**Remark 1.3.10.** 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 2 congruences in the $\Gamma_1(N)$ case.

## 1.4 Examples of Modular Forms of Level 1

In this section you will finally see some examples of modular forms of level 1! We will first introduce the Eisenstein series, one of each weight, then define $\Delta$, which is a cusp form of weight 12. In Section 1.5 we will prove the structure theorem, which says that using addition and multiplication of these forms, we can generate all modular forms of level 1.

For an even integer $k \geq 4$, the *non-normalized weight $k$ Eisenstein series* is

$$G_k(z) = \sum_{m,n\in\mathbb{Z}}^{*} \frac{1}{(mz+n)^k},$$

where for a given $z$, the sum is over all $m, n \in \mathbb{Z}$ such that $mz + n \neq 0$.

**Proposition 1.4.1.** *The function $G_k(z)$ is a modular form of weight $k$, i.e., $G_k \in M_k(\mathrm{SL}_2(\mathbb{Z}))$.*

*Proof.* See [Ser73, § VII.2.3] for a proof that $G_k(z)$ defines a holomorphic function on $\mathfrak{h}^*$. To see that $G_k$ is modular, observe that

$$G_k(z+1) = \sum^{*} \frac{1}{(m(z+1)+n)^k} = \sum^{*} \frac{1}{(mz+(n+m))^k} = \sum^{*} \frac{1}{(mz+n)^k},$$

and

$$G_k(-1/z) = \sum^{*} \frac{1}{(-m/z+n)^k} = \sum^{*} \frac{z^k}{(-m+nz)^k} = z^k \sum^{*} \frac{1}{(mz+n)^k} = z^k G_k(z).$$

□

**Proposition 1.4.2.** *$G_k(\infty) = 2\zeta(k)$, where $\zeta$ is the Riemann zeta function.*

*Proof.* Taking the limit as $z \to i\infty$ in the definition of $G_k(z)$, we obtain $\sum_{n\in\mathbb{Z}}^{*} \frac{1}{n^k}$, since the terms involving $z$ all go to 0 as $z \mapsto i\infty$. This sum is twice $\zeta(k) = \sum_{n\geq 1} \frac{1}{n^k}$. □

For example,

$$G_4(\infty) = 2\zeta(4) = \frac{1}{3^2 \cdot 5}\pi^4$$

and

$$G_6(\infty) = 2\zeta(6) = \frac{2}{3^3 \cdot 5 \cdot 7}\pi^6.$$

### 1.4.1 The Cusp Form $\Delta$

Suppose $E = \mathbb{C}/\Lambda$ is an elliptic curve over $\mathbb{C}$, viewed as a quotient of $\mathbb{C}$ by a lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, with $\omega_1/\omega_2 \in \mathfrak{h}$. Then

$$\wp_\Lambda(u) = \frac{1}{u^2} + \sum_{k=4,\ (k \text{ even})}^{\infty} (k-1)G_k(\omega_1/\omega_2)u^{k-2},$$

and

$$(\wp')^2 = 4\wp^3 - 60G_4(\omega_1/\omega_2)\wp - 140G_6(\omega_1/\omega_2).$$

The discriminant of the cubic $4x^3 - 60G_4(\omega_1/\omega_2)x - 140G_6(\omega_1/\omega_2)$ is $16\Delta(\omega_1/\omega_2)$, where

$$\Delta = (60G_4)^3 - 27(140G_6)^2$$

is a cusp form of weight 12.

**Lemma 1.4.3.** *The cusp form $\Delta$ has a 0 only at $\infty$.*

*Proof.* Let $\omega_1, \omega_2$ be as above. Since $E$ is an elliptic curve, $\Delta(\omega_1/\omega_2) \neq 0$. □

### 1.4.2 Fourier Expansions of Eisenstein Series

Recall from (1.2.3) that elements $f$ of $M_k(\mathrm{SL}_2(\mathbb{Z}))$ can be expressed as formal power series in terms of $q(z) = e^{2\pi i z}$, and that this expansion is called the Fourier expansion of $f$. The following proposition gives the Fourier expansion of the Eisenstein series $G_k(z)$.

