1

Modular Forms, Elliptic Curves, and Modular Curves

This chapter introduces three central objects of the book.

Modular forms are functions on the complex upper half plane. A matrix group called the modular group acts on the upper half plane, and modular forms are the functions that transform in a nearly invariant way under the action and satisfy a holomorphy condition. Restricting the action to subgroups of the modular group called congruence subgroups gives rise to more modular forms.

A *complex elliptic curve* is a quotient of the complex plane by a lattice. As such it is an Abelian group, a compact Riemann surface, a torus, and—nonobviously—in bijective correspondence with the set of ordered pairs of complex numbers satisfying a cubic equation of the form E in the preface.

A *modular curve* is a quotient of the upper half plane by the action of a congruence subgroup. That is, two points are considered the same if the group takes one to the other.

These three kinds of object are closely related. Modular curves are mapped to by *moduli spaces*, equivalence classes of complex elliptic curves enhanced by associated torsion data. Thus the points of modular curves represent enhanced elliptic curves. Consequently, functions on the moduli spaces satisfying a homogeneity condition are essentially the same thing as modular forms.

Related reading: Gunning [Gun62], Koblitz [Kob93], Schoeneberg [Sch74], and Chapter 7 of Serre [Ser73] are standard first texts on this subject. For modern expositions of classical modular forms in action see [Cox84] (reprinted in [BBB00]) and [Cox97].

1.1 First definitions and examples

The *modular group* is the group of 2-by-2 matrices with integer entries and determinant 1,

$$\mathrm{SL}_2(\mathbf{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbf{Z}, ad - bc = 1 \right\}.$$

The modular group is generated by the two matrices

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

(Exercise 1.1.1). Each element of the modular group is also viewed as an automorphism (invertible self-map) of the Riemann sphere $\widehat{\mathbf{C}} = \mathbf{C} \cup \{\infty\}$, the fractional linear transformation

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}, \quad \tau \in \widehat{\mathbf{C}}.$$

This is understood to mean that if $c \neq 0$ then $-d/c$ maps to ∞ and ∞ maps to a/c, and if $c = 0$ then ∞ maps to ∞. The identity matrix I and its negative $-I$ both give the identity transformation, and more generally each pair $\pm\gamma$ of matrices in $\mathrm{SL}_2(\mathbf{Z})$ gives a single transformation. The group of transformations defined by the modular group is generated by the maps described by the two matrix generators,

$$\tau \mapsto \tau + 1 \quad \text{and} \quad \tau \mapsto -1/\tau.$$

The *upper half plane* is

$$\mathcal{H} = \{\tau \in \mathbf{C} : \mathrm{Im}(\tau) > 0\}.$$

Readers with some background in Riemann surface theory—which is not necessary to read this book—may recognize $\mathcal{H}$ as one of the three simply connected Riemann surfaces, the other two being the plane $\mathbf{C}$ and the sphere $\widehat{\mathbf{C}}$. The formula

$$\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}, \quad \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbf{Z})$$

(Exercise 1.1.2(a)) shows that if $\gamma \in \mathrm{SL}_2(\mathbf{Z})$ and $\tau \in \mathcal{H}$ then also $\gamma(\tau) \in \mathcal{H}$, i.e., the modular group maps the upper half plane back to itself. In fact the modular group acts on the upper half plane, meaning that $I(\tau) = \tau$ where I is the identity matrix (as was already noted) and $(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau))$ for all $\gamma, \gamma' \in \mathrm{SL}_2(\mathbf{Z})$ and $\tau \in \mathcal{H}$. This last formula is easy to check (Exercise 1.1.2(b)).

Definition 1.1.1. *Let k be an integer. A meromorphic function $f : \mathcal{H} \longrightarrow \mathbf{C}$ is* ***weakly modular of weight*** *k if*

