Chapter 29

Classical modular group

In this section, we introduce the classical modular group $\mathrm{SL}_2(\mathbb{Z})$, examine the hyperbolic quotient in detail, and we discuss some arithmetic applications.

29.1 The fundamental domain

The *classical modular group* is the group

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

The group $\mathrm{PSL}_2(\mathbb{Z})$ acts faithfully on the upper half-plane $\mathbf{H}^2$ by linear fractional transformations, and moreover when equipped with the hyperbolic metric this action is by orientation-preserving isometries.

Since $\mathbb{Z} \subseteq \mathbb{R}$ is discrete, so too is $\mathrm{SL}_2(\mathbb{Z}) \subseteq \mathrm{M}_2(\mathbb{Z}) \subseteq \mathrm{M}_2(\mathbb{R})$ discrete, and therefore $\mathrm{PSL}_2(\mathbb{Z}) \leq \mathrm{PSL}_2(\mathbb{R})$ is a Fuchsian group. Therefore, by Proposition 28.5.2, the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbf{H}^2$ is wandering and proper. [[We actually prove this below by direct computation, so maybe this chapter should move.]]

Our first order of business is to try to understand the structure of the classical modular group in terms of this action. Let

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}).$$

Then $Sz = -1/z$ for $z \in \mathbf{H}^2$, so S maps the unit circle $\{z \in \mathbb{C} : |z| = 1\}$ to itself, fixing the point $z = i$; and $Tz = z + 1$ for $z \in \mathbf{H}^2$ acts by translation. We compute that $S^2 = 1$ (in $\mathrm{PSL}_2(\mathbb{Z})$) and

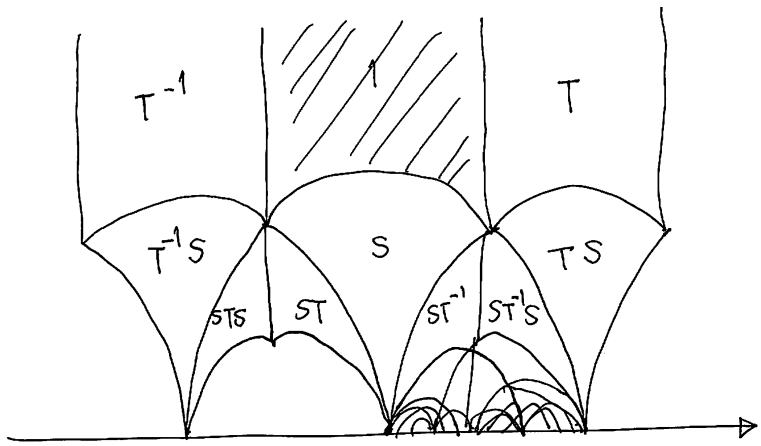
$$ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

so $(ST)^3 = 1$.

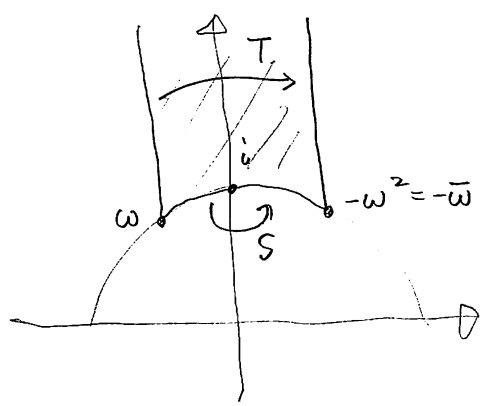
In a moment, we will see that $\mathrm{PSL}_2(\mathbb{Z})$ is generated by S, T, with a minimal set of relations given by $S^2 = (ST)^3 = 1$. To do so, we examine a fundamental set (cf. Definition 28.1.13) for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbf{H}^2$, as follows. Let

$$\text{¤} = \{z \in \mathbf{H}^2 : |\mathrm{Re}\, z| \leq 1 \text{ and } |z| \geq 1\}.$$

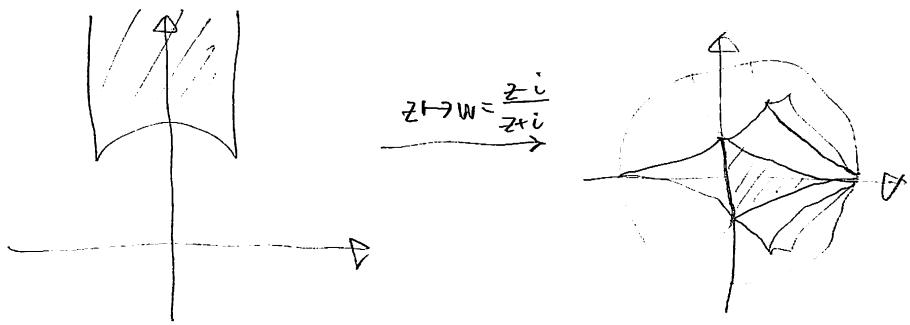
The set ¤ is a hyperbolic triangle with vertices at $\omega = (-1 + \sqrt{-3})/2$ and $-\omega^2 = (1 + \sqrt{-3})/2$ and ∞. Its translates by words in S, T looks as follows:



By the Gauss–Bonnet Theorem 27.5.5 (or Exercise 29.1), the hyperbolic area of ¤ is $\pi - 2(\pi/3) = \pi/3$. The elements S, T act on the edges of this triangle as follows.



In the unit disc, the triangle ¤ looks like this:



The following three lemmas describe the relationship of the set ⌑ to Γ.

Lemma 29.1.1. *For all $z \in \mathsf{H}^2$, there exists a word $\gamma \in \langle S, T \rangle$ such that $\gamma z \in$ ⌑.*

Proof. In fact, we can determine such a word algorithmically. First, we translate z so that $|\operatorname{Re} z| \leq 1/2$. If $|z| \geq 1$, we are done; otherwise, if $|z| < 1$, then

$$\operatorname{Im}\left(\frac{-1}{z}\right) = \frac{\operatorname{Im} z}{|z|^2} > \operatorname{Im} z. \tag{29.1.2}$$

We then repeat this process, obtaining a sequence of elements $z = z_1, z_2, \ldots$ with $\operatorname{Im} z_1 < \operatorname{Im} z_2 < \ldots$. We claim that this process terminates after finitely many steps. Indeed, we have (27.2.8)

$$\operatorname{Im}(gz) = \frac{\operatorname{Im} z}{|cz+d|^2}, \text{ for } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{R}),$$

and the number of $c, d \in \mathbb{Z}$ such that $|cz + d| < 1$ is finite: the set $\mathbb{Z} + \mathbb{Z}z \subseteq \mathbb{C}$ is a lattice, so there are only finitely many elements of bounded norm. Upon termination, we have found a word γ in S, T such that $\gamma z \in$ ⌑. □

The procedure described in the proof of Lemma 29.1.1 is called a *reduction algorithm*.

