# The j-Function and the Monster

Asa Scherer

August 16, 2010

# Chapter 1

# Introduction

In a set of Hauptmoduls lived a function by the name of Jay. The year was 1979. Jay was quite old, though whether he was 100 or had lived forever was a matter only mathematical philosophers cared about. This particular day, Jay went about his usual business of generating other modular functions. Jay had always been connected to many of his mathematical-object friends. Little did anyone know, Jay held a dark secret. He was also connected... to a Monster.

Now that I have the attention of all my readers aged 5 to 10 and no one else, let's delve into some advanced mathematics!

In this ridiculous introduction, our fellow Jay is standing in for the Klein $j$-invariant, a complex-valued function that has many fascinating properties, not least of all that any modular function can be written as a rational function of the $j$-function. The mysterious Monster is the Fischer-Greiss Monster group, the largest of the sporadic simple groups. The real protagonists at the heart of this paper are John Conway and Simon Norton, who formulated the conjecture connecting these two seemingly disparate objects, and Richard Borcherds, who proved [Bor92] their conjecture in 1992.

The first published notion that the $j$-function was in any way related to the Monster came in 1979, when Conway and Norton noted in [CN79] that each coefficient in the $q$-expansion of the $j$-function could be written as a (nontrivial) integral linear combination of the dimensions of irreducible representations of the Monster. For example, the first relevant coefficient, 196884, can be written $196883 + 1$, where 196883 is the dimension of the smallest non-trivial representation of the Monster, and 1 is the dimension of the trivial representation. This observation led to their conjecture, which they titled "monstrous moonshine." This is a rather mysterious and evocative name for a mathematical conjecture, meant to insinuate that it is "distilling information illegally" [Gan04] from the Monster. It also evokes a sense of absurdity, that this connection is so far-fetched that it must be just a coincidence. This, of course, is not the case. Monstrous moonshine indeed illustrates a profound relationship between the $j$-function. In fact, the conjecture goes beyond just the $j$-function, but the $j$-function serves as an especially illustrative case of the conjecture.

Before we proceed any further, let us meet our main characters.

## 1.1 The Monster

Don't let the Monster group's name fool you! It's really quite a friendly group. Unless you're trying to analyze any piece of it, really, in which case it is quite a monster.

Before we define what the monster really is, we recall some group theoretical definitions:

**Definition 1.1.1.** *A* **simple group** $G$ *is a group with no nontrivial normal subgroups.*

Normal subgroups, of course, are subgroups $H$ where $ghg^{-1} \in H$ for all $g \in G$ and for all $h \in H$. By nontrivial we mean subgroups that are not the whole group or the trivial subgroup.

Simple groups are important to the study of groups, as any finite group can be decomposed into a composition series:

**Definition 1.1.2.** *A* **composition series** *is an inclusion chain of normal subgroups*

$$1 = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft H_3 \triangleleft \cdots \triangleleft G,$$

*where* $H_{i+1}/H_i$ *is simple for all* $i \geq 1$.

The Jordan-Holder theorem states that any such series is unique up to permutation and isomorphism. So, in essence, simple groups can be considered the "building blocks" of all finite groups, analogous to prime numbers in number theory.

The classification of all finite simple groups was a massive undertaking, only completed in 1983 [Sol01]. The results of this achievement give us the following complete list of finite simple groups:

Infinite families:

1. The cyclic groups $\mathbb{Z}/p\mathbb{Z}$, $p$ prime
2. The alternating groups $A_n$, $n \geq 5$
3. 16 infinite families of Lie type.

The rest of the simple groups are:

4. Exactly 26 so-called "sporadic" groups.

The **Monster group** $\mathbb{M}$ is the largest of these sporadic simple groups, with group order

$$|\mathbb{M}| = 2^{45} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 [\text{Gan04}].$$

So... It's huge. And yet not one of its many nontrivial subgroups is normal.

The Monster was postulated to exist in 1973 by Bernd Fischer and Robert Griess, though it was not explicitly constructed until 1980, when Griess constructed it as the group of automorphisms of a particular 196883-dimensional algebra. The Monster has since been built using other methods. [Gan04] The Monster is a very complicated group, having 194 conjugacy classes, and it contains 19 of the other sporadic simple groups as subgroups or quotients of subgroups, which include the adorably-named Baby Monster. (See [Gan04] and [Sol01] for more information.)

