$$\frac{t}{e^t-1}+\frac{t}{2}=\frac{t}{2}\cdot\frac{e^t+1}{e^t-1}$$

is even, it follows that $B_1 = -1/2$ and $B_k = 0$ for all other odd k. The Bernoulli numbers will be motivated, discussed, and generalized in Chapter 4.

(a) Show that $B_2 = 1/6$, $B_4 = -1/30$, and $B_6 = 1/42$.

(b) Use the expressions for $\pi\cot\pi\tau$ from the section to show

$$1-2\sum_{k=1}^{\infty}\zeta(2k)\tau^{2k}=\pi\tau\cot\pi\tau=\pi i\tau+\sum_{k=0}^{\infty}B_k\frac{(2\pi i\tau)^k}{k!}.$$

Use these to show that for $k \geq 2$ even, the Riemann zeta function satisfies

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

so in particular $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$, and $\zeta(6) = \pi^6/945$. Also, this shows that the normalized Eisenstein series of weight k

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

has rational coefficients with a common denominator.

(c) Equate coefficients in the relation $E_8(\tau) = E_4(\tau)^2$ to establish formula (1.3).

(d) Show that $a_0 = 0$ and $a_1 = (2\pi)^{12}$ in the Fourier expansion of the discriminant function Δ from the text.

1.1.8. Recall that μ_3 denotes the complex cube root of unity $e^{2\pi i/3}$. Show that $\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right](\mu_3) = \mu_3 + 1$ so that by periodicity $g_2(\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right](\mu_3)) = g_2(\mu_3)$. Show that by modularity also $g_2(\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right](\mu_3)) = \mu_3^4 g_2(\mu_3)$ and therefore $g_2(\mu_3) = 0$. Conclude that $g_3(\mu_3) \neq 0$ and $j(\mu_3) = 0$. Argue similarly to show that $g_3(i) = 0$, $g_2(i) \neq 0$, and $j(i) = 1728$.

1.1.9. This exercise shows that the modular invariant $j : \mathcal{H} \longrightarrow \mathbf{C}$ is a surjection. Suppose that $c \in \mathbf{C}$ and $j(\tau) \neq c$ for all $\tau \in \mathcal{H}$. Consider the integral

$$\frac{1}{2\pi i}\int_\gamma\frac{j'(\tau)d\tau}{j(\tau)-c}$$

where γ is the contour shown in Figure 1.1 containing an arc of the unit circle from $(-1+i\sqrt{3})/2$ to $(1+i\sqrt{3})/2$, two vertical segments up to any height greater than 1, and a horizontal segment. By the Argument Principle the integral is 0. Use the fact that j is invariant under $\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$ to show that the integrals over the two vertical segments cancel. Use the fact that j is invariant under $\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right]$ to show that the integrals over the two halves of the circular arc cancel. For the integral over the remaining piece of γ make the change of coordinates $q = e^{2\pi i\tau}$, remembering that $j'(\tau)$ denotes derivative with respect to τ and that $j(\tau) = 1/q + \cdots$, and compute that it equals 1. This contradiction shows that $j(\tau) = c$ for some $\tau \in \mathcal{H}$ and j surjects.

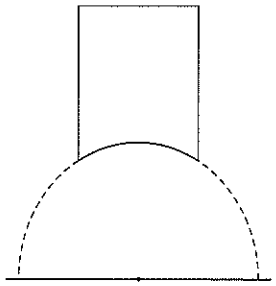

Figure 1.1. A contour

1.2 Congruence subgroups

Section 1.1 stated that if a meromorphic function $f : \mathcal{H} \longrightarrow \mathbf{C}$ satisfies

$$f(\gamma(\tau))=(c\tau+d)^k f(\tau)\quad\text{for }\gamma=\begin{bmatrix}1&1\\0&1\end{bmatrix}\text{ and }\gamma=\begin{bmatrix}0&-1\\1&0\end{bmatrix}$$

then f is weakly modular, i.e,

$$f(\gamma(\tau))=(c\tau+d)^k f(\tau)\quad\text{for all }\gamma=\begin{bmatrix}a&b\\c&d\end{bmatrix}\in \mathrm{SL}_2(\mathbf{Z}).$$

Replacing the modular group $\mathrm{SL}_2(\mathbf{Z})$ in this last condition by a subgroup Γ generalizes the notion of weak modularity, allowing more examples of weakly modular functions.

