Modular Forms and Elliptic Curves

Sriram Gopalakrishnan

February 6, 2019

Abstract

We define what it means for a function to be a modular form, prove fundamental theorems about modular forms, and explore the relationship between lattice functions and modular forms. We conclude by giving a small glimpse of the relationship between modular forms and elliptic curves.

1 Introduction

In this paper, we focus on the fundamentals of modular forms. We first give a definition of a modular form through a careful series of theorems and proofs. We follow with a discussion of lattices and their relations to modular forms. We give a common example of a lattice function that is also a modular form, namely Eisenstein series and we conclude by providing some motivations for the study of modular forms by exploring their relationship with elliptic curves. This paper follows Chapter 7 of J.P. Serre’s text *A Course in Arithmetic*, while filling in details that Serre omits. The final proof follows that of Washington in his book *Elliptic Curves, Number Theory, and Cryptography*.

2 Preliminary

2.1 The Modular Group

Recall the definition of the special linear group of $2 \times 2$ matrices over the integers:

$$SL_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{array}{c} \begin{array}{c} a, b, c, d \in \mathbb{Z}, \\ ad - bc = 1 \end{array} \end{array} \right\}$$

We call $G = SL_2(\mathbb{Z})/\pm 1$ where 1 is the identity element (the identity matrix) in $SL_2(\mathbb{Z})$ the modular group. The modular group forms the starting point for our discussion of modular forms, so it is beneficial to state and prove some facts about it. We define the complex upper half plane $\mathcal{H}$ as follows:

$$\mathcal{H} := \{ z \in \mathbb{C} \mid \text{Im}(z) > 0 \}$$

What follows is a discussion and development of the $G$-action on $\mathcal{H}$.

Let $g \in G$ be a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then, for every $g \in G$, $z \in \mathcal{H}$, the action of $g$ on $z$ is given by

$$gz = \frac{az + b}{cz + d}$$
Let \( S, T \in G \) where \( S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \), \( T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \). The \( S \) and \( T \) actions on a complex variable \( z \in \mathbb{H} \) are then
\[
Sz = -\frac{1}{z} \\
Tz = z + 1
\]
Furthermore, \( S^2 = 1 \) and \( (ST)^3 = 1 \). Now, let \( D := \{ z \in \mathbb{H} \mid |z| \geq 1, |\text{Re}(z)| \leq \frac{1}{2} \} \). The following figure represents the transformations of \( D \) by the elements:
\[
\{1, T, -T, T^{-1}S, STS, ST, S, ST^{-1}, ST^{-1}S, TS \} \in G
\]

**Theorem 2.1.1.** The modular group \( G \) is generated by the elements \( S \) and \( T \).

**Proof.** We will give an explicit expression of an arbitrary element \( g \in G \) in terms of \( S \) and \( T \). For some matrix in \( G \), we have the following multiplications on the left by the elements \( S \) and \( T \).
\[
S \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}, \quad T^n \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + nc & b + nd \\ c & d \end{pmatrix} \quad (1)
\]
Now let \( g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) be an arbitrary element in \( G \). Suppose \( c \neq 0 \). If \( |a| > |c| \), write \( a = cq + r \) (division algorithm), where \( 0 \leq r < |c| \). By (1), the upper left entry of the matrix \( T^{-q}g \) is \( a - qc = r < |c| \). We can apply \( S \) to \( T^{-q}g \) to swap the rows of \( T^{-q}g \). Once more, if our new matrix has a nonzero entry in the bottom left spot, we can perform the division algorithm again to obtain a new power of \( T \) by which we can multiply \( T^{-q}S \) by to again reduce the element in the bottom left entry. We can continue this process until we obtain a matrix with lower left entry 0. Since this matrix must still be in \( G \) (as it is a product of matrices in \( G \)), it must have integer entries and determinant 1. Thus, it is of the form
\[
\begin{pmatrix} \pm 1 & m \\ 0 & \pm 1 \end{pmatrix}
\]
where \( m \in \mathbb{Z} \) and the diagonal entries have the same sign. This matrix is either \( T^m \) or \(-T^{-m}\), so there exists \( h \in G \) that is the multiple of powers of \( T \) and copies of \( S \) such that \( h g = \pm T^n \) for some \( n \in \mathbb{Z} \). As \( T^m \in G \) and \( S^2 = I \), we can write \( g = \pm h^{-1} T^n \) where \( h^{-1} \) is generated by \( S \) and \( T \) and we are done.

\[ \square \]

**Theorem 2.1.2.** Let \( D, G, \) and \( H \) be as above.

1. For every \( z \in H \), there exists \( g \in G \) such that \( g z \in D \).
2. Suppose \( z, z' \in H \) are congruent modulo the \( G \)-action. That is, suppose \( z \) and \( z' \) have the same orbit under the \( G \)-action. Then,
   - \( (i) \) \( \text{Re}(z) = \pm \frac{1}{2} \) and \( z = z' \pm 1 \) or
   - \( (ii) \) \( |z| = 1 \) and \( z' = -\frac{1}{z} \)
3. Fix \( z \in D \) and let \( G_z = \{ g \in G \mid g z = z \} \) be the stabilizer of \( z \) under the \( G \)-action. \( G_z = \{ 1 \} \) except if:
   - \( (i) \) \( z = i \), in which case \( G_z \) is generated by \( S \) and is a group of order 2;
   - \( (ii) \) \( z = e^{\frac{2 \pi i}{3}} \), in which case \( G_z \) is generated by \( ST \) and is a group of order 3;
   - \( (iii) \) \( z = e^{\frac{2 \pi i}{2}} \), in which case \( G_z \) is generated by \( TS \) and is a group of order 3.