## 1.2 The $j$-function

**Definition 1.2.1.** *The $j$-function is a complex-valued function defined on all $\tau \in \mathbb{C}$ such that*

$$j(\tau) = 1728 \cdot \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2},$$

*where $g_2(\tau)$ and $g_3(\tau)$ are certain infinite sums over all the points in a particular lattice, as defined in Section 2.4.*

Jay has many guises, though! Setting $q = e^{2\pi i\tau}$, we can write

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots := \frac{1}{q} + \sum_{n=0}^{\infty} c(n)q^n,$$

as seen in [Gan04]. This expression is called the *q-expansion* of $j$, and it is in these integer coefficients that we find the fascinating connection with the Monster. For instance, Conway and Norton's original paper presenting monstrous moonshine [CN79] noted that

$$\begin{aligned} 196884 &= 196883 + 1 \\ 21493760 &= 21296876 + 196883 \\ 864299970 &= 842609326 + 2 \cdot 21296876 + 2 \cdot 196883 + 2 \cdot 1, \end{aligned}$$

where the numbers on the right are dimensions of irreducible representations of the Monster. (We define representations in Section 2.1.)

The $j$-function has quite a few rather remarkable properties on its own, some of which we will explore in Chapter 3. Namely, we will focus on proving two main theorems. First, though, some more definitions are in order:

**Definition 1.2.2.** *The group $SL_2(\mathbb{Z})$ is defined as the multiplicative group of all two-by-two matrices with integer entries and determinant 1; that is,*

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1 \right\}.$$

**Definition 1.2.3.** *We write $SL_2(\mathbb{Z})\backslash\mathbb{H}$ to denote the quotient of the upper half-plane $\mathbb{H}$ by the action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$ (which will be defined in Chapter 2).*

We have two main goals in this paper. First, we will focus on proving the following properties of $j(\tau)$:

**Theorem 1.2.4.** *The $j$-function is a bijection between $SL_2(\mathbb{Z})\backslash\mathbb{H}$ and $\mathbb{C}$.*

**Theorem 1.2.5.** *Every modular function is a rational function of $j(\tau)$.*

Secondly, we will give the reader context and understanding of the actual statement of monstrous moonshine. We will first establish some context for these theorems by presenting some preliminary material in Chapter 2, including a brief introduction to representation theory, lattices, and modular forms. Chapter 3, following the logical flow laid out in [Cox89], covers

the proof of our two main theorems, Theorems 1.2.4 and 1.2.5, and an additional property of $j(\tau)$ [Bor92] regarding the denominator formula. Chapter 4 defines the moonshine module, necessary to understand monstrous moonshine, and then states Borcherds' theorem, concluding by touching on a few of the related areas of moonshine research beyond the original conjecture.

A brief note: This paper assumes the reader to have a basic knowledge of group theory and complex analysis, but in general, we will be fairly explicit in defining our terms; many of these will be covered in Chapter Two.

# Chapter 2

# Preliminaries

Treat this chapter as a sort of smorgasbord of mathematical theory; a sampling of the delicious tools needed to understand the $j$-function and its Monstrous connection. We begin with an appetizer of Representation Theory, follow with a salad of Lattice, and finish with a Modular Function main course.

## 2.1 Representation Theory

Linear algebra is an incredibly useful tool, finding applications scattered throughout various mathematical and scientific disciplines. The beauty of linear algebra is that once we associate some sort of mathematical object to a matrix, we can instantly make many observations about the matrix, which then may apply to the original object. Group theorists in particular use linear algebra to simplify certain tasks of group structure analysis using maps called *representations*. In this section, we review some basic facts about representations of finite groups over $\mathbb{C}$. For more information, see [FH91].

**Definition 2.1.1.** *Given a finite group $G$, a* **representation of $G$ on a vector space $V$ over $\mathbb{C}$** *is a map $\rho$ from $G$ to the group of linear automorphisms of $V$, $GL(V)$, such that $\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2)$.*

So, essentially, a representation transfers group properties into a linear algebraic context, where our linear transformations behave as their preimage group elements do. A note: We frequently refer to $V$ itself as the representation, rather than the map $\rho$. Since our representations are vector spaces, we can certainly consider subspaces that are also representations.

**Definition 2.1.2.** *Let vector space $V$ be a representation of group $G$. Let $W$ be a subspace of $V$. If $\rho(g)(\mathbf{v}) \in W$ for all $\mathbf{v} \in W$, then we call $W$ a* **subrepresentation** *of $V$ with respect to $G$.*

As we have introduced the concept of subrepresentation, we wish to now define the most "basic" type of representation:

**Definition 2.1.3.** *An* **irreducible representation for** *$G$ is a representation $V$ that cannot be expressed as a direct sum of subrepresentations.*

In fact, we get a stronger result telling us that irreducible representations are our "representation building blocks":

**Theorem 2.1.4.** *For any representation $V$ of $G$, we can express $V$ as a unique direct sum of irreducible representations [FH91].*

**Remark:** Recall that if $A = (a_{ij})$ is a complex $n \times n$ matrix, then the trace of $A$ is given by $\mathrm{tr}(A) = \sum_{i=1}^{n} a_{ii}$, the sum of the diagonal entries in $A$.