**Proposition 1.4.4.** *For every even integer $k \geq 4$, we have*

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

*where $\sigma_d(n)$ is the sum of the $d$th powers of the divisors of $n$.*

*Proof.* See [Ser73, §VII.4], which uses a series of clever manipulations of series, starting with the identity

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

□

From a computational point of view, the $q$-expansion for $G_k$ from Proposition 1.4.4 is unsatisfactory, because it involves transcendental numbers. To understand more clearly what is going on, we introduce the *Bernoulli numbers* $B_n$ for $n \geq 0$ *defined* by the following equality of formal power series:

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}. \tag{1.4.1}$$

Expanding the power series on the left we have

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \frac{x^2}{12} - \frac{x^4}{720} + \frac{x^6}{30240} - \frac{x^8}{1209600} + \cdots$$

As this expansion suggests, the Bernoulli numbers $B_n$ with $n > 1$ odd are 0 (see Exercise 7.6). Expanding the series further, we obtain the following table:

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{30},$$

$$B_{10} = \frac{5}{66}, \quad B_{12} = -\frac{691}{2730}, \quad B_{14} = \frac{7}{6}, \quad B_{16} = -\frac{3617}{510}, \quad B_{18} = \frac{43867}{798},$$

$$B_{20} = -\frac{174611}{330}, \quad B_{22} = \frac{854513}{138}, \quad B_{24} = -\frac{236364091}{2730}, \quad B_{26} = \frac{8553103}{6}.$$

Use the `bernoulli` command to compute Bernoulli numbers in SAGE.

```
sage: bernoulli(12)
-691/2730
sage: bernoulli(50)
495057205241079648212477525/66
```

For us, the significance of the Bernoulli numbers is their connection with values of $\zeta$ at positive even integers.

**Proposition 1.4.5.** *If $k \geq 2$ is an even integer, then*

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

*Proof.* The proof in [Ser73, §VII.4] involves manipulating a power series expansion for $z\cot(z)$. □

**Definition 1.4.6** (Normalized Eisenstein Series)**.** The *normalized Eisenstein series* of even weight $k \geq 4$ is

$$E_k = \frac{(k-1)!}{2 \cdot (2\pi i)^k} \cdot G_k$$

Combining Propositions 1.4.4 and 1.4.5 we see that

$$E_k = -\frac{B_k}{2k} + q + \sum_{n=2}^{\infty} \sigma_{k-1}(n) q^n. \tag{1.4.2}$$

It is thus now simple to explicitly write down Eisenstein series (see Exercise 7.8).

**Warning 1.4.7.** Our series $E_k$ is normalized so that the coefficient of $q$ is 1, but often in the literature $E_k$ is normalized so that the constant coefficient is 1. We use the normalization with the coefficient of $q$ equal to 1, because then the eigenvalue of the $n$th Hecke operator (see Section 1.7) is the coefficient of $q^n$. Our normalization is also convenient when considering congruences between cusp forms and Eisenstein series.

## 1.5 Structure Theorem

If $f$ is a nonzero meromorphic function on $\mathfrak{h}$ and $w \in \mathfrak{h}$, let $\mathrm{ord}_w(f)$ be the largest integer $n$ such that $f/(w-z)^n$ is holomorphic at $w$. If $f = \sum_{n=m}^{\infty} a_n q^n$ with $a_m \neq 0$, let $\mathrm{ord}_\infty(f) = m$. We will use the following theorem to give a presentation for the vector space of modular forms of weight $k$; this presentation will allow us to obtain an algorithm to compute a basis for this space.

Let $\mathcal{F}$ be the subset of $\mathfrak{h}$ of numbers $z$ with $|z| \geq 1$ and $\mathrm{Re}(z) \leq 1/2$. This is the standard fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$.