Lemma 29.1.3. *Let $z, z' \in$ ⌑, and suppose $z \in \operatorname{int}($⌑$)$ lies in the interior of ⌑. If $z' = \gamma z$ with $\gamma \in \Gamma$, then $\gamma = 1$ and $z = z'$.*

Proof. Let $z' = \gamma z$ with $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. We have $\operatorname{Im} z' = (\operatorname{Im} z)/|cz+d|^2$. First suppose that $\operatorname{Im} z' \geq \operatorname{Im} z$; then

$$|cz+d|^2 = (c \operatorname{Re} z + d)^2 + c^2 (\operatorname{Im} z)^2 \leq 1. \tag{29.1.4}$$

Since $\operatorname{Im} z > \operatorname{Im} \omega = \sqrt{3}/2$, from (29.1.4) we conclude that $c^2 \leq 4/3$ so $|c| \leq 1$. If $c = 0$ then $ad - bc = ad = 1$ so $a = d = \pm 1$, and then $z' = \gamma z = z \pm b$, which immediately implies $b = 0$ so $\gamma = 1$ as claimed. If instead $|c| = 1$, then the conditions

$$(c\operatorname{Re} z + d)^2 \leq 1 - (\operatorname{Im} z)^2 \leq 1 - 3/4 = 1/4 \quad \text{and} \quad |\operatorname{Re} z| < 1/2$$

together imply $d = 0$; but then $|cz + d| = |z| \leq 1$, and since $z \in \operatorname{int}(\mathrm{¤})$ we have $|z| > 1$, a contradiction.

If instead $\operatorname{Im} z' < \operatorname{Im} z$, we interchange the roles of z, z' and have strict inequality in (29.1.4); by the same argument and the weaker inequality $|\operatorname{Re} z| \leq 1/2$, we then obtain $|z| < 1$, a contradiction. □

Lemma 29.1.5. *The elements S, T generate $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$.*

Proof. Let $z_0 = 2i \in \operatorname{int}(\mathrm{¤})$. Let $\gamma \in \Gamma$, and let $z' = \gamma z$. By Lemma 29.1.1, there exists γ' a word in S, T such that $\gamma' z' \in \mathrm{¤}$. By Lemma 29.1.3, we have $\gamma' z' = (\gamma'\gamma)z = z$, so $\gamma'\gamma = 1$ and $\gamma = \gamma' \in \langle S, T\rangle$. □

Although we have worked in $\mathrm{PSL}_2(\mathbb{Z})$ throughout, it follows from Lemma 29.1.5 that the matrices S, T also generate $\mathrm{SL}_2(\mathbb{Z})$, since $S^2 = -1$.

The following corollary is an immediate consequence of Lemmas 29.1.1 and 29.1.3.

Corollary 29.1.6. *The set ¤ is a fundamental set for $\mathrm{PSL}_2(\mathbb{Z}) \circlearrowright \mathbf{H}^2$.*

29.1.7. If $z \in \mathrm{¤}$ has $\operatorname{Stab}_\Gamma(z) \neq \{1\}$, then we claim that one of the following holds:

(i) $z = i$, and $\operatorname{Stab}_\Gamma(i) = \langle S\rangle \simeq \mathbb{Z}/2\mathbb{Z}$;

(ii) $z = \omega$, and $\operatorname{Stab}_\Gamma(\omega) = \langle ST\rangle \simeq \mathbb{Z}/3\mathbb{Z}$; or

(iii) $z = -\omega^2$, and $\operatorname{Stab}_\Gamma(-\omega^2) = \langle TS\rangle = T\operatorname{Stab}_\Gamma(\omega)T^{-1}$.

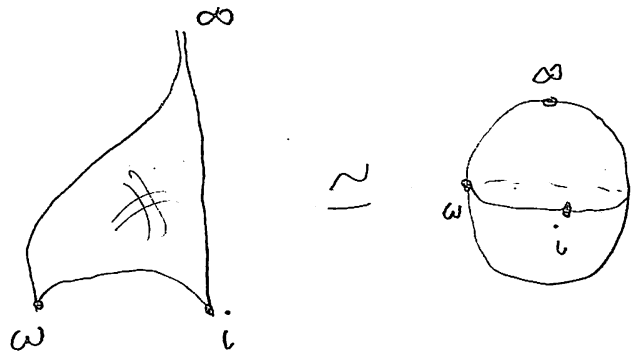
Indeed, let $\gamma z = z$ with $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\gamma \neq 1$. Then $cz^2 + (d-a)z - b = 0$, so $c \neq 0$ and

$$z = \frac{(a-d) + \sqrt{D}}{2c} \quad \text{where } D = \operatorname{Tr}(\gamma)^2 - 4 \in \mathbb{Z}_{<0}.$$

Thus we have $D = -4$ or $D = -3$. In either case, since $z \in \mathrm{¤}$ we have $\operatorname{Im} z \geq \sqrt{3}/2$, we must have $c = \pm 1$, and replacing $\gamma \leftarrow -\gamma$ we may take $c = 1$. If $D = -4$, then $\operatorname{Tr}(\gamma) = a + d = 0$ so $z = a + i$, and so $a = 0 = d$ and $c = 1 = -b$, i.e., $z = i$ and we have case (i). If the discriminant is -3, then a similar argument gives $z = ((a \pm 1) + \sqrt{-3})/2$ so $a = 0$, and we are in cases (ii) or (iii).

Let $Y = \Gamma\backslash\mathbf{H}^2$. Gluing together the fundamental set, we obtain a homeomorphism

$$Y = \Gamma\backslash\mathbf{H}^2 \simeq \mathbb{P}^1(\mathbb{C}) - \{\infty\} \simeq \mathbb{C}.$$



The orbit of the limit point ∞ under Γ is $\mathbb{P}^1(\mathbb{Q}) \subseteq \partial\mathbf{H}^2$, so letting $\mathcal{H}^* = \mathbf{H}^2 \cup \mathbb{P}^1(\mathbb{Q})$, we have a homeomorphism

$$X = \Gamma\backslash\mathcal{H}^* \simeq \mathbb{P}^1(\mathbb{C}).$$

Away from the orbits $\Gamma i, \Gamma\omega$ with nontrivial stabilizer, the complex structure on $\mathbf{H}^2$ descends and gives the quotient $Y - \{\Gamma i, \Gamma\omega\}$ the structure of a Riemann surface. By studying the moduli of lattices, later we will give an explicit holomorphic identification $j : Y \to \mathbb{C}$.