**Proof.** Let \( G' \leq G \) be the subgroup of \( G \) generated by \( S \) and \( T \). Let \( g \in G' \), \( g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \). Suppose \( z \in H \), \( z = r + si \). Then,

\[
\text{Im}(gz) = \text{Im} \left( \frac{az + b}{cz + d} \right) = \text{Im} \left( \frac{ar + asi + b}{cr + csi + d} \right) = \text{Im} \left( \frac{(ar + b) + asi}{(cr + d) + csi} \right) = \text{Im} \left( \frac{(da - bc)si}{cz + d|^2} \right)
\]

\[
= \frac{\text{Im}(z)}{|cz + d|^2}
\]

Fix \( M \in \mathbb{Z} \). Then, \( |\{(c, d) \in \mathbb{Z}^2 \mid |cz + d| < M\}| < \infty \). Thus, there exists a pair \((c, d)\) such that \( |cz + d| \) is minimal and consequently \( \frac{\text{Im}(z)}{|cz + d|^2} \) is maximized. In other words, we can find \( h \in G' \) such that \( \text{Im}(hz) = \frac{\text{Im}(z)}{|cz + d|^2} \) is maximized. We now choose an integer \( n \) such that \( |\text{Re}(T^n h z)| \leq \frac{1}{2} \).

Let \( z' = T^n h z \). Then,

\[
\text{Im} \left( \frac{-1}{z'} \right) = \frac{\text{Im} \left( z' \right)}{|z'|^2}
\]

so if \( |z'| < 1 \), \( \text{Im} \left( \frac{-1}{z'} \right) > \text{Im} (z') \). As this is impossible, \( |z'| \geq 1 \). Therefore, \( g' = T^n h z \) is in the fundamental domain \( D \). Let \( z \in D \) and choose \( g \in G \), \( g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) such that \( g z \in D \). Suppose \( \text{Im}(gz) \leq \text{Im}(z) \). Then, replace the pair \((z, g)\) with \((gz, g^{-1})\) to obtain \( \text{Im}(g^{-1}gz) = \text{Im}(z) \leq \text{Im}(gz) \). We can thus assume without loss of generality, that \( \text{Im}(gz) \geq \text{Im}(z) \), so \( |cz + d| \leq 1 \). This is only possible if \( |c| < 2 \), so we consider the cases \( c = -1, 0, 1 \).

Suppose \( c = 0 \). Since \( g \) is an element of the modular group, its determinant must be 1. Therefore,
d = \pm 1$. Therefore, $gz = z \pm b$. Since $z, gz \in D$, $|\text{Re}(z)| \leq \frac{1}{2}$ and $|\text{Re}(gz)| \leq \frac{1}{2}$. Hence, we have

$$b = \begin{cases} 0 & \text{if } g = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, |\text{Re}(z)| = |\text{Re}(gz)| < \frac{1}{2} \\ -1 & \text{if } \text{Re}(z) = \frac{1}{2}, \text{Re}(gz) = -\frac{1}{2} \\ 1 & \text{if } \text{Re}(z) = -\frac{1}{2}, \text{Re}(gz) = \frac{1}{2} \end{cases}$$

If $c = 1$, $|z + d| \leq 1$, so $d = 0$, unless

$$z = \begin{cases} e^{\frac{2\pi i}{3}} \implies d = 0 \text{ or } 1 \\ e^{\pi i / 3} \implies d = 0 \text{ or } -1 \end{cases}$$

When $d = 0$, $|z| = 1$, and $b = -1$. Therefore, $gz = a - \frac{1}{2}$ (equivalently when $z = e^{\frac{2\pi i}{3}}$ or $z = e^{\pi i / 3}$), in which case $a = 0$, $-1$ or $a = 0, 1$. When $z = e^{\frac{2\pi i}{3}}$ and $d = 1$, $a - b = 1$ and $\frac{a - 1}{1 + e^{2\pi i / 3}} = a + e^{2\pi i / 3}$, implying that $a = 0, 1$. Similarly, we find that when $z = e^{\pi i / 3}$ and $d = -1$, $a$ must be $0$ or $-1$. Suppose $c = -1$. We can change the signs of all $a, b, c, d$ in $g$, which does not change the $g$-action on an element in $H$, and follow the same argument as the case when $c = 1$.

\begin{proof}

\end{proof}

\subsection{Lattices}

We begin with the definition of a lattice. There are many equivalent definitions, but we will use the following one for the sake of this paper.

