^k_{\vec{r}}(\tau), \quad k \geq 2.
\end{aligned}$$

Proposition 4.7.4. *If* $\gcd(a,c)=1$, *then*

$$\operatorname{ord}_{\frac{a}{c}} \mathfrak{k}_{\vec{r}}(\tau) = \binom{\operatorname{frac}(\vec{r}.(a,c)^{\intercal})}{2},$$

where $\operatorname{frac}(x)$ *denotes the fractional part of* x *that satisfies* $0 \le \operatorname{frac}(x) < 1$.

Proof. Note that with $z = u\tau + v$

$$\begin{aligned}\mathfrak{k}_{u,v}(\tau) &= q_z^{(u-1)/2}\frac{(q_z;q)_\infty(q/q_z;q)_\infty}{(q;q)_\infty^2}\\ &= e((u-1)(u\tau+v)/2)\frac{(e(u\tau+v);q)_\infty(e(\tau-u\tau-v);q)_\infty}{(q;q)_\infty^2}\\ &= e((u-1)v/2)q^{u(u-1)/2}\frac{(e(v)q^u;q)_\infty(e(-v)q^{1-u};q)_\infty}{(q;q)_\infty^2}.\end{aligned}$$

If $0 < u < 1$, then the lowest power of q in this expression is $q^{u(u-1)/2}$. For general real u we can shift u by integers without chaninging the order. Finally, the general proposition follows combining this with Proposition 4.7.3. □

Proposition 4.7.5 ([11])**.** *For* $\vec{r} = (r_1, r_2) \in \frac{1}{N}\mathbb{Z}^2$,

1. *For* $k = -\sum_{\vec{r}} m(\vec{r})$, *the form* $\prod_{\vec{r}} \mathfrak{k}_{\vec{r}}(\tau)^{m(\vec{r})}$ *is in* $M_k^!(\Gamma(N))$ *if and only if*

$$\begin{aligned}\sum_{\vec{r}} m(\vec{r})(Nr_1)^2 &\equiv 0 \bmod N\gcd(2,N),\\ \sum_{\vec{r}} m(\vec{r})(Nr_2)^2 &\equiv 0 \bmod N\gcd(2,N),\\ \sum_{\vec{r}} m(\vec{r})(Nr_1)(Nr_2) &\equiv 0 \bmod N.\end{aligned}$$

2. *The form* $\sum_{\vec{r}} m(\vec{r})\mathfrak{e}^1_{\vec{r}}(\tau)$ *is in* $M_1(\Gamma(N))$ *if and only if* $\sum_{\vec{r}} m(\vec{r})r_1 = 0$.
3. *The form* $\sum_{\vec{r}} m(\vec{r})\mathfrak{e}^2_{\vec{r}}(\tau)$ *is in* $M_2(\Gamma(N))$ *if and only if* $\sum_{\vec{r}} m(\vec{r}) = 0$.
4. *The form* $\sum_{\vec{r}} m(\vec{r})\mathfrak{e}^k_{\vec{r}}(\tau)$ *is in* $M_k(\Gamma(N))$ *for any* $k \ge 3$.

We will give a generator x_N for the function field $A_0(\Gamma(N))$ for $N < 6$ in Section 4.9. The following theorem tells us that two ratios of Klein forms suffice for $N \ge 6$.

Theorem 4.7.6 ([9])**.** *For* $N \ge 6$, *we have* $A_0(\Gamma(N)) = \mathbb{C}(x_{2,N}(\tau), x_{3,N}(\tau))$, *where*

$$x_{r,N}(\tau) = \left(\frac{\mathfrak{k}_{r/N,0}(N\tau)}{\mathfrak{k}_{1/N,0}(N\tau)}\right)^{\gcd(2,r,N)}.$$

Furthermore, $x_{3,N}$ *is integral over* $\mathbb{Q}[x_{2,N}]$.

Exercise 4.7.7 (Representation of $\mathrm{SL}_2(\mathbb{Z}_p)$ on $\mathbb{C}^{\frac{p-1}{2}}$)**.** *Let* $p > 3$ *be a prime and for* $1 \le n \le \frac{p-1}{2}$ *set*

$$x_n(\tau) = q^{\frac{n(n-p)}{2p}}\frac{(q^p;q^p)_\infty(q^i;q^p)_\infty(q^{p-i};q^p)_\infty}{(q;q)_\infty^{3p}}. \tag{4.7.1}$$

1. *Use the representation*

$$\sqrt{p}\zeta_8^{p-1}\zeta_{4p}^{(p-1)(n-p)}x_n(\tau)=\prod_{j=0}^{p-1}\mathfrak{k}_{\frac{n}{p},\frac{j}{p}}(\tau)\prod_{j=1}^{\frac{p-1}{2}}\mathfrak{k}_{\frac{0}{p},\frac{j}{p}}(\tau)$$

and Proposition 4.7.5 to deduce that $x_n\in M^!_{\frac{1-3p}{2}}(\Gamma(p))$. *Hint:* $p^2\equiv 1 \bmod 24$.

2. *Set* $X(\tau)=(x_1(\tau),\dots,x_{\frac{p-1}{2}}(\tau))$. *Use the representation*

$$x_n(\tau)=i\zeta_{2p}^{-n}\frac{\Theta\left[\begin{smallmatrix}\frac{1}{2}+\frac{n}{p}\\ \frac{1}{2}\end{smallmatrix}\right](0|p\tau)}{\eta(\tau)^{3p}}$$

and Proposition 2.8.3 to deduce that $X|_T=\rho(T).X$ *and* $X|_S=\rho(S).X$ *where*

$$\rho(T)_{i,i}=\zeta_p^{\frac{i(i-p)}{2}},\quad \rho(T)_{i,j}=0,$$
$$\rho(S)_{i,j}=\frac{(-1)^{i+j-1+\frac{p^2-1}{8}}}{\sqrt{(-1)^{\frac{p-1}{2}}p}}(\zeta_p^{ij}-\zeta_p^{-ij}).$$

Hint: After applying S, *you will have to dissect the* θ*-series in* $\frac{\tau}{p}$ *to get a* θ*-series in* $p\tau$.

3. *We now have a homomorphism* $\rho:\mathrm{SL}_2(\mathbb{Z})\to\mathrm{GL}_{\frac{p-1}{2}}(\mathbb{C})$ *that is defined on the generators* S *and* T *as above and* $\rho(-I)=(-1)^{(p+1)/2}$. *By lifting the matrices modulo* p, *deduce that* $M\mapsto\rho(M)$ *is a representation of* $\mathrm{SL}_2(\mathbb{Z}_p)$.

4.8 Building congruence modular forms from η products

Proposition 4.8.1. *Let* $\gcd(a,c)=1$ *and* $M\in\mathbb{Z}^{2\times 2}$ *with* $\det M>0$. *Then,*

$$\mathrm{ord}_{\frac{a}{c}}\eta|_M(\tau)=\frac{1}{24}\frac{\gcd(M.(a,c)^\intercal)^2}{\det(M)}.$$

Proof. It suffices to prove this when $\frac{a}{c}=\frac{1}{0}$, that is,

$$\mathrm{ord}_\infty(m_{21}\tau+m_{22})^{-1/2}\eta\left(\frac{m_{11}a+m_{12}}{m_{21}\tau+m_{22}}\right)=\frac{\gcd(m_{11},m_{21})^2}{\det(M)}$$

For this, we seek a $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\in\Gamma(1)$, such that

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}m_{11} & m_{12}\\ m_{21} & m_{22}\end{pmatrix}=\begin{pmatrix}A & B\\ 0 & D\end{pmatrix}.$$

The order will then be given by $\frac{A}{24D}$. We obtain $c=\frac{-m_{21}}{\gcd(m_{11},m_{21})}$ and $d=\frac{m_{11}}{\gcd(m_{11},m_{21})}$ and the result easily follows. □

We record a simple fact here. If $\Gamma_1>\Gamma_2$, then

$$\mathrm{ord}_{\Gamma_2}(f)=\mathrm{ord}_{\Gamma_1}(f)[\Gamma_1:\Gamma_2].$$

Proposition 4.8.2. *For any integer $N \geq 1$,*

$$\mathrm{ord}_{\Gamma_0(N)}(j(\tau)) = \mathrm{ord}_{\Gamma_0(N)}(j(N\tau)) = [\Gamma(1) : \Gamma_0(N)].$$

Proof. The function $j(\tau)$ has a simple pole at each cusp $\frac{a}{c}$, which translates to a pole of order $\frac{N}{c\gcd(c,N/c)}$ with respect to $\Gamma_0(N)$. Therefore,

$$\mathrm{ord}_{\Gamma_0(N)}(j(\tau)) = \sum_{c|N} \frac{N\phi(\gcd(c, N/c))}{c\gcd(c, N/c)}.$$

The function $j(N\tau)$ has a pole at $\frac{a}{c}$ of order $\frac{N}{c\gcd(c,N/c)} \cdot \frac{\gcd(c,N)^2}{N}$. Therefore,

$$\mathrm{ord}_{\Gamma_0(N)}(j(\tau)) = \sum_{c|N} \frac{N\phi(\gcd(c, N/c))}{c\gcd(c, N/c)} \frac{\gcd(c, N)^2}{N}.$$

These sums are the same by the substitution $c \to N/c$ □

Proposition 4.8.3. *Set $\Gamma = \Gamma_0(N)$ and suppose that $f(\tau) = \prod_{l|N} \eta(l\tau)^{r_l}$ and that the three numbers*

$$k = \tfrac{1}{2}\sum_{l|N} r_l, \quad \mathrm{ord}_\infty(f, \Gamma) = \tfrac{1}{24}\sum_{l|N} l r_l, \quad \mathrm{ord}_0(f, \Gamma) = \tfrac{1}{24}\sum_{l|N} \tfrac{N}{l} r_l,$$

are all integers. Then, for any $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ with odd d, f satisfies

$$f|_{g,k}(\tau) = \left(\frac{(-1)^k \prod_{l|N} l^{|r_l|}}{d}\right) f(\tau).$$

Remark 4.8.4. *In the case that d is even, c must be odd and we can recover the multiplier for such d by*

$$f|_{g,k}(\tau) = \left(\frac{(-1)^k \prod_{l|N} l^{|r_l|}}{c+d}\right) f(\tau).$$

simply be replacing τ by $\tau - 1$.

Proof. Assuming d is odd, the multiplier system for η (Exercise 2.12.6) has the form

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right) = \left(\frac{c}{|d|}\right) \zeta_{24}^{3d+d(b-c)+ac(1-d^2)} \sqrt{-i(c\tau+d)}\eta(\tau),$$
$$\text{or} \quad \eta\left(l\frac{a\tau+b}{c\tau+d}\right)^{r_l} = \left(\frac{c^{|r_l|}l^{|r_l|}}{|d|}\right) \zeta_{24}^{3dr_l+dblr_l-(ad^2-a+d)\frac{c}{N}\frac{N}{l}r_l} (-i(c\tau+d))^{\frac{r_l}{2}} \eta(l\tau)^{r_l},$$

since $l\frac{a\tau+b}{c\tau+d} = \frac{a(l\tau)+bl}{\frac{c}{N}\frac{N}{l}(l\tau)+d}$. Therefore

$$\begin{aligned}\frac{f|_{g,k}(\tau)}{f(\tau)} &= (-i)^k \left(\frac{c^{2|k|}\prod_{l|N} l^{|r_l|}}{|d|}\right) \zeta_{24}^{6dk+24db\,\mathrm{ord}_\infty(f,\Gamma)-24(ad^2-a+d)\frac{c}{N}\,\mathrm{ord}_0(f,\Gamma)} \\ &= \left(\frac{(-1)^k \prod_{l|N} l^{|r_l|}}{d}\right),\end{aligned}$$

since k, $\mathrm{ord}_\infty(f, \Gamma)$, and $\mathrm{ord}_0(f, \Gamma)$ are all integers. □

For $l \mid N$, the order of $\eta(l\tau)$ at the cusp $\frac{a}{c}$ is given by $\frac{\gcd(l,c)^2}{24l}$ by Proposition 4.8.1, while the width of this cusp with respect to $\Gamma_0(N)$ is given by $\frac{N}{\gcd(N,c^2)}$, as in Proposition 4.3.3. Using this facts and Section 4.4, we can write down generators for $\Gamma_0(N)$ for some N.

Example 4.8.5. $\Gamma_0(18)$. *There are eight cusps* $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{6}, \frac{5}{6}, \frac{1}{9}, \frac{1}{18}$. *The function*

$$x = \eta(1\tau)^{-2}\eta(2\tau)^1\eta(3\tau)^1\eta(6\tau)^{-1}\eta(9\tau)^{-1}\eta(18\tau)^2$$

can be verified to be in $A_0(\Gamma_0(18))$ *with a simple pole at* $\frac{1}{1}$ *and a simple zero at* $\frac{1}{18}$. *It is thus a Hauptmodul for* $\Gamma_0(18)$. *We can also write down a function with a simple pole at* $\frac{1}{1}$ *and a simple zero at* $\frac{1}{9}$,

$$1 + 2x = \eta(1\tau)^{-2}\eta(2\tau)^1\eta(3\tau)^0\eta(6\tau)^0\eta(9\tau)^2\eta(18\tau)^{-1}.$$

Example 4.8.6. $\Gamma_0(33)$. *There are four cusps* $\frac{1}{1}, \frac{1}{3}, \frac{1}{11}, \frac{1}{33}$. *The functions*

$$x = \frac{\eta(3\tau)\eta(33\tau)}{\eta(\tau)\eta(11\tau)},$$
$$y = \frac{\eta(3\tau)^6\eta(11\tau)^6}{\eta(\tau)^6\eta(33\tau)^6},$$

can be verified to have, for x, *simple poles at* $\frac{1}{1}$ *and* $\frac{1}{11}$, *and for* y, *quintuple poles at* $\frac{1}{1}$ *and* $\frac{1}{33}$. *The orders of the functions* x *and* y *with respect to* $\Gamma_0(33)$ *are thus* 2 *and* 10. *Since* $x + y$ *has odd order and* x *has order* 2, x *and* y *generate* $A_0(\Gamma_0(33))$ *by Proposition 4.4.8. The relation of degree* 2 *in* y *and degree* 10 *in* x *is*

$$\frac{(y-1)^2}{y} = \frac{(3x^2 + x + 1)\left(9x^4 + 15x^3 + 14x^2 + 5x + 1\right)^2}{x^5}.$$

Following [8], the η function can be generalized to any even real Dirichlet character χ. Set

$$\eta_\chi(\tau) = q^{-\frac{1}{2}L(-1,\chi)} \prod_{n=1}^{\infty}(1-q^n)^{\chi(n)}, \quad (\chi(-1) = 1).$$

Here $L(s,\chi)$ is the Dirichlet series $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$, which converges for $s > 1$ and can be analytically continued to $\mathbb{C}$ with a possible pole at $s = 1$. When χ is the function 1 identically, we recover the usual η function because of the value $L(-1,1) = \zeta(-1) = -\frac{1}{12}$. It suffices to study primitive characters because if χ is a character modulo k and $\chi(n) = \chi_1(n)\chi_0(n)$ where χ_1 is the primitive character modulo $\Delta | k$ and $\chi_0(n)$ is the principal character modulo k, then

$$\eta_\chi(\tau) = \prod_{l \mid \frac{k}{\Delta}} \eta_{\chi_1}(l\tau)^{\mu(l)\chi_1(l)}.$$

It should be pointed out at this point that the only real even primitive characters are given by

$$\chi(n) = \left(\frac{\Delta}{n}\right),$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Kronecker symbol and Δ is a fundamental discriminant (see definition 7.3.1). The period of this character is Δ.

Proposition 4.8.7 ([8])**.** *Let* $\Delta > 1$ *be a fundamental discriminant and* χ *the associated primitive real even character. Set* $\chi'(n)$ *to be* $\chi(n)$ *if* Δ *is a prime, and* 1 *otherwise. Then, for any* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\Delta)$, η_χ *satisfies the transformation formula*

$$\eta_\chi\left(\frac{a\tau + b}{c\tau + d}\right) = \chi'(d)\eta_\chi(\tau)^{\chi(d)} \times \begin{cases} \zeta_5^{ab} & , \Delta = 5 \\ \zeta_{16}^{a-d+bc-8b} & , \Delta = 8 \\ 1 & , \Delta > 8 \end{cases}.$$

4.9 $\Gamma(N)$ and regular polyhedron

It is known that the finite groups acting faithfully on $\mathbb{C}_\infty$ are exactly

$\mathbb{Z}_n$	the cyclic group of order n,
$\mathbb{Z}_n \rtimes \mathbb{Z}_2$	the dihedral group of order $2n$,
A_4	the symmetries of the tetrahedron of order 12,
S_4	the symmetries of the octahedron of order 24,
A_5	the symmetries of the icosahedron of order 60.

For the modular group, it turns out that restricting to normal subgroups of genus 0 puts a restriction on the first two types, and there is a finite list of possible groups. First, for any subgroup Γ with $\mu = [\overline{\Gamma}(1) : \overline{\Gamma}]$, let e_2 (resp. e_3, e_∞) denote the number of equivalent classes under Γ of the points $\Gamma(1)(i)$ (resp. $\Gamma(1)(e(\frac{1}{3}))$, $\Gamma(1)(\infty)$). Equivalently, e_2, e_3 and e_∞ are the number of cycles in the permutations S and O and T in the permutation representation of Γ. Thus, $e_m = \epsilon_m + \frac{\mu - \epsilon_m}{m}$ for $m = 2, 3, \infty$ since $e_\infty = \epsilon_\infty$. Next, suppose that $\overline{\Gamma}$ is a normal subgroup of $\overline{\Gamma}(1)$. This means that all of the cycles of S and O and T have the same length, and therefore that $e_m | \mu$ for $m = 2, 3, \infty$. Thus, in this case we can define n_m by

$$\mu = n_2 e_2 = n_3 e_3 = n_\infty e_\infty,$$

and this corresponds to the triplet (n_2, n_3, n_∞) describing the branching information of Γ. The genus formula may be rearranged as

$$\frac{2 - 2g}{\mu} = \frac{1}{n_2} + \frac{1}{n_3} + \frac{1}{n_\infty} - 1. \tag{4.9.1}$$

Note that n_2 is either 1 or 2 and n_3 is either 1 or 3, while n_∞, which is the width of any cusp, has no such restriction. An easy consequence is that $\mu \equiv 0 \bmod 6$ if $\mu > 3$. Also, if $\Gamma_2 \trianglelefteq \Gamma_1 \trianglelefteq \Gamma(1)$, then each $n_m(\Gamma_1)$ divides $n_m(\Gamma_2)$.

Proposition 4.9.1. *For prime p with $p \geq 5$, $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ is simple.*

Proof. Suppose that there were a non-trivial normal subgroup G of $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$. By the second isomorphism theorem for groups, this would imply the existence of a group G' such that $\Gamma(p) \trianglelefteq G' \trianglelefteq \Gamma(1)$. This is impossible because the branching information for $\Gamma(p)$, $(2, 3, p)$, has the possible divisors $(2, 3, p)$, $(2, 1, p)$, $(1, 3, p)$, $(1, 1, p)$, $(2, 3, 1)$, $(2, 1, 1)$, $(1, 3, 1)$, $(1, 1, 1)$. It is easy to check that all but the first and last two possibilities are ruled out by (4.9.1), and these two possibilities are ruled out because the correspond to trivial choices of G. □

Proposition 4.9.2. *If $\overline{\Gamma}$ is a proper normal subgroup of $\overline{\Gamma}(1)$ with finite index and genus 0, then Γ is one of the following:*

Γ	$\overline{\Gamma}(1)/\overline{\Gamma}$	(n_2, n_3, n_∞)
Γ^2	$\mathbb{Z}_2$	$(2, 1, 1)$
Γ^3	$\mathbb{Z}_3$	$(1, 3, 1)$
$\Gamma(2)$	S_3	$(2, 3, 2)$
$\Gamma(3)$	A_4	$(2, 3, 3)$
$\Gamma(4)$	S_4	$(2, 3, 4)$
$\Gamma(5)$	A_5	$(2, 3, 5)$

Proof. We first deal with the case $n_2 = n_3 = 1$. In this case, (4.9.1) is $\frac{2}{\mu} = 1 + \frac{1}{n_\infty}$ and so $\mu = 1 = n_\infty$. So in this case, $\overline{\Gamma} = \overline{\Gamma}(1)$. Next, suppose that $n_2 = 1$ and $n_3 = 3$, so that $\frac{2}{\mu} = \frac{1}{3} + \frac{1}{n_\infty}$. Since $\mu \geq n_\infty$ this implies that $\mu = 3$ and that $\Gamma = \Gamma^3$ as this is the only normal subgroup of index 3. Next, suppose that $n_2 = 2$ and $n_3 = 1$, so that $\frac{2}{\mu} = \frac{1}{2} + \frac{1}{n_\infty}$. Since $\mu \geq n_\infty$ this implies that $\mu = 2$ and that $\Gamma = \Gamma^2$ as this

is the only normal subgroup of index 2. Next, suppose that $n_2 = 2$ and $n_3 = 3$, so that $\frac{2}{\mu} = -\frac{1}{6} + \frac{1}{n_\infty}$. This implies that $n_\infty = 2, 3, 4, 5$ with corresponding $\mu = 6, 12, 24, 60$. Set $G = \overline{\Gamma}(1)/\overline{\Gamma}$ so that $\mu = |G|$. We will first determine G up to isomorphism and then $\overline{\Gamma}$ exactly. Note that G is generated (modulo Γ) by S, ST and T with $S^2 = (ST)^3 = T^{n_\infty} = 1$.