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

Section 1.2 will show that if this transformation law holds when γ is each of the generators $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ then it holds for all $\gamma \in \mathrm{SL}_2(\mathbf{Z})$. In other words, f is weakly modular of weight k if

$$f(\tau+1) = f(\tau) \quad \text{and} \quad f(-1/\tau) = \tau^k f(\tau).$$

Weak modularity of weight 0 is simply $\mathrm{SL}_2(\mathbf{Z})$-invariance, $f \circ \gamma = f$ for all $\gamma \in \mathrm{SL}_2(\mathbf{Z})$. Weak modularity of weight 2 is also natural: complex analysis relies on path integrals of differentials $f(\tau)d\tau$, and $\mathrm{SL}_2(\mathbf{Z})$-invariant path integration on the upper half plane requires such differentials to be invariant when τ is replaced by any $\gamma(\tau)$. But (Exercise 1.1.2(c))

$$d\gamma(\tau) = (c\tau + d)^{-2} d\tau,$$

and so the relation $f(\gamma(\tau))d(\gamma(\tau)) = f(\tau)d\tau$ is

$$f(\gamma(\tau)) = (c\tau + d)^2 f(\tau),$$

giving Definition 1.1.1 with weight $k = 2$. Weight 2 will play an especially important role later in this book since it is the weight of the modular form in the Modularity Theorem. The weight 2 case also leads inexorably to higher even weights—multiplying two weakly modular functions of weight 2 gives a weakly modular function of weight 4, and so on. Letting $\gamma = -I$ in Definition 1.1.1 gives $f = (-1)^k f$, showing that the only weakly modular function of any odd weight k is the zero function, but nonzero odd weight examples exist in more general contexts to be developed soon. Another motivating idea for weak modularity is that while it does not make a function f fully $\mathrm{SL}_2(\mathbf{Z})$-invariant, at least $f(\tau)$ and $f(\gamma(\tau))$ always have the same zeros and poles since the factor $c\tau + d$ on $\mathcal{H}$ has neither.

Modular forms are weakly modular functions that are also holomorphic on the upper half plane and holomorphic at ∞. To define this last notion, recall that $\mathrm{SL}_2(\mathbf{Z})$ contains the translation matrix

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} : \tau \mapsto \tau + 1,$$

for which the factor $c\tau + d$ is simply 1, so that $f(\tau + 1) = f(\tau)$ for every weakly modular function $f : \mathcal{H} \longrightarrow \mathbf{C}$. That is, weakly modular functions are $\mathbf{Z}$-periodic. Let $D = \{q \in \mathbf{C} : |q| < 1\}$ be the open complex unit disk, let $D' = D - \{0\}$, and recall from complex analysis that the $\mathbf{Z}$-periodic holomorphic map $\tau \mapsto e^{2\pi i \tau} = q$ takes $\mathcal{H}$ to D'. Thus, corresponding to f, the function $g : D' \longrightarrow \mathbf{C}$ where $g(q) = f(\log(q)/(2\pi i))$ is well defined even though the logarithm is only determined up to $2\pi i\mathbf{Z}$, and $f(\tau) = g(e^{2\pi i \tau})$. If f is holomorphic on the upper half plane then the composition g is holomorphic on the punctured disk since the logarithm can be defined holomorphically about each point, and so g has a Laurent expansion $g(q) = \sum_{n \in \mathbf{Z}} a_n q^n$ for $q \in D'$. The relation $|q| = e^{-2\pi \mathrm{Im}(\tau)}$ shows that $q \to 0$ as $\mathrm{Im}(\tau) \to \infty$. So, thinking of ∞ as lying far in the imaginary direction, define f to be *holomorphic at* ∞ if g extends holomorphically to the puncture point $q = 0$, i.e., the Laurent series sums over $n \in \mathbf{N}$. This means that f has a *Fourier expansion*

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f) q^n, \quad q = e^{2\pi i \tau}.$$

Since $q \to 0$ if and only if $\mathrm{Im}(\tau) \to \infty$, showing that a weakly modular holomorphic function $f : \mathcal{H} \longrightarrow \mathbf{C}$ is holomorphic at ∞ doesn't require computing its Fourier expansion, only showing that $\lim_{\mathrm{Im}(\tau)\to\infty} f(\tau)$ exists or even just that $f(\tau)$ is bounded as $\mathrm{Im}(\tau) \to \infty$.

Definition 1.1.2. *Let k be an integer. A function $f : \mathcal{H} \longrightarrow \mathbf{C}$ is a **modular form of weight** k if*

(1) *f is holomorphic on $\mathcal{H}$,*
(2) *f is weakly modular of weight k,*
(3) *f is holomorphic at ∞.*

The set of modular forms of weight k is denoted $\mathcal{M}_k(\mathrm{SL}_2(\mathbf{Z}))$.