\textbf{Definition 2.2.1.} Let $V$ be a finite dimensional real vector space. A lattice $\Gamma$ of $V$ is a discrete subgroup of $V$ (where $V$ is viewed as a group) that generates $V$.

Consider the vector space $\mathbb{C}$ over the field $\mathbb{R}$. Let $\mathcal{R}$ be the set of lattices of $\mathbb{C}$. Let

$$M := \left\{ (\omega_1, \omega_2) \in \mathbb{C}^2 \mid \text{Im} \left( \frac{\omega_1}{\omega_2} \right) > 0 \right\}$$

The condition that $\text{Im} \left( \frac{\omega_1}{\omega_2} \right) > 0$ is equivalent to saying that $\omega_1$ and $\omega_2$ cannot both be real. We associate the lattice $\Gamma(\omega_1, \omega_2) = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ with the lattice basis $\{\omega_1, \omega_2\}$. Suppose

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \ (\omega_1, \omega_2) \in M$$

Then, the pair $\{\omega'_1, \omega'_2\}$ where $\omega'_1 = a\omega_1 + b\omega_2$ and $\omega'_2 = c\omega_1 + d\omega_2$ forms a different lattice basis for $\Gamma(\omega_1, \omega_2)$. Indeed, let $z = \frac{a}{c}$ and $z' = \frac{b}{d}$. Then,

$$z' = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\frac{\omega_1}{\omega_2} + b}{c\frac{\omega_1}{\omega_2} + d} = \frac{az + b}{cz + d} = gz$$

\textbf{Theorem 2.2.1.} Two elements of $M$ define the same lattice if and only if they are congruent modulo the $SL_2(\mathbb{Z})$ action.
Proof. We have shown above that if \((\omega_1, \omega_2)\) and \((\omega'_1, \omega'_2)\) are congruent modulo the \(SL_2(\mathbb{Z})\) action, then they define the same lattice. We will now show the converse. Suppose \((\omega_1, \omega_2)\) and \((\omega'_1, \omega'_2)\) are both in \(M\) and both define the same lattice. Then, since \((\omega_1, \omega_2)\) lies in the lattice generated by \((\omega'_1, \omega'_2)\), we can write

\[
\begin{bmatrix}
\omega_1 \\
\omega_2
\end{bmatrix} = \begin{bmatrix} a & b \\
c & d \end{bmatrix} \begin{bmatrix}
\omega'_1 \\
\omega'_2
\end{bmatrix} = P \begin{bmatrix}
\omega'_1 \\
\omega'_2
\end{bmatrix}
\]

We can represent \((\omega'_1, \omega'_2)\) as a linear combination of \((\omega_1, \omega_2)\) likewise. If we invert \(P\), we get

\[
P^{-1} \begin{bmatrix} \omega_1 \\
\omega_2
\end{bmatrix} = \begin{bmatrix}
\omega'_1 \\
\omega'_2
\end{bmatrix}
\]

Thus, \(\det(P) = \det(P^{-1}) = \det(P)^{-1}\), where \(P\) and \(P^{-1}\) both have integer entries. Hence, \(\det(P) = \pm 1\). Suppose \(\det(P) = -1\). Then, \(\text{Im} \left( \omega'_1 \omega_2 \right) = -\text{Im} \left( \omega_1 \omega_2 \right)\). But since both \((\omega_1, \omega_2)\) and \((\omega'_1, \omega'_2)\) are in \(M\), the signs must be the same. Thus, \(\det(P) = 1\), and so \(P \in SL_2(\mathbb{Z})\). \(\square\)

Due to Theorem 2.2.1, we can write the definition of \(\mathcal{R}\) as \(M/SL_2(\mathbb{Z})\). Now, suppose we start with some \((\omega_1, \omega_2) \in M\). As usual, we call the lattice generated by \((\omega_1, \omega_2)\) \(\Gamma(\omega_1, \omega_2) \in \mathcal{R}\). Scale the pair \((\omega_1, \omega_2)\) by \(\lambda \in \mathbb{C}^\times\) to arrive at \((\lambda \omega_1, \lambda \omega_2)\). Then, the lattice generated by \((\lambda \omega_1, \lambda \omega_2)\) is \(\lambda \Gamma\) and is equivalent to the action of an element in \(SL_2(\mathbb{Z})\) on \(\Gamma\). In other words, the action of scaling on \(M\) commutes with the action of \(SL_2(\mathbb{Z})\) on \(\mathcal{R}\). Thus, the map

\[
(\omega_1, \omega_2) \mapsto z = \frac{\omega_1}{\omega_2}
\]

(2)

gives a transformation of the action of \(SL_2(\mathbb{Z})\) on \(M\) to the \(G\) action on \(H\). Furthermore, the map given by (2) defines a bijection between \(\mathcal{R}/\mathbb{C}^\times\) and \(H/G\). Recall that we can associate to each \(\Gamma\) in \(\mathbb{C}\) an elliptic curve \(E_\Gamma = \mathbb{C}/\Gamma\). If \(\Gamma' = \lambda \Gamma\), then the elliptic curves \(E_\Gamma\) and \(E_{\Gamma'}\) are isomorphic. This gives us yet another equivalent description of \(H/G\) - namely that it is the set of isomorphism classes of elliptic curves. Particularly, two elliptic curves are isomorphic if the lattices defining them are in the same equivalence class in \(\mathcal{R}/\mathbb{C}^\times\).

