*Chapter 1*

# Modular Forms

This chapter introduces modular forms and congruence subgroups, which are central objects in this book. We first introduce the upper half plane and the group $\mathrm{SL}_2(\mathbb{Z})$ then recall some definitions from complex analysis. Next we define modular forms of level 1 followed by modular forms of general level. In Section 1.4 we discuss congruence subgroups and explain a simple way to compute generators for them and determine element membership. Section 1.5 lists applications of modular forms.

We assume familiarity with basic number theory, group theory, and complex analysis. For a deeper understanding of modular forms, the reader is urged to consult the standard books in the field, e.g., [**Lan95, Ser73, DI95, Miy89, Shi94, Kob84**]. See also [**DS05**], which is an excellent first introduction to the theoretical foundations of modular forms.

## 1.1. Basic Definitions

The group

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1 \text{ and } a, b, c, d \in \mathbb{R} \right\}$$

acts on the *complex upper half plane*

$$\mathfrak{h} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$$

by *linear fractional transformations*, as follows. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R})$, then for any $z \in \mathfrak{h}$ we let

$$\gamma(z) = \frac{az + b}{cz + d} \in \mathfrak{h}. \tag{1.1.1}$$

Since the determinant of $\gamma$ is 1, we have

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

**Definition 1.1** (Modular Group)**.** The *modular group* is the group of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$.

For example, the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{1.1.2}$$

are both elements of $\mathrm{SL}_2(\mathbb{Z})$; the matrix $S$ induces the function $z \mapsto -1/z$ on $\mathfrak{h}$, and $T$ induces the function $z \mapsto z + 1$.

**Theorem 1.2.** *The group* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by* $S$ *and* $T$*.*

**Proof.** See e.g. [**Ser73**, §VII.1]. □

In SAGE we compute the group $\mathrm{SL}_2(\mathbb{Z})$ and its generators as follows:

```
sage: G = SL(2,ZZ); G
Modular Group SL(2,Z)
sage: S, T = G.gens()
sage: S
[ 0 -1]
[ 1  0]
sage: T
[1 1]
[0 1]
```

**Definition 1.3** (Holomorphic and Meromorphic)**.** Let $R$ be an open subset of $\mathbb{C}$. A function $f : R \to \mathbb{C}$ is *holomorphic* if $f$ is complex differentiable at every point $z \in R$, i.e., for each $z \in R$ the limit

$$f'(z) = \lim_{h \to 0} \frac{f(z+h) - f(z)}{h}$$

exists, where $h$ may approach 0 along any path. A function $f : R \to \mathbb{C} \cup \{\infty\}$ is *meromorphic* if it is holomorphic except (possibly) at a discrete set $S$ of points in $R$, and at each $\alpha \in S$ there is a positive integer $n$ such that $(z - \alpha)^n f(z)$ is holomorphic at $\alpha$.

The function $f(z) = e^z$ is a holomorphic function on $\mathbb{C}$; in contrast, $1/(z - i)$ is meromorphic on $\mathbb{C}$ but not holomorphic since it has a pole at $i$. The function $e^{-1/z}$ is not even meromorphic on $\mathbb{C}$.

Modular forms are holomorphic functions on $\mathfrak{h}$ that transform in a particular way under a certain subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Before defining general modular forms, we define modular forms of level 1.

## 1.2. Modular Forms of Level 1

**Definition 1.4** (Weakly Modular Function)**.** A *weakly modular function* of *weight* $k \in \mathbb{Z}$ is a meromorphic function $f$ on $\mathfrak{h}$ such that for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and all $z \in \mathfrak{h}$ we have

$$f(z) = (cz + d)^{-k} f(\gamma(z)). \tag{1.2.1}$$

The constant functions are weakly modular of weight 0. There are no nonzero weakly modular functions of odd weight (see Exercise 1.4), and it is not obvious that there are any weakly modular functions of even weight $k \geq 2$ (but there are, as we will see!). The product of two weakly modular functions of weights $k_1$ and $k_2$ is a weakly modular function of weight $k_1 + k_2$ (see Exercise 1.3).

When $k$ is even, (1.2.1) has a possibly more conceptual interpretation; namely (1.2.1) is the same as

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

Thus (1.2.1) simply says that the weight $k$ "differential form" $f(z)(dz)^{k/2}$ is fixed under the action of every element of $\mathrm{SL}_2(\mathbb{Z})$.