29.2 Binary quadratic forms

We pause to give an application to quadratic forms and class groups, following Gauss. An *(integral) binary quadratic form*, abbreviated in this section to simply *form*, is an expression $Q(x, y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$; we define the *discriminant* of a form Q to be $d = \mathrm{disc}(Q) = b^2 - 4ac$. A form Q is *primitive* if $\gcd(a, b, c) = 1$, and Q is *positive definite* if $Q(x, y) > 0$ for all nonzero $(x, y) \in \mathbb{R}^2$; after completing the square, we see that a form is positive definite if and only if $a > 0$ and $d < 0$. For a negative discriminant $d < 0$, let

$$\mathcal{Q}_d = \{Q(x, y) = ax^2 + bxy + cy^2 : a > 0,\ \mathrm{disc}(Q) = d\}$$

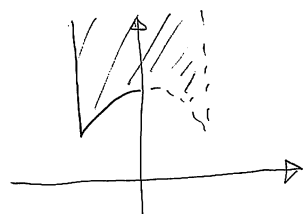
be the set of primitive, positive definite forms of discriminant d. The group Γ acts on $\mathcal{Q}_d$ the right by change of variable: for $\gamma \in \Gamma$, we define $(Q^\gamma)(x, y) = Q((x, y)\gamma)$, and verify that $\mathrm{disc}(Q^\gamma) = \mathrm{disc}(Q) = d$. We say that Q, Q' are *equivalent* if $Q' = Q^\gamma$ for some $\gamma \in \Gamma$.

We claim that the number of equivalence classes $h(d) = \#\mathcal{Q}_d/\Gamma$ is finite. Indeed, to any $Q \in \mathcal{Q}_d$, we associate the unique root

$$z_Q = \frac{-b + \sqrt{|d|}i}{2a} \in \mathbf{H}^2$$

of $Q(z, 1) = 0$. Then $z_{Q^\gamma} = \gamma^{-1}(z)$ for $\gamma \in \Gamma$. Therefore, by the reduction theory of the previous section, we can replace Q up to equivalence by a form such that $z_Q \in \mathcal{F}$.

If we further insist that $\operatorname{Re} z < 1/2$ and $\operatorname{Re} z < 0$ if $|z| = 1$, then this representative is unique.



Thus

$$-\frac{1}{2} \leq \operatorname{Re} z_Q = -\frac{b}{2a} < \frac{1}{2}$$

so $-a < b \leq a$, or equivalently,

$$|b| \leq a \text{ and } (b \geq 0 \text{ if } |b| = a);$$

and

$$|z_Q| = \frac{b^2 - d}{4a^2} = \frac{c}{a} \geq 1$$

so $a \leq c$ and $b \geq 0$ if equality holds. In sum, every positive definite form Q is equivalent to a ($\mathrm{SL}_2(\mathbb{Z})$-)*reduced* form satisfying

$$|b| \leq a \leq c \quad \text{with } b \geq 0 \text{ if } |b| = a \text{ or } a = c.$$

We now show that there are only finitely many reduced forms with given discriminant $d < 0$, i.e., that $h(d) < \infty$. The inequalities $|b| \leq a \leq c$ imply that

$$|d| = 4ac - b^2 \geq 3a^2,$$

so $a \leq \sqrt{|d|/3}$ and $|b| \leq a$, so there are only finitely many possibilities for a, b; and then $c = (b^2 - d)/(4a)$ is determined. This gives an efficient method to compute the set $\mathcal{Q}_d/\Gamma$ efficiently.

Let $S = \mathbb{Z} \oplus \mathbb{Z}[(d + \sqrt{d})/2] \subset K = \mathbb{Q}(\sqrt{d})$ be the quadratic ring of discriminant $d < 0$. Let $\operatorname{Pic}(S)$ be the group of invertible fractional ideals of S modulo principal ideals. Then there is a bijection

$$\begin{aligned} \mathcal{Q}_d/\Gamma &\leftrightarrow \operatorname{Pic}(S) \\ [ax^2 + bxy + cy^2] &\mapsto [\mathfrak{a}] = \left[\left(a, \frac{-b + \sqrt{d}}{2}\right)\right] \end{aligned}$$

(Exercise 29.7). So in the same stroke, we have proven the finiteness of the class number $\# \operatorname{Pic}(S) < \infty$.

29.3 Functions on lattices, and complex tori

In this section, we pursue an interpretation of the quotient $\Gamma\backslash\mathbf{H}^2$ with $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ as a moduli space of lattices.

A *lattice* $\Lambda \subset \mathbb{C}$ is a subgroup $\Lambda = \mathbb{Z}z_1 + \mathbb{Z}z_2$ with z_1, z_2 linearly independent over $\mathbb{R}$; the elements z_1, z_2 are a *basis* for Λ.

Two lattices Λ, Λ' are *homothetic* if there exists $u \in \mathbb{C}^\times$ such that $\Lambda' = u\Lambda$, and we write $\Lambda \sim \Lambda'$. Let $\Lambda = \mathbb{Z}z_1 + \mathbb{Z}z_2$ be a lattice. Then without loss of generality (interchanging z_1, z_2), we may assume $\mathrm{Im}(z_2/z_1) > 0$, and then we call z_1, z_2 an *oriented basis*. Then we have the homothety

$$\Lambda \sim z_1^{-1}\Lambda = \mathbb{Z} + \mathbb{Z}\tau$$

where $\tau = z_2/z_1 \in \mathbf{H}^2$; this representative of the homothety class is unique up to the action of Γ, as follows.