3 Modular Forms and Lattice Functions

3.1 Modular Forms

We begin with a short description of what a meromorphic complex function is.

Definition 3.1.1. A complex-valued function \(f(z)\) is meromorphic on an open set \(D\) of the complex plane if it is holomorphic (resp. complex differentiable, analytic) on all of \(D\) except for a finite set of isolated points, called poles.

A meromorphic function is the ratio of two holomorphic functions. That is, if \(f\) and \(g\) are holomorphic functions, then \(\frac{f(z)}{g(z)}\) is meromorphic and has poles at the zeroes of \(g(z)\). With this brief recollection of the idea of a meromorphic function, we are ready to give our first major definition pertaining to modular forms.

Definition 3.1.2. A weakly modular function of weight \(2k\) (resp. \(k, -2k\)) where \(k \in \mathbb{Z}\) is a function that is meromorphic on \(\mathcal{H}\) and satisfies

\[
f(z) = (cz + d)^{-2k} f \left( \frac{az + b}{cz + d} \right)
\]

for all \(\begin{bmatrix} a & b \\
c & d \end{bmatrix} \in SL_2(\mathbb{Z})\).
Theorem 3.1.1. Suppose $f$ is a meromorphic function on $\mathcal{H}$. Then $f$ is a weakly modular function of weight $2k$ if and only if it satisfies both

\begin{align*}
  f(z + 1) &= f(z) 
  \tag{3} \\
  f\left(\frac{-1}{z}\right) &= z^{2k} f(z) 
  \tag{4}
\end{align*}

Proof. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and consider the derivative of $gz$, with respect to $z$

\[
\frac{d(gz)}{dz} = d\left(\frac{az + b}{cz + d}\right) = \frac{a(cz + d) - c(az + b)}{(cz + d)^2} = \frac{ac - ad - ac - cb}{(cz + d)^2} = \frac{ad - bc}{(cz + d)^2} = 1
\]

Thus, we can write

\[
\frac{f(gz)}{f(z)} = \left(\frac{d(gz)}{dz}\right)^{-k} \tag{5}
\]

By Theorem 2.1.1, the modular group $G$ is generated by the elements $S$ and $T$. Thus, if $f$ is a meromorphic function on $\mathcal{H}$, and (5) is satisfied for $S$ and $T$, then $f$ is a weakly modular function of weight $2k$. For $S$, we can write (5) as $f\left(\frac{-1}{z}\right) = z^{2k} f(z)$, so (4) is satisfied. Likewise for $T$ we have $f(z + 1) = f(z)$, so (3) is satisfied. The same argument in reverse works to show the converse. \qed

Suppose (3) is satisfied. Then, $f$ is a periodic function of period 1, so we can represent $f$ with a Fourier series. That is, $f$ can be represented as a function of $q = e^{2\pi i z}$. Let $\tilde{f}$ be this representation of $f$. $f$ is meromorphic on $\mathcal{H}$, so $\tilde{f}$ is meromorphic on the (punctured) unit disk $|q| < 1$ with the origin removed. Under the conformal mapping that takes $f$ to $\tilde{f}$ (resp, $z \mapsto e^{2\pi i z}$), the point $i\infty$ gets sent to $e^{2\pi i (i\infty)} = e^{-2\pi/\infty} = 0$. Thus, if $f$ extends to a meromorphic (resp. holomorphic) function at the origin, we say that $f$ is meromorphic (resp. holomorphic) at infinity. In other words, if $\tilde{f}$ extends to a meromorphic (resp. holomorphic) function at the origin, then $\tilde{f}$ has a Laurent expansion in some neighborhood of the origin given by

\[
\tilde{f}(q) = \sum_{-\infty}^{\infty} a_n q^n
\]

where $a_n = 0$ when $n < 0$. Finally, we come to the definition of modular functions and modular forms.

Definition 3.1.3. If $f$ is a weakly modular function and extends to a meromorphic function at infinity, we call $f$ a modular function. In this case, we set $f(\infty) = \tilde{f}(0)$.

Definition 3.1.4. Suppose $f$ is a complex-valued function. Then, we call $f$ a modular form if

(i) $f(z) = (cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right)$,

6
(ii) $f$ is holomorphic on $\mathcal{H}$, and

(iii) $f$ is holomorphic at $\infty$.

In this case, we once again set $f(\infty) = \tilde{f}(0)$. If $f(\infty) = \tilde{f}(0) = 0$ (that is, if $f$ assumes the value of $0$ at $\infty$, or equivalently if the constant term in the Laurent expansion of $\tilde{f}(q)$ is $0$), then we call $f$ a modular cusp form.