First, suppose that $|G| = 6$, $(2, 3, 2)$. Since S has order 2 and ST has order 3 but their product T has order 2 (not 6), G cannot be Abelian, and so $G \simeq S_3$.

Next, suppose that $|G| = 12$, $(2, 3, 3)$. A Sylow 3 subgroup cannot be normal, because otherwise its quotient would correspond to a normal subgroup of $\overline{\Gamma}(1)$ of index 4 which doesn't exist. Since A_4 is the only group of order 12 that doesn't have a normal Sylow 3 subgroup, $G \simeq A_4$.

Next, suppose that $|G| = 24$, $(2, 3, 4)$. As before, there are 4 Sylow 3 subgroups, and we obtain a homomorphism $\phi : G \to S_4$ by the action of G on the 4 Sylow 3 subgroups where $\operatorname{im}\phi \simeq A_4, S_4$ since these are the only transitive subgroups of S_4 whose order is divisible by 6. If $\operatorname{im}\phi = A_4$, then this corresponds to another normal subgroup $\overline{\Gamma}_1$ of index 12. The only group with index 12 corresponds to the triplet $(2, 3, 3)$, which does not divide the triplet $(2, 3, 4)$. Hence $\operatorname{im}\phi = S_4$ and so $G \simeq S_4$.

Finally, suppose that $|G| = 60$, $(2, 3, 5)$. Since the only triplets dividing $(2, 3, 5)$ are the trivial ones, G must be simple. Standard group theory arguments using the Sylow 2 subgroup show that A_5 is the only simple group of order 60.

To finish the proof, we need to show that $\Gamma(N)$ is the only possibility for Γ when the branching information is $(2, 3, N)$ (and $g = 0$). By Proposition 4.3.1, the groups $\overline{\Gamma}(2), \overline{\Gamma}(3), \overline{\Gamma}(4), \overline{\Gamma}(5)$ have the correct indexes in $\overline{\Gamma}(1)$, that is

$$\mu = \frac{12N}{6-N} = [\overline{\Gamma}(1) : \overline{\Gamma}(N)] = \begin{cases} \frac{1}{2}N^3 \prod_{p|N}\left(1 - \frac{1}{p^2}\right) & , N \geq 3 \\ 6 & , N = 2 \end{cases},$$

for $N = 2, 3, 4, 5$. Consider $\overline{\Gamma} \cap \overline{\Gamma}(N)$ for $N = 2, 3, 4, 5$. We know that $\overline{\Gamma} \cap \overline{\Gamma}(N)$ is a normal subgroup of $\overline{\Gamma}$, but be do not know a priori that the genus of $\overline{\Gamma} \cap \overline{\Gamma}(N)$ is 0. However, we are given that both $\overline{\Gamma}$ and $\overline{\Gamma}(N)$ have cusp width N, and so $\overline{\Gamma} \cap \overline{\Gamma}(N)$ has cusp width N. This means that the branching data of $\overline{\Gamma} \cap \overline{\Gamma}(N)$ is $(2, 3, N)$ and if μ and g denote the index and genus of $\overline{\Gamma} \cap \overline{\Gamma}(N)$, we have

$$\frac{2 - 2g}{\mu} = \frac{1}{2} + \frac{1}{3} + \frac{1}{N} - 1.$$

Since the right hand side is strictly positive for $N = 2, 3, 4, 5$, g is forced to be 0 and μ is forced to be $12N/(6 - N)$. This means that $[\overline{\Gamma}(1) : \overline{\Gamma} \cap \overline{\Gamma}(N)] = [\overline{\Gamma}(1) : \overline{\Gamma}(N)]$, which forces $\overline{\Gamma} = \overline{\Gamma}(N)$. □

Although we deduced that there is only one normal subgroup of genus 0 with branching data $(2, 3, N)$ for $N = 2, 3, 4, 5$, this result does not need to hold for higher genera. For example, all normal subgroups of genus 1 have branching data $(2, 3, 6)$, and there are infinitely many of them ([16]).

Having classified all of the normal subgroup Γ of $\Gamma(1)$ with genus 0, let us turn now to the problem of constructing the spaces $M_k(\Gamma)$ for these Γ. The groups Γ^2 and Γ^3 are not very interesting, as (Exercise 4.9.9)

$$A_0(\Gamma^2) = \mathbb{C}(\sqrt{j - 1728}), \quad A_0(\Gamma^3) = \mathbb{C}(j^{1/3}).$$

so let us turn to $\Gamma(N)$ for $N = 2, 3, 4, 5$. Assuming that there is a Hauptmodul, say $f_N(\tau)$, for these $\Gamma(N)$, it is possible to show that there is a Hauptmodul x_N that is uniquely determined by

$$x_N(\tau) = q^{-\frac{1}{N}}(1 + \text{integral powers of } q).$$

Since $\Gamma(N)$ is a normal subgroup of $\Gamma(1)$, there must be constants A, B, C, D, depending on N, such that

$$f_N|_T = \frac{Af_N + B}{Cf_N + D}.$$

By rescaling the matrix $\overline{M} = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, we may assume that one of its eigenvalues is 1. If the other eigenvalue were 1, then $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ would be similar to either $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. The first is a contradiction because $\overline{M}^N = I$ since $T^N \in \Gamma(N)$. If the second were true then f_N would be invariant under T and so N divides $\operatorname{ord}_\infty(f_N(\tau) - f_N(\infty), \Gamma(N)) \neq 0$, which is a contradiction because $f_N(\tau) - f_N(\infty)$ is also a Hauptmodul for $\Gamma(N)$. We now have $M = P^{-1}\left(\begin{smallmatrix} \zeta & 0 \\ 0 & 1 \end{smallmatrix}\right)P$ where ζ is an N^{th} root of unity. Setting $x_N = P(f_N)$ gives $x_N|_T = \zeta_N^r x_N$ for some integer r and so $q^{-r/N}x_N$ has an expansion in integral powers of q. Since x_N is also a Hauptmodul, $r = \pm 1$ and we choose $r = -1$ which gives x_N a simple pole at ∞. It will be shown that the following functions are such Hauptmoduln for Γ_N.

$$\begin{aligned}
x_2(\tau) &= \frac{(q^{1/2};q^{1/2})_\infty^8 + (-q^{1/2};-q^{1/2})_\infty^8}{2q^{1/2}(q^2;q^2)_\infty^8} = q^{-\frac{1}{2}}(1 + 20q - 62q^2 + 216q^3 - 641q^4 + \cdots), \\
x_3(\tau) &= \frac{(q^{1/3};q^{1/3})_\infty^3 + 3q^{1/3}(q^3;q^3)_\infty^3}{q^{1/3}(q^3;q^3)_\infty^3} = q^{-\frac{1}{3}}(1 + 5q - 7q^2 + 3q^3 + 15q^4 + \cdots), \\
x_4(\tau) &= \frac{(q^2;q^2)_\infty^6}{q^{1/4}(q;q)_\infty^2(q^4;q^4)_\infty^4} = q^{-\frac{1}{4}}(1 + 2q - q^2 - 2q^3 + 3q^4 + 2q^5 + \cdots), \\
x_5(\tau) &= \frac{(q^2;q^5)_\infty(q^3;q^5)_\infty}{q^{1/5}(q;q^5)_\infty(q^4;q^5)_\infty} = q^{-\frac{1}{5}}(1 + q - q^3 + q^5 + q^6 - q^7 - 2q^8 + \cdots).
\end{aligned} \tag{4.9.2}$$

A more uniform (but multi-valued) definition of the modular function x_N is

$$\begin{aligned}
x_N &= \frac{j^{-\frac{N-6}{12N}}\,{}_2F_1\left(\begin{matrix} \frac{N-6}{12N}, \frac{5N-6}{12N} \\ \frac{N-1}{N} \end{matrix}\middle| \frac{1728}{j}\right)}{j^{-\frac{N+6}{12N}}\,{}_2F_1\left(\begin{matrix} \frac{N+6}{12N}, \frac{5N+6}{12N} \\ \frac{N+1}{N} \end{matrix}\middle| \frac{1728}{j}\right)} \\
&= q^{-\frac{1}{N}}\left(1 + \tfrac{120}{N(N^2-1)}q + \tfrac{180(N-5)(3N^2+21N+8)}{N^2(N+1)^2(4N^2-1)}q^2 + \cdots\right),
\end{aligned} \tag{4.9.3}$$

where j is the j function. This representation will be proven in Chapter 8 where Proposition 4.9.4 below can be utilized.

Proposition 4.9.3. *For $N = 2, 3, 4, 5$, x_N is a Hauptmodul for $\Gamma(N)$ and x_N^N is a Hauptmodul for $\Gamma_1(N)$. The action of T on x is given by*

$$x_N|_T = \zeta_N^{-1}x_N.$$

The action of S on x_N is given in the following table.

N	$x_N\|_S$
2	$\frac{8x+192}{x-1}$
3	$\frac{3x+18}{x-3}$
4	$\frac{2x+4}{x-2}$
5	$\frac{(1+\sqrt{5})x+2}{2x-1-\sqrt{5}}$

Proof. We only deal with the case $N = 5$ as the other cases are similar and simpler. By Proposition 4.7.2, x_5 has the representation

$$x_5(\tau) = \zeta_5^{-1}\prod_{i=0}^{4}\frac{\mathfrak{k}_{\frac{2}{5},\frac{i}{5}}(\tau)}{\mathfrak{k}_{\frac{1}{5},\frac{i}{5}}(\tau)},$$

hence we see immediately from Proposition 4.7.5 that $x_5 \in M_0^!(\Gamma(5))$. Next, suppose that $\frac{a}{c}$ is a cusp of $\Gamma(5)$ and that $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$. By Proposition 4.7.4,

$$\tfrac{1}{5}\operatorname{ord}_{\frac{a}{c}}(x_5, \Gamma(5)) = \sum_{i=0}^{4}\binom{\operatorname{frac}\left(\frac{2a+ic}{5}\right)}{2} - \sum_{i=0}^{4}\binom{\operatorname{frac}\left(\frac{a+ic}{5}\right)}{2}.$$

If $(c,5)=1$, it is easy to see that both of these sums are $-2/5$ (which is $(1-N^2)/12N$ when $N=5$), so x_5 has no zeros or poles at these cusps. The only cusps of $\Gamma(5)$ whose denominators are divisible by 5 are represented by $\frac{1}{5}, \frac{2}{5}$, where x_5 has a simple pole and simple zero, respectively. We now know that x_5 is a Hauptmodul for $\Gamma(5)$ since x_5 clearly has no poles in $\mathbb{H}$. It is clear from the q-series expansion of x_5 that $x_5|_T = \zeta_5^{-1}x_5$. From this we can deduce that $x_5^5 \in A_0(\Gamma_1(5))$ since $\Gamma_1(5)$ is generated by $\Gamma(5)$ and T. Since the cusps for $\Gamma_1(5)$ are a subset of the cusps for $\Gamma(5)$, the only possible location of a pole of x_5^5 on $\overline{\mathbb{H}}/\Gamma_1(5)$ is at the cusp $\frac{1}{5}$ (equivalent to ∞), where x_5^5 has a simple pole with respect to $\Gamma_1(5)$. Finally, by Propositions 4.7.3 and 4.7.1, the q-series expansion of $x_5|_S$ is

$$\begin{aligned} x_5|_S &= \zeta_5^{-1}\prod_{i=0}^{4}\frac{\mathfrak{k}_{\frac{i}{5},\frac{-2}{5}}(\tau)}{\mathfrak{k}_{\frac{i}{5},\frac{-1}{5}}(\tau)} \\ &= -\zeta_5^3\frac{1-\zeta_5^3}{1-\zeta_5^4}\frac{(\zeta_5^2q^{1/5};q^{1/5})_\infty(\zeta_5^3q^{1/5};q^{1/5})_\infty}{(\zeta_5^1q^{1/5};q^{1/5})_\infty(\zeta_5^4q^{1/5};q^{1/5})_\infty} \\ &= \frac{1+\sqrt{5}}{2}+\frac{5+\sqrt{5}}{2}q^{1/5}+\frac{5+3\sqrt{5}}{2}q^{2/5}+O(q^{3/5}). \end{aligned}$$

From these first few terms it is a simple matter to determine the constants A, B, C and D in the relation

$$x_5|_S = \frac{Ax_5+B}{Cx_5+D},$$

which must exist because $x_5|_S$ is a Hauptmodul for $\Gamma(5)$ since this is a normal subgroup of $\Gamma(1)$. □

Proposition 4.9.4. *Let $\{f(z),z\}$ denote the Schwarzian derivative*

$$\{f(z),z\} = \frac{f'''(z)}{f'(z)} - \frac{3}{2}\left(\frac{f''(z)}{f'(z)}\right)^2.$$

Then,

$$\{x_N,j\} = \frac{\frac{1}{2}(1-N^{-2})j(j-1728)-120j+1327104}{j^2(j-1728)^2}.$$

Proof. Since the Schwarzian derivative is invariant under $\mathrm{GL}_2(\mathbb{C})$ and $\Gamma(1)$ acts on x_N by a subgroup of $\mathrm{GL}_2(\mathbb{C})$, as a function of τ, $\{x_N,j\}$ is in $A_0(\Gamma(1))$. We assert that in fact $j^2(j-1728)^2\{x_N,j\}$ is a polynomial of degree 2 in j. First at any point $\tau_0 \in \mathbb{H}$ that is not $\Gamma(1)$ equivalent to either i or $e(\frac{1}{3})$, $j(\tau)$ has an expansion $j(\tau) = b_0 + b_1(\tau-\tau_0)+\cdots$ where $b_1 \neq 0$. Therefore, since the function x_N does not ramify anywhere, it has an expansion in the neighborhood of τ_0 in the form $x_N = a_0 + a_1(j-j(\tau_0)) + a_2(j-j(\tau_0))^2+\cdots$ where $a_1 \neq 0$. Therefore,

$$\{x_N,j\} = \frac{6\,(a_1a_3-a_2^2)}{a_1^2} + \frac{24(a_2^3-2a_1a_3a_2+a_1^2a_4)}{a_1^3}(j-j(\tau_0))+\cdots$$

remains finite at this location. In the neighborhood of i, j has an expansion $j = 1728 + b_2(\tau-i)^2+\cdots$, so x_N has an expansion $x_N = a_0 + a_1(j-1728)^{1/2} + a_2(j-1728)^{2/2}+\cdots$ where $a_1 \neq 0$. Therefore,

$$(j-1728)^2\{x_N,j\} = \frac{3}{8} + \frac{3(a_1a_3-a_2^2)}{2a_1^2}(j-1728)+\cdots$$

remains finite also at i. In the neighborhood of $e(\frac{1}{3})$, x_N has an expansion $x_N = a_0 + a_1j^{1/3} + a_2j^{2/3}+\cdots$ where $a_1 \neq 0$. Therefore, we have the expansion

$$j^2\{x_N,j\} = \frac{4}{9} + \frac{2(a_1a_3-a_2^2)}{3a_1^2}j^{4/3}+\cdots,$$

which, when taken with the previous three expansions, shows that $j^2(j-1728)^2\{x_N,j\}$ has possible poles only at ∞. At ∞ we have the expansions $j = q^{-1} + 744 + \cdots$ and $x_N = q^{-1/N}(1 + b_1 q + \cdots)$, so x_N has the expansion $x_N = j^{1/N}(1 + a_1 j^{-1} + a_2 j^{-2} + \cdots)$ in terms of j. From this we obtain the expansion

$$\{x_N, j\} = \left(\tfrac{1}{2} - \tfrac{1}{2N^2}\right) j^{-2} + \cdots \text{ (decending powers of } j),$$

which shows that $j^2(j-1728)^2\{x_N,j\}$ is a polynomial of degree 2 in j with leading coefficient $\frac{1}{2} - \frac{1}{2N^2}$. If $P(j)$ denotes this polynomial, then the expansions of $(j-1728)^2\{x_N,j\}$ and $j^2\{x_N,j\}$ show that $1728^{-2}P(1728) = \frac{3}{8}$ and $1728^{-2}P(0) = \frac{4}{9}$, which uniquely determines the polynomial. □

Proposition 4.9.5. *For $N = 2, 3, 4, 5$, $j(\tau)$, $j(N\tau)$, $\frac{\eta(\tau/N)^{24}}{\eta(N\tau)^{24}}$, $\frac{\eta(\tau)^{24}}{\eta(N\tau)^{24}}$ have the following representations as rational functions of x_N.*

N	$j(\tau)$	$j(N\tau)$	$\frac{\eta(\tau/N)^{24}}{\eta(N\tau)^{24}}$	$\frac{\eta(\tau)^{24}}{\eta(N\tau)^{24}}$
2	$\frac{(x^2+192)^3}{(x^2-64)^2}$	$\frac{(x^2-48)^3}{x^2-64}$	$(x-8)^3$	x^2-64
3	$\frac{x^3(x^3+216)^3}{(x^3-27)^3}$	$\frac{x^3(x^3-24)^3}{x^3-27}$	$(x-3)^8$	$(x^3-27)^2$
4	$\frac{(x^8+224x^4+256)^3}{x^4(x^4-16)^4}$	$\frac{(x^8-16x^4+16)^3}{x^4(x^4-16)}$	$(x-2)^{15}(1+2x^{-1})^3$	$(x^4-16)^3$
5	$\frac{(x^{20}+228x^{15}+494x^{10}-228x^5+1)^3}{x^5(x^{10}-11x^5-1)^5}$	$\frac{(x^{20}-12x^{15}+14x^{10}+12x^5+1)^3}{x^{25}(x^{10}-11x^5-1)}$	$(x-1-x^{-1})^{24}$	$(x^5-11-x^{-5})^4$

Proof. Let us first show that

$$j(\tau) = \frac{A(x_N)^3}{C(x_N)^N} = 1728 + \frac{B(x_N)^2}{C(x_N)^N},$$

where A, B, and C are polynomials of degrees $\frac{4N}{6-N}$, $\frac{6N}{6-N}$, and $\frac{6+N}{6-N}$. Then using the fact that these rational functions should contain only powers of x_N that are divisible by N, it is easy to compute the coefficients of A, B and C by comparing the q-series expansions. At every cusp of $\overline{\mathbb{H}}/\Gamma(N)$ $j(\tau)$ has a pole of order N. Since x has a pole at the cusp ∞, the degree of C should be $\mu/N-1$, where $\mu = [\overline{\Gamma} : \overline{\Gamma}(N)] = 12N/(6-N)$. At every point in $\Gamma(1)(i)/\Gamma(N)$, $j(\tau) - 1728$ has a double zero, hence B has degree $\mu/2$. Similarly, A must have degree $\mu/3$.

We know that $j(N\tau)$ is a function of order μ on $\Gamma(N)$ by Proposition 4.8.2. Therefore,

$$j(N\tau) = \frac{A'(x_N)^3}{C'(x_N)} = 1728 + \frac{B'(x_N)^2}{C'(x_N)},$$

where A', B', and C' are polynomials of degrees $\mu/3$, $\mu/2$, and $\mu - N^2$. C' has a different degree from C because $j(N\tau)$ has a pole of order N^2 at ∞. In this case the order of $j(N\tau)$ is slight more difficult to calculate at the cusps of $\Gamma(N)$ since the order of the pole of $j(N\tau)$ at the cusp $\frac{a}{c}$ of $\Gamma(N)$ is $\gcd(c,N)^2$. We will explain the factorization of C' in the cases of $N = 4, 5$. Two cusps of $\Gamma(5)$ are $\frac{1}{5}$ and $\frac{2}{5}$, and $j(5\tau)$ has a pole of order 25 at each of these. Since $\frac{1}{5}$ is equivalent to ∞, this cusp does not contribute any factor to C', but $\frac{2}{5}$ contributes a factor x^{25}. All of the other cusps of $\Gamma(5)$ have $\gcd(c,5) = 1$, so they contribute simple factors to C'. The cusps of $\Gamma(4)$ are $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{2}{1}, \frac{4}{1}$, which contribute factors to C' of multiplicities $1, 4, 1, 0, 1, 1$.