Lemma 29.3.1. *We have $\mathbb{Z} + \mathbb{Z}\tau \sim \mathbb{Z} + \mathbb{Z}\tau'$ with $\tau, \tau' \in \mathbf{H}^2$ if and only if $\Gamma\tau = \Gamma\tau'$.*

Proof. For $\tau, \tau' \in \mathbb{C} - \mathbb{R}$, we have $\mathbb{Z} + \mathbb{Z}\tau \sim \mathbb{Z} + \mathbb{Z}\tau'$ if and only if there exists $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ and $u \in \mathbb{C}^\times$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau \\ 1 \end{pmatrix} = u \begin{pmatrix} \tau' \\ 1 \end{pmatrix}$$

so $u(a\tau + b) = \tau'$ and $u(c\tau + d) = 1$. Eliminating u gives equivalently

$$\tau' = \frac{a\tau + b}{c\tau + d}.$$

Finally, if $\tau, \tau' \in \mathbf{H}^2$ then $g \in \mathrm{PSL}_2(\mathbb{Z})$, and conversely the action of Γ preserves $\mathbf{H}^2$; so since g is well-defined as an element of $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$, we have the result. $\square$

Therefore, we have a bijection

$$\begin{aligned} Y = \Gamma\backslash\mathbf{H}^2 &\to \{\Lambda \subset \mathbb{C} \text{ lattice}\}/\sim \\ \Gamma\tau &\mapsto [\mathbb{Z} + \mathbb{Z}\tau]; \end{aligned}$$

that is to say, $Y = \Gamma\backslash\mathbf{H}^2$ parametrizes complex lattices up to homothety.

To a lattice Λ, we associate the complex torus $\mathbb{C}/\Lambda$ (of rank 1); two such tori $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic as Riemann surfaces if and only if $\Lambda \sim \Lambda'$. Therefore, the space Y also parametrizes complex tori.

In particular, like Y, the set of homothety classes has a natural structure of a Riemann surface and we seek now to make this explicit. There are natural functions on lattices that allow us to go beyond a bijection and realize the complex structure on Y explicitly.

Let $\Lambda \subset \mathbb{C}$ be a lattice. To write down complex moduli, it is natural to average over Λ in a convergent way, as follows.

Definition 29.3.2. The *Eisenstein series* of weight $k \in \mathbb{Z}_{>2}$ for Λ to be

$$G_k(\Lambda) = \frac{1}{2} \sum_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} \frac{1}{\lambda^k}.$$

If k is odd, then $G_k(\Lambda) = 0$ identically, so let $k \in 2\mathbb{Z}_{\geq 2}$.

Lemma 29.3.3. *The series $G_k(\Lambda)$ converges absolutely.*

Proof. Up to homothety (which does not affect convergence), we may assume $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, with $\tau \in \mathbf{H}^2$. Then we consider the corresponding absolute sum

$$\sum_{\substack{\lambda \in \mathbb{Z}+\mathbb{Z}\tau \\ \lambda \neq 0}} \frac{1}{|\lambda|^k} = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{|m + n\tau|^k}. \tag{29.3.4}$$

The number of pairs (m, n) with $r \leq |m\tau + n| < r + 1$ is the number of lattice points in an annulus of area $\pi(r + 1)^2 - \pi r^2 = O(r)$, so there are $O(r)$ such points; and thus the series (29.3.4) is majorized by (a constant multiple of) $\sum_{r=1}^{\infty} r^{1-k}$, which is convergent for $k > 2$. □

29.3.5. For $z \in \mathbf{H}^2$ and $k \in 2\mathbb{Z}_{\geq 2}$, define

$$G_k(z) = G_k(\mathbb{Z} + \mathbb{Z}z) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m + nz)^k}.$$

Lemma 29.3.6. *$G_k(z)$ is holomorphic for $z \in \mathbf{H}^2$, and*

$$G_k(\gamma z) = (cz + d)^k G_k(z)$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z})$.

Proof. This is true for $z \in ¤$ since then

$$|m + nz|^2 = m^2 + 2mn \operatorname{Re} z + n^2|z|^2 \geq m^2 - mn + n^2 = |m + n\omega|^2$$

thus $|G_k(z)| \leq |G_k(\omega)|$ and so by the Weierstrass M-test, $G_k(z)$ is holomorphic for $z \in ¤$ (by Morera's theorem, uniformly convergence implies holomorphicity). But now for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, we claim that

$$G_k(\gamma z) = (cz + d)^k G_k(z)$$

(and note this does not depend on the choice of sign): indeed, we have

$$\frac{1}{m(gz) + n} = \frac{cz + d}{(am + cn)z + (bm + dn)}$$

and the map

$$(m,n) \mapsto (m,n)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (am+cn, bm+dn)$$

is a permutation of $\mathbb{Z}^2 - \{(0,0)\}$, so by absolute convergence we may rearrange the sum and we have

$$G_k(\gamma z) = (cz+d)^k G_k(z);$$

by transport, since $\Gamma\square = \mathbf{H}^2$, we see that $G_k(z)$ is holomorphic on all of $\mathbf{H}^2$. $\square$

29.3.7. To produce holomorphic functions that are well-defined on the quotient $\Gamma\backslash\mathbf{H}^2$, we can take ratios of Eisenstein series; in the next section, we exhibit a map

$$j : \mathbf{H}^2 \to \mathbb{C}$$

obtained in this way that defines a biholomorphic identification $\Gamma\backslash\mathbf{H}^2 \to \mathbb{C}$ (Theorem 29.4.13).

29.4 Classical modular forms

In the previous section, we saw that natural sums (Eisenstein series) defined functions on $\mathbf{H}^2$ that transformed with respect to $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ with a natural invariance. In this section, we pursue this more systematically.

Definition 29.4.1. Let $k \in 2\mathbb{Z}$. A map $f : \mathbf{H}^2 \to \mathbb{C}$ is *weight k invariant* under Γ if

$$f(\gamma z) = (cz+d)^k f(z) \quad \text{for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}). \tag{29.4.2}$$

29.4.3. Since $\mathrm{PSL}_2(\mathbb{Z})$ is generated by S, T, a map f is weight k invariant if and only if both

$$\begin{aligned} f(z+1) &= f(z) \\ f(-1/z) &= z^k f(z) \end{aligned}$$

for all $z \in \mathbf{H}^2$. Put a third way, since

$$\frac{\mathrm{d}(\gamma z)}{\mathrm{d}z} = \frac{1}{(cz+d)^2}$$

the weight k invariance (29.4.2) can be rewritten

$$f(\gamma z)\,\mathrm{d}(\gamma z)^{\otimes k} = f(z)\,\mathrm{d}z^{\otimes k}$$

so the expression $f(z)\,\mathrm{d}z^{\otimes k}$ is invariant under Γ.