By Theorem 1.2, the group $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices $S$ and $T$ of (1.1.2), so to show that a meromorphic function $f$ on $\mathfrak{h}$ is a weakly modular function, all we have to do is show that for all $z \in \mathfrak{h}$ we have

$$f(z+1) = f(z) \qquad \text{and} \qquad f(-1/z) = z^k f(z). \tag{1.2.2}$$

Suppose $f$ is a weakly modular function of weight $k$. A *Fourier expansion* of $f$, if it exists, is a representation of $f$ as $f(z) = \sum_{n=m}^{\infty} a_n e^{2\pi i n z}$, for all $z \in \mathfrak{h}$. Let $q = q(z) = e^{2\pi i z}$, which we view as a holomorphic function on $\mathbb{C}$. Let $D'$ be the open unit disk with the origin removed, and note that $q$ defines a map $\mathfrak{h} \to D'$. By (1.2.2) we have $f(z+1) = f(z)$, so there is a function $F : D' \to \mathbb{C}$ such that $F(q(z)) = f(z)$. This function $F$ is a complex-valued function on $D'$, but it may or may not be well behaved at 0.

Suppose that $F$ is well behaved at 0, in the sense that for some $m \in \mathbb{Z}$ and all $q$ in a neighborhood of 0 we have the equality

$$F(q) = \sum_{n=m}^{\infty} a_n q^n. \tag{1.2.3}$$

If this is the case, we say that $f$ is *meromorphic at* $\infty$. If, moreover, $m \geq 0$, we say that $f$ is *holomorphic at* $\infty$. We also call (1.2.3) the *q-expansion* of $f$ about $\infty$.

**Definition 1.5** (Modular Function)**.** A *modular function* of *weight* $k$ is a weakly modular function of weight $k$ that is meromorphic at $\infty$.

**Definition 1.6** (Modular Form)**.** A *modular form* of *weight* $k$ (and *level* 1) is a modular function of weight $k$ that is holomorphic on $\mathfrak{h}$ and at $\infty$.

If $f$ is a modular form, then there are numbers $a_n$ such that for all $z \in \mathfrak{h}$,

$$f(z) = \sum_{n=0}^{\infty} a_n q^n. \tag{1.2.4}$$

**Proposition 1.7.** *The above series converges for all* $z \in \mathfrak{h}$.

**Proof.** The function $f(q)$ is holomorphic on $D$, so its Taylor series converges absolutely in $D$. □

Since $e^{2\pi i z} \to 0$ as $z \to i\infty$, we set $f(\infty) = a_0$.

**Definition 1.8** (Cusp Form)**.** A *cusp form* of *weight* $k$ (and *level* 1) is a modular form of weight $k$ such that $f(\infty) = 0$, i.e., $a_0 = 0$.

Let $\mathbb{C}[[q]]$ be the ring of all *formal power series* in $q$. If $k = 2$, then $dq = 2\pi i q dz$, so $dz = \frac{1}{2\pi i}\frac{dq}{q}$. If $f(q)$ is a cusp form of weight 2, then

$$2\pi i f(z)dz = f(q)\frac{dq}{q} = \frac{f(q)}{q}dq \in \mathbb{C}[[q]]dq.$$

Thus the differential $2\pi i f(z)dz$ is holomorphic at $\infty$, since $q$ is a local parameter at $\infty$.

## 1.3. Modular Forms of Any Level

In this section we define spaces of modular forms of arbitrary level.

**Definition 1.9** (Congruence Subgroup)**.** A *congruence subgroup* of $\mathrm{SL}_2(\mathbb{Z})$ is any subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that contains

$$\Gamma(N) = \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$$

for some positive integer $N$. The smallest such $N$ is the *level of* $\Gamma$.

The most important congruence subgroups in this book are

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

and

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$

where $*$ means any element. Both groups have level $N$ (see Exercise 1.6).