The identities for the η quotients are left as exercises. □

Proposition 4.9.6. *For $N = 2, 3, 4, 5$, set $y_N(\tau) = x_N(\frac{\tau}{N})^N$.*

1. *$y_N(\tau)$ is a rational function of $x_N(\tau)$ of degree N. Explicitly,*

N	y_N *in terms of* x_N
2	$\frac{(x+24)^2}{x+8}$
3	$\frac{(x+6)^3}{x^2+3x+9}$
4	$\frac{(x+2)^4}{x(x^2+4)}$
5	$\frac{x(x^4+3x^3+4x^2+2x+1)}{x^4-2x^3+4x^2-3x+1}$

2. *$x_N(\tau)$ is expressible in terms of $y_N(\tau)$ and radicals. Specifically, there are constants $A, B, \ldots, C', D'$, depending on N, such that*

$$\left(\frac{Ax_N + B}{Cx_N + D}\right)^N = \frac{A'y_N + B'}{C'y_N + D'}.$$

Proof. (1). Since $x_N(\tau)^N \in M_0^!(\Gamma_1(N))$ and

$$\begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix}^{-1} = \begin{pmatrix} a & \frac{b}{N} \\ Nc & d \end{pmatrix} \in \Gamma_1(N),$$

if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(N)$, it follows that $y_N = x_N(\frac{\tau}{N})^N \in M_0^!(\Gamma(N))$. We claim that y_N has poles only at the cusps $\frac{1}{1}, \frac{1}{2}, \cdots, \frac{1}{N}$ of $\overline{\mathbb{H}}/\Gamma(N)$ at that these are all simple poles. From this claim it follows that $y_N = R_N(x_N)$ where R_N is some rational function of degree N. In order to prove this claim, recall that x_N has a pole only at the cusp $\frac{1}{N}$ (similar to $\frac{1}{0}$) of $\overline{\mathbb{H}}/\Gamma(N)$. Therefore, y_N has a pole at $\frac{a}{c}$ if and only if $\frac{a}{NC}$ is equivalent to $\frac{1}{0}$. Writing $\frac{a}{Nc}$ in lowest terms (assuming $\gcd(a, c) = 1$), we need

$$\left(\frac{a}{\gcd(a, N)}, \frac{Nc}{\gcd(a, N)}\right) \equiv (\pm 1, 0) \bmod N.$$

This implies that $\gcd(a, N)$ divides c, which means that $\gcd(a, N) = 1$, and so $a \equiv \pm 1 \mod N$. Next, to find the order of y_N at the cusp $\frac{1}{k}$, notice that

$$\begin{aligned} y_N\left(\frac{\tau}{k\tau + 1}\right) &= x_N\left(\frac{1}{N}\frac{\tau}{k\tau + 1}\right)^N \\ &= x_N\left(\frac{\frac{\tau}{N}}{Nk\frac{\tau}{N} + 1}\right)^N \\ &= x_N\left(\frac{\tau}{N}\right)^N \\ &= q^{-1/N} + \cdots, \end{aligned}$$

which shows that y_N has a simple pole at $\frac{1}{k}$ as claimed.

(2). Let the constants A, B, C, D be determined by the action of S on x_N, i.e.

$$x_N|_S = \frac{Ax_N + B}{Cx_N + D}.$$

First, we have

$$\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}^{-1} = \begin{pmatrix} d & -\frac{c}{N} \\ -Nb & a \end{pmatrix} \in \Gamma_1(N),$$

if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$. This means that $x_N(\frac{-1}{N\tau})^N$ is invariant under $\Gamma_1(N)$ so $x_N(\frac{-1}{N\tau})^N = F_N(x_N(\tau)^N)$ where F_N is a rational function. We have already shown that

$$x_N\left(\frac{\tau}{N}\right)^N = R_N(x_N(\tau)),$$

where R_N is a rational function of degree N. Replacing τ with $\frac{-N}{\tau}$ in this equation gives

$$x_N\left(\tfrac{-1}{\tau}\right)^N = R_N\left(x_N\left(\tfrac{-N}{\tau}\right)\right),$$

or

$$\left(\frac{Ax_N + B}{Cx_N + D}\right)^N = R_N\left(\frac{Ay_N^{1/N} + B}{Cy_N^{1/N} + D}\right).$$

Replacing τ by $\frac{\tau}{N}$ in $x_N(\frac{-1}{N\tau})^N = F_N(x_N(\tau)^N)$, we derive an equation of the form

$$\left(\frac{Ax_N + B}{Cx_N + D}\right)^N = F_N\left(y_N\right).$$

Comparing these last two equation and keeping in mind that R_N is a rational function of degree N, we see that F_N must be a rational function of degree 1 and the assertion of the proposition holds. □

Proposition 4.9.7.

$$M_k(\Gamma(3)) = \bigoplus_{\substack{a+b=k\\ a,b\geq 0}} \mathbb{C}\frac{\eta(3\tau)^{3a}\eta(\tau/3)^{3b}}{\eta(\tau)^k},$$

$$M_k(\Gamma(4)) = \bigoplus_{\substack{a+b=2k\\ a,b\geq 0}} \mathbb{C}\eta(4\tau)^{2b-2a}\eta(2\tau)^{5a-b}\eta(\tau)^{-2a},$$

$$M_k(\Gamma(5)) = \bigoplus_{\substack{a+b=5k\\ a,b\geq 0}} \mathbb{C}\frac{\eta(5\tau)^{15k}}{\eta(\tau)^{3k}}\mathfrak{k}_{\frac{1}{5},\frac{0}{5}}(5\tau)^a\mathfrak{k}_{\frac{2}{5},\frac{0}{5}}(5\tau)^b.$$

Proof. For $N = 3, 4, 5$, these bases for $M_k(\Gamma(N))$ follow from the observation that there is a $f_N(\tau) \in M^!_{-1}(\Gamma(N))$ with a pole only at ∞. Specifically,

$$f_3(\tau) = \frac{\eta(\tau)}{\eta(3\tau)^3},$$

$$f_4(\tau) = \frac{\eta(2\tau)^2}{\eta(4\tau)^4},$$

$$f_5(\tau) = \frac{\eta(\tau)^3}{\eta(5\tau)^{15}\mathfrak{k}_{\frac{1}{5},\frac{0}{5}}(5\tau)^5},$$

with poles only at ∞ of orders 1, 2 and 5, respectively. It follows that if $f \in M_k(\Gamma(N))$, then $f_N^k f \in M^!_0(\Gamma(N))$ and has a pole at ∞ of order at most k, $2k$, $5k$, respectively, and thus is a polynomial in x_N of at most this degree.

Let us prove the claim about f_5. We first observe that $\frac{\eta(5\tau)^5}{\eta(\tau)} \in M^!_2(\Gamma(5))$ by Proposition 4.8.3 and $\mathfrak{k}_{\frac{1}{5},\frac{0}{5}}(5\tau) \in M^!_{-1}(\Gamma(5))$ by Proposition 4.7.5. Since, by Propositions 4.7.4 and 4.8.1,

$$\begin{aligned}\tfrac{1}{5}\operatorname{ord}_{\frac{a}{c}}\left(\frac{\eta(\tau)^3}{\eta(5\tau)^{15}\mathfrak{k}_{\frac{1}{5},\frac{0}{5}}(5\tau)^5}, \Gamma(5)\right) &= \frac{3}{24}\frac{\gcd(1,c)^2}{1} - \frac{15}{24}\frac{\gcd(5,c)^2}{5} - 5\sum_{i=0}^{4}\binom{\operatorname{frac}\left(\frac{a+ic}{5}\right)}{2}\\ &= \begin{cases} -1 & , \frac{a}{c} \equiv \frac{1}{5} \bmod \Gamma(5)\\ 0 & , \frac{a}{c} \equiv \frac{2}{5} \bmod \Gamma(5)\\ 2 & , \text{otherwise}\end{cases},\end{aligned}$$

the claim for f_5 is verified. □

Exercise 4.9.8. *Obtain and explain the formulas for the η quotients in Proposition 4.9.5.*

Exercise 4.9.9. *Show the following. Sections 4.4 and 4.5 will be helpful, and one should recall the definitions of Γ^2 and Γ^3 in Section 2.11.*

1. *Γ^2 (resp. Γ^3) is the only normal subgroup of $\Gamma(1)$ of index 2 (resp. 3).*

2. $\overline{\Gamma}^2$ *is freely generated by* $\left(\begin{smallmatrix}-1 & -1\\ 1 & 0\end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix}0 & -1\\ 1 & -1\end{smallmatrix}\right)$*, each of order* 3.

3. $\overline{\Gamma}^3$ *is freely generated by* $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1 & -1\\ 2 & -1\end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix}1 & -2\\ 1 & -1\end{smallmatrix}\right)$*, each of order* 2.

4. *The commutator subgroup* $\overline{\Gamma}(1)'$ *of* $\overline{\Gamma}(1)$ *is* $\overline{\Gamma}^2 \cap \overline{\Gamma}^3$*, has genus* 1*, and is freely generated by* $\left(\begin{smallmatrix}1 & 1\\ 1 & 2\end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix}2 & 1\\ 1 & 1\end{smallmatrix}\right)$.

5. $A_0(\Gamma^2) = \mathbb{C}(\sqrt{j-1728})$.

6. $A_0(\Gamma^3) = \mathbb{C}(j^{1/3})$.

7. $A_0(\Gamma^2 \cap \Gamma^3) = \mathbb{C}(j^{1/3}, \sqrt{j-1728})$

4.10 Representations by $x^2 + y^2$

Proposition 4.10.1. *For any integer* $k \geq 1$

1. $\Theta_3(2\tau)^{2k} \in M_k(\Gamma_1(4))$.

2. $\dim M_k(\Gamma_1(4)) = \lfloor \frac{k+2}{2} \rfloor$.

3. $\dim S_k(\Gamma_1(4)) = \max(\lfloor \frac{k-3}{2} \rfloor, 0)$.

Proof. (1). Exercise 2.12.5 gives

$$\Theta_3\left(\frac{a\tau+b}{c\tau+d}\right) = \left(\frac{c}{d}\right) e\left(\frac{d-1}{8}\right) \sqrt{c\tau+d}\; \Theta_3(\tau)$$

for any $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma_\vartheta$ with d odd. Since

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & 2b \\ \frac{c}{2} & d \end{pmatrix} \in \Gamma_\vartheta$$

if $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma_1(4)$, it follows that $\Theta_3(2\tau)^2 \in M_1(\Gamma_1(4))$.

(2). Proposition 4.9.7 gives

$$M_k(\Gamma(4)) = \bigoplus_{\substack{a+b=2k \\ a,b\geq 0}} \mathbb{C}\eta(4\tau)^{2b-2a}\eta(2\tau)^{5a-b}\eta(\tau)^{-2a}.$$

Since $M_k(\Gamma_1(4))$ is the subspace of $M_k(\Gamma(4))$ consisting of forms with expansions in integral powers of q and

$$\eta(4\tau)^{2b-2a}\eta(2\tau)^{5a-b}\eta(\tau)^{-2a} = q^{b/4}(q^4;q^4)_\infty^{2b-2a}(q^2;q^2)_\infty^{5a-b}(q;q)_\infty^{-2a},$$

we must have

$$M_k(\Gamma_1(4)) = \bigoplus_{\substack{a+b=2k \\ a,b\geq 0 \\ b\equiv 0 \bmod 4}} \mathbb{C}\eta(4\tau)^{2b-2a}\eta(2\tau)^{5a-b}\eta(\tau)^{-2a},$$

which implies that $\dim M_k(\Gamma_1(4)) = \lfloor \frac{k+2}{2} \rfloor$.

(3). $M_5(\Gamma_1(4))$ is spanned by the three functions f_i in the following table, where the orders are given at the cusps. Note that the cusps of $\Gamma_1(4)$ are represented by $\frac{1}{0}$, $\frac{0}{1}$, and $\frac{1}{2}$, with widths 1, 4, and 1.

f_i	$\frac{\eta(2\tau)^{50}}{\eta(\tau)^{20}\eta(4\tau)^{20}}$	$\frac{\eta(2\tau)^{26}}{\eta(\tau)^{12}\eta(4\tau)^{4}}$	$\frac{\eta(2\tau)^{2}\eta(4\tau)^{12}}{\eta(\tau)^{4}}$
$\mathrm{ord}_{\frac{1}{0}}(f_i,\Gamma_1(4))$	0	1	2
$\mathrm{ord}_{\frac{0}{1}}(f_i,\Gamma_1(4))$	0	0	0
$\mathrm{ord}_{\frac{1}{2}}(f_i,\Gamma_1(4))$	$\frac{5}{2}$	$\frac{3}{2}$	$\frac{1}{2}$

If $A \neq 0$, then $f_2 + Af_3$ has a zero of lowest possible order at the two cusps $\frac{1}{0}$ and $\frac{1}{2}$. Lets try to determine A so that it also has a simple zero at the cusp $\frac{0}{1}$.

$$\begin{aligned}\frac{\eta(2\tau)^{26}}{\eta(\tau)^{12}\eta(4\tau)^{4}} + A\frac{\eta(2\tau)^{2}\eta(4\tau)^{12}}{\eta(\tau)^{4}}\Big|_{S,5} &= -\frac{iA\eta\left(\frac{\tau}{4}\right)^{12}\eta\left(\frac{\tau}{2}\right)^{2}}{8192\eta(\tau)^{4}} - \frac{i\eta\left(\frac{\tau}{2}\right)^{26}}{512\eta\left(\frac{\tau}{4}\right)^{4}\eta(\tau)^{12}} \\ &= \frac{(A+16)+(64-12A)q^{1/4}+O(q^{2/4})}{8i}.\end{aligned}$$

With $A = -16$, we see that there is a form $f_2 - 16f_3 \in S_5(\Gamma_1(4))$ with simple zeros at the regular cusps and a zero of order $\frac{1}{2}$ at the irregular cusp. Also, $f_2 - 16f_3$ has no zeros on $\mathbb{H}$ by the valence formula. It follows that $S_k(\Gamma_1(4)) = (f_2 - 16f_3)M_{k-5}(\Gamma_1(4))$. □

Proposition 4.10.2.

$$\begin{aligned}\Theta_3(2\tau)^2 &= 2i\mathfrak{e}^1_{\frac{0}{4},\frac{1}{4}} &&= 1 + 4\sum_{\substack{n=1\\2\nmid n}}^{\infty}(-1)^{\frac{n-1}{2}}\frac{q^n}{1-q^n},\\ \Theta_3(2\tau)^4 &= 3\mathfrak{e}^2_{\frac{0}{4},\frac{0}{4}} - 2\mathfrak{e}^2_{\frac{0}{4},\frac{1}{4}} - 1\mathfrak{e}^2_{\frac{0}{4},\frac{2}{4}} &&= 1 + 8\sum_{\substack{n=1\\4\nmid n}}^{\infty}\frac{nq^n}{1-q^n},\\ \Theta_3(2\tau)^6 &= -2i\mathfrak{e}^3_{\frac{0}{4},\frac{1}{4}} - \tfrac{1}{4}\sum_{j=0}^{3}\mathfrak{e}^3_{\frac{1}{4},\frac{j}{4}} &&= 1 + 16\sum_{n=1}^{\infty}\frac{n^2q^n}{1+q^{2n}} - 4\sum_{\substack{n=1\\2\nmid n}}^{\infty}(-1)^{\frac{n-1}{2}}\frac{n^2q^n}{1-q^n},\\ \Theta_3(2\tau)^8 &= \tfrac{15}{2}\mathfrak{e}^4_{\frac{0}{4},\frac{0}{4}} - 1\mathfrak{e}^4_{\frac{0}{4},\frac{1}{4}} - \tfrac{1}{2}\mathfrak{e}^4_{\frac{0}{4},\frac{2}{4}} &&= 1 + \sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n}\cdot\begin{cases}12 & , n \equiv 2 \bmod 4\\ 16 & , \textit{otherwise}\end{cases}.\end{aligned}$$

4.11 Building congruence modular forms from Θ functions

Riemann's Θ function with characteristic $\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right] \in \mathbb{R}^{2\times g}$ is defined as

$$\Theta\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](z|\Omega) = \sum_{n\in\mathbb{Z}^g} e\left(\tfrac{1}{2}(n+\alpha).\Omega.(n+\alpha) + (z+\beta).(n+\alpha)\right),$$

where $z \in \mathbb{C}^g$ and $\Omega \in \mathbb{C}^{g\times g}$ is symmetric with positive definite imaginary part so that the sum is absolutely convergent. The Θ function without characteristics is defined as $\Theta(z|\Omega) = \Theta\left[\begin{smallmatrix}0\\ 0\end{smallmatrix}\right](z|\Omega)$. Since

$$\Theta\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](z|\Omega) = e(\alpha.(z+\beta) + \tfrac{1}{2}\alpha.\Omega.\alpha)\Theta(z+\alpha.\Omega+\beta|\Omega),$$

the function with characteristics is no more general but is slightly more convenient to work with. We will mainly make use of this function in the case $z = 0$ and $\Omega = \tau Q$ where τ is the usual variable in $\mathbb{H}$ and Q is a symmetric positive definite matrix in $\mathbb{Q}^{g\times g}$. In this case set $\Theta_Q\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](\tau) = \Theta\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](\tau Q)$. When the variable z is set to zero, it is commonly omitted from the notation so that $\Theta\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](\Omega) = \Theta\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](0|\Omega)$.

Note that Riemann's Θ function doesn't change much if the characteristics change in sign or by integer vectors, i.e.

$$\Theta\left[\begin{smallmatrix}-\alpha\\-\beta\end{smallmatrix}\right](\Omega) = \Theta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](\Omega),$$
$$\Theta\left[\begin{smallmatrix}\alpha+s\\\beta+t\end{smallmatrix}\right](\Omega) = e(\alpha.t)\Theta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](\Omega), \quad s,t \in \mathbb{Z}^g.$$

Proposition 4.11.1. *We have the following properties of* $\Theta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](z|\Omega)$.

1. *Quasi-periodicity: For any* $s,t \in \mathbb{Z}^g$,

$$\Theta\left[\begin{smallmatrix}\alpha+s\\\beta+t\end{smallmatrix}\right](z|\Omega) = e(\alpha.t)\Theta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](z|\Omega),$$
$$\Theta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](z+s.\Omega+t|\Omega) = e(\alpha.t-\beta.s-\tfrac{1}{2}s.\Omega.s-s.z)\Theta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](z|\Omega).$$

2. *Parity for half-integer characteristics: If* $\alpha,\beta \in \frac{1}{2}\mathbb{Z}^g$, *then*

$$\Theta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](-z|\Omega) = (-1)^{4\alpha.\beta}\Theta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](z|\Omega).$$

3. *For any* $A,B,C,D \in \mathbb{Z}^{g\times g}$ *such that* $G = \left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right)$ *is a symplectic matrix, i.e.*

$$\begin{pmatrix} A & B\\ C & D\end{pmatrix}\begin{pmatrix} 0 & I\\ -I & 0\end{pmatrix}\begin{pmatrix} A^\intercal & C^\intercal\\ B^\intercal & D^\intercal\end{pmatrix} = \begin{pmatrix} 0 & I\\ -I & 0\end{pmatrix},$$

and $AB^\intercal, CD^\intercal$ *have even diagonal, there is an eighth root of unity* $\epsilon(G)$, *depending only on* G *and the choice of the square root such that*

$$\Theta\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right]\left(z.(C\Omega+D)^{-1}|(A\Omega+B)(C\Omega+D)^{-1}\right) = \epsilon\sqrt{\det(C\Omega+D)}e\left(\tfrac{1}{2}z.(C\Omega+D)^{-1}C.z\right)$$
$$\times e(-\tfrac{1}{2}\alpha.AB^\intercal.\alpha - \alpha.BC^\intercal.\beta - \tfrac{1}{2}\beta.CD^\intercal.\beta)\Theta\left[\begin{smallmatrix}\alpha.A+\beta.C\\ \alpha.B+\beta.D\end{smallmatrix}\right](z|\Omega)$$

Proof. Properties (1) and (2) are straightforward. It suffices to show (3) for $\alpha = \beta = \vec{0}$ since the Θ function with characteristics is no more general than the function without. (3) is proven [17, page 168] by showing that the group of symplectic matrices is generated by the three types

$$\begin{pmatrix} A & 0\\ 0 & A^{-\intercal}\end{pmatrix}, A \in \mathrm{GL}_g(\mathbb{Z}) \quad \Theta(z.A^\intercal|A.\Omega.A^\intercal) = \Theta(z|\Omega)$$
$$\begin{pmatrix} I & B\\ 0 & I\end{pmatrix}, B \in \mathbb{Z}^{g\times g} \quad \Theta(z+B|\Omega) = \Theta(z|\Omega) \text{ if } B \text{ has even diagonal}$$
$$\begin{pmatrix} 0 & -I\\ I & 0\end{pmatrix} \quad \Theta(z.\Omega^{-1}|\Omega^{-1}) = \sqrt{\det(-i\Omega)}e(\tfrac{1}{2}z.\Omega^{-1}.z)\Theta(z|\Omega)$$

The transformations for the first two types are straightforward, and the third transformation follows from the g-dimensional Poisson summation formula.

□

We first give the behavior of $\Theta_Q\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](\tau)$ under the generators of $\Gamma(1)$. Proposition 4.11.2 implies that the functions

$$\left\{\Theta_Q\left[\begin{smallmatrix}\alpha\\\beta\end{smallmatrix}\right](\tau) \mid \alpha,\beta \in \tfrac{1}{N}\mathbb{Z}^g \bmod 1,\ \beta.Q^{-1} \in \tfrac{1}{N}\mathbb{Z}^g\right\}$$

are transformed linear among themselves (in weight $g/2$) by $\Gamma(1)$, as well as the same for the functions

$$\left\{\Theta_Q\left[\begin{smallmatrix}\alpha\\0\end{smallmatrix}\right](\tau) \mid \alpha \in \tfrac{1}{N}\mathbb{Z}^g \bmod 1,\ \alpha.Q \in \mathbb{Z}^g\right\}.$$

Thus we obtain a homomorphism from $\Gamma(1)$ to $\mathrm{GL}_k(\mathbb{C})$ for some k. Proposition 4.11.3 shows that the kernel of this homomorphism is a congruence subgroup, and we will work out explicit examples in the case when Q corresponds to the quadratic form x^2+xy+y^2 and other interesting forms as well.