Let $g \in G$. Then, if $\rho$ is a representation for $G$ on $V$, $\rho(g)$ is a linear transformation from $V$ to itself. But, we know from linear algebra that any linear transformation can be expressed as a matrix, considering some standard, ordered arrangement of basis vectors. Hence we can talk about the trace of $\rho(g)$'s associated matrix. It is easily shown that this number is independent of choice of basis for $V$, which leads us to the following definition.

**Definition 2.1.5.** *Let $g \in G$, and let $\rho$ be a representation for $G$ on $V$. Let $M_g$ be the matrix with respect to some ordered basis corresponding to $\rho(g)$. Then the trace of $M_g$ is called the* **character of $g$ with respect to the representation** *$V$, frequently denoted $\chi_V(g)$.*

Note that the character of the identity element $e \in G$ with respect to a representation $V$ is always equal to the dimension of $V$, call it $n$, since $\rho(e)$ is the identity transformation, and thus its associated $n \times n$ matrix is just $I_n$, the $n \times n$ identity matrix. To get a better feel for what a representation really is, we present a brief example.

**Example.**

Let $G = S_3$ be the symmetric group of order 3, that is, the group of permutations of three elements. Let $W$ be the vector space over $\mathbb{C}$ generated by the basis

$$B = \{(1,0,0), (0,1,0), (0,0,1)\}.$$

That is, $W = \mathbb{C}^3$. Define the representation map $\rho$ like so: $\rho(g) = T_g$, where $T_g$ is defined by

$$T_g(z_1, z_2, z_3) = (z_{g^{-1}(1)}, z_{g^{-1}(2)}, z_{g^{-1}(3)}),$$

where $g^{-1}(n)$ denotes the number (1, 2, or 3) that is sent to position $n$ by the permutation $g$. Let's pick a specific $g$: Say, $g = (12)$, that is, the transposition that sends 1 to 2, 2 to 1, and 3 to itself. Then we can note where $\rho(g) = T_g$ sends our basis elements:

$$T_g(1,0,0) = (0,1,0)$$
$$T_g(0,1,0) = (1,0,0)$$
$$T_g(0,0,1) = (0,0,1)$$

Hence our matrix associated with $T_g$ (with respect to our given ordered basis) is

$$M_g := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus, the character of $g$ with respect to representation $W$ is

$$\mathrm{Tr}(M_g) = 0 + 0 + 1 = 1.$$

Note that any other permutation of order 2 in $S_3$ will also have character 1, and that any permutation of order 3 has a character of 0 (since none of the elements are fixed.) The identity element, of course, has character 3 as expected, since $dim(W) = 3$.

In fact, these observations can be correctly generalized by the following statement:

**Theorem 2.1.6.** *With respect to a given representation $V$ of group $G$, any two elements of the same conjugacy class of $G$ have the same character. [FH91]*

**Remark:** Thus, if we are interested in finding every group element's character, we only need to pick one representative from each conjugacy class. In fact, we have a further correlation between conjugacy classes and representations: The number of irreducible representations of a group $G$ is equal to the number of congruence classes of $G$. [FH91]

Continuing our example, it turns out that our representation $W = \mathbb{C}^3$ is not actually irreducible, and can be expressed as the direct sum of a 1-dimensional and a 2-dimensional vector space. In particular, we can write $W = U \oplus V$, where $U = \mathrm{span}\{(1,1,1)\}$, and $V = \{(z_1, z_2, z_3) | z_1 + z_2 + z_3 = 0\}$. $U$ is clearly irreducible, since it has dimension 1, and in fact $V$ is irreducible, too [FH91]. Thus the direct sum $U \oplus V$ is the unique decomposition of $W = \mathbb{C}^3$ into irreducible representations of $S_3$.

## 2.2 Lattices

A **lattice** $L$ is an additive subgroup of $\mathbb{C}$ generated by two $\mathbb{R}$-linearly independent complex numbers $\omega_1$ and $\omega_2$. That is, $L = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$, with $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. This last requirement gives us the desired linear independence of $\omega_1$ and $\omega_2$. Geometrically, it is equivalent to saying that the two points do not lie on the same vector beginning at the origin, when viewing the complex plane as analogous to $\mathbb{R}^2$. Notationally, we write

$$L = [\omega_1, \omega_2] = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}.$$

Visually, lattices create nice parallelogram-tilings of $\mathbb{C}$. Two different lattices can be related in a particular way:

**Definition 2.2.1.** *The lattices $L = [\omega_1, \omega_2]$ and $L' = [\omega_1', \omega_2']$ are said to be* **homothetic** *if there exists $\lambda \in \mathbb{C}$ such that $L' = \lambda L$. That is, $[\omega_1', \omega_2'] = [\lambda\omega_1, \lambda\omega_2]$.*

Note that this property, homothety, defines an equivalence class on the set of all complex lattices; that is, we can look at the collection of all possible complex lattices and partition them by which lattices are homothetic to one another. We will call these equivalence classes **homothety classes**.