Let $f : \mathbf{H}^2 \to \mathbb{C}$ be a meromorphic map that is weight k invariant under Γ. Then $f(z+1) = f(z)$, and *if* f admits a Fourier series expansion in $q = \exp(2\pi i z)$

$$f(z) = \sum_{n \gg -\infty}^{\infty} a_n q^n \in \mathbb{C}((q))$$

with $a_n \in \mathbb{C}$, then we say that f is *meromorphic* at ∞, and if further $a_n = 0$ for $n < 0$, we say f is *holomorphic* at ∞.

Definition 29.4.4. Let $k \in 2\mathbb{Z}$. A *meromorphic modular form of weight* k is a meromorphic map $f : \mathbf{H}^2 \to \mathbb{C}$ that is weight k invariant under Γ and meromophic at ∞. A *meromorphic modular function* is a meromorphic modular form of weight 0.

A *(holomorphic) modular form of weight* k is a holomorphic map $f : \mathbf{H}^2 \to \mathbb{C}$ that is weight k invariant under Γ and holomorphic at ∞.

Lemma 29.4.5. *The Eisenstein series $G_k(z)$ is a holomorphic modular form of weight $k \in 2\mathbb{Z}_{\geq 2}$ with Fourier expansion*

$$G_k(z) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

where

$$\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$$

and

$$\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}.$$

Proof. We start with the formula

$$\pi \cot(\pi z) = \sum_{m=-\infty}^{\infty} \frac{1}{z+m} = \lim_{M\to\infty} \sum_{m=-M}^{M} \frac{1}{z+m} \tag{29.4.6}$$

(Exercise 29.10); since

$$\cot(\pi z) = \frac{\cos(\pi z)}{\sin(\pi z)} = i\frac{q+1}{q-1} = i\left(1 + \frac{2}{q-1}\right)$$

we obtain the Fourier expansion

$$\pi \cot(\pi z) = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n. \tag{29.4.7}$$

Equating (29.4.6)–(29.4.7) and differentiating $k-1$ times, we find that

$$\sum_{m=0}^{\infty} \frac{1}{(m+z)^k} = \frac{1}{(k-1)!}(2\pi i)^k \sum_{n=1}^{\infty} n^{k-1} q^n \tag{29.4.8}$$

(since k is even). Thus

$$G_k(z) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m+nz)^k} = 2\zeta(k) + 2\sum_{n=1}^{\infty}\sum_{m=-\infty}^{\infty} \frac{1}{(m+nz)^k}$$

so replacing $n \leftarrow a$ in (29.4.8) and then substituting $z \leftarrow nz$, summing we obtain

$$\begin{aligned} G_k(z) &= 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{d=1}^{\infty}\sum_{a=1}^{\infty} d^{k-1}q^{ad} \\ &= 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\Big(\sum_{d|n} d^{k-1}\Big)q^n \end{aligned}$$

as claimed. The fact that G_k is holomorphic at ∞ then follows by definition. □

We accordingly define the *normalized Eisenstein series* by

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

where

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

(Exercise 29.11), and $B_k \in \mathbb{Q}^\times$ are *Bernoulli numbers*. We have

$$\begin{aligned} E_4(z) &= 1 + 240q + 2160q^2 + \dots \\ E_6(z) &= 1 - 504q - 16632q^2 + \dots \end{aligned}$$

29.4.9. A meromorphic modular function descends to a function on $\Gamma\backslash\mathbf{H}^2 = Y$; although this is not true for forms of weight $k \neq 0$, the order of pole or zero $\operatorname{ord}_z(f)$ is well defined on the orbit Γz. The order of the stabilizer $e_z = \#\operatorname{Stab}_\Gamma(z)$ is well defined on the orbit Γz, since points in the same orbit have conjugate stabilizers.

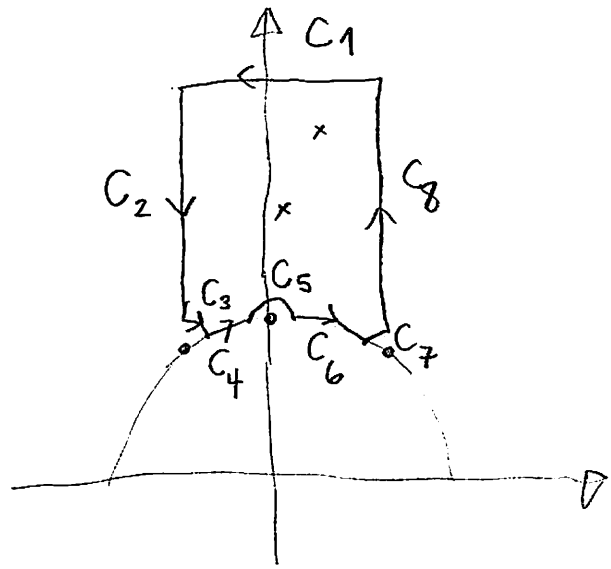
If f is a meromorphic modular form, then f has only a finite number of zeros or poles in Y (i.e., only finitely many Γ-orbits of zeros or poles): indeed, since f is meromorphic at ∞, there exists $\epsilon > 0$ such that f has no zero or pole with $0 < |q| < \epsilon$, i.e., with $\operatorname{Im} z > M = \log(1/\epsilon)/(2\pi)$; but the part of ¤ with $\operatorname{Im} z \leq M$ is compact, and since f is meromorphic in $\mathbf{H}^2$, it has only a finite number of zeros or poles.

Proposition 29.4.10. *Let $f : \mathbf{H}^2 \to \mathbb{C}$ be a meromorphic modular function of weight k, not identically zero. Then*

$$\operatorname{ord}_\infty(f) + \sum_{\Gamma z \in \Gamma\backslash\mathbf{H}^2} \frac{1}{e_z}\operatorname{ord}_z(f) = \frac{k}{12}. \tag{29.4.11}$$

The sum in Proposition 29.4.11 makes sense, by Paragraph 29.4.9.