For example, a subgroup arises from the *four squares problem* in number theory, to find the number of ways (if any) that a given nonnegative integer n can be expressed as the sum of four integer squares. To address this, define more generally for nonnegative integers n and k the *representation number* of n by k squares,

$$r(n,k)=\#\{v\in\mathbf{Z}^k : n=v_1^2+\cdots+v_k^2\}.$$

Note that if $i + j = k$ then $r(n, k) = \sum_{l+m=n} r(l, i)r(m, j)$, summing over nonnegative values of l and m that add to n (Exercise 1.2.1). This looks like the rule $c_n = \sum_{l+m=n} a_l b_m$ relating the coefficients in the formal product of two power series,

$$\left(\sum_{l=0}^{\infty}a_l q^l\right)\left(\sum_{m=0}^{\infty}b_m q^m\right)=\sum_{n=0}^{\infty}c_n q^n.$$

So consider the *generating function* of the representation numbers, meaning the power series with nth coefficient $r(n, k)$,

$$\theta(\tau,k)=\sum_{n=0}^{\infty}r(n,k)q^n,\quad q=e^{2\pi i\tau},\ \tau\in\mathcal{H}.$$

$$\widehat{\varphi_1+\varphi_2} = \hat{\varphi}_1 + \hat{\varphi}_2 \quad \text{if } \varphi_1+\varphi_2 \neq 0. \tag{1.7}$$

We will cite this fact in Chapter 6.

For one more example, some complex tori have endomorphisms other than the multiply-by-N maps $[N]$, in which case they have *complex multiplication*. Let $\tau = \sqrt{d}$ for some squarefree $d \in \mathbf{Z}^-$ such that $d \equiv 2, 3 \pmod 4$, or let $\tau = (-1+\sqrt{d})/2$ for squarefree $d \in \mathbf{Z}^-$, $d \equiv 1 \pmod 4$. Then the set $\mathcal{O} = \tau\mathbf{Z} \oplus \mathbf{Z}$ is a ring. (Readers with background in number theory will recognize it as the ring of integers in the imaginary quadratic number field $\mathbf{Q}(\sqrt{d})$.) Let Λ be any ideal of $\mathcal{O}$ and let m be any element of $\mathcal{O}$. Then $m\Lambda \subset \Lambda$, so multiplying by m gives an endomorphism of $\mathbf{C}/\Lambda$. In particular, the ring of endomorphisms of $\mathbf{C}/\Lambda_i$ is isomorphic to $\Lambda_i = i\mathbf{Z} \oplus \mathbf{Z}$ rather than to $\mathbf{Z}$, and similarly for the ring of endomorphisms of $\mathbf{C}/\Lambda_{\mu_3}$ where $\mu_3 = e^{2\pi i/3}$.

Let Λ be a lattice. The N-torsion subgroup of the additive torus group $\mathbf{C}/\Lambda$,

$$E[N] = \{P \in \mathbf{C}/\Lambda : [N]P = 0\} = \langle \omega_1/N + \Lambda\rangle \times \langle \omega_2/N + \Lambda\rangle,$$

is analogous to the N-torsion subgroup of the multiplicative circle group $\mathbf{C}^*/\mathbf{R}^+ \cong \{z \in \mathbf{C} : |z| = 1\} \cong \mathbf{R}/\mathbf{Z}$, the complex Nth roots of unity

$$\boldsymbol{\mu}_N = \{z \in \mathbf{C} : z^N = 1\} = \langle e^{2\pi i/N}\rangle.$$