Now that we have lattices, we can define some important pieces of the $j$-function.

**Definition 2.2.2.** *Let $n \geq 3$, and let $L$ be a lattice. Then*

$$G_n(L) = \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^n}$$

*is called the* **Eisenstein series of order $n$ for $L$.**

You may now be asking, "What, if any, $n$ do we know this expression to converge for?" Well, that's a good question, hypothetical reader, one which we will now answer:

**Lemma 2.2.3.** *Suppose $L$ is a lattice and $s \in \mathbb{R}$ with $s > 2$. Then the series*

$$G_s(L) = \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^s}$$

*converges absolutely.*

*Proof.* Let $\omega_1$, $\omega_2 \in \mathbb{C}$ be the generators of $L$, that is, $L = [\omega_1, \omega_2]$. So then we need to show that

$$\sum_{\omega \in L \setminus \{0\}} \frac{1}{|\omega|^s} = \sum_{m,n} \frac{1}{|m\omega_1 + n\omega_2|^s}$$

converges, where the expression on the right is a sum over all integer pairs $(m, n) \neq (0, 0)$.

Define

$$M = \min\{|x\omega_1 + y\omega_2| : x^2 + y^2 = 1\}.$$

Let $x$ and $y$ be real numbers such that at least one of $x$ and $y$ is nonzero. Note that

$$\left(\frac{x}{\sqrt{x^2+y^2}}\right)^2 + \left(\frac{y}{\sqrt{x^2+y^2}}\right)^2 = \frac{x^2+y^2}{x^2+y^2} = 1.$$

Hence, by the definition of $M$,

$$\left|\frac{x}{\sqrt{x^2+y^2}}\omega_1 + \frac{y}{\sqrt{x^2+y^2}}\omega_2\right| = \frac{|x\omega_1 + y\omega_1|}{\sqrt{x^2+y^2}} \geq M,$$

and so

$$|x\omega_1 + y\omega_2| \geq M\sqrt{x^2+y^2}$$

for all $x, y \in \mathbb{R}$.

We picked $x$ and $y$ so that at least one of them was nonzero to avoid having a zero denominator in our earlier expression, but this inequality is clearly true for $x = y = 0$, so it holds for all $x, y \in \mathbb{R}$.

But then

$$\sum_{m,n} \frac{1}{|m\omega_1 + n\omega_2|^s} \leq \frac{1}{M^s} \sum_{m,n} \frac{1}{(m^2+n^2)^{s/2}}.$$

Consider, then, the integral

$$\iint\limits_{x^2+y^2 \geq 1} \frac{1}{(x^2+y^2)^{s/2}} dx\ dy.$$

If this integral converges, we are done. Rewriting in terms of traditional polar coordinates $r$ and $\theta$, we have

$$\int_{r=1}^{\infty}\int_{\theta=0}^{2\pi}\frac{1}{r^s}r\,d\theta\;dr=\int_{r=1}^{\infty}\int_{\theta=0}^{2\pi}\frac{1}{r^{s-1}}d\theta\;dr.$$

Evaluating this expression with rudimentary calculus, we get

$$\int_{r=1}^{\infty}\frac{2\pi}{r^{s-1}}dr.$$

Since $s>2$, then $s-1>1$, and so this integral exists and is a finite number. It follows that

$$\sum_{m,n}\frac{1}{|m\omega_1+n\omega_2|^s}$$

must converge.

□

Hence, any Eisenstein series of order greater than 2 converges absolutely. Two particularly important Eisenstein series that we are especially interested in are

$$g_2(L)=60G_4(L)=60\sum_{\omega\in L\setminus\{0\}}\frac{1}{\omega^4}$$

and

$$g_3(L)=140G_6(L)=140\sum_{\omega\in L\setminus\{0\}}\frac{1}{\omega^6}.$$

We introduce now an important lattice-based function that will play a part in the proofs in Chapter 3.

**Definition 2.2.4.** *The* **Weierstrass $\wp$-function** *is defined by the following:*

$$\wp(z;L)=\frac{1}{z^2}+\sum_{\omega\in L\setminus\{0\}}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right)$$

*for $z\in\mathbb{C}$ and $L$ a lattice, where the sum on the right is a sum over all nonzero lattice points $\omega$ of $L$.*

If it is clear (or doesn't matter) which lattice we are referring to, $\wp(z;L)$ can be abbreviated to simply $\wp(z)$. The following lemmas about the $\wp$-function can be found in [Cox89]:

**Lemma 2.2.5.** *The set of singularities of $\wp(z;L)$ is exactly equal to the set of lattice points in $L$.*

This lemma becomes fairly clear intuitively by looking at the denominator terms in $\wp(z;L)$.