Let $k$ be an integer. Define the *weight $k$ right action* of $\mathrm{GL}_2(\mathbb{Q})$ on the set of all functions $f : \mathfrak{h} \to \mathbb{C}$ as follows. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$, let

$$(f^{[\gamma]_k})(z) = \det(\gamma)^{k-1}(cz+d)^{-k} f(\gamma(z)). \tag{1.3.1}$$

**Proposition 1.10.** *Formula* (1.3.1) *defines a right action of* $\mathrm{GL}_2(\mathbb{Z})$ *on the set of all functions* $f : \mathfrak{h} \to \mathbb{C}$*; in particular,*

$$f^{[\gamma_1\gamma_2]_k} = (f^{[\gamma_1]_k})^{[\gamma_2]_k}.$$

**Proof.** See Exercise 1.7. □

**Definition 1.11** (Weakly Modular Function)**.** A *weakly modular function* of weight $k$ for a congruence subgroup $\Gamma$ is a meromorphic function $f : \mathfrak{h} \to \mathbb{C}$ such that $f^{[\gamma]_k} = f$ for all $\gamma \in \Gamma$.

A central object in the theory of modular forms is the *set of cusps*

$$\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}.$$

An element $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{P}^1(\mathbb{Q})$ by

$$\gamma(z) = \begin{cases} \frac{az+b}{cz+d} & \text{if } z \neq \infty, \\ \frac{a}{c} & \text{if } z = \infty. \end{cases}$$

Also, note that if the denominator $c$ or $cz+d$ is 0 above, then

$$\gamma(z) = \infty \in \mathbb{P}^1(\mathbb{Q}).$$

The set of *cusps for a congruence subgroup* $\Gamma$ is the set $C(\Gamma)$ of $\Gamma$-orbits of $\mathbb{P}^1(\mathbb{Q})$. (We will often identify elements of $C(\Gamma)$ with a representative element from the orbit.) For example, the lemma below asserts that if $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, then there is exactly one orbit, so $C(\mathrm{SL}_2(\mathbb{Z})) = \{[\infty]\}$.

**Lemma 1.12.** *For any cusps* $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$ *there exists* $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ *such that* $\gamma(\alpha) = \beta$.

**Proof.** This is Exercise 1.8. □

**Proposition 1.13.** *For any congruence subgroup* $\Gamma$*, the set* $C(\Gamma)$ *of cusps is finite.*

**Proof.** This is Exercise 1.9. □

See [**DS05**, §3.8] and Algorithm 8.12 below for more discussion of cusps and results relevant to their enumeration.

In order to define modular forms for general congruence subgroups, we next explain what it means for a function to be holomorphic on the *extended upper half plane*

$$\mathfrak{h}^* = \mathfrak{h} \cup \mathbb{P}^1(\mathbb{Q}).$$

See [**Shi94**, §1.3–1.5] for a detailed description of the correct topology to consider on $\mathfrak{h}^*$. In particular, a basis of neighborhoods for $\alpha \in \mathbb{Q}$ is given by the sets $\{\alpha\} \cup D$, where $D$ is an open disc in $\mathfrak{h}$ that is tangent to the real line at $\alpha$.

Recall from Section 1.2 that a weakly modular function $f$ on $\mathrm{SL}_2(\mathbb{Z})$ is holomorphic at $\infty$ if its $q$-expansion is of the form $\sum_{n=0}^{\infty} a_n q^n$.

In order to make sense of holomorphicity of a weakly modular function $f$ for an arbitrary congruence subgroup $\Gamma$ at any $\alpha \in \mathbb{Q}$, we first prove a lemma.

**Lemma 1.14.** *If $f : \mathfrak{h} \to \mathbb{C}$ is a weakly modular function of weight $k$ for a congruence subgroup $\Gamma$ and if $\delta \in \mathrm{SL}_2(\mathbb{Z})$, then $f^{[\delta]_k}$ is a weakly modular function for $\delta^{-1}\Gamma\delta$.*

**Proof.** If $s = \delta^{-1}\gamma\delta \in \delta^{-1}\Gamma\delta$, then

$$(f^{[\delta]_k})^{[s]_k} = f^{[\delta s]_k} = f^{[\delta\delta^{-1}\gamma\delta]_k} = f^{[\gamma\delta]_k} = f^{[\delta]_k}.$$