Proposition 4.11.2. *Suppose that $Q \in \mathbb{Z}^{g\times g}$ has even diagonal and that N is a positive integer with $NQ^{-1} \in \mathbb{Z}^{g\times g}$. Then*

$$\Theta_Q\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](\tau+1) = e\left(-\tfrac{1}{2}\alpha.Q.\alpha\right)\Theta_Q\left[\begin{smallmatrix}\alpha\\ \beta+\alpha.Q\end{smallmatrix}\right](\tau),$$
$$\frac{\sqrt{\det Q}}{(-i\tau)^{g/2}}\Theta_Q\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]\left(-\tfrac{1}{\tau}\right) = e(-\alpha.\beta)\sum_{\substack{r\in\mathbb{Z}^g/N\mathbb{Z}^g\\ Q.r\equiv 0 \bmod N}}\Theta_Q\left[\begin{smallmatrix}\frac{r}{N}-\beta.Q^{-1}\\ \alpha.Q\end{smallmatrix}\right](\tau).$$

Proof. The transformation under T is straightforward. The transformation under S follows from the g-dimensional Poisson summation formula. □

Proposition 4.11.3. *Suppose that $Q \in \mathbb{Q}^{g\times g}$ is symmetric and positive definite. If $g = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma(1)$ is such that bQ, cQ^{-1} are integral and abQ, cdQ^{-1} have even diagonals. Then,*

$$\Theta_{MQM^\intercal}\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](\tau) = \Theta_Q\left[\begin{smallmatrix}\alpha.M\\ \beta.M^{-\intercal}\end{smallmatrix}\right](\tau), \quad M \in \mathrm{GL}_g(\mathbb{Z}),$$
$$\Theta_{Q^{-1}}\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]\left(-\tfrac{1}{\tau}\right) = e(-\alpha.\beta)\sqrt{\det(-i\tau Q)}\Theta_Q\left[\begin{smallmatrix}\beta\\ -\alpha\end{smallmatrix}\right](\tau),$$
$$\Theta_Q\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]\left(\tfrac{a\tau+b}{c\tau+d}\right) = e\left(-\tfrac{1}{2}ab\alpha.Q.\alpha - bc\alpha.\beta - \tfrac{1}{2}cd\beta.Q^{-1}.\beta\right)$$
$$\times\, \epsilon_Q(c,d)(c\tau+d)^{g/2}\Theta_Q\left[\begin{smallmatrix}a\alpha+cQ^{-1}.\beta\\ bQ.\alpha+d\beta\end{smallmatrix}\right](\tau),$$

Here the quantity $\epsilon_Q(c,d)$, depending only on c and d, is the eighth root of unity

$$\epsilon_Q(c,d) = \frac{c^{g/2}}{(cd)^{g/2}}\sum_{n\in\mathbb{Z}^g/d\mathbb{Z}^g}\zeta_{2d}^{-cn.Q^{-1}.n}$$
$$= \frac{(ic)^{-g/2}}{\sqrt{\det Q}}\sum_{n\in\mathbb{Z}^g/c\mathbb{Z}^g}\zeta_{2c}^{+dn.Q.n},$$

where it is assumed that cdQ is integral with even diagonal in this last sum (so that it is well-defined).

Proof. The three transformations are a straightforward application of Proposition 4.11.1. The equality for $\epsilon_Q(c,d)$ follows by letting $\tau \to -\frac{d}{c}$ in the third transformation an comparing the first terms of the asmypotics, similarly to Proposition 2.9.1. □

Proposition 4.11.4. *Let all of the hypothesis of Proposition 4.11.3 hold as well as the assumption that cdQ is integral with even diagonal. For an automorphism $\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta_n))$, let x^σ denote $\sigma(x)$ and $x^{\sigma-1}$ denote $\sigma(x)/x$.*

1. *If Q is integral and has even diagonal, then*

$$\epsilon_Q(c,d) = \left(\sqrt{\det icQ}\right)^{\sigma-1}, \text{ where } \sigma : \zeta_c \mapsto \zeta_c^d.$$

2. *If Q is integral and d is odd, then*

$$\epsilon_Q(c,d) = \left(\sqrt{\det icQ}\right)^{\sigma-1}, \text{ where } \sigma : \zeta_{2c} \mapsto \zeta_{2c}^d.$$

3. *If $Q \in \mathbb{Z}^{2\times 2}$ has even diagonal, then*

$$\epsilon_Q(c,d) = \begin{cases}\left(\frac{d}{\det Q}\right) & , \det Q \text{ odd}\\ \left(\frac{2\det Q}{d}\right)\zeta_8^{d-1} & , \det Q \text{ even}\end{cases}.$$

Proof. (1). □

4.12 Representations by x^2+xy+y^2 and other quadratic forms

The quadratic form x^2+xy+y^2 arises from the case $Q = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$. Let us save space notationally by writing $\Theta\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right](\tau) = \Theta\left[\begin{smallmatrix}\alpha/3\\ \beta/3\end{smallmatrix}\right]\left(\left(\begin{smallmatrix} 2\tau & 1\tau \\ 1\tau & 2\tau \end{smallmatrix}\right)\right)$ for the time being. Propositions 4.11.3 and 4.11.4 give

$$\begin{aligned}
\Theta\left[\begin{smallmatrix}0,0\\ 0,0\end{smallmatrix}\right]|_g(\tau) &= \quad \left(\tfrac{d}{3}\right)\Theta\left[\begin{smallmatrix}0,0\\ 0,0\end{smallmatrix}\right](\tau),\\
\Theta\left[\begin{smallmatrix}1,1\\ 0,0\end{smallmatrix}\right]|_g(\tau) &= \zeta_3^{bd}\left(\tfrac{d}{3}\right)\Theta\left[\begin{smallmatrix}1,1\\ 0,0\end{smallmatrix}\right](\tau),\\
\Theta\left[\begin{smallmatrix}0,0\\ 1,2\end{smallmatrix}\right]|_g(\tau) &= \zeta_3^{ac}\left(\tfrac{d}{3}\right)\Theta\left[\begin{smallmatrix}0,0\\ 1,2\end{smallmatrix}\right](\tau),
\end{aligned} \tag{4.12.1}$$

for any $g = \left(\begin{smallmatrix} a & b \\ -3c & d \end{smallmatrix}\right) \in \Gamma_0(3)$. These Θ functions, i.e.

$$\begin{aligned}
\Theta\left[\begin{smallmatrix}0,0\\ 0,0\end{smallmatrix}\right](\tau) &= \sum_{x,y\in\mathbb{Z}^2} q^{x^2+xy+y^2},\\
\Theta\left[\begin{smallmatrix}1,1\\ 0,0\end{smallmatrix}\right](\tau) &= \sum_{x,y\in\frac{1}{3}+\mathbb{Z}^2} q^{x^2+xy+y^2},\\
\Theta\left[\begin{smallmatrix}0,0\\ 1,2\end{smallmatrix}\right](\tau) &= \sum_{x,y\in\mathbb{Z}^2} q^{x^2+xy+y^2}\zeta_3^{x-y},
\end{aligned}$$

are the three functions introduced in [4].

Proposition 4.12.1. *For any integer $k \geq 1$*

1. $\Theta\left[\begin{smallmatrix}0,0\\ 0,0\end{smallmatrix}\right](\tau)^k \in M_k(\Gamma_1(3))$.
2. $\dim M_k(\Gamma_1(3)) = \lfloor \frac{k+3}{3} \rfloor$.
3. $\dim S_k(\Gamma_1(3)) = \max(\lfloor \frac{k-3}{3} \rfloor, 0)$.

Proof. The proof of these results is similar to Proposition 4.10.1. The form in $S_6(\Gamma_1(3))$ with a simple pole at $\frac{1}{0}$ (width 1) and a simple pole at $\frac{0}{1}$ (width 3) is $\eta(\tau)^6\eta(3\tau)^6$, by Proposition 4.8.3. □

Proposition 4.12.2.

$$\Theta\left[\begin{smallmatrix}0,0\\ 0,0\end{smallmatrix}\right](\tau)^3 = \Theta\left[\begin{smallmatrix}1,1\\ 0,0\end{smallmatrix}\right](\tau)^3 + \Theta\left[\begin{smallmatrix}0,0\\ 1,2\end{smallmatrix}\right](\tau)^3$$

Proof. By (4.12.1), the three functions $\Theta\left[\begin{smallmatrix}0,0\\ 0,0\end{smallmatrix}\right](\tau)^3$, $\Theta\left[\begin{smallmatrix}1,1\\ 0,0\end{smallmatrix}\right](\tau)^3$, $\Theta\left[\begin{smallmatrix}0,0\\ 1,2\end{smallmatrix}\right](\tau)^3$ are all in $M_3(\Gamma_1(3))$. Since this space has dimension 2 by Proposition 4.12.1, there must be a nontrivial linear relation between these functions. This is easily found using the first three terms of the q-series expansions. □

Proposition 4.12.3. *Let χ be the odd character modulo 6. Then,*

$$\Theta\left[\begin{smallmatrix}0,0\\ 0,0\end{smallmatrix}\right](\tau) = 2\sqrt{-3}\mathfrak{e}_{\frac{0}{3},\frac{1}{3}}(\tau) = 1 + 6\sum_{n=1}^{\infty}\frac{\chi(n)q^n}{1-q^n}.$$

This concludes the study of the quadratic form $Q = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$. We will now focus unimodular lattices, and in particular on the E_8 lattice. The E_8 lattice is defined as

$$E_8 = \{(x_1, \ldots, x_2) \in \mathbb{Z}^8 \cup (\mathbb{Z}+\tfrac{1}{2})^8 \mid x_1 + \cdots + x_8 \in 2\mathbb{Z}\}.$$

A basis for the E_8 lattice can be given as the columns of the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & -1 & -1/2 \\ 0 & 0 & 0 & 0 & 1 & -1 & -1 & 1/2 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 1/2 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 1/2 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 1/2 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 1/2 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1/2 \end{pmatrix}.$$

Note that $\det A = -1$. The associated quadratic form is

$$Q_8 = A^\intercal A = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & 0 & -1 \\ 0 & 0 & 0 & 0 & -1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 2 \end{pmatrix}.$$

Proposition 4.12.4. *Let $Q \in \mathbb{Z}^{g\times g}$ be a symmetric positive definite matrix with even diagonal and* $\det Q = 1$.

1. $g \equiv 0 \bmod 8$
2. $\Theta_Q(\tau) \in M_{g/2}(\Gamma(1))$.

Proof. (1). By Proposition 4.11.3 with $\alpha = \beta = 0$ and $M = Q^{-1}$, we have $\Theta_{Q^{-1}}(-\frac{1}{\tau}) = \Theta_Q(-\frac{1}{\tau}) = (i\tau)^{g/2}\Theta_Q(\tau)$ and $\Theta_Q(\tau+1) = \Theta_Q(\tau)$. Therefore,

$$\Theta_Q(\tau) = (i/\tau)^{g/2}\Theta_Q(1-\tfrac{1}{\tau}).$$

Iterating this three times gives $\Theta_Q(\tau) = (i/\tau)^{g/2}(i\tau/(\tau-1))^{g/2}(i(1-\tau))^{g/2}\Theta_Q(\tau)$. Since $\Theta_Q(\tau)$ clearly does not vanish identically, this implies that

$$\left(\frac{i}{\tau}\right)^{g/2}\left(\frac{i\tau}{\tau-1}\right)^{g/2}(i(1-\tau))^{g/2} = 1.$$

Setting $\tau = e(\frac{1}{3})$ and simplifying, we find that the left hand side is ζ_8^g. Thus, $g \equiv 0 \bmod 8$.

(2). This is now clear since $\Theta_Q(\tau) = \sum_{n\in\mathbb{Z}^g} q^{\frac{1}{2}n.Q.n}$ has a q-series exansion in non-negative powers of q. □

We can derive from this proposition the fact that $\Theta_{Q_8}\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right](\tau) \in M_4(\Gamma(1))$, and so

$$\begin{aligned} E_4(\tau) &= \Theta_{Q_8}(\tau) \\ &= \sum_{x\in\mathbb{Z}^8} q^{x_1^2+x_2^2+x_3^2+x_4^2+x_5^2+x_6^2+x_7^2+x_8^2-x_1x_2-x_2x_3-x_3x_4-x_4x_5-x_5x_6-x_5x_7-x_6x_8} \end{aligned}$$

4.13 Subgroups up to index 7: non-congruence examples

Recall that if a subgroup Γ of $\Gamma(1)$ contains some $\Gamma(N)$ then it is called a congruence subgroup. In this section we are concerned with the elements of $\Gamma(1)$ only up to their action on $\mathbb{H}$, so we suppress the bars over all of the subgroups of $\Gamma(1)$. For any subgroup Γ and cusp $\alpha \in \mathbb{Q}$, let $h_\Gamma(\alpha)$ denote the width of the cusp α for Γ. Also, let Γ^c, called the congruence closure of Γ, be the smallest congruence subgroup of $\Gamma(1)$ that contains Γ. Clearly, Γ is a congruence subgroup if and only if $\Gamma = \Gamma^c$. The following proposition relates Γ, Γ^c and level(Γ).

Proposition 4.13.1. *Suppose* $[\Gamma(1) : \Gamma] < \infty$. *Set* $N = \text{level}(\Gamma)$ *and let* $\phi : \Gamma(1) \to \text{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ *be the map that reduces matrices modulo* N. *Let* ϕ^{-1} *take subgroups of* $\text{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ *to the corresponding groups between* $\Gamma(1)$ *and* $\Gamma(N)$. *Then,* $\Gamma^c = \phi^{-1}(\phi(\Gamma))$.

Remark 4.13.2. *There are much faster ways for testing if* Γ *is a congruence subgroup and computing the congruence closure using presentations for* $\text{PSL}_2(\mathbb{Z}/N\mathbb{Z})$. *See [20]. The main result for odd* N *is:* Γ *is congruence if and only if* $(R^2T^{\frac{N-1}{2}})^3$ *acts trivially on the cosets* $\Gamma(1)\backslash\Gamma$. *Recall that* $R = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ *and* $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

Proposition 4.13.3. *Suppose* Γ *is a congruence subgroup of level* N. *Then, if* $\Gamma \geq \Gamma(l)$ *then* $N \mid l$.

Proof. Exercise. □

The following Proposition, due to Wohlfart, says that the level of a congruence subgroup Γ is the smallest l satisfying $\Gamma \geq \Gamma(l)$.

Proposition 4.13.4. *Suppose* Γ *is a congruence subgroup of level* N. *Then,* $\Gamma \geq \Gamma(N)$ *and*

$$N = \text{lcm}(h_\Gamma(0), h_\Gamma(1), h_\Gamma(\infty)).$$

Proof. Set $m = \text{lcm}(h(0), h(1), h(\infty))$. Since the hypothesis is that Γ is a congruence subgroup, let l be such that $\Gamma \geq \Gamma(l)$. Since $\Gamma \geq \Gamma(l)$ and the width of every cusp for $\Gamma(l)$ is l, l must be a multiple of each of these three widths $h(0)$, $h(1)$, $h(\infty)$, and so $m \mid l$. Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv I \bmod m$ be any matrix in $\Gamma(m)$. We must show that $M \in \Gamma$. By multiplying by powers of $\left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ m & 1 \end{smallmatrix}\right)$, which are in both Γ and $\Gamma(m)$, we may make some simplifying assumptions on M.

- $\underline{\gcd(d, l) = 1}$. Note that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)^{n_1} = \left(\begin{smallmatrix} a & b+amn_1 \\ c & d+cmn_1 \end{smallmatrix}\right)$. Since $\gcd(d, mc) = 1$ by the assumption $M \in \Gamma(m)$, there is an integer n_1 so that $\gcd(d + cmn_1, l) = 1$ (for example, since $d + cm\mathbb{Z}$ contains infinitely many primes).

- $\underline{b \equiv 0 \bmod l}$. Note that $\left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)^{n_2}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a+cmn_2 & b+dmn_2 \\ c & d \end{smallmatrix}\right)$. Since $m \mid b$ and $\gcd(d, l) = 1$, there is a n_2 such that $b + dmn_2 \equiv 0 \bmod l$.

- $\underline{c \equiv 0 \bmod l}$. Note that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ m & 1 \end{smallmatrix}\right)^{n_3} = \left(\begin{smallmatrix} a+bmn_3 & b \\ c+dmn_3 & d \end{smallmatrix}\right)$. Since $m \mid c$ and $\gcd(d, l) = 1$, there is a n_3 such that $c + dmn_3 \equiv 0 \bmod l$.

Therefore, we may assume $M \equiv \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \bmod l$ where $ad \equiv 1 \bmod l$. However, modulo l, M is congruent to M', where $M' = \left(\begin{smallmatrix} a & ad-1 \\ 1-ad & d(2-ad) \end{smallmatrix}\right)$. Therefore, there is a matrix $L \in \Gamma(l) \leq \Gamma$ with $M = LM'$. M' can be written as the product of three matrices with trace 2 as

$$M' = \begin{pmatrix} 1 & 0 \\ d-1 & 1 \end{pmatrix}\begin{pmatrix} a & 1-a \\ a-1 & 2-a \end{pmatrix}\begin{pmatrix} 1 & 1-d \\ 0 & 1 \end{pmatrix}.$$

The last matrix in this product fixes ∞, and $h(\infty)|1 - d$ because $d \equiv 1 \bmod m$. This implies that the last matrix is in Γ. Dido for the second matrix $\left(= \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1-a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)^{-1}\right)$ and the cusp 1. Dido for the first matrix and the cusp 0.

Finally, let N denote the level of Γ, that is, $\mathrm{lcm}(\{h_\Gamma(\alpha)\}_{\alpha\in\overline{\mathbb{Q}}})$. We have just seen that $\Gamma \geq \Gamma(m)$. However, we have $m|N$ by the definition of m, and $N|m$ by Proposition 4.13.3. Therefore, $N = m$.

□

The number of subgroups of $\overline{\Gamma}$ and size of the conjugacy classes as computed in [18] are as follows.

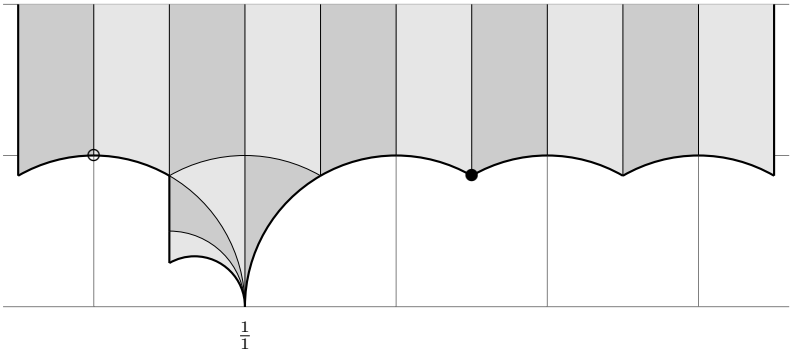
index	1	2	3	4	5	6	7
No. of subgroups	1	1	4	8	5	22	42
No. of conjugacy classes	1	1	2	2	1	8	6

All of the subgroups Γ of $\Gamma(1)$ with index ≤ 7 except $\Gamma^2 \cap \Gamma^3$ have genus 0. It turns out that if we assume the existence of a Hauptmodul, x_Γ, for each of these genus 0 subgroups Γ, we can find x_Γ as an explicit algebraic function of j. Let us illustrate with, for example, the conjugacy class of subgroups of index 7 in Table 4.1 with $(\epsilon_\infty, \epsilon_2, \epsilon_3) = (2, 1, 1)$ and cusp widths $5 + 2$. We first fix x by putting its pole at the cusp with width 5 (and setting its residue to be 1) and its zero at the cusp with width 0. Since there is one elliptic point of each order for this subgroup, we have an equation of the form

$$j = \frac{(x + a_1)(x^2 + a_2x + a_3)^3}{x^2} = 1728 + \frac{(x + b_1)(x^3 + b_2x^2 + b_3x + b_4)^2}{x^2}.$$

It is possible to determine the constants a_i and b_i algebraically by equating coefficients on powers of x. It turns out that there are five distinct sets of solutions, corresponding to the five conjugate subgroups that have a cusp width of 5 at ∞. In the table, x has been rescaled so that the defining relation with j is rational.

Note that the groups of index 7 in the last four entries in Table 4.1 are not congruence subgroups because the least common multiples of the cusp widths are 6, 10 and 12, respectively, and none of the indexes $[\Gamma(1) : \Gamma(6)] = 72$, $[\Gamma(1) : \Gamma(10)] = 360$, and $[\Gamma(1) : \Gamma(12)] = 576$ is divisible by 7. Let Γ^{52} denote the subgroup with cusp widths $5 + 2$ and fundamental domain



.

Note that once the locations of the two elliptic points are specified, there is only one way to pair the edges while obeying the cusp widths of 5 and 2, so this defines a subgroup of $\Gamma(1)$. Since Table 4.1 gives the Hauptmodul x as a explicit algebraic function of j, it is a simple matter to obtain the q-series expansion of x from that of j. For the group Γ^{52}, we have

$$x(\tau) = 7 \cdot 7^{2/5}q^{-1/5} - 28 + \frac{278}{7^{2/5}}q^{1/5} - \frac{2540}{7 \cdot 7^{4/5}}q^{2/5} + \frac{116185}{343 \cdot 7^{1/5}}q^{3/5} + \frac{2924644}{2401 \cdot 7^{3/5}}q^{4/5} + \cdots,$$
$$x(1 - 1/\tau) = \frac{512000}{343\sqrt{-7}}q^{1/2} + \frac{69632000}{117649}q + \frac{488364032000}{40353607\sqrt{-7}}q^{3/2} + \frac{340869677056000}{96889010407}q^2 + \cdots.$$

The function $x(\tau)$ is a Hauptmodul for Γ^{52}. The Hauptmoduln for the other six groups in this conjugacy class are $x(1 - 1/(\tau + i))$, and $x(\tau + j)$ for $i = 0, 1$ and $j = 1, 2, 3, 4$.