**Lemma 2.2.6.** *The Laurent expansion of $\wp(z)$ for the lattice $L$ takes the form*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} p(g_2(L), g_3(L)) z^{2n},$$

*where $p(g_2(L), g_3(L))$ is a polynomial with rational coefficients, independent of $L$, in $g_2(L)$ and $g_3(L)$.*

Proofs of these lemmas can be found in [Cox89]. Another function, which turns out to be an important piece of the $j$-function, is called the discriminant of the lattice $L$.

**Definition 2.2.7.** *The discriminant of the lattice $L$, denoted $\Delta(L)$, is given by*

$$\Delta(L) = g_2(L)^3 - 27 g_3(L)^2.$$

**Remark:** As it just so happens, $\Delta(L)$ is the discriminant of the polynomial $p(x) = 4x^3 - g_2 x - g_3$, which, incidentally, the Weirstrauss $\wp$-function satisfies like so, as mentioned by [Cox89]:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

The roots of this polynomial $p(x)$ are $e_1 = \wp(\omega_1/2)$, $e_2 = \wp(\omega_2/2)$, and $e_3 = \wp(\frac{\omega_1+\omega_2}{2})$. In fact, these roots are distinct [Apo90]. Hence, since the discriminant of a polynomial is a product of differences of its roots, we get the following lemma:

**Lemma 2.2.8.** *For any lattice $L$, the discriminant $\Delta(L)$ is nonzero.*

## 2.3 Modular Functions

Modular functions: Is there anything more beautiful? Probably, but that won't stop this mathematician from waxing hyperbolic! But before we get to these awe-inspiring paragons of beauty, we must first introduce some context.

$\mathrm{SL}_2(\mathbb{Z})$, as noted before, is defined as the group, under multiplication, of $2 \times 2$ matrices with integer entries and determinant 1. In the context of modular functions, we call the group $\mathrm{SL}_2(\mathbb{Z})$ the **modular group** $\Gamma$. It turns out that $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half-plane $\mathbb{H} = \{a + bi \in \mathbb{C} : b > 0\}$ through linear fractional transformations like so:

If $\tau \in \mathbb{H}$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

An easy calculation shows that the action of $\mathrm{SL}_2(\mathbb{Z})$ takes elements of $\mathbb{H}$ to $\mathbb{H}$. We have a nice property of $\mathrm{SL}_2(\mathbb{Z})$ in that it is generated by two matrices: [Apo90]

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Note that

$$T \cdot \tau = \tau + 1 \quad \text{and} \quad S \cdot \tau = -\frac{1}{\tau}.$$

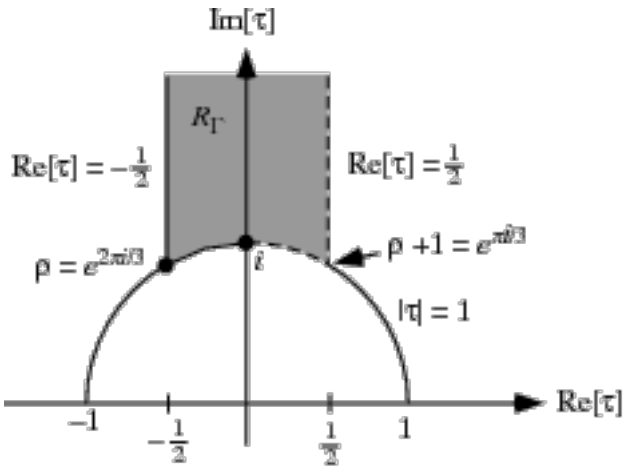


Figure 2.1: The Fundamental region $F$, here denoted $R_\Gamma$[BB87].

As we will see, modular forms have the property that they are invariant under $\mathrm{SL}_2(\mathbb{Z})$. Hence, we wish to analyze which points in $\mathbb{H}$ are "$\mathrm{SL}_2(\mathbb{Z})$-equivalent," that is, when two points $\tau, \tau' \in \mathbb{H}$ are such that $\tau' = \gamma \cdot \tau$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Specifically, is there a nice subregion of $\mathbb{H}$ where every point is $\mathrm{SL}_2(\mathbb{Z})$-distinct to every other point in the region and every $\mathrm{SL}_2(\mathbb{Z})$ equivalence class is represented? Why, yes! Yes, there is. This region is

$$F = \left\{ z \in \mathbb{C} : |z| > 1, -\frac{1}{2} \leq Re(z) < \frac{1}{2} \right\} \cup \left\{ z \in \mathbb{C} : |z| = 1, -\frac{1}{2} \leq Re(z) \leq 0 \right\},$$

and is called a fundamental region of the modular group $\Gamma$ (see Figure 2.3).
$F$ has the following properties:

1. Any two distinct points in $F$ are not $\mathrm{SL}_2(\mathbb{Z})$-equivalent.
2. For any $\tau \in \mathbb{H}$, there is a point $\tau'$ in $F$ such that $\tau$ and $\tau'$ are $\mathrm{SL}_2(\mathbb{Z})$-equivalent.