### 3.2 Lattice Functions

Once again, we begin with a definition.

**Definition 3.2.1.** Suppose $F$ is a function on $\mathcal{R}$ (the set of lattices of $\mathbb{C}^\times$) and $k \in \mathbb{Z}$. $F$ is a modular lattice function of weight $2k$ if

$$F(\lambda \Gamma) = \lambda^{-2k} F(\Gamma)$$

for all lattices $\Gamma \in \mathcal{R}$ and all $\lambda \in \mathbb{C}^\times$.

Now suppose $F$ is a lattice function of weight $2k$ and let $(\omega_1, \omega_2) \in M$. $F(\omega_1, \omega_2)$ is the value of $F$ on the lattice $\Gamma(\omega_1, \omega_2)$. Then, (6) gives us

$$F(\lambda \omega_1, \lambda \omega_2) = \lambda^{-2k} F(\omega_1, \omega_2)$$

Let $\lambda = \omega_2$. By the map given in the preliminary lattice section by (2) $z = \frac{\omega_1}{\omega_2}$, there exists a function $f$ on $\mathcal{H}$ such that

$$F(\omega_1, \omega_2) = \omega_2^{-2k} f(z)$$

If we say that $F$ is invariant under $SL_2(\mathbb{Z})$,

$$f(z) = (cz + d)^{-2k} f \left( \frac{az + b}{cz + d} \right) \text{ for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

Likewise, if a function $f$ satisfies (9), then by (8), we can identify $f$ with a function $F$ on $\mathcal{R}$ of weight $2k$. This gives us our main result, namely that modular lattice functions of weight $2k$ can be identified with modular functions of weight $2k$ and vice versa.

### 3.3 Eisenstein Series

We begin with the definition of Eisenstein series.

**Definition 3.3.1** (Eisenstein Series). Let $k \in \mathbb{Z}, k > 1$ and let $\Gamma$ be as usual, a lattice in $\mathbb{C}^\times$. Then,

$$G_k(\Gamma) = \sum_{0 \neq \gamma \in \Gamma} \frac{1}{\gamma^{2k}}$$

We call $G_k$ the Eisenstein series of index $k$.

This series is absolutely convergent (see Serre). Furthermore,

$$G_k(\lambda \Gamma) = \sum_{0 \neq \gamma \in \Gamma} \frac{1}{(\lambda \gamma)^{2k}} = \lambda^{-2k} \sum_{0 \neq \gamma \in \Gamma} \frac{1}{\gamma^{2k}} = \lambda^{-2k} G_k(\Gamma)$$

7
Therefore, we see that $G_k$ is a lattice function of weight $2k$. We can thus view $G_k$ as a function on $M$.

$$G_k(\omega_1, \omega_2) = \sum_{(0,0) \neq (m,n)} \frac{1}{(m\omega_1 + n\omega_2)^{2k}}$$

Now consider, as in the lattice preliminary section, the map $((\omega_1, \omega_2)) \mapsto z = \frac{\omega_1}{\omega_2}$. We can write

$$G_k(\omega_1, \omega_2) = \sum_{(0,0) \neq (m,n)} \frac{1}{(mz + n)^{2k}}$$

Here, $G_k(z)$ differs from $G_k(\omega_1, \omega_2)$ by a factor of $\omega_2^{2k}$.

**Theorem 3.3.1.** Let $k \in \mathbb{Z}$, $k > 1$. Then, $G_k(z)$ is a modular form of weight $2k$ with $G_k(\infty) = 2\zeta(2k)$.

*Proof.* $G_k$ is convergent (see Serre). Thus, in conjunction with the argument that $G_k$ is a lattice function of weight $2k$, $G_k$ is weakly modular of weight $2k$. Suppose now that $z \in D$, the fundamental domain of the $G$-action on $\mathbb{H}$. Then, we have

$$|mz + n|^2 = m^2z\bar{z} + 2mnRe(z) + n^2 \geq m^2 - mn + n^2 = |m\rho - n|^2$$

where $\rho = e^{\frac{2\pi i}{3}}$. The series $\sum_{(0,0) \neq (m,n)} \frac{1}{|m\rho - n|^2}$ converges in $D$ (see Serre) and thus in $gD$ for $g \in G$. The set $\{gD | g \in G\}$ covers $\mathbb{H}$, so $G_k$ is holomorphic on all of $\mathbb{H}$. We now show that $G_k$ has a limit as $z \to i\infty$, and thus $G_k$ is “holomorphic at infinity.” We can again suppose $Z \in \mathbb{H}$.