**Theorem 1.5.1** (Valence Formula)**.** *Suppose $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ is nonzero. Then*

$$\mathrm{ord}_\infty(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \sum_{w\in D}^{*} \mathrm{ord}_w(f) = \frac{k}{12},$$

*where* $\sum_{w\in D}^{*}$ *is the sum over elements of $\mathcal{F}$ other than $i$ or $\rho$.*

*Proof.* Serre proves this theorem in [Ser73, §VII.3] using the residue theorem from complex analysis. □

Let $M_k = M_k(\mathrm{SL}_2())$ denote the complex vector space of modular forms of weight $k$ for $\mathrm{SL}_2(\mathbb{Z})$, and let $S_k = S_k(\mathrm{SL}_2())$ denote the subspace of weight $k$ cusp forms for $\mathrm{SL}_2(\mathbb{Z})$. We have an exact sequence

$$0 \to S_k \to M_k \to \mathbb{C}$$

that sends $f \in M_k$ to $f(\infty)$. When $k \geq 4$ is even, the space $M_k$ contains the Eisenstein series $G_k$ and $G_k(\infty) = 2\zeta(k) \neq 0$, so the map $M_k \to \mathbb{C}$ is surjective, so the following sequence is exact:

$$0 \to S_k \to M_k \to \mathbb{C} \to 0 \qquad (\text{when } k \geq 4 \text{ is even})$$

Thus when $k \geq 4$ is even $\dim(S_k) = \dim(M_k) - 1$ hence

$$M_k = S_k \oplus \mathbb{C}G_k.$$

**Proposition 1.5.2.** *For $k < 0$ and $k = 2$, we have $M_k = 0$.*

*Proof.* Suppose $f \in M_k$ is nonzero yet $k = 2$ or $k < 0$. By Theorem 1.5.1,

$$\mathrm{ord}_\infty(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \sum_{w\in D}^{*} \mathrm{ord}_w(f) = \frac{k}{12} \leq 1/6.$$

This is impossible because each quantity on the left-hand side is nonnegative so whatever the sum is, it is too big (or 0, in which $k = 0$). □

**Theorem 1.5.3.** *Multiplication by $\Delta$ defines an isomorphism $M_{k-12} \to S_k$.*

*Proof.* (We follow [Ser73, §VII.3.2] closely.) We apply Theorem 1.5.1 to $G_4$ and $G_6$. If $f = G_4$, then

$$\operatorname{ord}_\infty(f) + \frac{1}{2}\operatorname{ord}_i(f) + \frac{1}{3}\operatorname{ord}_\rho(f) + \sum_{w\in D}^{*} \operatorname{ord}_w(f) = \frac{4}{12} = \frac{1}{3},$$

with the ords all nonnegative, so $\operatorname{ord}_\rho(G_4) = 1$ and $\operatorname{ord}_w(G_4) = 0$ for all $w \neq \rho$. Likewise $\operatorname{ord}_i(G_6) = 1$ and $\operatorname{ord}_w(G_6) = 0$ for all $w \neq i$. Thus $\Delta(i) \neq 0$, so $\Delta$ is not identically 0 (this also follows from Lemma 1.4.3 above). Since $\Delta$ has weight 12 and $\operatorname{ord}_\infty(\Delta) \geq 1$, Theorem 1.5.1 implies that $\Delta$ has a simple zero at $\infty$ and does not vanish on $\mathfrak{h}$. Thus if $f \in S_k$ and we let $g = f/\Delta$, then $g$ is holomorphic and satisfies the appropriate transformation formula, so $g$ is a modular form of weight $k - 12$. □

**Corollary 1.5.4.** *For $k = 0, 4, 6, 8, 10, 14$, the vector space $M_k$ has dimension 1, with basis 1, $G_4$, $G_6$, $E_8$, $E_{10}$, and $E_{14}$, respectively, and $S_k = 0$.*

*Proof.* Combining Proposition 1.5.2 with Theorem 1.5.3 we see that the spaces $M_k$ for $k \leq 10$ can not have dimension bigger than 1, since then $M_{k'} \neq 0$ for some $k' < 0$. Also $M_{14}$ has dimension at most 1, since $M_2$ has dimension 0. Each of the indicated spaces of weight $\geq 4$ contains the indicated Eisenstein series, so has dimension 1, as claimed. □

**Corollary 1.5.5.** $\dim M_k = \begin{cases} 0 & \text{if } k \text{ is odd,} \\ \lfloor k/12 \rfloor & \text{if } k \equiv 2 \pmod{12}, \\ \lfloor k/12 \rfloor + 1 & \text{if } k \not\equiv 2 \pmod{12}, \end{cases}$ *where $\lfloor x \rfloor$ is the biggest integer $\leq x$.*