So, basically, whenever we're dealing with $\mathrm{SL}_2(\mathbb{Z})$-invariance of some kind, we can restrict our analysis to $F$. A side note: The generating matrices $S$ and $T$ transform $F$ in predictable and visually lovely ways (see Figure 2.2). We now define modular functions.

**Definition 2.3.1.** *A function $f : \mathbb{H} \to \mathbb{C}$ is called a* **modular function** *if it satisfies the following:*

1. *$f$ is meromorphic in the upper half-plane $\mathbb{H}$.*
2. *$f(\gamma \cdot \tau) = \tau$ for any $\gamma \in SL_2(\mathbb{Z})$ and all $\tau \in \mathbb{H}$.*
3. *The function $f$ has a Fourier expansion at $i\infty$ of the form*

$$f(\tau) = \sum_{n=-m}^{\infty} a(n) q^n,$$

*where $q = e^{2\pi i \tau}$, and $m$ is some integer.*

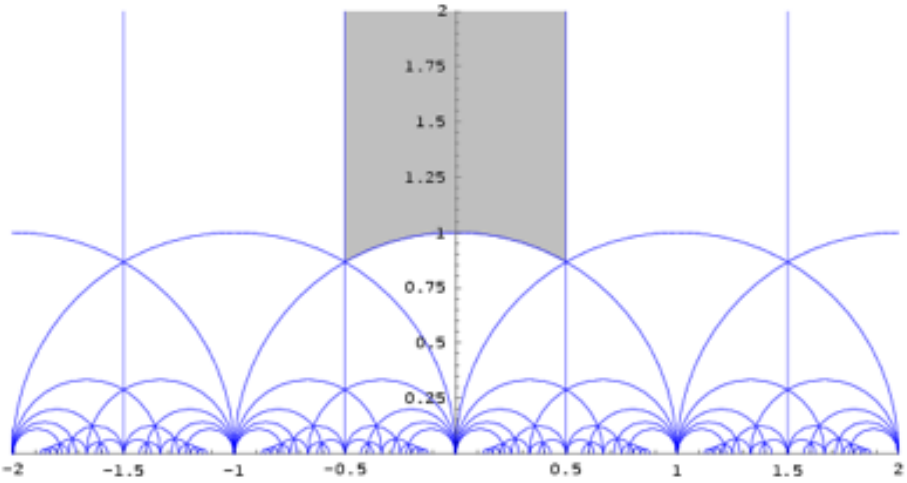


Figure 2.2: Each region bounded by the circles and lines of this figure represent a fundamental region for $\Gamma$, reached by transforming $F$ via some combination of matrices $S$ and $T$. [Arm]

Property 2 gives us modularity; that is, $f$ is invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. Some notes on Property 3: First of all, when considering the behavior of $f$ at infinity, we mean $i\infty$. The reason for this is due to the $\mathrm{SL}_2(\mathbb{Z})$-invariance of $f$; moving toward $z$-values with real part approaching $\infty$, the function values just keep cycling through the same values – picture moving your input points to the left through the Fundamental Domain F.

Secondly, this Fourier expansion in property 3 is called the **$q$-expansion of** $f$ and can be thought of as the Fourier expansion at $i\infty$, since $\lim_{\tau \to i\infty} e^{2\pi i \tau} = 0$. If $m > 0$, then $f$ has a pole of order $m$ at $i\infty$. If $m \leq 0$, then $f$ is analytic at $i\infty$. Another way of stating property 3 is that $f$ is **meromorphic at the cusp** or **meromorphic at** $\infty$.

**Remark:** Modular functions are a specific case of a more general type of function called a modular form. Basically, a modular form is like a modular function but with a slightly modified notion of $\mathrm{SL}_2(\mathbb{Z})$-invariance. More precisely, a **modular form** $f(\tau)$ **of weight** $k$ is a function, either meromorphic or holomorphic on $\mathbb{H}$, that has Property 3 of Definition 2.3.1, and $f(\gamma \cdot \tau) = (c\tau + d)^k f(\tau)$, where $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. In particular, a modular function is a modular form of weight 0.

It turns out that holomorphic modular forms of weight $k$ form a finite dimensional vector space $M_k$, with a basis given by certain products of $G_4$ and $G_6$. Hence we can consider certain linear operators that map $M_k$ to $M_k$. One such operator, which we will need in a later proof, is called a Hecke operator. The following definition and lemma can be found in [Apo90].