□

Fix a weakly modular function $f$ of weight $k$ for a congruence subgroup $\Gamma$, and suppose $\alpha \in \mathbb{Q}$. In Section 1.2 we constructed the $q$-expansion of $f$ by using that $f(z) = f(z+1)$, which held since $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. There are congruence subgroups $\Gamma$ such that $T \notin \Gamma$. Moreover, even if we are interested only in modular forms for $\Gamma_1(N)$, where we have $T \in \Gamma_1(N)$ for all $N$, we will still have to consider $q$-expansions at infinity for modular forms on groups $\delta^{-1}\Gamma_1(N)\delta$, and these need not contain $T$. Fortunately, $T^N = \left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma(N)$, so a congruence subgroup of level $N$ contains $T^N$. Thus we have $f(z+H) = f(H)$ for some positive integer $H$, e.g., $H = N$ always works, but there may be a smaller choice of $H$. The minimal choice of $H > 0$ such that $\left(\begin{smallmatrix} 1 & H \\ 0 & 1 \end{smallmatrix}\right) \in \delta^{-1}\Gamma\delta$, where $\delta(\infty) = \alpha$, is called the *width of the cusp* $\alpha$ relative to the group $\Gamma$ (see Section 1.4.1). When $f$ is meromorphic at infinity, we obtain a Fourier expansion

$$f(z) = \sum_{n=m}^{\infty} a_n q^{n/H} \tag{1.3.2}$$

in powers of the function $q^{1/H} = e^{2\pi iz/H}$. We say that $f$ is holomorphic at $\infty$ if in (1.3.2) we have $m \geq 0$.

What about the other cusps $\alpha \in \mathbb{P}^1(\mathbb{Q})$? By Lemma 1.12 there is a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(\infty) = \alpha$. We declare $f$ to be *holomorphic at the cusp* $\alpha$ if the weakly modular function $f^{[\gamma]_k}$ is holomorphic at $\infty$.

**Definition 1.15** (Modular Form)**.** A *modular form* of integer *weight* $k$ for a congruence subgroup $\Gamma$ is a weakly modular function $f : \mathfrak{h} \to \mathbb{C}$ that is holomorphic on $\mathfrak{h}^*$. We let $M_k(\Gamma)$ denote the space of weight $k$ modular forms of weight $k$ for $\Gamma$.

**Proposition 1.16.** *If a weakly modular function $f$ is holomorphic at a set of representative elements for $C(\Gamma)$, then it is holomorphic at every element of $\mathbb{P}^1(\mathbb{Q})$.*

**Proof.** Let $c_1, \ldots, c_n \in \mathbb{P}^1(\mathbb{Q})$ be representatives for the set of cusps for $\Gamma$. If $\alpha \in \mathbb{P}^1(\mathbb{Q})$, then there is $\gamma \in \Gamma$ such that $\alpha = \gamma(c_i)$ for some $i$. By hypothesis $f$ is holomorphic at $c_i$, so if $\delta \in \mathrm{SL}_2(\mathbb{Z})$ is such that $\delta(\infty) = c_i$, then $f^{[\delta]_k}$ is holomorphic at $\infty$. Since $f$ is a weakly modular function for $\Gamma$,

$$f^{[\delta]_k} = (f^{[\gamma]_k})^{[\delta]_k} = f^{[\gamma\delta]_k}. \tag{1.3.3}$$

But $\gamma(\delta(\infty)) = \gamma(c_i) = \alpha$, so (1.3.3) implies that $f$ is holomorphic at $\alpha$. □

## 1.4. Remarks on Congruence Subgroups

Recall that a congruence subgroup is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that contains $\Gamma(N)$ for some $N$. Any congruence subgroup has finite index in $\mathrm{SL}_2(\mathbb{Z})$, since $\Gamma(N)$ does. What about the converse: is every finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ a congruence subgroup? This is the *congruence subgroup problem*. One can ask about the congruence subgroup problem with $\mathrm{SL}_2(\mathbb{Z})$ replaced by many similar groups. If $p$ is a prime, then one can prove that every finite index subgroup of $\mathrm{SL}_2(\mathbb{Z}[1/p])$ is a congruence subgroup (i.e., contains the kernel of reduction modulo some integer coprime to $p$), and for any $n > 2$, all finite index subgroups of $\mathrm{SL}_n(\mathbb{Z})$ are congruence subgroups (see [**Hum80**]). However, there are numerous finite index subgroups of $\mathrm{SL}_2(\mathbb{Z})$ that are not congruence subgroups. The paper [**Hsu96**] contains an *algorithm* to decide if certain finite index subgroups are congruence subgroups and gives an example of a subgroup of index 12 that is not a congruence subgroup.