Proof. To prove this theorem, we perform a contour integration $\frac{1}{2\pi i}\frac{\mathrm{d}f}{f}$ on the boundary of ⌑. More precisely, first assume that f has neither zero nor pole on the boundary of ⌑ except possibly at $i, \omega, -\omega^2$. We consider the contour C containing all zeros or poles of f in $\mathrm{int}(⌑)$:



By the argument principle, we have

$$\frac{1}{2\pi i}\int_C \frac{\mathrm{d}f}{f} = \sum_{z\in\mathrm{int}(⌑)} \mathrm{ord}_z(f).$$

We write C as the sum of several contours as indicated. In the change of variable $z \mapsto q = e^{2\pi i z}$, the contour C_1 transforms into a circle centered at $q = 0$ with negative orientation whose only enclosed zero or pole is ∞. Thus

$$\frac{1}{2\pi i}\int_{C_1} = -\,\mathrm{ord}_\infty(f).$$

We have $T^{-1}(C_8) = C_2$ with opposite orientation; since $f(z+1) = f(z)$, these contributions cancel. On C_3, as the radius of this arc of a circle tends to 0, we have

$$\frac{1}{2\pi i}\int_{C_2} \frac{\mathrm{d}f}{f} \to \frac{1}{2\pi i}\left(\frac{-\pi i}{3}\right) = -\frac{1}{6}$$

as the angle formed with ω by the endpoints of C_2 is $\pi/3$ (Exercise 29.8). Similarly,

$$\frac{1}{2\pi i}\int_{C_5} \frac{\mathrm{d}f}{f} \to -\frac{1}{2} \quad \text{and} \quad \frac{1}{2\pi i}\int_{C_7} \frac{\mathrm{d}f}{f} \to -\frac{1}{6}.$$

Finally, we have $S(C_6) = C_4$ with opposite orientation; but now $f(Sz) = z^k f(z)$ so

$$\frac{\mathrm{d}f(Sz)}{\mathrm{d}z} = kz^{k-1}f(z) + z^k\frac{\mathrm{d}f(z)}{\mathrm{d}z}$$

and hence

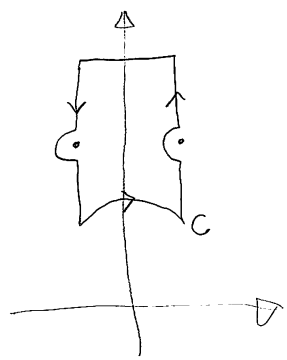
$$\frac{\mathrm{d}f(Sz)}{f(Sz)} = k\frac{\mathrm{d}z}{z} + \frac{\mathrm{d}f(z)}{f(z)},$$

and thus taking the difference we obtain

$$\frac{1}{2\pi i}\int_{C_4\cup C_6}\frac{\mathrm{d}f}{f} = \frac{1}{2\pi i}\int_{C_4} -k\frac{\mathrm{d}z}{z} \to \frac{-k}{2\pi i}\left(\frac{-\pi i}{6}\right) = \frac{k}{12}$$

as the angle formed with 0 is now $\pi/6$. Summing, we obtain the result.

If f has a zero or pole on the boundary of $\mathfrak{F}$, we repeat the same argument with a contour modified as follows:



The details are requested in Exercise 29.9. □

29.4.12. We have $E_4(STz) = (z+1)^4 E_4(z)$, so since $(ST)(\omega) = \omega$, we have

$$E_4(\omega) = (\omega+1)^4 E_4(\omega) = \omega^2 G_4(\omega)$$

so $E_4(\omega) = 0$. By Proposition 29.4.10, we conclude that $E_4(z)$ has no other zeros (or poles) in $\mathfrak{F}$. Similarly,

$$E_6(i) = E_6(Si) = i^6 E_6(i) = -E_6(i)$$

so $E_6(i) = 0$ and $E_6(z)$ has no other zeros.

For the same reason, the function

$$\Delta(z) = \frac{E_4(z)^3 - E_6(z)^2}{1728} = q - 24q^2 + 252q^3 - \dots$$

is a modular form of weight 12 with no zeros in $\mathbf{H}^2$.

Theorem 29.4.13. *The function*

$$j(z) = \frac{E_4(z)^3}{\Delta(z)} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots$$

is a meromorphic modular function, holomorphic in $\mathbf{H}^2$*, defining a biholomorphic identification*

$$Y = \Gamma\backslash\mathbf{H}^2 \to \mathbb{C}.$$

Proof. The function j is weight 0 invariant under Γ as the ratio of two forms that are weight 12 invariant. Since E_4 is holomorphic in $\mathbf{H}^2$, and Δ is holomorphic and has no zeros in $\mathbf{H}^2$, the ratio is holomorphic. We have that $j(z)$ has a simple pole at $z = \infty$, corresponding to a simple zero of Δ at $z = \infty$. We have $j(i) = 1728$, and $j(z) - 1728$ has a double zero at i, and $j(\omega) = 0$ is a triple zero.

To conclude that j defines a biholomorphic identification, we show that $j(z) - c$ has a unique zero $\Gamma z \in Y$. If $c \neq 0, 1728$, this follows immediately from Proposition 29.4.10; if $c = 0, 1728$, the results follow for the same reason from the multiplicity of the zero. □

29.5 Congruence subgroups

The finite-index subgroups of $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ play a central role in what follows, and of particular importance are those subgroups defined by congruence conditions on the entries.

Definition 29.5.1. Let $N \in \mathbb{Z}_{\geq 1}$. The *congruence subgroup* $\Gamma(N) \trianglelefteq \Gamma$ of *level* N is

$$\begin{aligned}\Gamma(N) &= \ker(\mathrm{PSL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})) \\ &= \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) : a \equiv d \equiv \pm 1 \pmod{N},\ b \equiv c \equiv 0 \pmod{N}\right\} \\ &= \left\{\gamma \in \mathrm{PSL}_2(\mathbb{Z}) : \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}\right\}.\end{aligned}$$

To avoid confusion, we will now write $\Gamma(1) = \mathrm{PSL}_2(\mathbb{Z})$.

29.5.2. By strong approximation for $\mathrm{SL}_2(\mathbb{Z})$ (Theorem 24.1.1), the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective for all $N \geq 1$, so we have an exact sequence

$$1 \to \Gamma(N) \to \Gamma(1) \to \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z}) \to 1.$$

Definition 29.5.3. A subgroup $\Gamma \leq \Gamma(1)$ is a *congruence subgroup* if $\Gamma \geq \Gamma(N)$ for some $N \geq 1$.

29.5.4. In addition to the congruence groups $\Gamma(N)$ themselves, we will make use of two other important congruence subgroups for $N \geq 1$:

$$\begin{aligned}\Gamma_0(N) &= \left\{\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N}\right\} \\ &= \left\{\gamma \in \mathrm{PSL}_2(\mathbb{Z}) : \gamma \equiv \pm \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N}\right\} \\ \Gamma_1(N) &= \left\{\gamma \in \mathrm{PSL}_2(\mathbb{Z}) : \gamma \equiv \pm \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N}\right\}\end{aligned} \tag{29.5.5}$$

Visibly, we have $\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N)$.