μ	$(\epsilon_\infty, \epsilon_2, \epsilon_3)$	cusps	Hauptmoduln	conj.
2	$(1,0,2)$	2	$j = x^2 + 1728$	1
3	$(1,3,0)$	3	$j = x^3$	1
3	$(2,1,0)$	$2+1$	$j = \frac{(x+16)^3}{x}$	3
4	$(1,2,1)$	4	$j = x(x+1)^3$	4
4	$(2,0,1)$	$3+1$	$j = \frac{(x+27)(x+3)^3}{x}$	4
5	$(1,1,2)$	5	$j = x^3(x^2 - 5x + 40)$	5
6	$(1,0,0)$	6	genus 1	1
6	$(1,0,3)$	6	$j = -27x^3(x^3 + 16)$	2
6	$(1,4,0)$	6	$j = 27(x^2 + 4)^3$	3
6	$(2,2,0)$	$3+3$	$j = \frac{x^3(x+12)^3}{(x+9)^3}$	3
6	$(2,2,0)$	$4+2$	$j = \frac{x^3(x+8)^3}{(x+4)^2}$	3
6	$(2,2,0)$	$5+1$	$j = \frac{(x^2+10x+5)^3}{x}$	6
6	$(3,0,0)$	$2+2+2$	$j = \frac{(x^2+192)^3}{(x^2-64)^2}$	1
6	$(3,0,0)$	$4+1+1$	$j = \frac{(x^2+48)^3}{x^2+64}$	3
7	$(1,3,1)$	7	$j = x(x^2 + \frac{7+7\sqrt{-7}}{2}x + \frac{-35+7\sqrt{-7}}{2})^3$	7
7	$(1,3,1)$	7	$j = x(x^2 + \frac{7-7\sqrt{-7}}{2}x + \frac{-35-7\sqrt{-7}}{2})^3$	7
7	$(2,1,1)$	$6+1$	$j = \frac{384(747-1763\sqrt{-3})(x+9)(x^2+(6+\sqrt{-3})x+\frac{1}{2}(3+\sqrt{-3}))^3}{823543x}$	7
7	$(2,1,1)$	$6+1$	$j = \frac{384(747+1763\sqrt{-3})(x+9)(x^2+(6-\sqrt{-3})x+\frac{1}{2}(3-\sqrt{-3}))^3}{823543x}$	7
7	$(2,1,1)$	$5+2$	$j = \frac{(x+125)(x^2+5x-1280)^3}{823543x^2}$	7
7	$(2,1,1)$	$4+3$	$j = \frac{(x+432)(x^2+80x-3888)^3}{-823543x^3}$	7

Table 4.1: The subgroups with $[\overline{\Gamma}(1) : \overline{\Gamma}] \leq 7$ and their Hauptmoduln

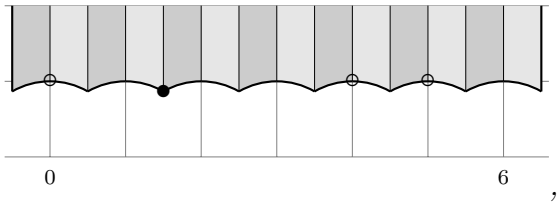
As Γ^{52} is non-congruence and has prime index in $\Gamma(1)$, its congruence closure must be the full modular group $\Gamma(1)$. Since x is clearly not invariant under $\Gamma(1)$, we have the q-series expansion of a modular function that is not invariant under $\Gamma(N)$ for any N (so in particular, it cannot be written in terms of the usual q-products). There are a few things to notice about the q-series coefficients of the function x:

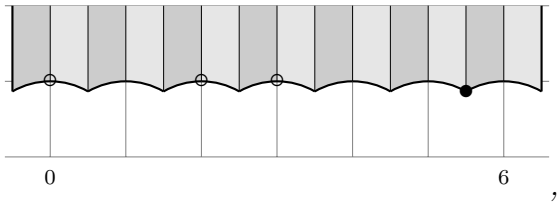
- The coefficients appear to have unbounded denominators. (The q-series expansions of the Hauptmoduln for the congruence subgroups in Table 4.1 all have bounded denominators.)
- Any Galois extension of $\mathbb{Q}$ containing the q-series coefficients of x and its six conjugate is not an Abelian extension.

Exercise 4.13.5. *Set $\alpha = \frac{-1+\sqrt{-7}}{2}$. Recall from Table 4.1 that supposedly there are 14 congruence subgroups of index 7 with $(\epsilon_\infty, \epsilon_2, \epsilon_3) = (1,3,1)$, whose Hauptmoduln x satisfy*

$$j = x(x^2 - \alpha x - 21 - 7\alpha)^3 \text{ or } \bar{\alpha} \text{ in place of } \alpha.$$

Since these are congruence subgroups, we should be able to solve for x in terms of q-products. Let us first fix two of these groups, Γ^7 and $\tilde{\Gamma}^7$, by the fundamental domains



,


,

respectively. The edge pairings for each of these fundamental domains are uniquely determined by the locations of the elliptic points (shown with dots).

1. *Show that* Γ^7 *and* $\tilde{\Gamma}^7$ *are congruence subgroups of level* 7 *by means of Proposition 4.13.1 via the following steps.*

   (a) *Show that* Γ^7 *is freely generated by* $S, T^4ST^{-4}, T^5ST^{-5}, T^2ST^{-1}$
   Show that $\tilde{\Gamma}^7$ *is freely generated by* $S, T^2ST^{-2}, T^3ST^{-3}, T^6ST^{-5}$.

   (b) *Let* G *and* $\tilde{G}$ *be the subgroups of* $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z}) \simeq \overline{\Gamma}(1)/\overline{\Gamma}(7)$ *generated respectively by the two sets of generators in (a) modulo* 7. *Show that* G *and* $\tilde{G}$ *have order* 24 *hence index* 7 *in* $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$.

2. *For* $j = 1, 2, 3$, *let* $u_j(\tau) = \pm\mathfrak{k}_{j/7,0}(7\tau)\eta(7\tau)^3/\eta(\tau)$, *with the signs fixed by*

$$\begin{aligned} u_1(\tau) &= -q^{17/42}(q;q^7)_\infty(q^6;q^7)_\infty(q^7;q^7)_\infty/(q;q)_\infty, \\ u_2(\tau) &= +q^{5/42}(q^2;q^7)_\infty(q^5;q^7)_\infty(q^7;q^7)_\infty/(q;q)_\infty, \\ u_3(\tau) &= +q^{-1/42}(q^3;q^7)_\infty(q^4;q^7)_\infty(q^7;q^7)_\infty/(q;q)_\infty. \end{aligned}$$

   Show that $u_1\eta(\tau)^4, u_2\eta(\tau)^4, u_3\eta(\tau)^4 \in S_2(\Gamma(7))$. *This is in fact a basis by Theorem 4.2.3.*

3. *Show that*

$$\begin{pmatrix} u_1\eta^4 \\ u_2\eta^4 \\ u_3\eta^4 \end{pmatrix}|_T = \begin{pmatrix} \zeta_7^4 & 0 & 0 \\ 0 & \zeta_7^2 & 0 \\ 0 & 0 & \zeta_7^1 \end{pmatrix} \begin{pmatrix} u_1\eta^4 \\ u_2\eta^4 \\ u_3\eta^4 \end{pmatrix},$$

$$\begin{pmatrix} u_1\eta^4 \\ u_2\eta^4 \\ u_3\eta^4 \end{pmatrix}|_S = \frac{1}{\sqrt{-7}} \begin{pmatrix} \zeta_7^6 - \zeta_7^1 & \zeta_7^5 - \zeta_7^2 & \zeta_7^3 - \zeta_7^4 \\ \zeta_7^5 - \zeta_7^2 & \zeta_7^3 - \zeta_7^4 & \zeta_7^6 - \zeta_7^1 \\ \zeta_7^3 - \zeta_7^4 & \zeta_7^6 - \zeta_7^1 & \zeta_7^5 - \zeta_7^2 \end{pmatrix} \begin{pmatrix} u_1\eta^4 \\ u_2\eta^4 \\ u_3\eta^4 \end{pmatrix}.$$

4. *Let* $x_i = \zeta_7^{3i}u_1^2 + \zeta_7^{5i}u_2^2 + \zeta_7^{6i}u_3^2 + \alpha(\zeta_7^i u_1u_3 + \zeta_7^{2i}u_2u_3 + \zeta_7^{4i}u_1u_2)$. *Show that* x_0 *is a Hauptmodul for* $\Gamma^7 \cap \Gamma^3$, *which is a subgroup of index* 21 *with* $(\epsilon_\infty, \epsilon_2, \epsilon_3) = (1, 9, 1)$. *Hint: show that* $x_0\eta^8 \in S_4(\Gamma^7)$. *Recall also that* $\eta^8 \in S_4(\Gamma^3)$.

5. *Show that* x_0^3 *is a Hauptmodul for* Γ^7 *and that the* x_i^3 *are Hauptmoduln for the conjugates of* Γ^7.

Chapter 5

Hecke Operators

5.1 Motivating Examples

Example 5.1.1. *Set*

$$\begin{aligned}
\delta(\tau) &= q(q;q)_\infty^2 (q^{11};q^{11})_\infty^2 = \sum_{n=1}^{\infty} a_n q^n, \\
\theta(\tau) &= \sum_{n,m} q^{m^2+mn+3n^2}, \\
x(\tau) &= \frac{\delta(\tau)}{\theta(\tau)^2}, \\
y(\tau) &= \frac{q\frac{d}{dq}\log x(\tau)}{\theta(\tau)^2}.
\end{aligned}$$

The functions x and y generate $A_0(\Gamma_0(11))$ and satisfy the relation [5],

$$y^2 = 1 - 20x + 56x^2 - 44x^3.$$

Proposition 5.1.2. *With a_n defined as in Example 5.1.1,*

1. *If $\gcd(m,n) = 1$,*
$$a_{mn} = a_m a_n.$$

2. *Recursion on prime powers:*
$$a_{p^{n+1}} = a_{p^n} a_p - \begin{cases} 0 & , p = 11 \\ p a_{p^{n-1}} & , p \neq 11 \end{cases}$$

3. *Relation to number of $\mathbb{F}_p$-points on the elliptic curve $y^2 = 1 - 20x + 56x^2 - 44x^3$:*
$$a_p = -\sum_{x=0}^{p-1} \left(\frac{1 - 20x + 56x^2 - 44x^3}{p} \right), \; p \neq 11.$$

Example 5.1.3. *Set*

$$\begin{aligned} z &= q\frac{d}{dq}\log\frac{\eta(17\tau)^3}{\eta(\tau)^3}, \\ \frac{1-x}{2x} &= \frac{1}{4\eta(\tau)^2\eta(17\tau)^2}\left(\sum_{n,m}(e^{\pi im}-e^{\pi in})q^{\frac{1}{4}n^2+\frac{17}{4}m^2}\right)^2, \\ y &= \frac{2}{z}q\frac{d}{dq}\log x, \\ xz &= \sum_{n=1}^{\infty}a_nq^n. \end{aligned}$$

The functions x and y generate $A_0(\Gamma_0(17))$ and satisfy the relation

$$y^2 = 1-16x-66x^2-48x^3-127x^4.$$

Proposition 5.1.4. *With a_n defined as in Example 5.1.3,*

1. *If $\gcd(m,n)=1$,*
$$a_{mn} = a_ma_n.$$
2. *Recursion on prime powers:*
$$a_{p^{n+1}} = a_{p^n}a_p - \begin{cases} 0 & , p=17 \\ pa_{p^{n-1}} & , p\neq 17 \end{cases}$$
3. *Relation to number of $\mathbb{F}_p$-points on the elliptic curve:*
$$a_p = -\left(\frac{-127}{p}\right) - \sum_{x=0}^{p-1}\left(\frac{1-16x-66x^2-48x^3-127x^4}{p}\right),\ p\neq 2,17.$$

Example 5.1.5. *Set*

$$x = q^{1/2}\frac{(q^5;q^5)_\infty^3}{(q;q)_\infty^3}, \quad y = q\frac{(q,q^4;q^5)_\infty^5}{(q^2,q^3;q^5)_\infty^5}.$$

The function field of

$$\Gamma = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \Big| \begin{array}{l} c\equiv 0 \mod 5 \\ d\equiv 1 \mod 5 \\ b+c\equiv 0 \mod 2 \end{array}\}$$

is generated by x and y and there is the relation

$$\frac{1}{x^2} = \frac{1}{y} - 11 - y.$$

The coefficients of

$$q^{1/2}(q;q)_\infty^2(q^5;q^5)_\infty^2 = \sum_{n=1}^{\infty}a_nq^{n/2}$$

have nice multiplicative properties and satsify

$$a_p = -\sum_{y=1}^{p-1}\left(\frac{y^{-1}_{\bmod p}-11-y}{p}\right),\ p\neq 2.$$

Example 5.1.6. *Set*

$$x = j(\tau)^{1/3}, \quad y = \sqrt{j(\tau) - 1728}.$$

The function field of $\Gamma(1)' = \Gamma^2 \cap \Gamma^3$ *is generated by* x *and* y *and there is the obvious relation*

$$y^2 = x^3 - 1728.$$

The coefficients of

$$q^{1/6}(q;q)_\infty^4 = \sum_{n=1}^{\infty} a_n q^{n/6}$$

have nice multiplicative properties and satsify

$$a_p = -\sum_{x=0}^{p-1} \left(\frac{x^3 - 1728}{p} \right), \; p \neq 2, 3.$$

Since the elliptic curve has complex multiplication, there is the simpler formula

$$a_p = \begin{cases} 0 & , \; p \equiv 2 \bmod 3 \\ -2a & , \; p \equiv 1 \bmod 3, \quad p = a^2 + 3b^2, \quad a \equiv 1 \bmod 3 \end{cases}.$$

Can this formula for a_p *be obtained from*

$$(q,q)_\infty = \sum_n (-1)^n q^{n(3n-1)/2}$$
$$(q,q)_\infty^3 = \sum_m (m + \tfrac{1}{2})(-1)^m q^{m(m+1)/2}$$

?

5.2 Definition of the Hecke operators

Recall the slash operator $|_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right),k}$ in weight k,

$$f|_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right),k}(\tau) = \frac{(ad-bc)^{k-1}}{(c\tau + d)^k} f\left(\frac{a\tau + b}{c\tau + d} \right).$$

Let

$$\Delta_n = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2} \mid ad - bc = n \}$$

be the set of matrices of determinant n. We let $\Delta_1 \backslash \Delta_n$ denote the equivalence classes of Δ_n under the action of the modular group (by multiplication on the left. It is not hard to see that

$$\Delta_1 \backslash \Delta_n = \{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \mid \alpha\delta = n, \quad 0 \leq \beta < \delta \}.$$

It is also useful to consider the set of primitive matrices of determinant n.

$$\Delta_n^* = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2} \mid ad - bc = n, \quad \gcd(a,b,c,d) = 1 \}.$$

$$\Delta_1 \backslash \Delta_n^* = \{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \mid \alpha\delta = n, \quad 0 \leq \beta < \delta, \quad \gcd(\alpha, \beta, \delta) = 1 \}.$$

Proposition 5.2.1. *Set* $g = \left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

1. $\Gamma_0(n) = \Gamma(1) \cap g^{-1}\Gamma(1)g$.
2. *Let* $\Gamma(1) = \cup_i \Gamma_0(n)\gamma_i$ *be a coset decomposition. Then*
$$\Delta_n^* = \Gamma(1)g\Gamma(1) = \cup_i \Gamma(1)g\gamma_i.$$
3. $\Gamma(1)$ *acts transitively (by right multiplication) on the cosets* $\Delta_1\backslash\Delta_n^*$.
4. *The action of* $\Gamma(1)$ *(by right multiplication) on the cosets* $\Delta_1\backslash\Delta_n$ *is transivie within matrices of the same content.*

If $f \in A_k(\Gamma(1))$, the Hecke operator T_n is defined as
$$T_n(f) = \sum_{g \in D_1\backslash D_n} f|_{g,k}.$$

Proposition 5.2.2. *If* $f = \sum_m a_m q^m \in A_k(\Gamma(1))$, *then*
$$T_n(f) = \sum_m q^m \sum_{d|\gcd(m,n)} d^{k-1} a_{mn/d^2},$$
and for prime p,
$$T_p(f) = \sum_m (a_{mp} + p^{k-1}a_{m/p})q^m.$$

Proof. □

Proposition 5.2.3. *If* $f \in A_k(\Gamma(1))$, *then*

1. $T_m(T_n(f)) = T_{mn}(f)$ *for* $\gcd(m,n) = 1$.
2. $T_p(T_{p^r}(f)) = T_{p^{r+1}}(f) + p^{k-1}T_{p^{r-1}}(f)$.
3. $T_m(T_n(f)) = \sum_{d|\gcd(m,n)} d^{k-1}T_{mn/d^2}(f)$.

Proof. □

5.3 Eigenforms

5.4 Newforms

Chapter 6

Modular Forms mod p

6.1 The structure of modular forms on $\mathrm{SL}_2(\mathbb{Z})$ mod p

6.2 The congruences for $p(n)$ mod 5,7,11 are the Unique Ramanujan Congruences

6.3 $24n \equiv 1 \mod 5^a 7^b 11^c$ implies $p(n) \equiv 0 \mod 5^a 7^{\lfloor \frac{b}{2} \rfloor + 1} 11^c$

Chapter 7

Modular Equations and Singular Values

7.1 Modular equations for j

Proposition 7.1.1 (Classical modular equation)**.** *For any integer $n \geq 2$ there is a polynomial $\Phi_n(X, Y)$ of degree $\phi(n) = n\prod_{p|n}(1 + 1/p)$ in X and Y such that:*

1. *$\Phi_n(X, Y)$ is irreducible.*
2. *$\Phi_n(X, Y)$ is symmetric in X and Y.*
3. *$\Phi_n(X, X)$ has leading coefficient ± 1 if n is not a square.*
4. *The zeros of $\Phi_n(X, j(\tau))$ occur exactly at the points*

$$X = j\left(\frac{\alpha\tau + \beta}{\delta}\right), \quad \begin{array}{l} \alpha\delta = n \\ 0 \leq \beta < \delta \\ \gcd(\alpha, \beta, \delta) = 1 \end{array}.$$

Proof. ... □

Proposition 7.1.2 (Canonical modular equation)**.** *For any integer $n \geq 2$ there is an irreducible polynomial $\Psi_n(X, Y)$ of degree $\psi(n)$ in X and Y such that $\Phi_n(f_n(\tau), j(\tau)) = 0$, where*

$$f_n(\tau) = \left(\frac{\eta(n\tau)}{\eta(\tau)}\right)^{\frac{24}{(24,n-1)}}.$$

7.2 Modular equations for the Weber functions

Weber's functions are defined as

$$\begin{aligned}
\gamma_3(\tau) &= \sqrt{j(\tau) - 1728} = \frac{E_6(\tau)}{\eta(\tau)^{12}} \\
\gamma_2(\tau) &= (j(\tau))^{1/3} = \frac{E_4(\tau)}{\eta(\tau)^8} \\
\mathfrak{f}(\tau) &= \zeta_{48}^{-1} \frac{\eta\left(\frac{\tau+1}{2}\right)}{\eta(\tau)} \\
\mathfrak{f}_1(\tau) &= \frac{\eta\left(\frac{\tau}{2}\right)}{\eta(\tau)} \\
\mathfrak{f}_2(\tau) &= \sqrt{2} \frac{\eta\left(2\tau\right)}{\eta(\tau)}
\end{aligned}$$

Proposition 7.2.1.

$$\begin{aligned}
\gamma_3(\tau) &\in M_0^!(\Gamma(2)), \\
\gamma_2(\tau) &\in M_0^!(\Gamma(3)), \\
\mathfrak{f}(\tau)^{24}, \mathfrak{f}_1(\tau)^{24}, \mathfrak{f}_2(\tau)^{24} &\in M_0^!(\Gamma(2)), \\
\mathfrak{f}(\tau)^{3}, \mathfrak{f}_1(\tau)^{3}, \mathfrak{f}_2(\tau)^{3} &\in M_0^!(\Gamma(16)), \\
\mathfrak{f}(\tau), \mathfrak{f}_1(\tau), \mathfrak{f}_2(\tau) &\in M_0^!(\Gamma(48)).
\end{aligned}$$

7.3 Quadratic Forms

Let $n < 0$ be a squarefree integer and consider the field $K = \mathbb{Q}(\sqrt{n})$. The ring of integers in K can be given as

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{n} & , n \not\equiv 1 \mod 4 \\ \mathbb{Z} + \mathbb{Z}\frac{-1+\sqrt{n}}{2} & , n \equiv 1 \mod 4 \end{cases}.$$

Therefore, the discriminant of K is given as

$$\operatorname{disc}(K) = \begin{cases} 4n & , n \not\equiv 1 \mod 4 \\ n & , n \equiv 1 \mod 4 \end{cases}. \tag{7.3.1}$$

Definition 7.3.1.