One can consider modular forms even for noncongruence subgroups. See, e.g., [**Tho89**] and the papers it references for work on this topic. We will not consider such modular forms further in this book. Note that modular symbols (which we define later in this book) *are* computable for noncongruence subgroups.

Finding coset representatives for $\Gamma_0(N)$, $\Gamma_1(N)$ and $\Gamma(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ is straightforward and will be discussed at length later in this book. To make the problem more explicit, note that you can quotient out by $\Gamma(N)$ first. Then the question amounts to finding coset representatives for a subgroup of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ (and lifting), which is reasonably straightforward.

Given coset representatives for a finite index subgroup $G$ of $\mathrm{SL}_2(\mathbb{Z})$, we can compute generators for $G$ as follows. Let $R$ be a set of coset representatives for $G$. Let $\sigma, \tau \in \mathrm{SL}_2(\mathbb{Z})$ be the matrices denoted by $S$ and $T$ in (1.1.2). Define maps $s, t : R \to G$ as follows. If $r \in R$, then there exists a unique $\alpha_r \in R$ such that $Gr\sigma = G\alpha_r$. Let $s(r) = r\sigma\alpha_r^{-1}$. Likewise, there is a unique $\beta_r$ such that $Gr\tau = G\beta_r$ and we let $t(r) = r\tau\beta_r^{-1}$. Note that $s(r)$ and $t(r)$ are in $G$ for all $r$. Then $G$ is generated by $s(R) \cup t(R)$.

**Proposition 1.17.** *The above procedure computes generators for $G$.*

**Proof.** Without loss of generality, assume that $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ represents the coset of $G$. Let $g$ be an element of $G$. Since $\sigma$ and $\tau$ generate $\mathrm{SL}_2(\mathbb{Z})$, it is possible to write $g$ as a product of powers of $\sigma$ and $\tau$. There is a procedure, which we explain below with an example in order to avoid cumbersome notation, which writes $g$ as a product of elements of $s(R) \cup t(R)$ times a right coset representative $r \in R$. For example, if

$$g = \sigma\tau^2\sigma\tau,$$

then $g = I\sigma\tau^2\sigma\tau = s(I)y\tau^2\sigma\tau$ for some $y \in R$. Continuing,

$$s(I)y\tau^2\sigma\tau = s(I)(y\tau)\tau\sigma\tau = s(I)(t(y)z)\tau\sigma\tau$$

for some $z \in R$. Again,

$$s(I)(t(y)z)\tau\sigma\tau = s(I)t(y)(z\tau)\sigma\tau = \cdots.$$

The procedure illustrated above (with an example) makes sense for arbitrary $g$ and, after carrying it out, writes $g$ as a product of elements of $s(R) \cup t(R)$ times a right coset representative $r \in R$. But $g \in G$ and $I$ is the right coset representative for $G$, so this right coset representative must be $I$. □

**Remark 1.18.** We could also apply the proof of Proposition 1.17 to write any element of $G$ in terms of the given generators. Moreover, we could use it to write any element $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ in the form $gr$, where $g \in G$ and $r \in R$, so we can decide whether or not $\gamma \in G$.

**1.4.1. Computing Widths of Cusps.** Let $\Gamma$ be a congruence subgroup of level $N$. Suppose $\alpha \in C(\Gamma)$ is a cusp, and choose $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(\infty) = \alpha$. Recall that the minimal $h$ such that $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \gamma^{-1}\Gamma\gamma$ is called the *width of the cusp* $\alpha$ for the group $\Gamma$. In this section we discuss how to compute $h$.

**Algorithm 1.19** (Width of Cusp)**.** *Given a congruence subgroup $\Gamma$ of level $N$ and a cusp $\alpha$ for $\Gamma$, this algorithm computes the width $h$ of $\alpha$. We assume that $\Gamma$ is given by congruence conditions, e.g., $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$.*

(1) [Find $\gamma$] Use the extended Euclidean algorithm to find $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(\infty) = \alpha$, as follows. If $\alpha = \infty$, set $\gamma = 1$; otherwise, write $\alpha = a/b$, find $c, d$ such that $ad - bc = 1$, and set $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

(2) [Compute Conjugate Matrix] Compute the following element of $\mathrm{Mat}_2(\mathbb{Z}[x])$:
$$\delta(x) = \gamma \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \gamma^{-1}.$$
Note that the entries of $\delta(x)$ are constant or linear in $x$.