The terms of $G_k$ for which $m \neq 0$ give us $G_k(z) \to 0$. The terms of $G_k$ for which $m = 0$ give us:

$$\lim_{z \to i\infty} G_k(z) = \sum_{n \neq 0} \frac{1}{n^{2k}} = 2\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = 2\zeta(2k)$$

Having developed an understanding of Eisenstein series as a modular form, we now describe a modular cusp form given by Eisenstein series of particular weights. Suppose we have the following:

$$g_2 = 60G_2, \quad g_3 = 140G_3$$

where $G_2$ is the Eisenstein series of weight 4 and $G_3$ is the Eisenstein series of weight 6. We have

$$g_2(\infty) = 120\zeta(4), \quad g_3(\infty) = 280\zeta(6)$$

by Theorem 3.3.1. The values of $\zeta(4)$ and $\zeta(6)$ are $\frac{\pi^4}{90}$ and $\frac{\pi^6}{945}$, respectively. Thus,

$$g_2(\infty) = \frac{4}{3}\pi^4, \quad g_3(\infty) = \frac{8}{27}\pi^6$$

Now let

$$\Delta = g_2^3 - 27g_3^2$$

Here, $G_k(z)$ differs from $G_k(\omega_1, \omega_2)$ by a factor of $\omega_2^{2k}$. 

**Theorem 3.3.1.** Let $k \in \mathbb{Z}$, $k > 1$. Then, $G_k(z)$ is a modular form of weight $2k$ with $G_k(\infty) = 2\zeta(2k)$.
Then,
\[
\Delta(\infty) = g_2(\infty)^3 - 27g_3(\infty)^2 = \frac{64}{27} \pi^{12} - \frac{64}{27} \pi^{12} = 0
\]

Since \( g_2 \) and \( g_3 \) are modular forms, \( \Delta \) is a modular form. Furthermore, it assumes the value 0 at infinity. Thus, it is a modular cusp form. Note that we do not know from this alone that the function \( \Delta \) is not the 0 function. In the next section, we explain why \( \Delta \) is not identically zero.

### 4 Modular Forms and Elliptic Curves

#### 4.1 The Weierstrass \( \wp \)-function

In this section, we will ignore issues of convergence of the \( \wp \) function.

**Definition 4.1.1.** Let \( \Gamma \) be a lattice in \( \mathbb{C}^2 \). Then, the Weierstrass \( \wp \)-function corresponding to \( \Gamma \) is

\[
\wp_{\Gamma}(z) = \frac{1}{z^2} + \sum_{\gamma \neq 0 \in \Gamma} \left( \frac{1}{(z-\gamma)^2} - \frac{1}{\gamma^2} \right)
\]

We denote the negative of the antiderivative of \( \wp(z) \) as \( \zeta_{\wp}(z) \). We have the explicit formulation of \( \zeta_{\wp}(z) \)

\[
\zeta_{\wp}(z) = \frac{1}{z} + \sum_{\gamma \neq 0} \left( \frac{1}{z-\gamma} + \frac{1}{\gamma} + \frac{z}{\gamma^2} \right)
\]

We can expand the summand to the following

\[
\frac{1}{z-\gamma} + \frac{1}{\gamma} + \frac{z}{\gamma^2} = \frac{z^2}{\gamma^3} - \frac{z^3}{\gamma^4} - \frac{z^4}{\gamma^5} \ldots
\]

Thus,

\[
\zeta_{\wp}(z) = \frac{1}{z} - \sum_{k=2}^{\infty} G_k(z) z^{2k-1}
\]

where \( G_k(z) \) is the Eisenstein series of index \( k \). The odd powers have disappeared here since \( \wp(z) \) is an even function. Note that \( \wp(z) = -\zeta'_{\wp}(z) \), so

\[
\wp(z) = \frac{1}{z^2} + \sum_{k=2}^{\infty} (2k-1) G_k(z) z^{2k-2}
\]

(11)

In terms of lattices, we can rewrite (9) as

\[
\wp_{\Gamma}(z) = \frac{1}{z^2} + \sum_{k=2}^{\infty} (2k-1) G_k(\Gamma) z^{2k-2}
\]

We now turn to the relationship between the Weierstrass \( \wp \)-function and elliptic curves. We by stating a theorem without proof that will be necessary to prove subsequent propositions.

**Theorem 4.1.1.** Let \( f \) be a doubly-periodic function on the lattice \( \Gamma \) and let \( F \) be the fundamental parallelogram of \( \Gamma \) (the parallelogram who’s left and bottom sides are \( (\omega_1, \omega_2) \), the basis for \( \Gamma \)). Then,

1. If \( f \) has no poles, then \( f \) is constant
2. If \( f \) is not constant, then \( f : \mathbb{C} \to \mathbb{C} \cup \infty \) is surjective. If \( n \) is the sum of the orders of the poles of \( f \) in \( F \), and \( z_0 \in \mathbb{C} \), then \( f(z) = z_0 \) has \( n \) solutions (if a solution has multiplicity > 1, then it will count towards \( n \) multiple times).