1. *A negative integer d is called a discriminant if $d \equiv 0, 1 \mod 4$.*
2. *A negative integer Δ is called a fundamental discriminant if it can be obtained from some squarefree n by formula* (7.3.1)*. These are the numbers Δ such that*

$$\begin{gathered}
\Delta \equiv 1 \bmod 4 \text{ and } \Delta \text{ is squarefree} \\
\text{or } \Delta \equiv 8, 12 \bmod 16 \text{ and } \Delta/4 \text{ is squarefree.}
\end{gathered}$$

3. *Any discriminant d can be written uniquely as $d = f^2\Delta$ where Δ is a fundamental discriminant and $f > 0$ is an integer. This f is called the conductor of the discriminant d.*

Definition 7.3.2. *Associate with a triple of integers (a, b, c) such that $a > 0$,$b^2 - 4ac < 0$ the following objects*

1. *the positive definite quadratic form $ax^2 + bxy + cy^2$*
2. *the discriminant $d = b^2 - 4ac$*
3. *$\tau_{a,b,c} = \frac{-b+\sqrt{d}}{2a} \in \mathbb{H}$*
4. *fractional ideal $\lambda(\frac{-b+\sqrt{d}}{2}\mathbb{Z} + a\mathbb{Z})$ of the order $\frac{d+\sqrt{d}}{2}\mathbb{Z} + \mathbb{Z}$, for any $\lambda \in K$*
5. *the following operation of $\mathbb{Z}^{2\times 2}$ on quadratics forms*

$$M \in \mathbb{Z}^{2\times 2} : ax^2 + bxy + cy^2 \mapsto aX^2 + bXY + cY^2 \text{ with } \begin{pmatrix} X \\ Y \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix}.$$

6. *conjugation operation $\overline{(a, b, c)} = (a, -b, c)$*

Definition 7.3.3. 1. *A quadratic form (a, b, c) is called reduced if*

$$0 \leq |b| \leq a \leq c \text{ and } b \geq 0 \text{ whenever } a = |b| \text{ or } a = c.$$

2. *A quadratic form (a, b, c) is called primitive if* $\gcd(a, b, c) = 1$.
3. *A quadratic form (a, b, c) is called* real *if $(a, -b, c)$ is $\Gamma(1)$–equivalent to (a, b, c) and* imaginary *otherwise. An equivalent characterization of real forms is those whose corresponding ideals square to principal ideals.*

Proposition 7.3.4. *Every quadratic form is equivalent (under $\Gamma(1)$) to a reduced form, and no two distinct reduced forms are equivalent. The real forms are precisely those lying on the even, odd, and free edges (Definition 4.5.2), that is, those where $j(\tau_{a,b,c}) \in \mathbb{R}$.*

Proof. The condition for (a, b, c) being reduced is exactly

$$|\operatorname{Re}(\tau)| \leq \frac{1}{2} \text{ and } |\tau| \geq 1 \text{ and } \operatorname{Re}(\tau) \leq 0 \text{ whenever } |\operatorname{Re}(\tau)| = \frac{1}{2} \text{ or } |\tau| = 1.$$

for $\tau = \frac{-b+\sqrt{d}}{2a}$. This is exactly the fundamental domain for $\Gamma(1)$. □

Definition 7.3.5. *Let $H(d)$ denote the equivalent classes of primitive forms of a given discriminant d under the action of $\Gamma(1)$. Also let $h(d)$ denote the size of $H(d)$.*

Proposition 7.3.6. $h(d) < \infty$.

Proof. If (a, b, c) is a reduced form with discriminant d then we see $b^2 \leq ac \leq -d/3$. There can only be a finite number of forms satisfying this. □

Example 7.3.7.

$$\begin{aligned} h(-163) &= 1 \quad H(-163) = \{(1, 1, 41)\} \\ h(-160) &= 4 \quad H(-160) = \{(1, 0, 40), (5, 0, 8), (4, 4, 11), (7, 6, 7)\} \end{aligned}$$

7.4 Singular Values of the j Function

Proposition 7.4.1. *For any discriminant d, the polynomial*

$$\mathcal{H}_d^j(X) = \prod_{(a,b,c)\in H(d)} \left(X - j\left(\tfrac{-b+\sqrt{d}}{2a}\right)\right)$$

has integer coefficients. Furthermore, if $d = r^2 - 4n$ for any integers r and n with $n > 1$, then $\mathcal{H}_d^j(X)$ divides $\Phi_n(X, X)$ (the modular equation for j).

7.5 Class Invariants

7.5.1 $\gamma_2(\tau)$

Proposition 7.5.1. *For* $\gcd(3, n) = 1$ *The polynomial*

$$\Phi_n^{\gamma_2}(x, \gamma_2(\tau)) = \prod_{\substack{\alpha\delta=n \\ \alpha,\delta>0 \\ \gcd(\alpha,\beta,\delta)=1 \\ \beta\equiv 0 \mod 3 \\ 0\le\beta<3\delta}} \left(x - \gamma_2\left(\frac{\alpha\tau+\beta}{\delta}\right)\right)$$

is in $\mathbb{Z}[x, \gamma_2(\tau)]$

Proof. The displayed set of functions is transitively permuted by Γ^3. Since $\gamma_2(\tau)$ is a generator of $A_0(\Gamma^3)$, the coefficient of this polynomial must be polynomials in $\gamma_2(\tau)$. □

Example 7.5.2. $\Phi_2^{\gamma_2}(x, y) = x^3 - x^2y^2 + 495xy + y^3 - 54000$.

Proposition 7.5.3. *Suppose (A, B, C) is a quadratic form with* $\gcd(3, A) = 1$, $B \equiv 0 \mod 3$, *and* $\gcd(3, D) = 1$. *Then*

$$\mathbb{Q}(\gamma_2(\tau_{A,B,C})) = \mathbb{Q}(j(\tau_{A,B,C})).$$

Proof. Suppose that $X = \gamma_2(\tau_{A,B,C})$ is a root of $\Phi_n^{\gamma_2}(X, X) = 0$ for some n with $\gcd(A, 3n) = 1$ and $n \equiv 2 \mod 3$. We will show that, although $X = \gamma_2(\tau)$ is a root of $\Phi_n^{\gamma_2}(X, X) = 0$, the quantities $\gamma_2(\tau \pm 1)$ are not roots of $\Phi_n^{\gamma_2}(X, X) = 0$. As the roots of $X^3 - j(\tau) = 0$ are $X = \gamma_2(\tau), \gamma_2(\tau \pm 1)$, the polynomials

$$\Phi_n^{\gamma_2}(X, X)$$
$$X^3 - j(\tau_{A,B,C}),$$

as elements of $\mathbb{Q}(j)[X]$, have a gcd of degree 1, and hence determine $X = \gamma_2(\tau_{A,B,C})$ as an element of $\mathbb{Q}(j(\tau_{A,B,C}))$.

Now suppose that $\gcd(3, A) = 1$, $B \equiv 0 \mod 3$, and $\gcd(3, D) = 1$ as in the proposition. The matrices that fix $\tau_{A,B,C}$ are of the form

$$\begin{pmatrix} x & -Cy \\ Ay & x + By \end{pmatrix},$$

for $x, y \in \mathbb{R}$. If $X = \gamma_2(\tau_{A,B,C})$ is a root of $\Phi_n^{\gamma_2}(X, X) = 0$ then

$$\frac{a\tau + b}{c\tau + d} = \frac{\alpha\tau + \beta}{\delta},$$

for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma^3$ and some α, β, δ as in Proposition 7.5.1. This means that

$$\begin{aligned}\begin{pmatrix} x & -Cy \\ Ay & x+By \end{pmatrix} &= \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \\ &= \begin{pmatrix} d\alpha & d\beta - b\delta \\ -c\alpha & a\delta - c\beta \end{pmatrix}.\end{aligned}$$

Let n denote the determinant of these matrices. Thus,

$$n = \alpha\delta = x^2 + Bxy + ACy^2.$$

Note also that $\gcd(x, y) = 1$ since all of these matrices are primitive. Next, choose x and y so that $\gcd(A, 3n) = 1$ (this is always possible). As α is a divisor of n, x and Ay, we must have $\alpha = \pm 1$, say $\alpha = 1$ and $\delta = n$. Note also that $y \not\equiv 0 \mod 3$ since $n \equiv 2 \mod 3$, and so $c \not\equiv 0 \mod 3$. Also,

$$\begin{aligned} By &= an - d - c\beta \\ &\equiv -(a+d) \mod 3 \\ &\equiv 0 \mod 3, \end{aligned}$$

since $3 \nmid c \implies 3 \mid (a+d)$ in the group Γ^3. This means that it is necessary that

$$B \equiv 0 \mod 3,$$

for $\gamma_2(\tau_{A,B,C})$ to be a root of $\Phi_n(x, x) = 0$. In particular, the numbers $\gamma_2(\tau_{A,B,C} \pm 1) = \gamma_2(\tau_{A,B\mp 2A,\ldots})$ are not roots of $\Phi_n(x, x) = 0$. □

Example 7.5.4. *Let us continue with* $\Phi_2^{\gamma_2}(x, y) = x^3 - x^2y^2 + 495xy + y^3 - 54000$. *Here*

$$\begin{aligned}\Phi_2^{\gamma_2}(X, X) &= X^4 - 2X^3 - 495X^2 + 54000 \\ &= (X - 20)(X - 12)(X + 15)^2\end{aligned}$$

The degree $n = 2$ *represented by the following principal forms:*

$$\begin{array}{lll} 2 = x^2 + y^2 & (A, B, C) = (1, 0, 1) & D = -4 \\ 2 = x^2 + 3xy + 4y^2 & (A, B, C) = (1, 3, 4) & D = -7 \\ 2 = x^2 + 2y^2 & (A, B, C) = (1, 0, 2) & D = -8 \end{array}$$

One can compute that

$$\gcd_X(X^4 - 2X^3 - 495X^2 + 54000, X^3 - j) = (j^2 - 990j + 26730000)X - (2j^2 + 191025j).$$

Thus, the equation

$$\gamma_2(\tau) = j(\tau)^{1/3} = \frac{2j(\tau)^2 + 191025j(\tau)}{j(\tau)^2 - 990j(\tau) + 26730000}$$

holds for the three values $\tau = \tau_{1,0,1}, \tau_{1,3,4}, \tau_{1,0,2}$. *Indeed, the following table is easily verified from this formula.*

D	τ	$j(\tau)$	$\gamma_2(\tau)$
-4	$\sqrt{-1}$	12^3	12
-7	$\frac{-3+\sqrt{-7}}{2}$	-15^3	-15
-8	$\sqrt{-2}$	20^3	20

Example 7.5.5. *As* $4 \equiv 1 \mod 3$, *the polynomial* $\Phi_4^{\gamma_2}(X, X) = (X^3 - 287496)(X^3 + 3375)^2$ *has all three roots in common with* $X^3 = j$ *and cannot be used to determine* $j^{1/3}$ *as an element of* $\mathbb{Q}(j)$.

7.6 Singular Values of the Weber Functions

The polynomial $\mathcal{H}_d^j(X)$ defined in Section 7.4 has quite large coefficients. It turns out that modular functions of higher level (e.g. $j^{1/3}$) provide the same extensions of $\mathbb{Q}$ with much smaller defining polynomials. Weber defined a class invariant $f(\tau)$ to be a modular function for which

$$\mathbb{Q}(f(\tau_{a,b,c})) = \mathbb{Q}(j(\tau_{A,B,C}))$$

where (a,b,c) ranges over some set of representatives of $H(d)$.

Definition 7.6.1. *For any integer N let $(a',b',c') := [(a,b,c)]_N$ denote any form equivalent to (a,b,c) for which*

$$\gcd(a',N) = 1 \text{ and } b' \equiv B \bmod 2N.$$

Proposition 7.6.2. *For any primitive form (a,b,c), $[(a,b,c)]_N$ exists.*

Proposition 7.6.3. *With $s = \gcd(3,d)$ and $(a,b,c) \in [H(d)]_3$, we have the class invariant*

$$\gamma_2(\tfrac{-b+\sqrt{d}}{2a})^s.$$

Proposition 7.6.4. *With $s = \gcd(2,d)$ and $(a,b,c) \in [H(d)]_2$, we have the class invariant*

$$\gamma_3(\tfrac{-b+\sqrt{d}}{2a})^s.$$

Proposition 7.6.5. *Let (a,b,c) range over $[H(d)]_{48}$. Set $\tau = \frac{-b+\sqrt{d}}{2a}$ and $s = \gcd(3,d)$. Then, we have the following table of class invariants. The $d \equiv 5 \bmod 8$ case is pure conjecture.*

condition	*class invariant*
$-d/4 \equiv 0 \bmod 8$	$2^{-3s}\mathfrak{f}_1(\tau)^{8s}$
$-d/4 \equiv 4 \bmod 8$	$\left(\frac{2}{a}\right)2^{-3s/2}\mathfrak{f}_1(\tau)^{4s}$
$-d/4 \equiv 2 \bmod 4$	$\left(\frac{2}{a}\right)2^{-s/2}\mathfrak{f}_1(\tau)^{2s}$
$-d/4 \equiv 1 \bmod 8$	$\left(\frac{2}{a}\right)2^{-s/2}\mathfrak{f}(\tau)^{2s}$
$-d/4 \equiv 5 \bmod 8$	$2^{-s}\mathfrak{f}(\tau)^{4s}$
$-d/4 \equiv 3 \bmod 8$	$2^{-\lfloor s/3 \rfloor}\mathfrak{f}(\tau)^{s}$
$-d/4 \equiv 7 \bmod 8$	$\left(\frac{2}{a}\right)2^{-s/2}\mathfrak{f}(\tau)^{s}$
$d \equiv 1 \bmod 8$	$\zeta_{48}^{sa}\mathfrak{f}_2(\tau)^s$
$d \equiv 5 \bmod 8, \lvert d\rvert < 300$	$\frac{\mathfrak{f}(\tau_\infty)^s}{2} + \frac{\mathfrak{f}(\tau_0)^s}{2} + \frac{\mathfrak{f}(\tau_1)^s}{2} - \frac{2}{\mathfrak{f}(\tau_\infty)^s} - \frac{2}{\mathfrak{f}(\tau_0)^s} - \frac{2}{\mathfrak{f}(\tau_1)^s}$

In the case $d \equiv 5 \bmod 8$, we should set $\tau_i = \frac{-b_i+\sqrt{4d}}{2a_i}$ where

$$\begin{aligned}(a_\infty,b_\infty,c_\infty) &= \left[\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right)(a,b,c)\right]_{48},\\ (a_0,b_0,c_0) &= \left[\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)(a,b,c)\right]_{48},\\ (a_1,b_1,c_1) &= \left[\left(\begin{smallmatrix}1&1\\0&2\end{smallmatrix}\right)(a,b,c)\right]_{48}.\end{aligned}$$

Example 7.6.6. *We have $h(-103) = 5$ and*

$$[H(-103)]_{48} = \{(17,769,8698),(19,-767,7742),(1,1,26),(23,865,8134),(29,97,82)\}.$$

According to Proposition 7.6.5,

$$\zeta_{48}^{17}\mathfrak{f}_2\left(\tfrac{-769+\sqrt{-103}}{34}\right),\quad \zeta_{48}^{19}\mathfrak{f}_2\left(\tfrac{767+\sqrt{-103}}{38}\right),\quad \zeta_{48}\mathfrak{f}_2\left(\tfrac{-1+\sqrt{-103}}{2}\right),$$
$$\zeta_{48}^{23}\mathfrak{f}_2\left(\tfrac{-865+\sqrt{-103}}{46}\right),\quad \zeta_{48}^{29}\mathfrak{f}_2\left(\tfrac{-97+\sqrt{-103}}{58}\right)$$

are roots of $x^5+2x^4+3x^3+3x^2+x-1$. *This is a much simpler polynomial than*

$$\mathcal{H}^j_{-103}(x) = x^5 + 70292286280125x^4 + 85475283659296875x^3$$
$$+4941005649165514137656250000x^2 + 133555277201141655061721191406 25x$$
$$+28826612937014029067466156005859375,$$

although they generate the same splitting field.

7.7 Shimura reciprocity

In this section d is a negative discriminant, *not necessarily fundamental*, and $\mathfrak{o} = (-b_1+\sqrt{d})\mathbb{Z}+\mathbb{Z}$ is the corresponding order, *not necessarily maximal*, of $K = \mathbb{Q}(\sqrt{\Delta})$, where Δ is the corresponding fundamental discriminant.

The automorphism group of the whole modular function field (of every level) is discribed by $\mathrm{GL}_2(\hat{\mathbb{Q}})$. The operation of this group on a given modular function f of level N with coefficients in $\mathbb{Q}(\zeta_N)$, i.e.

$$f \in A_0(\Gamma(N), \mathbb{Q}(\zeta_N)) := A_0(\Gamma(N)) \cap \mathbb{Q}(\zeta_N)((q^{1/N}))$$

is as follows. Every matrix $m \in \mathrm{GL}_2(\hat{\mathbb{Q}})$ can be written as $m = u.v$ where $u \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ and $v \in \mathrm{GL}_2^+(\mathbb{Q})$. The representation is not unique, but this does not matter for the definition

$$f^m(\tau) = f^u(v\tau),$$

where $v\tau$ is the usual fractional–linear transformation, and f^u has the following definition. First project u modulo N to obtain a matrix $\tilde{u} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. This matrix $\tilde{u}$ can be written as a product of matrices of the form $\left(\begin{smallmatrix}1 & 0\\ 0 & \delta\end{smallmatrix}\right)$ and matrices in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. The former matrices operate as $\zeta_N \mapsto \zeta_N^\delta$ and the latter operate via their lifts to $\mathrm{SL}_2(\mathbb{Z})$. Shimura reciprocity is then the simple statement that, for any $\tau \in K \cap \mathbb{H}$, any modular function f with no pole at τ, and any idele $z \in J_K$,

$$f(\tau)^{(z^{-1}, K^{\mathrm{ab}}/K)} = f^{m(z)}(\tau),$$

where $m(z)$ is the matrix representing $\hat{K}$–multiplication with respect to the $\hat{\mathbb{Q}}$–basis $\{\tau, 1\}$. Explicitly,

$$\begin{aligned}(m_\tau)_{\mathfrak{p}} : K_{\mathfrak{p}}^* &\to \mathrm{GL}_2(\mathbb{Q}_p)\\ s\tau + t &\mapsto \left(\begin{smallmatrix} t+(\tau+\bar{\tau})s & -\tau\bar{\tau}s \\ s & t\end{smallmatrix}\right).\end{aligned}$$

First, it turns out that an idele responsible for transforming j–values can be given by

$$z_{\mathfrak{p}} = \begin{cases} a & \mathfrak{p} \nmid a \\ \frac{-b+\sqrt{d}}{2} & \mathfrak{p} \mid a,\ \mathfrak{p} \nmid c \\ \frac{-b+\sqrt{d}}{2} - a & \mathfrak{p} \mid a,\ \mathfrak{p} \mid c \end{cases}. \tag{7.7.1}$$

The matrix in $\mathrm{GL}_2(\hat{\mathbb{Q}})$ corresponding to this z^{-1} by Shimura reciprocity applied to modular functions evaluated at $\tau_1 = \frac{-b_1+\sqrt{d}}{2}$ factors into $u.v$, where $v = \left(\begin{smallmatrix}1 & (b_1-b)/2\\ 0 & a\end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{Q})$, and $u \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ has components

$$u_p = \begin{cases} \left(\begin{smallmatrix} a & \frac{b-b_1}{2} \\ 0 & 1\end{smallmatrix}\right) & p \nmid a \\ \left(\begin{smallmatrix} \frac{-b_1-b}{2} & -c \\ 1 & 0\end{smallmatrix}\right) & p \mid a,\ p \nmid c \\ \left(\begin{smallmatrix} \frac{-b_1-b}{2}-a & \frac{b_1-b}{2}-a \\ 1 & -1\end{smallmatrix}\right) & p \mid a,\ p \mid c \end{cases}. \tag{7.7.2}$$

Theorem 7.7.1. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be $\mathfrak{o}$-ideals. Suppose $\mathfrak{o} = \frac{-b_1+\sqrt{d}}{2}\mathbb{Z}+\mathbb{Z}$, $\mathfrak{b} = \frac{-b+\sqrt{d}}{2}\mathbb{Z}+a\mathbb{Z}$, and $\sigma_{\mathfrak{b}}$ is defined by the Artin symbol $(z^{-1}, K^{ab}/K)$ where z is the idele with components* (7.7.1)*. Then,*

$$\begin{aligned} j(\mathfrak{o})^{\sigma_{\mathfrak{b}}} &= j(\mathfrak{b}), \\ \frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{o})} &\in K(j(\mathfrak{o})), \\ \left(\frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{o})}\right)^{\sigma_{\mathfrak{b}}} &= \frac{\Delta(\mathfrak{a}\mathfrak{b})}{\Delta(\mathfrak{b})} \end{aligned}$$

Theorem 7.7.2. *The following are units in $\mathbb{Q}(j(\mathfrak{o}))$.*

$$\begin{aligned} &\mathbf{N}\mathfrak{a}^{12}\frac{|\Delta(\mathfrak{a})|^2}{|\Delta(\mathfrak{o})|^2} = \frac{\Delta(\mathfrak{a})\Delta(\mathfrak{a}^{-1})}{\Delta(\mathfrak{o})^2} \quad \textit{for any } \mathfrak{o}\textit{-ideal } \mathfrak{a}\textit{, and} \\ &\mathbf{N}\mathfrak{a}^{6}\frac{\Delta(\mathfrak{a})}{\Delta(\mathfrak{o})} \quad \textit{provided } \mathfrak{a}^2 = (\mathbf{N}\mathfrak{a})\mathfrak{o}, \\ &[?]\frac{\Delta(\mathfrak{a})\Delta(\mathfrak{b})}{\Delta(\mathfrak{o})\Delta(\mathfrak{a}\mathfrak{b})} \quad \textit{for any } \mathfrak{o}\textit{-ideals } \mathfrak{a} \textit{ and } \mathfrak{b}. \end{aligned}$$

Proof. The first two displayed expressions are invariant under scaling $\mathfrak{a}$ by principal ideals, so it suffices to prove them when $\mathfrak{a} = \mathfrak{p}$ is prime. □

In addition to the idele (7.7.1), which moves j–values, it is useful to isolate those ideles which fix the j–values. These will be those for which $z_{\mathfrak{p}} \in \mathfrak{o}_{\mathfrak{p}}^*$.