A sort of inner product exists on $E[N]$ with values in $\boldsymbol{\mu}_N$, the *Weil pairing*

$$e_N : E[N] \times E[N] \longrightarrow \boldsymbol{\mu}_N.$$

To define this, let P and Q be points in $E[N]$, possibly equal. If $\Lambda = \omega_1\mathbf{Z} \oplus \omega_2\mathbf{Z}$ with $\omega_1/\omega_2 \in \mathcal{H}$ then

$$\begin{bmatrix} P \\ Q \end{bmatrix} = \gamma \begin{bmatrix} \omega_1/N + \Lambda \\ \omega_2/N + \Lambda \end{bmatrix} \quad \text{for some } \gamma \in \mathrm{M}_2(\mathbf{Z}/N\mathbf{Z})$$

since $\omega_1/N + \Lambda$ and $\omega_2/N + \Lambda$ generate $E[N]$. The Weil pairing of P and Q is

$$e_N(P, Q) = e^{2\pi i \det\gamma/N}.$$

This makes sense even though $\det\gamma$ is defined only modulo N. It is independent of how the basis $\{\omega_1, \omega_2\}$ is chosen (and once the basis is chosen the matrix γ is uniquely determined since its entries are reduced modulo N), remembering the normalization $\omega_1/\omega_2 \in \mathcal{H}$ (Exercise 1.3.3(a)). If P and Q generate $E[N]$ then the matrix γ lies in the group $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ of invertible 2-by-2 matrices with entries in $\mathbf{Z}/N\mathbf{Z}$, making $\det\gamma$ invertible modulo N and $e_N(P, Q)$ therefore a primitive complex Nth root of unity. See Exercise 1.3.3(b–d) for more properties of the Weil pairing, in particular that the Weil pairing is preserved under isomorphisms of complex tori. We will use the Weil pairing in the Section 1.5.

Exercises

1.3.1. Prove Lemma 1.3.1.

1.3.2. Prove Corollary 1.3.3. (A hint for this exercise is at the end of the book.)

1.3.3. (a) Show that the Weil pairing is independent of which basis $\{\omega_1, \omega_2\}$ is used, provided $\omega_1/\omega_2 \in \mathcal{H}$.

(b) Show that the Weil pairing is bilinear, alternating, and nondegenerate. (Remember that the group $\boldsymbol{\mu}_N$ is multiplicative.)

(c) Show that the Weil pairing is compatible with N. This means that for positive integers N and d, the diagram

$$\begin{array}{ccc} E[dN] \times E[dN] & \xrightarrow{e_{dN}(\cdot,\cdot)} & \boldsymbol{\mu}_{dN} \\ {\scriptstyle d(\cdot,\cdot)}\downarrow & & \downarrow{\scriptstyle .d} \\ E[N] \times E[N] & \xrightarrow{e_N(\cdot,\cdot)} & \boldsymbol{\mu}_N \end{array}$$

commutes, where the vertical maps are suitable multiplications by d. (A hint for this exercise is at the end of the book.)

(d) Let Λ and Λ' be lattices with $m\Lambda = \Lambda'$ for some $m \in \mathbf{C}$. Show that the isomorphism of complex elliptic curves $\mathbf{C}/\Lambda \xrightarrow{\sim} \mathbf{C}/\Lambda'$ given by $z + \Lambda \mapsto mz + \Lambda'$ preserves the Weil pairing.

1.4 Complex tori as elliptic curves

This section shows how complex tori $\mathbf{C}/\Lambda$ can also be viewed as cubic curves of the sort mentioned back in the preface. These cubic curves are called *elliptic* despite not being ellipses, due to a connection between them and the arc length of an actual ellipse. The presentation here is terse, so the reader may want to consult a relevant complex analysis text such as [JS87].

The meromorphic functions on a complex torus are what relate it to a cubic curve. Given a lattice Λ, the meromorphic functions $f : \mathbf{C}/\Lambda \longrightarrow \widehat{\mathbf{C}}$ on the torus are naturally identified with the Λ-periodic meromorphic functions $f : \mathbf{C} \longrightarrow \widehat{\mathbf{C}}$ on the plane. Exercise 1.4.1 derives some basic properties of these functions in general. The most important specific example is the *Weierstrass $\wp$-function*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda}{}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right), \quad z \in \mathbf{C},\ z \notin \Lambda.$$

(The primed summation means to omit $\omega = 0$.) Subtracting $1/\omega^2$ from $1/(z-\omega)^2$ makes the summand roughly z/ω^3, cf. the sketched proof of Proposition 1.4.1 to follow, so the sum converges absolutely and uniformly on compact subsets of $\mathbf{C}$ away from Λ. Correcting the summand this way prevents