**Definition 2.3.2.** *For a fixed integer $k$ and any $n \in \mathbb{N}$, the* **$n$th Hecke operator** *$T_n$ is defined on $M_k$ by*

$$(T_n f)(\tau) = n^{k-1} \sum_{d|n} d^{-k} \sum_{b=0}^{d-1} f\left(\frac{n\tau + bd}{d^2}\right).$$

What we are really interested in, though, is the Fourier expansion of such Hecke-operated functions:

**Lemma 2.3.3.** *If $f \in M_k$ and $f$ has the Fourier expansion*

$$f(\tau) = \sum_{m=0}^{\infty} c(m) q^m,$$

*then $T_n f$ has the Fourier expansion*

$$(T_n f)(\tau) = \sum_{m=0}^{\infty} \left( \sum_{d|(m,n)} d^{k-1} c\left(\frac{mn}{d^2}\right) \right) q^m.$$

Thus if our function $f$ is a modular function; that is, an element of $M_0$, this expansion becomes

$$(T_n f)(\tau) = \sum_{m=0}^{\infty} \left( \sum_{d|(m,n)} \frac{1}{d} \cdot c\left(\frac{mn}{d^2}\right) \right) q^m \ .$$

Further exploration of modular functions can be found in [Apo90] and [Ser73].

## 2.4 Jay at Last!

Now we finally have the tools to define the $j$-function. Let's do so!

**Definition 2.4.1.** *The $j$-invariant of a lattice $L$ is defined as the complex number*

$$j(L) = 1728 \cdot \frac{g_2(L)^3}{g_2(L)^3 - 27 g_3(L)^2},$$

*where $g_2$ and $g_3$ are the previously-defined modified Eisenstein series.*

Note that the denominator of $j$ is $g_2(L)^3 - 27 g_3(L)^2 = \Delta(L)$. This is handy, since Lemma 2.2.8 tells us that $\Delta(L)$ is never 0 for any lattice $L$. The $j$-function itself is defined like so:

**Definition 2.4.2.** *The* **$j$-function** *$j(\tau)$ is defined as a complex-valued function such that, for any $\tau \in \mathbb{H}$,*

$$j(\tau) = j([1, \tau]),$$

*that is, $j(\tau)$ is the $j$-invariant of the lattice $[1, \tau]$.*

*Similarly, we modify our old series $g_2$ and $g_3$ so that*

$$g_2(\tau) = g_2([1, \tau]) = 60 \sum_{m,n} \frac{1}{(m + n\tau)^4}$$

*and*

$$g_3(\tau) = g_3([1, \tau]) = 140 \sum_{m,n} \frac{1}{(m + n\tau)^6}.$$

*So then we have that*

$$j(\tau) = 1728 \cdot \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2}.$$

The $j$-function has many important properties, such as the following:

**Lemma 2.4.3.** *The $j$-function is holomorphic on the upper half plane $\mathbb{H}$.*

We will use this lemma as a fact. A good proof, relying on the uniform convergence of $g_2$ and $g_3$ can be found in [Cox89].

# Chapter 3

# Properties of $j(\tau)$

## 3.1 Proof of Theorem 1.2.4

Recall that Theorem 1.2.4 states that $j(\tau)$ is a bijection between $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ and $\mathbb{C}$. Our first step is to show that $j(L)$, as an invariant, characterizes a lattice $L$ with respect to its homothetic lattices. (Recall the definition of *homothetic*, Definition 2.2.1.)

**Theorem 3.1.1.** *If $L$ and $L'$ are lattices in $\mathbb{C}$, then $j(L) = j(L')$ if and only if $L$ and $L'$ are homothetic.*

*Proof.* ($\Leftarrow$) Suppose $L$ and $L'$ are homothetic; that is, $L' = \lambda L$ for some $\lambda \in \mathbb{C}$. We know

$$g_2(L') = g_2(\lambda L) = 60 \sum_{\omega \in L\backslash\{0\}} \frac{1}{(\lambda\omega)^4} = \frac{1}{\lambda^4} 60 \sum_{\omega \in L\backslash\{0\}} \frac{1}{\omega^4} = \lambda^{-4} g_2(L).$$

Similarly,

$$g_3(L') = g_3(\lambda L) = 140 \sum_{\omega \in L\backslash\{0\}} \frac{1}{(\lambda\omega)^6} = \frac{1}{\lambda^6} 140 \sum_{\omega \in L\backslash\{0\}} \frac{1}{\omega^6} = \lambda^{-6} g_3(L).$$