**Proposition 4.1.1.** The values \( \wp_T \left( \frac{\omega_i}{2} \right) \) are distinct for each \( \omega_i \).

**Proof.** \( \wp'(z) \) is doubly periodic, so \( \wp'(\frac{\omega_i}{2}) = \wp'(-\frac{\omega_i}{2}) \). \( \wp' \) is even, so \( \wp'(-\frac{\omega_i}{2}) = -\wp'(\frac{\omega_i}{2}) \). Thus,

\[
\wp'(\frac{\omega_i}{2}) = 0, \quad i = 1, 2, 3
\]  
(12)

Therefore, each \( \wp \left( \frac{\omega_i}{2} \right) \) is a root of \( 4x^3 - 2gx - g_3 \). Let

\[
h_i(z) = \wp(z) - \wp \left( \frac{\omega_i}{2} \right)
\]

Then, \( h_i \left( \frac{\omega_i}{2} \right) = h'_i \left( \frac{\omega_i}{2} \right) = 0 \). In other words, \( h_i \) vanishes with order of vanishing at least 2 at the points \( \frac{\omega_i}{2} \). Let \( F \) be the fundamental parallelogram of the lattice \( \Gamma \) on which \( \wp \) is defined. Then, \( h_i(z) \) has a single pole in \( F \) (the double pole at \( z = 0 \)). By Theorem 4.1.1, we can deduce that \( \frac{\omega_i}{2} \) is the only zero of \( h_i(z) \). Particularly, \( h_i \left( \frac{\omega_i}{2} \right) \) is nonzero when \( j \neq i \). Therefore, each of \( \wp \left( \frac{\omega_i}{2} \right) \) are distinct. \( \square \)

**Proposition 4.1.2.** Let \( E : y^2 = f(x) = 4x^3 - 2gx - g_3 \). Then,

\[
\Phi : \mathbb{C}/\Gamma \to E(\mathbb{C})
\]
(13)

\[
z \mapsto \left( \wp_T(z), \wp'_T(z) \right)
\]
(14)

\[
0 \mapsto \infty
\]
(15)

is an isomorphism of groups. That is, the elliptic curve \( E \) is isomorphic to the elliptic curve defined by \( C/\Gamma \).

The proof of this proposition is not trivial. A sketch is provided below.

**Proof.** We begin by showing that \( \Phi \) is surjective. Let \( (x, y) \in E(\mathbb{C}) \). The function \( \wp(z) - x \) has a double pole, so it cannot be constant. Thus, it must have zeroes. Therefore, there exists \( z \in \mathbb{C} \) such that \( \wp(z) = x \). We have

\[
\wp'(z) = y^2
\]

so \( \wp(z) = \pm y \). If \( \wp'(z) = y \), then we have shown surjectivity, since we have found an element in \( C/\Gamma \) that maps to \( (x, y) \in E(\mathbb{C}) \) for every \( (x, y) \in E(\mathbb{C}) \). If \( \wp'(z) = -y \), then since \( \wp'(z) \) is an even function, \( \wp'(-z) = y \), and \( \wp(-z) = x \), so \( -z \mapsto (x, y) \).

Next, we show that \( \Phi \) is injective. Suppose \( \wp(z_1) = \wp(z_2) \) and \( \wp'(z_1) = \wp'(z_2) \) and \( z_1 \) and \( z_2 \) are not congruent modulo \( \Gamma \) (that is, they do not lie on the same lattice in \( \mathbb{C} \)). The poles of \( \wp(z) \) all lie in \( \Gamma \), so if \( z_1 \) is a pole for \( \wp \), then \( z_1 \in \Gamma \) and thus, \( z_2 \in \Gamma \). But this would mean that \( z_1 \) and \( z_2 \) would be congruent modulo \( \Gamma \). So, we may assume that \( z_1 \) is not a pole of \( \wp \) and thus does not lie in \( \Gamma \). Consider the function

\[
h(z) = \wp(z) - \wp(z_1)
\]

One can check that \( h(z) \) has a double pole at \( z = 0 \) and no other poles in the fundamental parallelogram of \( \Gamma \). By Theorem 4.1.1, \( h(z) \) has exactly 2 zeroes. Suppose now that \( z_1 = \frac{\omega_i}{2} \) for some \( i \). Then, (12) tells us that \( \wp' \left( \frac{\omega_i}{2} \right) = 0 \), so \( z_1 \) is a double root of \( h(z) \). Since we know that \( h(z) \) has only two roots, \( z_1 \) is the only root of \( h(z) \). We can conclude that \( z_2 = z_1 \). If \( z_1 \)
does not take the form \( \frac{1}{2\omega} \), then since \( h(-z_1) = h(z_1) = 0 \), and since \( z_1 \) is not congruent to \(-z_1\) modulo \( \Gamma \), the two zeroes of \( h(z) \) are \( z_1 \) and \(-z_1\) modulo \( \Gamma \). So, \( z_2 \) is congruent to \(-z_1\) modulo \( \Gamma \). However,

\[
y = \varphi'(z_2) = \varphi'(-z_1) = -\varphi'(z_1) = -y
\]

so \( \varphi'(z_1) = y = 0 \). However, \( \varphi'(z) \) has a triple pole, and so only three zeroes in \( F \). (12) tells us that the three zeroes occur at \( \frac{1}{2\omega} \) for \( i = 1, 2, 3 \). But, \( z \neq \frac{1}{2\omega} \). This gives a contradiction, so \( z_1 \) is congruent to \( z_2 \) modulo \( \Gamma \), and thus \( \Phi \) is injective.