It is easy to check that $\mathcal{M}_k(\mathrm{SL}_2(\mathbf{Z}))$ forms a vector space over $\mathbf{C}$ (Exercise 1.1.3(a)). Holomorphy at ∞ will make the dimension of this space, and of more spaces of modular forms to be defined in the next section, finite. We will compute many dimension formulas in Chapter 3. When f is holomorphic at ∞ it is tempting to define $f(\infty) = g(0) = a_0$, but the next section will show that this doesn't work in a more general context.

The product of a modular form of weight k with a modular form of weight l is a modular form of weight $k + l$ (Exercise 1.1.3(b)). Thus the sum

$$\mathcal{M}(\mathrm{SL}_2(\mathbf{Z})) = \bigoplus_{k \in \mathbf{Z}} \mathcal{M}_k(\mathrm{SL}_2(\mathbf{Z}))$$

forms a ring, a so-called graded ring because of its structure as a sum.

The zero function on $\mathcal{H}$ is a modular form of every weight, and every constant function on $\mathcal{H}$ is a modular form of weight 0. For nontrivial examples of modular forms, let $k > 2$ be an even integer and define the *Eisenstein series of weight k* to be a 2-dimensional analog of the Riemann zeta function $\zeta(k) = \sum_{d=1}^{\infty} 1/d^k$,

$$G_k(\tau) = {\sum_{(c,d)}}' \frac{1}{(c\tau + d)^k}, \quad \tau \in \mathcal{H},$$

where the primed summation sign means to sum over nonzero integer pairs $(c, d) \in \mathbf{Z}^2 - \{(0, 0)\}$. The sum is absolutely convergent and converges uniformly on compact subsets of $\mathcal{H}$ (Exercise 1.1.4(c)), so G_k is holomorphic on $\mathcal{H}$ and its terms may be rearranged. For any $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbf{Z})$, compute that

$$
\begin{aligned}
G_k(\gamma(\tau)) &= {\sum_{(c',d')}}' \frac{1}{\left(c'\left(\frac{a\tau+b}{c\tau+d}\right)+d'\right)^k} \\
&= (c\tau+d)^k {\sum_{(c',d')}}' \frac{1}{((c'a+d'c)\tau+(c'b+d'd))^k}.
\end{aligned}
$$

But as (c', d') runs through $\mathbf{Z}^2 - \{(0,0)\}$, so does $(c'a + d'c, c'b + d'd) = (c', d')\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ (Exercise 1.1.4(d)), and so the right side is $(c\tau + d)^k G_k(\tau)$, showing that G_k is weakly modular of weight k. Finally, G_k is bounded as $\operatorname{Im}(\tau) \to \infty$ (Exercise 1.1.4(e)), so it is a modular form.

To compute the Fourier series for G_k, continue to let $\tau \in \mathcal{H}$ and begin with the identities

$$
\frac{1}{\tau} + \sum_{d=1}^{\infty}\left(\frac{1}{\tau-d}+\frac{1}{\tau+d}\right) = \pi\cot\pi\tau = \pi i - 2\pi i \sum_{m=0}^{\infty} q^m, \quad q = e^{2\pi i\tau} \tag{1.1}
$$

(Exercise 1.1.5—the reader who is unhappy with this unmotivated incanting of unfamiliar expressions for a trigonometric function should be reassured that it is a standard rite of passage into modular forms; but also, Exercise 1.1.6 provides other proofs, perhaps more natural, of the following formula (1.2)). Differentiating (1.1) $k-1$ times with respect to τ gives for $\tau \in \mathcal{H}$ and $q = e^{2\pi i\tau}$,

$$
\sum_{d\in\mathbf{Z}} \frac{1}{(\tau+d)^k} = \frac{(-2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty} m^{k-1}q^m, \quad k \geq 2. \tag{1.2}
$$

For even $k > 2$,

$$
{\sum_{(c,d)}}' \frac{1}{(c\tau+d)^k} = \sum_{d\neq 0}\frac{1}{d^k} + 2\sum_{c=1}^{\infty}\left(\sum_{d\in\mathbf{Z}}\frac{1}{(c\tau+d)^k}\right),
$$

so again letting ζ denote the Riemann zeta function and using (1.2) gives

$$
{\sum_{(c,d)}}' \frac{1}{(c\tau+d)^k} = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{c=1}^{\infty}\sum_{m=1}^{\infty} m^{k-1}q^{cm}.
$$

Rearranging the last expression gives the Fourier expansion

$$
G_k(\tau) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n, \quad k > 2,\ k \text{ even}
$$

where the coefficient $\sigma_{k-1}(n)$ is the arithmetic function

$$
\sigma_{k-1}(n) = \sum_{\substack{m|n \\ m>0}} m^{k-1}.
$$

Exercise 1.1.7(b) shows that dividing by the leading coefficient gives a series having rational coefficients with a common denominator. This *normalized* Eisenstein series $G_k(\tau)/(2\zeta(k))$ is denoted $E_k(\tau)$. The Riemann zeta function will be discussed further in Chapter 4.