*Proof.* As we have seen above, the formula is true when $k \leq 12$. By Theorem 1.5.3, the dimension increases by 1 when $k$ is replaced by $k + 12$. □

**Theorem 1.5.6.** *The space $M_k$ has as basis the modular forms $G_4^a G_6^b$, where $a, b$ are all pairs of nonnegative integers such that $4a + 6b = k$.*

*Proof.* We first prove by induction that the modular forms $G_4^a G_6^b$ generate $M_k$, the cases $k \leq 12$ being clear (e.g., when $k = 0$ we have $a = b = 0$ and basis 1). Choose some pair of integers $a, b$ such that $4a + 6b = k$ (it is an elementary exercise to show these exist). The form $g = G_4^a G_6^b$ is not a cusp form, since it is nonzero at $\infty$. Now suppose $f \in M_k$ is arbitrary. Since $M_k = S_k \oplus \mathbb{C}G_k$, there is $\alpha \in \mathbb{C}$ such that $f - \alpha g \in S_k$. Then by Theorem 1.5.3, there is $h \in M_{k-12}$ such that $f - \alpha g = \Delta h$. By induction, $h$ is a polynomial in $G_4$ and $G_6$ of the required type, and so is $\Delta$, so $f$ is as well.

Suppose there is a nontrivial linear relation between the $G_4^a G_6^b$ for a given $k$. By multiplying the linear relation by a suitable power of $G_4$ and $G_6$, we may assume that that we have such a nontrivial relation with $k \equiv 0 \pmod{12}$. Now divide the linear relation by $G_6^{k/12}$ to see that $G_4^3/G_6^2$ satisfies a polynomial with coefficients in $\mathbb{C}$. Hence $G_4^3/G_6^2$ is a root of a polynomial, hence a constant, which is a contradiction since the $q$-expansion of $G_4^3/G_6^2$ is not constant. □

**Algorithm 1.5.7** (Basis for $M_k$)**.** Given integers $n$ and $k$, this algorithm computes a basis of $q$-expansions for the complex vector space $M_k$ mod $q^n$. The $q$-expansions output by this algorithm have coefficients in $\mathbb{Q}$.

- [Simple Case] If $k = 0$ output the basis with just 1 in it, and terminate; otherwise if $k < 4$ or $k$ is odd, output the empty basis and terminate.
- [Power Series] Compute $E_4$ and $E_6$ mod $q^n$ using the formula from (1.4.2) and the definition (1.4.1) of Bernoulli numbers.
- [Initialize] Set $b = 0$.
- [Enumerate Basis] For each integer $b$ between 0 and $\lfloor k/6 \rfloor$, compute $a = (k - 6b)/4$. If $a$ is an integer, compute and output the basis element $E_4^a E_6^b \mod q^n$. When we compute, e.g., $E_4^a$, do the computation by finding $E_4^m \pmod{q^n}$ for each $m \leq a$, and save these intermediate powers, so they can be reused later, and likewise for powers of $E_6$.

*Proof.* This is simply a translation of Theorem 1.5.6 into an algorithm, since $E_k$ is a nonzero scalar multiple of $G_k$. That the $q$-expansions have coefficients in $\mathbb{Q}$ follows from (1.4.2). □

**Example 1.5.8.** We compute a basis for $M_{24}$, which is the space with smallest weight whose dimension is bigger than 1. It has as basis $E_4^6$, $E_4^3 E_6^2$, and $E_6^4$, whose explicit expansions are

$$\begin{aligned} E_4^6 &= \frac{1}{191102976000000} + \frac{1}{132710400000}q + \frac{203}{44236800000}q^2 + \cdots \\ E_4^3 E_6^2 &= \frac{1}{3511517184000} - \frac{1}{12192768000}q - \frac{377}{4064256000}q^2 + \cdots \\ E_6^4 &= \frac{1}{64524128256} - \frac{1}{32006016}q + \frac{241}{10668672}q^2 + \cdots \end{aligned}$$

In Section 1.6, we will discuss properties of the reduced row echelon form of any basis for $M_k$, which have better properties than the above basis.