(3) [Solve] The congruence conditions that define $\Gamma$ give rise to four linear congruence conditions on $x$. Use techniques from elementary number theory (or enumeration) to find the smallest simultaneous positive solution $h$ to these four equations.

**Example 1.20.** (1) Suppose $\alpha = 0$ and $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$. Then $\gamma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ has the property that $\gamma(\infty) = \alpha$. Next, the congruence condition is
$$\delta(x) = \gamma \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \gamma^{-1} = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N}.$$
Thus the smallest positive solution is $h = N$, so the width of 0 is $N$.

(2) Suppose $N = pq$ where $p, q$ are distinct primes, and let $\alpha = 1/p$. Then $\gamma = \left(\begin{smallmatrix} 1 & 0 \\ p & 1 \end{smallmatrix}\right)$ sends $\infty$ to $\alpha$. The congruence condition for $\Gamma_0(pq)$ is
$$\delta(x) = \gamma \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \gamma^{-1} = \begin{pmatrix} 1 - px & x \\ -p^2 x & px + 1 \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{pq}.$$
Since $p^2 x \equiv 0 \pmod{pq}$, we see that $x = q$ is the smallest solution. Thus $1/p$ has width $q$, and symmetrically $1/q$ has width $p$.

**Remark 1.21.** For $\Gamma_0(N)$, once we enforce that the bottom left entry is 0 (mod $N$) and use that the determinant is 1, the coprimality from the other two congruences is automatic. So there is one congruence to solve in the $\Gamma_0(N)$ case. There are two congruences in the $\Gamma_1(N)$ case.

## 1.5. Applications of Modular Forms

The above definition of modular forms might leave the impression that modular forms occupy an obscure corner of complex analysis. This is *not* the case! Modular forms are highly geometric, arithmetic, and topological objects that are of extreme interest all over mathematics:

(1) **Fermat's last theorem:** Wiles' proof [**Wil95**] of Fermat's last theorem uses modular forms extensively. The work of Wiles et al. on modularity also massively extends computational methods for elliptic curves over $\mathbb{Q}$, because many elliptic curve algorithms, e.g., for computing $L$-functions, modular degrees, Heegner points, etc., require that the elliptic curve be modular.

(2) **Diophantine equations:** Wiles' proof of Fermat's last theorem has made available a wide array of new techniques for solving certain diophantine equations. Such work relies crucially on having access to tables or software for computing modular forms. See, e.g., [**Dar97, Mer99, Che05, SC03**]. (Wiles did not need a computer, because the relevant spaces of modular forms that arise in his proof have dimension 0!) Also, according to Siksek (personal communication) the paper [**BMS06**] would "have been entirely impossible to write without [the algorithms described in this book]."

(3) **Congruent number problem:** This ancient open problem is to determine which integers are the area of a right triangle with rational side lengths. There is a potential solution that uses modular forms (of weight 3/2) extensively (the solution is conditional on truth of the Birch and Swinnerton-Dyer conjecture, which is not yet known). See [**Kob84**].

(4) **Topology:** Topological modular forms are a major area of current research.

(5) **Construction of Ramanujan graphs:** Modular forms can be used to construct almost optimal expander graphs, which play a role in communications network theory.

(6) **Cryptography and Coding Theory:** Point counting on elliptic curves over finite fields is crucial to the construction of elliptic curve cryptosystems, and modular forms are relevant to efficient algorithms for point counting (see [**Elk98**]). Algebraic curves that are associated to modular forms are useful in constructing and studying certain error-correcting codes (see [**Ebe02**]).

(7) **The Birch and Swinnerton-Dyer conjecture:** This central open problem in arithmetic geometry relates arithmetic properties of elliptic curves (and abelian varieties) to special values of $L$-functions. Most deep results toward this conjecture use modular forms extensively (e.g., work of Kolyvagin, Gross-Zagier, and Kato). Also, modular forms are used to compute and prove results about special values of these $L$-functions. See [**Wil00**].