Since the set of modular forms is a graded ring, we can make modular forms out of various sums of products of the Eisenstein series. For example, $\mathcal{M}_8(\mathrm{SL}_2(\mathbf{Z}))$ turns out to be 1-dimensional. The functions $E_4(\tau)^2$ and $E_8(\tau)$ both belong to this space, making them equal up to a scalar multiple and therefore equal since both have leading term 1. Expanding out the relation $E_4^2 = E_8$ gives a relation between the divisor-sum functions σ_3 and σ_7 (Exercise 1.1.7(c)),

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{i=1}^{n-1} \sigma_3(i)\sigma_3(n-i), \quad n \geq 1. \tag{1.3}$$

The modular forms that, unlike Eisenstein series, have constant term equal to 0 play an important role in the subject.

Definition 1.1.3. *A* ***cusp form*** *of weight k is a modular form of weight k whose Fourier expansion has leading coefficient $a_0 = 0$, i.e.,*

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n, \quad q = e^{2\pi i\tau}.$$

The set of cusp forms is denoted $\mathcal{S}_k(\mathrm{SL}_2(\mathbf{Z}))$.

So a modular form is a cusp form when $\lim_{\mathrm{Im}(\tau)\to\infty} f(\tau) = 0$. The limit point ∞ of $\mathcal{H}$ is called the *cusp of* $\mathrm{SL}_2(\mathbf{Z})$ for geometric reasons to be explained in Chapter 2, and a cusp form can be viewed as vanishing at the cusp. The cusp forms $\mathcal{S}_k(\mathrm{SL}_2(\mathbf{Z}))$ form a vector subspace of the modular forms $\mathcal{M}_k(\mathrm{SL}_2(\mathbf{Z}))$, and the graded ring

$$\mathcal{S}(\mathrm{SL}_2(\mathbf{Z})) = \bigoplus_{k\in\mathbf{Z}} \mathcal{S}_k(\mathrm{SL}_2(\mathbf{Z}))$$

is an ideal in $\mathcal{M}(\mathrm{SL}_2(\mathbf{Z}))$ (Exercise 1.1.3(c)).

For an example of a cusp form, let

$$g_2(\tau) = 60G_4(\tau), \qquad g_3(\tau) = 140G_6(\tau),$$

and define the *discriminant function*

$$\Delta : \mathcal{H} \longrightarrow \mathbf{C}, \qquad \Delta(\tau) = (g_2(\tau))^3 - 27(g_3(\tau))^2.$$

Then Δ is weakly modular of weight 12 and holomorphic on $\mathcal{H}$, and $a_0 = 0$, $a_1 = (2\pi)^{12}$ in the Fourier expansion of Δ (Exercise 1.1.7(d)). So indeed

$\Delta \in \mathcal{S}_{12}(\mathrm{SL}_2(\mathbf{Z}))$, and Δ is not the zero function. Section 1.4 will show that in fact $\Delta(\tau) \neq 0$ for all $\tau \in \mathcal{H}$ so that the only zero of Δ is at ∞.

It follows that the *modular function*

$$j : \mathcal{H} \longrightarrow \mathbf{C}, \qquad j(\tau) = 1728 \frac{(g_2(\tau))^3}{\Delta(\tau)}$$

is holomorphic on $\mathcal{H}$. Since the numerator and denominator of j have the same weight, j is $\mathrm{SL}_2(\mathbf{Z})$-invariant,

$$j(\gamma(\tau)) = j(\tau), \qquad \gamma \in \mathrm{SL}_2(\mathbf{Z}),\ \tau \in \mathcal{H},$$

and in fact it is also called *the modular invariant*. The expansion

$$j(\tau) = \frac{(2\pi)^{12} + \cdots}{(2\pi)^{12} q + \cdots} = \frac{1}{q} + \cdots$$