## 1.6 The Victor Miller Basis

**Lemma 1.6.1** (Victor Miller)**.** *The space $S_k$ has a basis $f_1, \ldots, f_d$ such that if $a_i(f_j)$ is the $i$th coefficient of $f_j$, then $a_i(f_j) = \delta_{i,j}$ for $i = 1, \ldots, d$. Moreover the $f_j$ all lie in $\mathbb{Z}[[q]]$.*

This is a straightforward construction involving $E_4$, $E_6$ and $\Delta$. The following proof very closely follows [Lan95, Ch. X, Thm. 4.4], which is in turn follows the first lemma of Victor Miller's thesis.

*Proof.* Let $d = \dim S_k$. Since $B_4 = -1/30$ and $B_6 = 1/42$, we note that

$$F_4 = -\frac{8}{B_4} \cdot E_4 = 1 + 240q + 2160q^2 + 6720q^3 + 17520q^4 + \cdots$$

and

$$F_6 = -\frac{12}{B_6} \cdot E_6 = 1 - 504q - 16632q^2 - 122976q^3 - 532728q^4 + \cdots$$

have $q$-expansions in $\mathbb{Z}[[q]]$ with leading coefficient 1. Choose integers $a, b \geq 0$ such that

$$4a + 6b \leq 14 \qquad \text{and} \qquad 4a + 6b \equiv k \pmod{12},$$

with $a = b = 0$ when $k \equiv 0 \pmod{12}$, and let

$$g_j = \Delta^j F_6^{2(d-j)+a} F_4^b, \qquad \text{for } j = 1, \ldots, d.$$

Then

$$a_j(g_j) = 1, \qquad \text{and} \qquad a_i(g_j) = 0 \qquad \text{when} \qquad i < j.$$

Hence the $g_j$ are linearly independent over $\mathbb{C}$, and thus form a basis for $S_k$. Since $F_4, F_6$, and $\Delta$ are all in $\mathbb{Z}[[q]]$, so are the $g_j$. The $f_i$ may then be constructed from the $g_j$ by Gauss elimination. The coefficients of the resulting power series lie in $\mathbb{Z}$ because each time we clear a column we use the power series $g_j$ whose leading coefficient is 1 (so no denominators are introduced). □

**Remark 1.6.2.** The basis coming from Victor Miller's lemma is canonical, since it is just the reduced row echelon form of any basis. Also the *integral* linear combinations are precisely the modular forms of level 1 with integral $q$-expansion.

We extend the Victor Miller basis to all $M_k$ by taking a multiple of $G_k$ with constant term 1, and subtracting off the $f_i$ from the Victor Miller basis so that the coefficients of $q, q^2, \ldots q^d$ of the resulting expansion are 0. We call the extra basis element $f_0$.

**Example 1.6.3.** If $k = 24$, then $d = 2$. Choose $a = b = 0$, since $k \equiv 0 \pmod{12}$. Then

$$g_1 = \Delta F_6^2 = q - 1032q^2 + 245196q^3 + 10965568q^4 + 60177390q^5 - \cdots$$

and

$$g_2 = \Delta^2 = q^2 - 48q^3 + 1080q^4 - 15040q^5 + \cdots$$

We let $f_2 = g_2$ and

$$f_1 = g_1 + 1032g_2 = q + 195660q^3 + 12080128q^4 + 44656110q^5 - \cdots.$$

**Example 1.6.4.** When $k = 36$, the Victor Miller basis, including $f_0$, is

$$\begin{aligned}
f_0 &= 1 + \quad 6218175600q^4 + 15281788354560q^5 + \cdots \\
f_1 &= \quad q + \quad 57093088q^4 + \quad 37927345230q^5 + \cdots \\
f_2 &= \quad q^2 + \quad 194184q^4 + \quad 7442432q^5 + \cdots \\
f_3 &= \quad q^3 - \quad 72q^4 + \quad 2484q^5 + \cdots
\end{aligned}$$

**Remark 1.6.5.** If you wish to write $f \in M_k$ as a polynomial in $E_4$ and $E_6$, then it is wasteful to compute the Victor Miller basis. Instead, use the upper triangular basis $\Delta^j F_6^{2(d-j)+a} F_4^b$, and match coefficients from $q^0$ to $q^d$.