In the remainder of this section, we consider as an extended example the case $N = 2$. We can equally well write

$$\Gamma(2) = \left\{\pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) : b \equiv c \equiv 0 \pmod{2}\right\}$$

We have

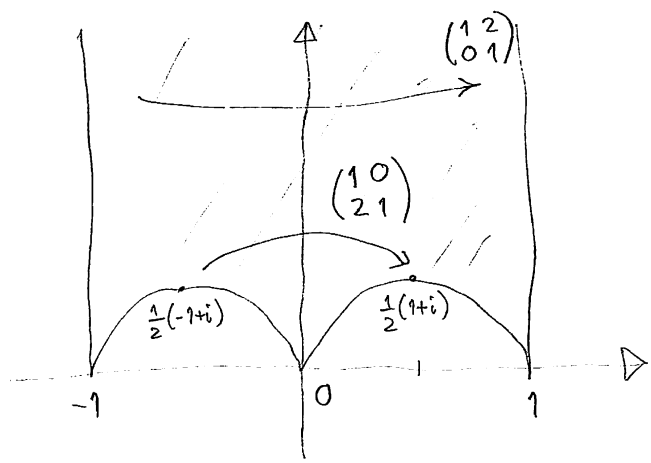
$$\Gamma(1)/\Gamma(2) \simeq \mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z}) = \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$$

the nonabelian group of order 6, so in particular $[\Gamma(1) : \Gamma(2)] = 6$.

We can uncover the structure of the group $\Gamma(2)$ in a manner similar to what we did for $\Gamma(1)$ in section 29.1—the details are requested in Exercise 29.12. The group $\Gamma(2)$ is generated by

$$T^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

which act on $\mathcal{H}$ by $z \mapsto z + 2$ and $z \mapsto z/(2z + 1)$, respectively, and a fundamental set ⌑ is given by

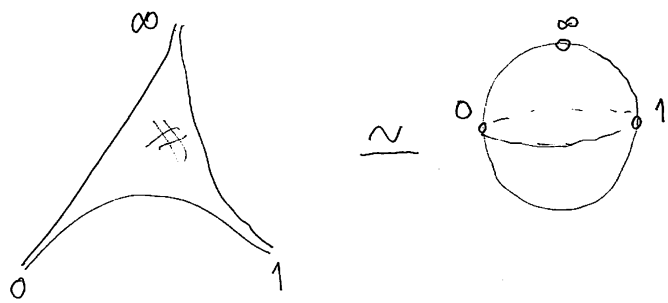


(In fact, later we will see from more general structural results on fundamental domains that $\Gamma(2)$ is freely generated by these two elements, so it is isomorphic to the free group on two generators.)

The action $\Gamma(2) \circlearrowright \mathbf{H}^2$ is free: by Paragraph 29.1.7, if $\gamma z = z$ with $\gamma \in \Gamma(2) \leq \Gamma(1)$, then γ is conjugate in $\Gamma(1)$ to either S, ST; but $\Gamma(2) \trianglelefteq \Gamma(1)$ is normal, so this implies that either $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ or $ST = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ belongs to $\Gamma(2)$, a contradiction.

Let $Y(2) = \Gamma(2)\backslash\mathbf{H}^2$. Then gluing together the fundamental set, we have a homeomorphism

$$Y(2) \simeq \mathbb{P}^1(\mathbb{C}) - \{0, 1, \infty\}$$



Indeed, the limit points of ¤ in $\partial\mathbf{H}^2$ are the points $-1, 0, 1, \infty$ and the points $-1, 1$ are identified in the quotient (by translation). The orbit of these points under $\Gamma(2)$ is $\mathbb{P}^1(\mathbb{Q}) \subseteq \partial\mathbf{H}^2$, so letting $\mathcal{H}^* = \mathbf{H}^2 \cup \mathbb{P}^1(\mathbb{Q})$, we have a homeomorphism

$$X(2) = \Gamma(2)\backslash\mathcal{H}^* \simeq \mathbb{P}^1(\mathbb{C}).$$

As with $X(1)$, this homeomorphism can be given by a holomorphic map

$$\lambda : X(2) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C});$$

the map λ is invariant under $z \mapsto z + 2$, so has a Fourier expansion in terms of $q^{1/2} = e^{\pi i z}$, and explicitly we have

$$\lambda(z) = 16q^{1/2} - 128q + 704q^{3/2} - 3072q^2 + 11488q^{5/2} - 38400q^3 + \dots. \quad (29.5.6)$$

and $\lambda(\gamma z) = \lambda(z)$ for all $\gamma \in \Gamma(2)$.

As a uniformizer for a congruence subgroup of $\mathrm{PSL}_2(\mathbb{Z})$, the function $\lambda(z)$ has a modular interpretation: there is a family of elliptic curves over $X(2)$ equipped with extra structure. Specifically, given $\lambda \in \mathbb{P}^1(\mathbb{C}) \setminus \{0, 1, \infty\}$, the corresponding elliptic curve with extra structure is given by the *Legendre curve*

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

equipped with the isomorphism $(\mathbb{Z}/2\mathbb{Z})^2 \xrightarrow{\sim} E[2]$ determined by sending the standard generators to the 2-torsion points $(0,0)$ and $(1,0)$. There is a forgetful map that forgets this additional torsion structure on a Legendre curve and remembers only isomorphism class; on the algebraic level, this corresponds to an expression of j in terms of λ, which is given by

$$j(\lambda) = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}; \tag{29.5.7}$$

From (29.5.7) (and the first term), the complete Puiseux series expansion (29.5.6) can be obtained recursively.

The congruence conditions (29.5.5) imply that $\Gamma_0(2) = \Gamma_1(2)$ has index 2 in $\Gamma(2)$, with the quotient generated by T, and we obtain a fundamental set by identifying the two ideal triangles in ¤ above.

29.6 Extensions and further reading

Exercises

29.1. Prove that $Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbf{H}^2$ has $\mathrm{area}(Y(1)) = \pi/3$ by direct integration (verifying the Gauss–Bonnet formula).