shows that j has a simple pole at ∞ (and is normalized to have residue 1 at the pole), so it is not quite a modular form. Let μ_3 denote the complex cube root of unity $e^{2\pi i/3}$. Easy calculations (Exercise 1.1.8) show that $g_3(i) = 0$ so that $g_2(i) \neq 0$ and $j(i) = 1728$, and $g_2(\mu_3) = 0$ so that $g_3(\mu_3) \neq 0$ and $j(\mu_3) = 0$. One can further show (see [Ros81], [CSar]) that

$$g_2(i) = 4\varpi_4^4, \qquad \varpi_4 = 2\int_0^1 \frac{dt}{\sqrt{1-t^4}} = 2\sqrt{\pi}\,\frac{\Gamma(5/4)}{\Gamma(3/4)}$$

and

$$g_3(\mu_3) = (27/16)\varpi_3^6, \qquad \varpi_3 = 2\int_0^1 \frac{dt}{\sqrt{1-t^3}} = 2\sqrt{\pi}\,\frac{\Gamma(4/3)}{\Gamma(5/6)}.$$

Here the integrals are *elliptic integrals*, and Γ is Euler's *gamma function*, to be defined in Chapter 4. Finally, Exercise 1.1.9 shows that the j-function surjects from $\mathcal{H}$ to $\mathbf{C}$.

Exercises

1.1.1. Let Γ be the subgroup of $\mathrm{SL}_2(\mathbf{Z})$ generated by the two matrices $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$. Note that $\left[\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]^n \in \Gamma$ for all $n \in \mathbf{Z}$. Let $\alpha = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ be a matrix in $\mathrm{SL}_2(\mathbf{Z})$. Use the identity

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b' \\ c & nc + d \end{bmatrix}$$

to show that unless $c = 0$, some matrix $\alpha\gamma$ with $\gamma \in \Gamma$ has bottom row (c, d') with $|d'| \leq |c|/2$. Use the identity

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & -a \\ d & -c \end{bmatrix}$$

to show that this process can be iterated until some matrix $\alpha\gamma$ with $\gamma \in \Gamma$ has bottom row $(0, *)$. Show that in fact the bottom row is $(0, \pm 1)$, and since $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]^2 = -I$ it can be taken to be $(0, 1)$. Show that therefore $\alpha\gamma \in \Gamma$ and so $\alpha \in \Gamma$. Thus Γ is all of $\mathrm{SL}_2(\mathbf{Z})$.

1.1.2. (a) Show that $\mathrm{Im}(\gamma(\tau)) = \mathrm{Im}(\tau)/|c\tau + d|^2$ for all $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbf{Z})$.
(b) Show that $(\gamma\gamma')(\tau) = \gamma(\gamma'(\tau))$ for all $\gamma, \gamma' \in \mathrm{SL}_2(\mathbf{Z})$ and $\tau \in \mathcal{H}$.
(c) Show that $d\gamma(\tau)/d\tau = 1/(c\tau + d)^2$ for $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbf{Z})$.

1.1.3. (a) Show that the set $\mathcal{M}_k(\mathrm{SL}_2(\mathbf{Z}))$ of modular forms of weight k forms a vector space over $\mathbf{C}$.

(b) If f is a modular form of weight k and g is a modular form of weight l, show that fg is a modular form of weight $k + l$.

(c) Show that $\mathcal{S}_k(\mathrm{SL}_2(\mathbf{Z}))$ is a vector subspace of $\mathcal{M}_k(\mathrm{SL}_2(\mathbf{Z}))$ and that $\mathcal{S}(\mathrm{SL}_2(\mathbf{Z}))$ is an ideal in $\mathcal{M}(\mathrm{SL}_2(\mathbf{Z}))$.

1.1.4. Let $k \geq 3$ be an integer and let $L' = \mathbf{Z}^2 - \{(0, 0)\}$.

(a) Show that the series $\sum_{(c,d) \in L'} (\sup\{|c|, |d|\})^{-k}$ converges by considering the partial sums over expanding squares.

(b) Fix positive numbers A and B and let

$$\Omega = \{\tau \in \mathcal{H} : |\mathrm{Re}(\tau)| \leq A, \mathrm{Im}(\tau) \geq B\}.$$

Prove that there is a constant $C > 0$ such that $|\tau + \delta| > C \sup\{1, |\delta|\}$ for all $\tau \in \Omega$ and $\delta \in \mathbf{R}$. (Hints for this exercise are at the end of the book.)

(c) Use parts (a) and (b) to prove that the series defining $G_k(\tau)$ converges absolutely and uniformly for $\tau \in \Omega$. Conclude that G_k is holomorphic on $\mathcal{H}$.