(8) **Serre's Conjecture on modularity of Galois representation:** Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the Galois group of an algebraic closure of $\mathbb{Q}$. Serre conjectured and many people have (nearly!) proved that every continuous homomorphism $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$, where $\mathbb{F}_q$ is a finite field and $\det(\rho(\text{complex conjugation})) = -1$, "arises" from a modular form. More precisely, for almost all primes $p$ the coefficients $a_p$ of a modular (eigen-)form $\sum a_n q^n$ are congruent to the traces of elements $\rho(\mathrm{Frob}_p)$, where $\mathrm{Frob}_p$ are certain special elements of $G_{\mathbb{Q}}$ called Frobenius elements. See [**RS01**] and [**DS05**, Ch. 9].

(9) **Generating functions for partitions:** The generating functions for various kinds of partitions of an integer can often be related to modular forms. Deep theorems about modular forms then translate into results about partitions. See work of Ramanujan, Gordon, Andres, and Ahlgren and Ono (e.g., [**AO01**]).

(10) **Lattices:** If $L \subset \mathbb{R}^n$ is an even unimodular lattice (the basis matrix has determinant $\pm 1$ and $\lambda \cdot \lambda \in 2\mathbb{Z}$ for all $\lambda \in L$), then the theta series

$$\theta_L(q) = \sum_{\lambda \in L} q^{\lambda \cdot \lambda}$$

is a modular form of weight $n/2$. The coefficient of $q^m$ is the number of lattice vectors with squared length $m$. Theorems and computational methods for modular forms translate into theorems and computational methods for lattices. For example, the 290 theorem of M. Bharghava and J. Hanke is a theorem about lattices, which asserts that an integer-valued quadratic form represents all positive integers if and only if it represents the integers up to 290; it is proved by doing many calculations with modular forms (both theoretical and with a computer).

## 1.6. Exercises

1.1 Suppose $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ has positive determinant. Prove that if $z \in \mathbb{C}$ is a complex number with positive imaginary part, then the imaginary part of $\gamma(z) = (az + b)/(cz + d)$ is also positive.

1.2 Prove that every rational function (quotient of two polynomials) is a meromorphic function on $\mathbb{C}$.

1.3 Suppose $f$ and $g$ are weakly modular functions for a congruence subgroup $\Gamma$ with $f \neq 0$.

(a) Prove that the product $fg$ is a weakly modular function for $\Gamma$.

(b) Prove that $1/f$ is a weakly modular function for $\Gamma$.

(c) If $f$ and $g$ are modular functions, show that $fg$ is a modular function for $\Gamma$.
(d) If $f$ and $g$ are modular forms, show that $fg$ is a modular form for $\Gamma$.

1.4 Suppose $f$ is a weakly modular function of odd weight $k$ and level $\Gamma_0(N)$ for some $N$. Show that $f = 0$.

1.5 Prove that $\mathrm{SL}_2(\mathbb{Z}) = \Gamma_0(1) = \Gamma_1(1) = \Gamma(1)$.

1.6 (a) Prove that $\Gamma_1(N)$ is a group.
(b) Prove that $\Gamma_1(N)$ has finite index in $\mathrm{SL}_2(\mathbb{Z})$ (Hint: It contains the kernel of the homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.)
(c) Prove that $\Gamma_0(N)$ has finite index in $\mathrm{SL}_2(\mathbb{Z})$.
(d) Prove that $\Gamma_0(N)$ and $\Gamma_1(N)$ have level $N$.

1.7 Let $k$ be an integer, and for any function $f : \mathfrak{h}^* \to \mathbb{C}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$, set $f^{[\gamma]_k}(z) = \det(\gamma)^{k-1} \cdot (cz + d)^{-k} \cdot f(\gamma(z))$. Prove that if $\gamma_1, \gamma_2 \in \mathrm{GL}_2(\mathbb{Z})$, then for all $z \in \mathfrak{h}^*$ we have

$$f^{[\gamma_1\gamma_2]_k}(z) = ((f^{[\gamma_1]_k})^{[\gamma_2]_k})(z).$$

1.8 Prove that for any $\alpha, \beta \in \mathbb{P}^1(\mathbb{Q})$, there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(\alpha) = \beta$.

1.9 Prove Proposition 1.13, which asserts that the set of cusps $C(\Gamma)$, for any congruence subgroup $\Gamma$, is finite.

1.10 Use Algorithm 1.19 to give an example of a group $\Gamma$ and cusp $\alpha$ with width 2.