29.2. Show that $\mathrm{PSL}_2(\mathbb{Z})$ is generated by T and $U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

29.3. In this exercise, we link the fact that $\mathrm{PSL}_2(\mathbb{Z})$ is generated by S, T to a kind of continued fraction via the Euclidean algorithm. Let $a, b \in \mathbb{Z}_{\geq 1}$ with $a \geq b$.

a) Show that there exist unique $q, r \in \mathbb{Z}$ such that $a = qb - r$ and $q \geq 2$ and $0 \leq r < b$.

From (a), define inductively $r_0 = a$, $r_1 = b$, and $r_{i-1} = q_i r_i - r_{i+1}$ with $0 \leq r_{i+1} < r_i$; we then have $r_1 > r_2 > \cdots > r_t > r_{t+1} = 0$ for some $t > 0$.

b) Show that $\gcd(a,b) = r_t$, and if $\gcd(a,b) = 1$ then

$$\frac{a}{b} = q_1 - \cfrac{1}{q_2 - \cfrac{1}{\cdots - \cfrac{1}{q_t}}}.$$

This kind of continued fraction is called a *negative-regular* or *Hirzebruch–Jung continued fraction* [Jun08, Hir53].

c) Show (by induction) that

$$\begin{pmatrix} q_t & -1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} 0 \\ r_t \end{pmatrix}.$$

Show that

$$\begin{pmatrix} \pm 1 & -1 \\ 1 & 0 \end{pmatrix} \in \langle S, T \rangle$$

and interpret the action of a matrix $\begin{pmatrix} q & -1 \\ 1 & 0 \end{pmatrix}$ with $q \in \mathbb{Z}$ in terms of the reduction algorithm to the fundamental set $\square$ for $\mathrm{PSL}_2(\mathbb{Z})$.

d) Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Show that there exists $W \in \langle S, T \rangle$ such that

$$AW = \begin{pmatrix} 1 & 0 \\ c' & 1 \end{pmatrix}$$

with $c' \in \mathbb{Z}$, and conclude that $\langle S, T \rangle = \mathrm{PSL}_2(\mathbb{Z})$.

29.4. In the proof of Lemma 29.1.1, we showed that the reduction algorithm terminates after finitely many steps directly. Prove this again using the fact that Γ is discrete and so Theorem 28.3.12(ii) holds.

29.5. Compute the class number $h(d)$ and the set of reduced (positive definite) binary quadratic forms of discriminant $d = -71$.

29.6. Let $\mathcal{Q}_d$ be the set of primitive, positive definite binary quadratic forms of discriminant $d < 0$.

a) Show that the group $\mathrm{GL}_2(\mathbb{Z})$ acts on $\mathcal{Q}_d$, with $\mathrm{PGL}_2(\mathbb{Z})$ acting faithfully.

b) Consider the action of $\mathrm{PGL}_2(\mathbb{Z})$ on H^2. Show that every $Q \in \mathcal{Q}_d$ is equivalent to a $\mathrm{GL}_2(\mathbb{Z})$-*reduced* form $ax^2 + bxy + cy^2$ satisfying

$$0 \leq b \leq a \leq c.$$

[Hint: Find a nice fundamental set $\square$ *for* $\mathrm{PGL}_2(\mathbb{Z})$*.]*

c) By transport, Paragraph 29.1.7 computes the stabilizer of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathcal{Q}_d$. Compute $\mathrm{Stab}_{\mathrm{PGL}_2(\mathbb{Z})}(Q)$ for $Q \in \mathcal{Q}_d$.

29.7. Let

$$S = \mathbb{Z} \oplus \mathbb{Z}[(d + \sqrt{d})/2] \subset K = \mathbb{Q}(\sqrt{d})$$

be the quadratic ring of discriminant $d < 0$. Let $\mathrm{Pic}(S)$ be the group of invertible fractional ideals of S modulo principal ideals. Show that the map

$$\begin{aligned} \mathcal{Q}_d/\Gamma &\to \mathrm{Pic}(S) \\ [ax^2 + bxy + cy^2] &\mapsto [\mathfrak{a}] = \left[\left(a, \frac{-b + \sqrt{d}}{2}\right)\right] \end{aligned}$$

is a bijection, where $\mathcal{Q}_d/\Gamma$ is the set of ($\mathrm{SL}_2(\mathbb{Z})$-)equivalence classes of (primitive, positive definite) binary quadratic forms of discriminant d.

29.8. Let $f : U \to \mathbb{C}$ be a meromorphic function in an open neighborhood $U \supseteq \mathbb{C}$ with $0 \in U$, and let C be the contour along the arc of a circle of radius $\epsilon > 0$ with total angle θ. Show that

$$\lim_{\epsilon \to 0} \int_C \frac{\mathrm{d}f}{f} = \theta i.$$

29.9. Complete the proof of Proposition 29.4.10 in case f has poles or zeros along the boundary of $\square$.

29.10. Prove the formula

$$\pi \cot(\pi z) = \sum_{m=-\infty}^{\infty} \frac{1}{z+m}$$

for $z \in \mathbb{C}$. *[Hint: the difference $h(z)$ of the left- and right-hand sides is bounded away from $\mathbb{Z}$, invariant under $z \mapsto T(z) = z+1$, and in a neighborhood of 0 is holomorphic (both sides have principal part $1/z$) so bounded, so $h(z)$ is bounded in $\mathbb{C}$ and hence constant.]*

29.11. In this exercise, we give Euler's evaluation of $\zeta(k)$ in terms of Bernoulli numbers. Define the series

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!} = 1 - \frac{x}{2} + \frac{1}{6}\frac{x^2}{2!} - \frac{1}{30}\frac{x^4}{4!} + \ldots \in \mathbb{Q}[[x]]. \tag{29.6.1}$$

a) Plug in $x = 2iz$ into (29.6.1) to obtain

$$z \cot z = 1 + \sum_{k=2}^{\infty} B_k \frac{(2iz)^k}{k!}.$$

b) Take the logarithmic derivative of

$$\sin z = z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2\pi^2}\right)$$

to show

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

c) Conclude that

$$\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k} = -\frac{1}{2}\frac{(2\pi i)^k}{k!} B_k$$

for $k \in 2\mathbb{Z}_{\geq 1}$.

29.12. Show that the elements

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

generate $\Gamma(2)$ in a similar manner as section 29.1, using the fundamental set

$$\square = \{z \in \mathbf{H}^2 : |\operatorname{Re} z| \leq 1, |2z \pm 1| \geq 1\}.$$

29.13. [[Exercise with $\Gamma_0(2) = \Gamma_1(2)$?]]