(d) Show that for $\gamma \in \mathrm{SL}_2(\mathbf{Z})$, right multiplication by γ defines a bijection from L' to L'.

(e) Use the calculation from (c) to show that G_k is bounded on Ω. From the text and part (d), G_k is weakly modular so in particular $G_k(\tau + 1) = G_k(\tau)$. Show that therefore $G_k(\tau)$ is bounded as $\mathrm{Im}(\tau) \to \infty$.

1.1.5. Establish the two formulas for $\pi \cot \pi\tau$ in (1.1). (A hint for this exercise is at the end of the book.)

1.1.6. This exercise obtains formula (1.2) without using the cotangent. Let $f(\tau) = \sum_{d \in \mathbf{Z}} 1/(\tau + d)^k$ for $k \geq 2$ and $\tau \in \mathcal{H}$. Since f is holomorphic (by the method of Exercise 1.1.4) and $\mathbf{Z}$-periodic and since $\lim_{\mathrm{Im}(\tau) \to \infty} f(\tau) = 0$, there is a Fourier expansion $f(\tau) = \sum_{m=1}^{\infty} a_m q^m = g(q)$ as in the section, where $q = e^{2\pi i \tau}$ and

$$a_m = \frac{1}{2\pi i} \int_\gamma \frac{g(q)}{q^{m+1}} dq$$

is a path integral once counterclockwise over a circle about 0 in the punctured disk D'.

(a) Show that

$$a_m = \int_{\tau=0+iy}^{1+iy} f(\tau)e^{-2\pi i m\tau}d\tau = \int_{\tau=-\infty+iy}^{+\infty+iy} \tau^{-k}e^{-2\pi i m\tau}d\tau \quad \text{for any } y > 0.$$

(b) Let $g_m(\tau) = \tau^{-k}e^{-2\pi i m\tau}$, a meromorphic function on $\mathbf{C}$ with its only singularity at the origin. Show that

$$-2\pi i \mathrm{Res}_{\tau=0} g_m(\tau) = \frac{(-2\pi i)^k}{(k-1)!}m^{k-1}.$$

(c) Establish (1.2) by integrating $g_m(\tau)$ clockwise about a large rectangular path and applying the Residue Theorem. Argue that the integral along the top side goes to a_m and the integrals along the other three sides go to 0.

(d) Let $h : \mathbf{R} \longrightarrow \mathbf{C}$ be a function such that the integral $\int_{-\infty}^{\infty} |h(x)|dx$ is finite and the sum $\sum_{d\in\mathbf{Z}} h(x+d)$ converges absolutely and uniformly on compact subsets and is infinitely differentiable. Then the *Poisson summation formula* says that

$$\sum_{d\in\mathbf{Z}} h(x+d) = \sum_{m\in\mathbf{Z}} \hat{h}(m)e^{2\pi i m x}$$

where $\hat{h}$ is the *Fourier transform* of h,

$$\hat{h}(x) = \int_{t=-\infty}^{\infty} h(t)e^{-2\pi i x t}dt.$$

We will not prove this, but the idea is that the left side sum symmetrizes h to a function of period 1 and the right side sum is the Fourier series of the left side since the mth Fourier coefficient is $\int_{t=0}^{1}\sum_{d\in\mathbf{Z}} h(t+d)e^{-2\pi i m t}dt = \hat{h}(m)$. Letting $h(x) = 1/\tau^k$ where $\tau = x + iy$ with $y > 0$, show that h meets the conditions for Poisson summation. Show that $\hat{h}(m) = e^{-2\pi m y}a_m$ with a_m from above for $m > 0$, and that $\hat{h}(m) = 0$ for $m \le 0$. Establish formula (1.2) again, this time as a special case of Poisson summation. We will see more Poisson summation and Fourier analysis in connection with Eisenstein series in Chapter 4. (A hint for this exercise is at the end of the book.)

1.1.7. The *Bernoulli numbers* B_k are defined by the formal power series expansion

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

Thus they are calculable in succession by matching coefficients in the power series identity

$$t = (e^t - 1)\sum_{k=0}^{\infty} B_k \frac{t^k}{k!} = \sum_{n=1}^{\infty}\left(\sum_{k=0}^{n-1}\binom{n}{k}B_k\right)\frac{t^n}{n!}$$

(i.e., the nth parenthesized sum is 1 if $n = 1$ and 0 otherwise) and they are rational. Since the expression

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

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.