Theorem 7.7.3. *Let $\mathfrak{o} = \tau_1\mathbb{Z}+\mathbb{Z}$ with $\tau_1 = \frac{-b_1+\sqrt{d}}{2}$ be an order of K, and let $f(\tau) \in \mathbb{Q}(\zeta_N)((q^{1/N}))$ have level N. The action of $\mathrm{Gal}(K^{ab}/K(j(\mathfrak{o})))$ on $f(\tau_1)$ can be identified with $(\mathfrak{o}/N\mathfrak{o})^*$ using*

$$\begin{aligned} m_{\tau_1} : (\mathfrak{o}/N\mathfrak{o})^* &\to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \\ s\tau_1 + t &\mapsto \left(\begin{smallmatrix} t-b_1 s & -c_1 s \\ s & t \end{smallmatrix}\right). \end{aligned}$$

For any $\tilde{z} \in (\mathfrak{o}/N\mathfrak{o})^*$, Shimura reciprocity becomes $f(\tau_1)^{\tilde{z}^{-1}} = f^{m_{\tau_1}(\tilde{z})}(\tau_1)$. $\tilde{z}$ can be lifted to any idele z for which $z_{\mathfrak{p}} \in \mathfrak{o}_{\mathfrak{p}}^*$, for all $\mathfrak{p}$ and $z_{\mathfrak{p}} \equiv \tilde{z} \mod N\mathfrak{o}_{\mathfrak{p}}$ for $\mathfrak{p} \mid N$.

7.8 Singular Values of the η Function

The goal here is to understand evaluations such as

$$\eta(\sqrt{-5}) = 2^{-3/4}5^{-1/4}\left(\frac{1+\sqrt{5}}{2}\right)^{-1/8}\pi^{-1/4}\frac{\Gamma(\frac{1}{20})^{1/8}\Gamma(\frac{3}{20})^{1/8}\Gamma(\frac{7}{20})^{1/8}\Gamma(\frac{9}{20})^{1/8}}{\Gamma(\frac{11}{20})^{1/8}\Gamma(\frac{13}{20})^{1/8}\Gamma(\frac{17}{20})^{1/8}\Gamma(\frac{19}{20})^{1/8}}.$$

There is always a transcendental product of Γ functions and another algebraic factor where units appear.

In this section let $d < 0$ be a fixed discriminant and let Δ and $f = d/\Delta$ be the associated fundamental discriminant and conductor. Also, set $h = h(d)$, let w be the number of roots of unity in $\mathbb{Q}(\sqrt{\Delta})$, and set $\chi(n) = (\frac{\Delta}{n})$ to be the usual Kronecker symbol. The Γ factor quantitiy $\Gamma_d > 0$ appearing in the Chowla–Selberg formula satisfies

$$\log(4\pi\sqrt{|d|}\,\Gamma_d^4) = \sum_{n=1}^{|\Delta|}\frac{w\chi(n)}{2h(\Delta)}\log\Gamma\left(n/|\Delta|\right) + \sum_{p^n||f}\frac{(1-p^{-n})\,(1-\chi(p))}{(1-p^{-1})\,(p-\chi(p))}\log p.$$

Weber's class invariants in Proposition 7.6.5 succeed in generating very small defining polynoimals. Weber's invariants fail to always be units and they also fail on discriminants $= 5 \pmod 8$. The following simple theorem, proved in Theorem 7.8.3 below where the conjugates of X_1 over $\mathbb{Q}$ are given, provides class invariants that are always units and directly evaluates the singular values of η. While the minimal polynomial for X_1 is quite large, it is frequently the case that a fractional power of X_1 has a much smaller minimal polynomial, as illustrated in Examples 7.8.4 and 7.8.5. Neither Weber's units nor the units of Theorem 7.7.2 enjoy the following full–rank property.

Theorem 7.8.1. *Let $(a_1 = 1, b_1, c_1)$ be in the identity class in $H(d)$ and define X_1 to satisfy*

$$\eta(\tfrac{-b_1+\sqrt{d}}{2}) = \zeta_{48}^{-b_1}(\tfrac{\sqrt{|d|}}{2})^{-1/4} X_1^{1/(24h)} \Gamma_d^{1/h}.$$

Then, $X_1 \in \mathbb{Q}(j(\frac{-b_1+\sqrt{d}}{2}))$, and for each $\mathfrak{b} \in H(d)$ we will have a $\mathbb{Q}$–conjugate $X_{\mathfrak{b}}$. The set of $X_{\mathfrak{b}}$ for real $\mathfrak{b}$ and $|X_{\mathfrak{b}}|^2 = X_{\mathfrak{b}} X_{\bar{\mathfrak{b}}}$ for the imaginary pair $\mathfrak{b}, \bar{\mathfrak{b}}$ generate a system of units of full rank.

For much of this section, a modified domain for the reduced forms will be more convenient. We take the usual fundamental domain but map the arc $|\tau| = 1$, $\pi/4 < \arg\tau < \pi/3$ to $\Re(\tau) = -1/2$ by $\tau \mapsto -1/(\tau+1)$. The resulting new definition of reduced will be called reduced$'$.

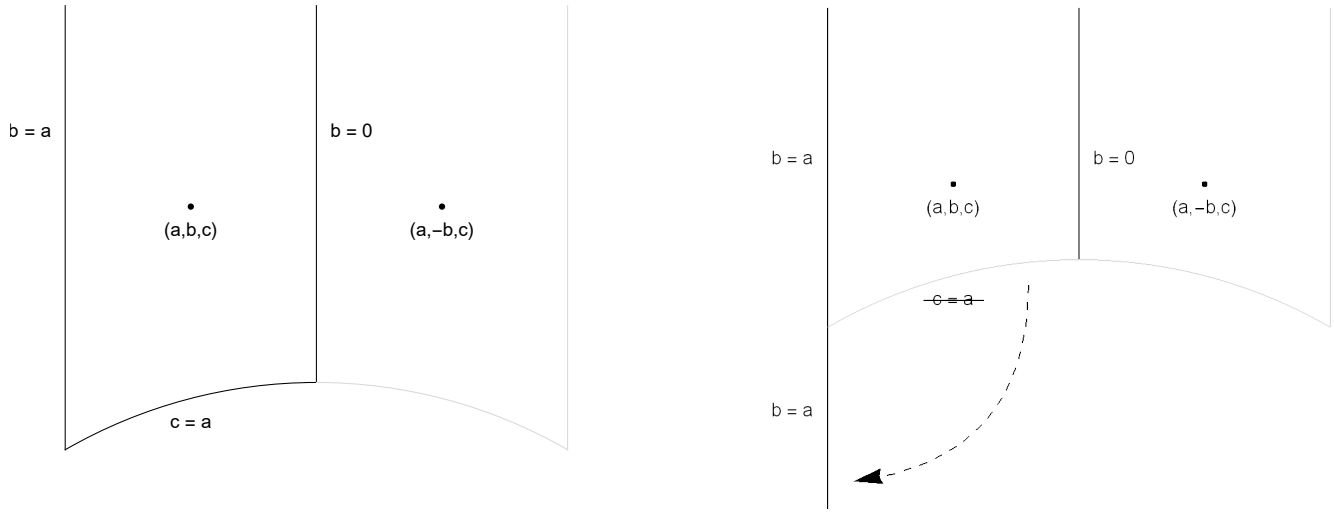


Figure 7.1: $\tau_{a,b,c} \in \mathbb{H}$ for reduced (left, usual domain of $\Gamma(1)$) and reduced$'$ (right) forms (a, b, c)

Define a modified η function as

$$\tilde{\eta}(\tau) = \mathrm{Im}(\tau)^{1/4} \eta(\tau).$$

The point of this slight modification is that now the absolute value remains invariant under $\mathrm{SL}_2(\mathbb{Z})$:

$$\tilde{\eta}(\tau+1) = \zeta_{24}\tilde{\eta}(\tau), \qquad \tilde{\eta}(-1/\tau) = (-\tau/\bar{\tau})^{1/4}\tilde{\eta}(\tau). \tag{7.8.1}$$

Also, set $\tilde{\eta}_{a,b,c} = \tilde{\eta}(\tau_{a,b,c})$ and $j_{a,b,c} = j(\tau_{a,b,c})$, etc. We will almost exclusively use the identity form in $H(d)$ in the form $(a_1 = 1, b_1, c_1)$. Hence, $\tilde{\eta}_1$ and j_1 etc. will denote the values of these functions at the corresponding $\tau_{1,b_1,c_1} = (-b_1 + \sqrt{d})/2$.

Our first task is to resolve the unspecified argument of the η–product in the Chowla–Selberg formula.

Proposition 7.8.2. *Fix a set of $\{(a, b, c)\}$ of representatives of $H(d)$. There exists a 48^{th} root of unity ζ_{48}^k and a $\mu \in \mathbb{Q}(\sqrt{d})$ of absolute value one (both depending on the choice of the $\{(a, b, c)\}$) with*

$$\prod_{(a,b,c)\in H} \tilde{\eta}_{a,b,c} = \zeta_{48}^k \mu^{1/4} \Gamma_d.$$

With the reduced$'$ set of representatives we may take $\mu = 1$ and $k = -\sum_{(a,b,c)} \frac{b}{a}$

Proof I. Because of (7.8.1), the truth of this proposition is independent of the choice of representatives of $H(d)$, hence we may take them to be reduced$'$. The Chowla–Selberg formula gives

$$\prod_{(a,b,c)\in H} |\tilde{\eta}_{a,b,c}| = \Gamma_d.$$

For the pair of imaginary forms (a,b,c) and $(a,-b,c)$ we have $\overline{\tilde{\eta}_{a,b,c}} = \tilde{\eta}_{a,-b,c}$, so $|\tilde{\eta}_{a,b,c}\tilde{\eta}_{a,-b,c}| = \tilde{\eta}_{a,b,c}\tilde{\eta}_{a,-b,c}$. Next, the real forms split into two case depending on their location in the fundamental domain. On $b=0$ (i.e. $\Re(\tau)=0$) we clearly have $|\tilde{\eta}_{a,b,c}| = \tilde{\eta}_{a,b,c}$. On $b=a$ (i.e. $\Re(\tau)=-1/2$) we have $|\tilde{\eta}_{a,b,c}| = \zeta_{48}\tilde{\eta}_{a,b,c}$. □

Proof II. Squaring both sides of the Chowla–Selberg formula and using the fact that $\overline{\tilde{\eta}_{a,b,c}} = \tilde{\eta}_{a,-b,c}$ gives

$$\prod_{(a,b,c)\in H} \tilde{\eta}_{a,b,c} \prod_{(a,b,c)\in H} \tilde{\eta}_{a,-b,c} = \Gamma_d^2.$$

Since the map $(a,b,c)\mapsto(a,-b,c)$ is inversion in the class group, each form $(a,-b,c)$ is equivalent to some (a',b',c') from the original choice of representatives of H. Furthermore, in each case, by (7.8.1), we have an equation of the form $\eta_{a,-b,c} = \zeta_{a,b,c}\mu_{a,b,c}^{1/4}\tilde{\eta}_{a',b',c'}$. Multiplying these all together and taking some square root gives the result with $\mu^{1/8}$ in place of $\mu^{1/4}$. To show that the quantity under the eighth root is a square, we first notice that it suffices to prove the result for the reduced set of representatives; any set of representatives transforms to this modulo a 24^{th} and a fourth root by (7.8.1). With this reduced set of representatives, the reciprocal transform in (7.8.1) is only applied with τ on $|\tau|=1$, so the quantity $\tau/\bar{\tau}$ is a square. □

Theorem 7.8.3. *Fix a set of $\{(a,b,c)\}$ of representatives of H with $(a_1=1,b_1,c_1)$ being the identity. There exists a polynomial $f(x)\in\mathbb{Q}[x]$ independent of the choice of representatives, and for each form (a,b,c), there exists a $\mu_{a,b,c}\in K:=\mathbb{Q}(\sqrt{d})$ (depending on the choice of representative) of absolute value one with*

$$(X_{a,b,c} :=) \quad (-1)^{b_1 h}\mu_{a,b,c}^6\frac{\tilde{\eta}_{a,b,c}^{24h}}{\Gamma_d^{24}} = f(j_{a,b,c}).$$

Furthermore, these h quantities $X_{a,b,c}$ are roots of a monic irreducible polynomial over $\mathbb{Z}$ with constant coefficient $(-1)^h$. The value of X corresponding to the identity form X_1 is a positive real. If (a,b,c) is reduced$'$ and real (i.e. $b=0$ or $b=a$), then $\mu_{a,b,c}^6=1$.

Proof. We can assume wlog that the forms (a_i,b_i,c_i) are reduced$'$. Let $\mathfrak{a}_1,\dots,\mathfrak{a}_h$ be the corresponding ideals $\frac{-b_i+\sqrt{d}}{2}\mathbb{Z}+a_i\mathbb{Z}$ with $\mathfrak{o}=\mathfrak{a}_1$ being the identity. The norm of $\mathfrak{a}_i$ is given by $\mathbf{N}\mathfrak{a}_i=a_i$, and we use the following definition of the Δ function on lattices:

$$\Delta(\omega_1\mathbb{Z}+\omega_2\mathbb{Z}) = \omega_2^{-12}\eta^{24}(\tfrac{\omega_1}{\omega_2}) = (\tfrac{\bar{\omega}_2}{\omega_2})^6\Im(\omega_1\bar{\omega}_2)^{-6}\tilde{\eta}^{24}(\tfrac{\omega_1}{\omega_2}) \tag{7.8.2}$$

This is independent of the choice of basis (ω_1,ω_2) of the lattice and homogeneous of degree -12 as $\Delta(\lambda\mathfrak{a}) = \lambda^{-12}\Delta(\mathfrak{a})$. By (7.8.2) and by Proposition 7.8.2, with $k:=\sum_i b_i/a_i$, we have the equalities

$$\begin{aligned}\tilde{\eta}_{a_i,b_i,c_i}^{24} &= (\tfrac{\sqrt{|d|}}{2}a_i)^6\Delta(\mathfrak{a}_i),\\ (-1)^k\Gamma_d^{24} &= \prod_i(\tfrac{\sqrt{|d|}}{2}a_i)^6\Delta(\mathfrak{a}_i).\end{aligned}$$

Thus, if we set $\mu_{a_1,b_1,c_1}=1$, then X_1 has the representation

$$X_1 = (-1)^{b_1h+k}\frac{\Delta(\mathfrak{o})^h}{\prod_i a_i^6\Delta(\mathfrak{a}_i)} = (-1)^{b_1h+k}\prod_i \mathbf{N}\mathfrak{a}_i^{-6}\frac{\Delta(\mathfrak{o})}{\Delta(\mathfrak{a}_i)},$$

and so by Theorem 7.7.1, $X_1 \in K(j_1)$, and by the first two assertions of Theorem 7.7.2, $|X_1|$ is a unit. Since X_1 is real and j_1 is real, $X_1 \in \mathbb{Q}(j_1)$ and X_1 is a unit. Now let $\mathfrak{b} = \frac{-b+\sqrt{d}}{2}\mathbb{Z} + a\mathbb{Z}$ correspond to any one of the reduced$'$ forms (a,b,c), and we will purposely confuse (a,b,c) and $\mathfrak{b}$ notationaly. Theorem 7.7.1 also gives a $\sigma = \sigma_{\mathfrak{b}} \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with

$$j_1^{\sigma} = j(\mathfrak{b}), \text{ and } X_1^{\sigma} = X_{\mathfrak{b}} = (-1)^{b_1 h + k} \frac{\Delta(\mathfrak{b})^h}{\prod_i a_i^6 \Delta(\mathfrak{a}_i \mathfrak{b})}.$$

For each i, the ideal $\mathfrak{a}_i\mathfrak{b}$ is equal to some other $\mathfrak{a}_j$ modulo principal ideals as this is the definition of the class group. Hence, for an accordingly defined operation $i + \mathfrak{b}$ on the indicies of these ideals, we have $\mathfrak{a}_i\mathfrak{b} = \lambda_i \mathfrak{a}_{i+\mathfrak{b}}$ for some $\lambda_i \in K$. Inserting this into the last equation gives

$$X_{\mathfrak{b}} = (-1)^{b_1 h + k} \frac{\Delta(\mathfrak{b})^h}{\prod_i a_i^6 \lambda_i^{-12} \Delta(\mathfrak{a}_{i+\mathfrak{b}})} = (-1)^{b_1 h + k} \prod_i \lambda_i^{12} \frac{\Delta(\mathfrak{b})^h}{\prod_i a_i^6 \Delta(\mathfrak{a}_i)} = (-1)^{b_1 h} \frac{\prod_i \lambda_i^{12}}{a^{6h}} \frac{\tilde{\eta}_{a,b,c}^{24h}}{\Gamma_d^{24}}.$$

We should therefore take $\mu_{\mathfrak{b}} = a^{-h} \Pi_i \lambda_i^2$, which is clearly an element of K. Since $a = \mathbf{N}\mathfrak{b}$ and $\lambda_i \mathfrak{o} = \mathfrak{a}_i \mathfrak{b} \mathfrak{a}_{i+\mathfrak{b}}^{-1}$, we see that $\mu_{\mathfrak{b}}$ is a generator of the principal ideal $\mathfrak{b}^{2h}/\mathbf{N}\mathfrak{b}^h = \mathfrak{b}^h/\bar{\mathfrak{b}}^h$, and therefore that $|\mu_{\mathfrak{b}}| = 1$. This formula $\mu_{\mathfrak{b}} = \lambda_{\mathfrak{b}}/\bar{\lambda}_{\mathfrak{b}}$ where $\mathfrak{b}^h = \lambda_{\mathfrak{b}}\mathfrak{o}$ requires care, as explain below; only $\mu_{\mathfrak{b}}^6$ is uniquely determined. For non-principle reduced$'$ real forms $\mathfrak{b}$, for which $\mathfrak{b}^2 = (\mathbf{N}\mathfrak{b})\mathfrak{o}$, it must be that h is even and therefore that $\mu_{\mathfrak{b}}^6 = 1$.