We have shown that \( \Phi \) is bijective, so all that remains in to show that \( \Phi \) is a group homomorphism. Once again, let \( z_1, z_2 \in \mathbb{C} \). Let

\[
\Phi(z_i) = P_i = (x_i, y_i)
\]

We provide some restrictions on \( P_1 \) and \( P_2 \). Namely, assume that both \( P_1 \) and \( P_2 \) are finite and that the line that goes through \( P_1 \) and \( P_2 \) intersects \( E \) in three distinct finite points. Practically speaking this means that \( P_1 \neq \pm P_2 \), \( P_1 + 2P_2 \neq \infty \), and \( 2P_1 + P_2 \neq \infty \). We can provide these restrictions without hindering the completeness of the proof because the addition formula on \( E \) is entirely different when \( P_1 = P_2 \) and the connection between double roots in algebraic calculation of points on \( E \) and double roots in the corresponding functions is not pertinent to proving the homomorphism. Let \( y = ax + b \) be the line passing through \( P_1 \) and \( P_2 \). Then, by the constraints defined prior, \( y = ax + b \) intersects \( E \) at a third distinct finite point. We will call this point \( P_3 \) and let

\[
\Phi(z_3) = P_3 = (x_3, y_3)
\]

where \( z_3 \in \mathbb{C} \). Using the standard group law formulas for points on \( E \), we have

\[
x_3 = 1 \cdot \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2
\]

\[
= \frac{1}{4} \left( \frac{\varphi'(z_2) - \varphi'(z_1)}{\varphi(z_2) - \varphi(z_1)} \right)^2 - \varphi(z_1) - \varphi(z_2)
\]

Now, let

\[
l(z) = \varphi'(z) - ax \varphi(z) - b
\]

\( l(z) \) has zeroes at \( z = z_1, z_2, z_3 \). Since \( l(z) \) has a triple pole at \( 0 \) and no other poles, it has three zeroes in \( F \). We can, by utilizing tools from complex analysis, write

\[
\varphi(z_1 + z_2) = \frac{1}{4} \left( \frac{\varphi'(z_2) - \varphi'(z_1)}{\varphi(z_2) - \varphi(z_1)} \right) - \varphi(z_1) - \varphi(z_2)
\]

It can be shown that this formula holds for all \( z \) for which it is defined (recall that we excluded some \( z \) due to our constraints on points on \( E \) that we consider). We now turn our attention to the \( y \)-coordinate. We need to compute \( \varphi'(z_1 + z_2) \). Differentiating \( \varphi'(z)^2 = 4\varphi(z)^3 - g_2 \varphi(z) - g_3 \) yields

\[
2\varphi'' \varphi' = (12\varphi^2 - g_2) \varphi'
\]

We can divide by \( \varphi' \) to obtain

\[
2\varphi''(z_2) = 12\varphi(z_2)^2 - g_2
\]

We can differentiate \( \varphi(z_1 + z_2) \) to get an expression \( \varphi'(z_1 + z_2) \) into which we can substitute (17). The resulting expression will give \( \varphi'(z_1 + z_2) \) in terms of \( \varphi(z_1), \varphi'(z_1), \varphi(z_2) \) and \( \varphi'(z_2) \).

We can show that this expression is equivalent to \(-y_3\). Therefore,

\[
(\varphi(z_1), \varphi'(z_1)) + (\varphi(z_2), \varphi'(z_2)) = (\varphi(z_1 + z_2), \varphi'(z_1 + z_2))
\]
In other words,

\[ \Phi(z_1) + \Phi(z_2) = \Phi(z_1 + z_2) \]  \hspace{1cm} (18)

However, we still have to check the cases of (18) when (16) is not defined. We can easily check the cases where \( \wp(z_i) = \infty \) and \( z_1 \) is congruent to \(-z_2 \) modulo \( \Gamma \). Suppose now that \( z_1 = z_2 \).

Then, let \( z_2 \to z_1 \) and use (16) and (17) in conjunction with l'Hopital's rule to get

\[ \wp(2z_1) = \frac{1}{4} \left( \frac{\wp''(z_1)}{\wp'(z_1)} \right)^2 - 2\wp(z_1) \]

\[ = \frac{1}{4} \left( \frac{6\wp(z_1)^2 - \frac{1}{2}g_2}{\wp'(z_2)} \right)^2 - 2\wp(z_1) \]

\[ = \frac{1}{4} \left( \frac{6x_1^2 - \frac{1}{2}g_2}{g_2} \right)^2 - 2x_1 \]

This is the formula for \( x_3 \) we get from addition formula with \( P_1 \) and \( P_2 \). We can differentiate with respect to \( z_1 \) to obtain a similar formula to (18). Therefore, we have

\[ \Phi(z_1) + \Phi(z_1) = \Phi(2z_1) \]

and we are done. \( \Box \)

Note that we can deduce from this that the modular cusp form \( \Delta \) is not identically 0, since its values are discriminants of nonsingular elliptic curves, as shown.

References