As for the constant coefficient, at this point all assumptions about reducedness of forms can be dropped and $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ can be an arbitrary set of representatives of $H(d)$. Similary, $\mathfrak{b}$ can be any $\mathfrak{o}$–ideal. For a principal ideal $\lambda\mathfrak{o}$, let $[\lambda\mathfrak{o}]$ denote a generator λ. As K contains at worst 12^{th} roots of unity, only $[\mathfrak{a}]^{12}$ is well–defined. The formula for $X_{\mathfrak{b}}$ and the Chowla–Selberg formula take the forms

$$\begin{aligned}
(-1)^{b_1 h} X_{\mathfrak{b}} &= (\tfrac{\sqrt{|d|}}{2})^{6h} \Gamma_d^{-24} [\mathfrak{b}^h]^{12} \Delta(\mathfrak{b})^h, \\
1 &= (\tfrac{\sqrt{|d|}}{2})^{12h} \Gamma_d^{-48} [\Pi_i \mathfrak{a}_i^2]^{12} \Pi_i \Delta(\mathfrak{a}_i)^2 \quad \text{for any } h, \\
-1 &= (\tfrac{\sqrt{|d|}}{2})^{6h} \Gamma_d^{-24} [\Pi_i \mathfrak{a}_i]^{12} \Pi_i \Delta(\mathfrak{a}_i) \quad \text{for odd } h.
\end{aligned}$$

In order to prove these, it is enough to notice that the right hand sides are functions of only the ideal classes and that the formulas are true when the ideals are reduced$'$ as above. The $h/2^{\text{th}}$ and the h^{th} powers of the last two equations show that $\Pi_i X_{\mathfrak{a}_i} = 1$ when h is even and odd, respectively. □

Example 7.8.4. *For discriminant -103, the five quantities*

$$-\frac{\tilde{\eta}_{1,1,26}^{120}}{\Gamma_{-103}^{24}}, \quad -\left(\frac{-5+\sqrt{-103}}{-5-\sqrt{-103}}\right)^6 \frac{\tilde{\eta}_{2,1,13}^{120}}{\Gamma_{-103}^{24}}, \quad -\left(\frac{5+\sqrt{-103}}{5-\sqrt{-103}}\right)^6 \frac{\tilde{\eta}_{2,-1,13}^{120}}{\Gamma_{-103}^{24}},$$
$$-\left(\frac{5+\sqrt{-103}}{5-\sqrt{-103}}\right)^{12} \frac{\tilde{\eta}_{4,3,7}^{120}}{\Gamma_{-103}^{24}}, \quad -\left(\frac{-5+\sqrt{-103}}{-5-\sqrt{-103}}\right)^{12} \frac{\tilde{\eta}_{4,-3,7}^{120}}{\Gamma_{-103}^{24}}$$

are roots of

$$x^5 - 18121127630x^4 + 1524409682770821566 35x^3$$
$$-13699549343369520851635x^2 + 60993014724637186605 0755x - 1.$$

Comparing with Example 7.6.6 , we see that this $\mathcal{H}_{-103}^{\eta}$ does better than $\mathcal{H}_{-103}^{j}$ on account of the constant coefficient ± 1 but is still much larger than Weber's. However, $X_{1,1,26}^{1/24}$ becomes comparable to Weber's as it is a root of

$$x^5 + 6x^4 + 15x^3 + 16x^2 + 8x - 1.$$

Example 7.8.5. *For discriminant* -972, $X_{1,0,243}^{1/72}$ *is a class invariant.*

$$X_{1,0,243}^{1/72}=\frac{\tilde{\eta}_{1,0,243}^3}{\Gamma_{-972}^{1/3}}=(3^{2/3}-2)(3^{1/3}-2^{1/3})(2^{2/3}-3^{1/3})\frac{3^{4/3}}{(1+2^{1/3})^4}\quad(=:x)$$

With $\alpha:2^{1/3}\mapsto\zeta_3 2^{1/3}$ *and* $\beta:3^{1/3}\mapsto\zeta_3 3^{1/3}$ *as the generators of* $\mathrm{Gal}(\mathbb{Q}(\sqrt{-3},j_{1,0,243})/\mathbb{Q}(\sqrt{-3}))$,

$$\zeta_4^{-1}\frac{\tilde{\eta}_{4,2,61}^3}{\Gamma_{-972}^{1/3}}=x^{\alpha},\quad \zeta_4\frac{\tilde{\eta}_{4,-2,61}^3}{\Gamma_{-972}^{1/3}}=x^{\alpha^2},\quad \zeta_{12}^{7}\frac{\tilde{\eta}_{9,6,28}^3}{\Gamma_{-972}^{1/3}}=x^{\beta},\quad \zeta_{12}^{-7}\frac{\tilde{\eta}_{9,-6,28}^3}{\Gamma_{-972}^{1/3}}=x^{\beta^2}$$
$$\zeta_{12}\left(\frac{-6+\sqrt{-972}}{-6-\sqrt{-972}}\right)^{3/4}\frac{\tilde{\eta}_{7,6,36}^3}{\Gamma_{-972}^{1/3}}=x^{\alpha\beta^2},\quad \zeta_{12}^{-1}\left(\frac{6+\sqrt{-972}}{6-\sqrt{-972}}\right)^{3/4}\frac{\tilde{\eta}_{7,-6,36}^3}{\Gamma_{-972}^{1/3}}=x^{\alpha^2\beta},$$
$$\zeta_{12}^{-1}\left(\frac{9+\sqrt{-972}}{9-\sqrt{-972}}\right)^{3/4}\frac{\tilde{\eta}_{13,4,19}^3}{\Gamma_{-972}^{1/3}}=x^{\alpha\beta},\quad \zeta_{12}\left(\frac{-9+\sqrt{-972}}{-9-\sqrt{-972}}\right)^{3/4}\frac{\tilde{\eta}_{13,-4,19}^3}{\Gamma_{-972}^{1/3}}=x^{\alpha^2\beta^2}.$$

Before trying to predict if $X_1^{1/72}$ is a class invariant, we should first predict using Shimura reciprocity which (hopefully small) integral power of $X_1^{1/24}$ is a class invariant. To do this, we will need the functions

$$\mathfrak{f}(\left(\begin{smallmatrix}\alpha&\beta\\0&\delta\end{smallmatrix}\right),\tau)=\sqrt{\alpha}\frac{\eta(\frac{\alpha\tau+\beta}{\delta})}{\eta(\tau)},\quad \alpha,\delta>0,\quad \gcd(\alpha,\beta,\delta)=1$$

For a fixed determinant $\alpha\delta=n$, these functions with the β chosen unique modulo δ are permuted up to 24^{th} roots of unity by $\Gamma(1)$, hence the 24^{th} powers of these functions, which are $\psi(n)$ in number, are the roots of a monic polynomial over $\mathbb{Z}[j(\tau)]$. With the reduced$'$ representatives (a,b,c), we can write

$$X_1^{1/24}=\prod_{(a,b,c)}\frac{a^{1/4}\zeta_{48}^{b_1-\mathbb{1}_{a=b}}}{\mathfrak{f}(\left(\begin{smallmatrix}1&(b_1-b)/2\\0&a\end{smallmatrix}\right),\tau_1)}\tag{7.8.3}$$

where the product excludes the identity form $(a_1=1,b_1,c_1)$, and $\tau_1=\tau_{a_1,b_1,c_1}$. The 48^{th} roots of unity and the $\mathfrak{f}$ functions present no problems for Shimura reciprocity: they are modular functions of level $48a$ evaluated at τ_1. What needs extra attention is the fourth root of the integer $\Pi a=:t$. Set $K=\mathbb{Q}(\sqrt{d})$. For $t\in\mathbb{Q}$, we have

$$t^{1/4}\in K^{\mathrm{ab}}\Leftrightarrow\begin{array}{l}|t|\in\mathbb{Q}^2,\text{ or}\\-d\in\mathbb{Q}^2,\text{ or}\\-d|t|\in\mathbb{Q}^2.\end{array}$$

In the case $t^{1/4}\notin K^{\mathrm{ab}}$, we simply must square both sides and consider powers of $X_1^{1/12}$. When it is in K^{ab}, we need formulas for its conjugates under $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. This is trivial in the first case as it is solved by the Kronecker symbol: we have explict representations $\sqrt{s}\in\mathbb{Q}(\zeta_{4|s|})$ such as

$$\sqrt{5}=\zeta_5^{0^2}+\zeta_5^{1^2}+\zeta_5^{2^2}+\zeta_5^{3^2}+\zeta_5^{4^2}$$
$$\sqrt{-7}=\zeta_7^{0^2}+\zeta_7^{1^2}+\zeta_7^{2^2}+\zeta_7^{3^2}+\zeta_7^{4^2}+\zeta_7^{5^2}+\zeta_7^{6^2},$$

and the action of $\sigma:\zeta\mapsto\zeta^k$ is given by $\sqrt{s}^{\sigma}=\left(\frac{s}{k}\right)\sqrt{s}$.

The third case also poses no problem as the essential quantity is the square root of a element of K. For this we have $\sqrt{\tau}=\zeta_8\eta(-1/\tau)/\eta(\tau)$ and the action follows from Shimura reciprocity.

The second case of $K=\mathbb{Q}(i)$ presents the greatest difficulty. In one approach, analogous to $\sqrt{s}\in\mathbb{Q}(\zeta_{4|s|})$, $t^{1/4}$ can be expressed explicitly as a modular function of level $48|t|$ (this needs to be checked,

the unambitious bound $256|t|^3$ is used below) evaluated at i, and the action of K^{ab}/K on $t^{1/4}$ can be determined via Shimura reciprocity:

$$2^{1/4} = \zeta_{48}^{-1}\frac{\eta(\frac{i+1}{2})}{\eta(i)},$$
$$3^{1/4} = \zeta_{12}^{-1}\frac{\eta(\frac{i+1}{3})^2}{\eta(i)^2}\frac{\eta(3i)}{\eta(\frac{3i-1}{2})}\frac{\eta(\frac{i+1}{2})}{\eta(i)},$$
$$5^{1/4} = \frac{x_5(i)+x_5(i)^{-1}}{2}\frac{\eta(\frac{i}{5})}{\eta(i)}, \quad x_5 \text{ defined by (4.9.2).}$$

However, there is no obvious pattern here and the approach quickly becomes intractable. Class field theory: the idele that we are using for mapping j_1 to $j_{a,b,c}$ via $j_1^{(z^{-1},K^{\mathrm{ab}}/K)} = j_{a,b,c}$ is given by $(z_p)_p$ where the components are defined in (7.7.1). One can then find an $x \in K^*$ with $xz^{-1} \equiv 1 \mod \mathfrak{c}$, where modulus $\mathfrak{c}$ can be taken as $-256t^3$ since this is the discriminant of the polynomial $X^4 - t$. Mapping xz^{-1} to an ideal (xz^{-1}) via

$$(xz^{-1}) = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(xz_{\mathfrak{p}}^{-1})}$$

gives an ideal prime to $\mathfrak{c}$, hence the action can be determined from the relevant $\mathrm{Frob}_{\mathfrak{p}}(K(t^{1/4})/K)$ (only $\mathfrak{p}$ prime to $\mathfrak{c}$ are relevant).

We now have formulas for the conjugates of $X_1^{1/24}$ (or $X_1^{1/12}$ in rare cases when $t^{1/4} \notin K^{\mathrm{ab}}$) assuming it lies in $\mathbb{Q}(j_1)$. If the assumption is wrong, the corresponding monic polynomial of degree h will not have integer coefficients, and we try again with a higher power of $X_1^{1/24}$. This must eventually succeed because $X_1 \in \mathbb{Q}(j_1)$. In order to be completely rigorous numerically, it must be pointed out that non-integrality can be detected and proven, but integrality cannot be proven numerically. Therefore, when the numerics strongly suggest that the coefficients are integers, we can invoke Theorem 7.7.3 to most likely prove that the given power of $X_1^{1/24}$ is in $\mathbb{Q}(j_1)$; we just need to check the action of the finite group $\mathfrak{o}/N\mathfrak{o}$ where N is the level of the function in (7.8.3).

Chapter 8

Hypergeometric Functions

8.1 Basic Properties of the ${}_2F_1(x)$ and ${}_3F_2(x)$ Series

Proposition 8.1.1. *The formula* (4.9.3) *is correct for* $N = 2, 3, 4, 5$ *at least for* $-i\tau > 0$ *(so* $j(\tau) > 1728$*).*

8.2 Jacobi's Inversion Formula and Generalizations

8.3 Solution of the General Quintic by Modular Functions

From Proposition 4.9.5,

$$j = \frac{(x^{20} + 228x^{15} + 494x^{10} - 228x^5 + 1)^3}{x^5(x^{10} - 11x^5 - 1)^5} \tag{8.3.1}$$

where j is the j function and x_5 is the Hauptmodul for $\Gamma(5)$ defined in (4.9.2) (the reciprocal of the Rogers-Ramanujan continued fraction). The solution for x as a function of j in this equation is the basic irrationality that can be used to resolve the simple group $A_5/1$ in the normal series

$$1 \triangleleft A_5 \triangleleft S_5$$

for S_5. The factor group $S_5/A_5 \simeq \mathbb{Z}_2$ corresponds to taking the square root of the discriminant of the quintic.

Proposition 8.3.1. *Let* $F = \mathbb{Q}(a, b, c, \zeta_5)$*. The splitting field of the quintic* $X^4 + 5\alpha X^2 + 5\beta X + \gamma$ *is* $F(\sqrt{D}, x)$ *where* D *is the discriminant of the quintic and*

$$x = \frac{j^{\frac{1}{60}}\, {}_2F_1\left(\begin{matrix} -\frac{1}{60}, \frac{29}{60} \\ \frac{4}{5} \end{matrix} \middle| \frac{1728}{j} \right)}{j^{-\frac{11}{60}}\, {}_2F_1\left(\begin{matrix} \frac{11}{60}, \frac{31}{60} \\ \frac{6}{5} \end{matrix} \middle| \frac{1728}{j} \right)}$$

and j *is some element of* $F(\sqrt{D})$*.*

Proof. Let $X_0, \ldots, X_4$ be the roots of the quintic, and let $\sqrt{D} = \prod_{i<j}(X_i - X_j)$ denote a fixed square root of the discriminant (D is not a square in F). Then, $\mathrm{Gal}(F(X_0, \ldots, X_4)/F(\sqrt{D})) \subseteq A_5$.

Let $\mathbb{I}_{60}$ denote the group of Möbius transformation on $\mathbb{C}_\infty$ giving the 60 symmetries of the regular icosahedron. We have already seen

$$\mathbb{I}_{60} \simeq \overline{\Gamma}(1)/\overline{\Gamma}(5) \simeq A_5,$$

with the correspondence on generators given by

element of $\mathbb{I}_{60}$	element of $\overline{\Gamma}(1)/\overline{\Gamma}(5)$	element of A_5
$x \mapsto \zeta_5^{-1} x$	$T\ \overline{\Gamma}(5)$	$\tau = (01234)$
$x \mapsto \frac{\phi x - 1}{x - \phi}$	$S\ \overline{\Gamma}(5)$	$\sigma = (12)(34)$

,

where $\phi = \frac{1+\sqrt{5}}{2}$ and $\bar{\phi} = \frac{1-\sqrt{5}}{2}$. For any $\pi \in A_5$, let M_π denote the corresponding element of $\mathbb{I}_{60}$. Set (for $i = 0, \ldots, 4$)

$$t_i = \sum_{j=0}^{4} \zeta_5^{ij} X_j.$$

Then, the action of A_5 on the t_i is

$$\tau \begin{pmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix} = \begin{pmatrix} \zeta_5^4 & 0 & 0 & 0 \\ 0 & \zeta_5^3 & 0 & 0 \\ 0 & 0 & \zeta_5^2 & 0 \\ 0 & 0 & 0 & \zeta_5^1 \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix},$$

$$\sigma \begin{pmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & -\bar{\phi} & \phi & -1 \\ -\bar{\phi} & -1 & 1 & \phi \\ \phi & 1 & -1 & -\bar{\phi} \\ -1 & \phi & -\bar{\phi} & 1 \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \end{pmatrix}.$$

Next, note that that vanishing of the coefficients of X^4 and X^3 gives $0 = t_0 = t_1 t_4 + t_2 t_3$, and set

$$\begin{aligned} x &= -\frac{t_2}{t_1} = +\frac{t_4}{t_3}, \\ \bar{x} &= +\frac{t_3}{t_1} = -\frac{t_4}{t_2}. \end{aligned} \tag{8.3.2}$$

The action of A_5 on x and $\bar{x}$ is given by

$$\begin{aligned} \tau(x) &= \zeta_5^{-1} x, \quad \sigma(x) = \frac{\phi x - 1}{x - \phi}, \\ \tau(\bar{x}) &= \zeta_5^{-2} \bar{x}, \quad \sigma(\bar{x}) = \frac{\bar{\phi}\bar{x} - 1}{\bar{x} - \bar{\phi}}. \end{aligned} \tag{8.3.3}$$

This means that the corresponding values of j and $\bar{j}$ (see (8.3.1)) are fixed by σ and τ, hence elements of $F(\sqrt{D})$. Since x was defined in terms of the X_i rationally over F, we have $F(\sqrt{D}, x) \subseteq F(X_0, X_1, X_2, X_3, X_4)$.

In order to establish the proposition, we must show that each X_i can be obtained as an element of $F(\sqrt{D}, x)$. Once we know x and $\bar{x}$, we know the ratios of the t_i by (8.3.2). Hence the ratios of the roots X_i are known since they are the inverse Fourier transform of the t_i and $t_0 = 0$. Once we know the ratios of the roots we know the roots because of the equation

$$\frac{1}{X_0} + \frac{1}{X_1} + \cdots + \frac{1}{X_4} = -\frac{5\beta}{\gamma},$$

so it suffices to demonstrate that $\bar{x}$ is an element of $F(\sqrt{D}, x)$. The reason for this lies in (8.3.3). Every transformation in $\mathbb{I}_{60}$ is defined over $\mathbb{Q}(\zeta_5)$. Therefore, for a given $M \in \mathbb{I}_{60}$, if $\overline{M}$ denotes M with the automorphism $\zeta_5 \mapsto \zeta_5^2$ applied, then we have

$$\pi(x) = M_\pi(x) \implies \pi(\bar{x}) = \overline{M}_\pi(\bar{x}), \quad \pi \in A_5, \tag{8.3.4}$$

since this holds on generators. Now let $M_1, \cdots, M_{60}$ denote the elements of $\mathbb{I}_{60}$ so that $\{M_i(x)\}_i$ is a list of conjugates of x under A_5. Since (8.3.1) has disinct roots as long as $j \neq 0, 1728, \infty$, this list contains 60 distinct elements. From (8.3.4) we see that $\{M_i(x)\}_i$ and $\{\overline{M}_i(\bar{x})\}_i$ are permuted identically under A_5, that is

$$\pi(M_i(x)) = M_j(x) \implies \pi(\overline{M}_i(\bar{x})) = \overline{M}_j(\bar{x}), \quad \pi \in A_5.$$

This means that the solutions for the a_k in the linear system

$$\overline{M}_i(\bar{x}) = \sum_{k=1}^{60} a_k M_i(x)^{k-1}, \quad i = 1, \ldots, 60$$

are all fixed by A_5 hence elements of $F(\sqrt{D})$. □

Remark 8.3.2. *It is possible to be much more explicit about the relationship between x and $\bar{x}$. In fact, we have*

$$\frac{\sqrt{x^{11} - 11x^6 - x}}{\sqrt{j - 1728}} \frac{(7x^5 - 1)\bar{x} + x^7 + 7x^2}{(x^{13} + 39x^8 - 26x^3)\bar{x} - 26x^{10} - 39x^5 + 1} \in F(\sqrt{D}).$$

See [7].

Remark 8.3.3. *This gives a solution to quintics with a missing x^4 and x^3 term. Unfortunately, it is not possibly to transform the general quintic to this form without introducing an accesory irrationality of degree 2. The modular equation (8.3.1) is simply too rigid to support a rational transformation in general. In a similar fashion, seventh degree equations with groups of order 168 can be resolved with the basic irrationality*

$$x = \frac{j^{\frac{1}{42}} \, {}_3F_2\left(\begin{matrix} -\frac{1}{42}, \frac{13}{42}, \frac{9}{14} \\ \frac{4}{14}, \frac{6}{14} \end{matrix} \middle| \frac{1728}{j} \right) j^{-\frac{5\cdot 2}{42}} \, {}_3F_2\left(\begin{matrix} \frac{5}{42}, \frac{19}{42}, \frac{11}{14} \\ \frac{5}{14}, \frac{8}{14} \end{matrix} \middle| \frac{1728}{j} \right)^2}{j^{-\frac{17\cdot 3}{42}} \, {}_3F_2\left(\begin{matrix} \frac{17}{42}, \frac{31}{42}, \frac{15}{14} \\ \frac{9}{14}, \frac{10}{14} \end{matrix} \middle| \frac{1728}{j} \right)^3}.$$

Here, the degree of the accessory irrationality need to transformation the general seventh degree of order 168 to this form is now four.

Chapter 9

Mock Modular Forms

Bibliography

[1] G. Andrews, B. C. Berndt, Ramanujan's Lost Notebook, Part III.

[2] T. M. Apostol, Modular Functions and Dirichlet Series in Number Theory, 2nd ed., New York: Springer-Verlag, 1997.

[3] A. O. L. Atkin, J. N. O'Brien, Some properties of $p(n)$ and $c(n)$ modulo powers of 13. Trans. Amer. Math. Soc. 126 (1976), 442-459.

[4] Borwein, J. M. and Borwein, P. B., A cubic counterpart of Jacobi's identity and the AGM, Trans. Amer. Math. Soc. 323 (1991), 691-701.

[5] S. Cooper, G. Jinqi, and Y. Dongxi, Hypergeometric transformation formulas of degrees 3, 7, 11 and 23, Journal of Mathematical Analysis and Applications, 421 2, Jan. (2015) 1358–1376.

[6] F. Diamond, J. Shurman, A First Course in Modular Forms, New York: Springer-Verlag, 2005.

[7] P. Gordon. Ueber die Auflösung der Gleichungen vom fünften Grade. Math. Ann., 13:375–404, 1869.

[8] T. Horie, N. Kanou, Certain Modular Functions Similar to the Dedekind eta Function, Abh. Math. Sem. Univ. Hamburg 72 (2002), 89-117.

[9] N. Ishida, Generators and equations for modular function fields of principal congruence subgroups, Acta Arithmetica LXXXV.3 (1998)

[10] M. I. Knopp, Modular Function in Analytic Number Theory, 2nd ed., Chelsea, New York, 1993.

[11] D. Kubert and S. Lang, Modular Units, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, New York-Berlin, 1981.

[12] R. S. Kulkarni, An arithmetic geometric method in the study of the subgroups of the modular group, American Journal of Mathematics 113 (1991), no. 6, 1053–1133.

[13] C. A. Kurth, L. Long, Computations with Finite Index Subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ using Farey Symbols.

[14] A. Lubotzky, Counting Finite Index Subgroups.

[15] M. Newman, Asymptotic formulas related to free products of cyclic groups, Math. Comp. 30 (1976), 838–846

[16] M. Newman, Classification of normal subgroups of the modular group.

[17] D. Mumford, Tata Lectures on Theta I.

[18] S. A. Vidal, Sur le classification et le dénombrement des sous-groupes du groupe modulaire et de leurs classes de conjugaison. Pub. IRMA, Lille 66(II):1-35, 2006. Preprint:http://arxiv.org/abs/math.CO/0702223

[19] D. Goldfeld, A. Lubotzky, L. Pyber, Counting Congruence Subgroups, Acta Mathematica, 2004, Volume 193, Issue 1, pp 73-104

[20] T. Hsu, IDENTIFYING CONGRUENCE SUBGROUPS OF THE MODULAR GROUP. Proc. Amer. Math. Soc. (124), no. 5, May 1996