So then

$$j(L') = 1728 \cdot \frac{g_2(L')^3}{g_2(L')^3 - 27 g_3(L')^2} = 1728 \cdot \frac{\lambda^{-12} g_2(L)^3}{\lambda^{-12} g_2(L)^3 - 27\lambda^{-12} g_3(L)^2}$$

$$= 1728 \cdot \frac{g_2(L)^3}{g_2(L)^3 - 27 g_3(L)^2} = j(L).$$

□

Now we prove the reverse implication.
($\Rightarrow$) Let $j(L) = j(L')$. Suppose we can find a $\lambda \in \mathbb{C}$ such that $g_2(L') = \lambda^{-4} g_2(L)$ and $g_3(L') = \lambda^{-6} g_3(L)$. Then $g_2(L') = g_2(\lambda L)$ and $g_3(L) = g_3(\lambda L)$, and by Lemma 2.2.6, we have that the Laurent expansion for $\wp(z; L')$ is

$$\wp(z; L') = \frac{1}{z^2} + \sum_{n=1}^{\infty} p(g_2(L'), g_3(L')) z^{2n} = \frac{1}{z^2} + \sum_{n=1}^{\infty} p(g_2(\lambda L), g_3(\lambda L)) z^{2n} = \wp(z; \lambda L).$$

Thus $\wp(z; L')$ and $\wp(z; \lambda L)$ have the same Laurent expansion about 0. So then these two functions agree on a neighborhood $U$ about the origin. But we have that $\wp(z; L')$ and $\wp(z; \lambda L)$ are analytic on the region $\Omega := \mathbb{C} \setminus (\lambda L \cup L')$, and the set

$$\{z \in \Omega : \wp(z; L') = \wp(z; \lambda L)\}$$

certainly has a limit point in $U \cap \Omega$, and hence

$$\wp(z; L') = \wp(z; \lambda L)$$

on all of $\Omega$, so $\wp(z; L')$ and $\wp(z; \lambda L)$ must have the same poles. Since, by Lemma 2.2.5, the lattice $L'$ is precisely the set of poles of $\wp(z; L')$, then $L' = \lambda L$. Thus, to complete this proof, we need only find a $\lambda \in \mathbb{C}$ such that $g_2(L') = \lambda^{-4} g_2(L)$ and $g_3(L') = \lambda^{-6} g_3(L)$.

Note that

$$g_2(L)^3 - 27 g_3(L)^2 = \Delta(L)$$

can never be 0 by Lemma 2.2.8. Thus, we have the following three cases:

- Case 1: $g_2(L') = 0$ and $g_3(L') \neq 0$. Then choose $\lambda$ so that $\lambda^6 = \frac{g_3(L)}{g_3(L')}$.
- Case 2: $g_3(L') = 0$ and $g_2(L') \neq 0$. Then choose $\lambda$ so that $\lambda^4 = \frac{g_2(L)}{g_2(L')}$.
- Case 3: $g_2(L') \neq 0$ and $g_3(L') \neq 0$. Then choose $\lambda$ such that $\lambda^4 = \frac{g_2(L)}{g_2(L')}$. Since we have that $j(L) = j(L')$, then

$$1728 \cdot \frac{g_2(L)^3}{g_2(L)^3 - 27 g_3(L)^2} = 1728 \cdot \frac{g_2(L')^3}{g_2(L')^3 - 27 g_3(L')^2}.$$

By substituting $\lambda^4 g_2(L')$ for $g_2(L)$, we get that

$$\frac{(\lambda^4 g_2(L'))^3}{(\lambda^4 g_2(L'))^3 - 27 g_3(L)^2} = \frac{g_2(L')^3}{g_2(L')^3 - 27 g_3(L')^2}.$$

Cross-multiplying and solving for $\lambda^{12}$ yields that

$$\lambda^{12} = \frac{-27 g_3(L)^2}{-27 g_3(L')^2} = \frac{g_3(L)^2}{g_3(L')^2}.$$

So then

$$\lambda^6 = \pm \frac{g_3(L)}{g_3(L')}.$$

Assume the sign on the right is $+$, since if not, we can replace $\lambda$ by $i\lambda$. Thus we have that $g_3(L') = \lambda^{-6} g_3(L)$.

Hence, in any of the cases, we can find a $\lambda \in \mathbb{C}$ such that $g_2(L') = \lambda^{-4} g_2(L)$ and $g_3(L') = \lambda^{-6} g_3(L)$.

□

**Remark:** We just showed that the $j$-invariant characterizes lattice homothety classes. Now, given some lattice $L = [\omega_1, \omega_2]$, there is a homothetic lattice $L' = [1, \frac{\omega_2}{\omega_1}]$ (by letting $\lambda = \frac{1}{\omega_1}$, renumbering if necessary so that $\frac{\omega_2}{\omega_1} \in \mathbb{H}$). But then, by Theorem 3.1.1 and Definition 2.4.2,

$$j(L) = j(L') = j\left(\frac{\omega_2}{\omega_1}\right)$$

. Hence the $j$-function in a sense represents all possible lattice homothety classes.

Theorem 3.1.1 leads directly to a very nice property of the $j$-function: invariance under the action of $\mathrm{SL}_2(\mathbb{Z})$.

**Theorem 3.1.2.** *If $\tau, \tau' \in \mathfrak{h}$, then $j(\tau) = j(\tau')$ if and only if $\tau' = \gamma\tau$ for some $\gamma \in SL_2(\mathbb{Z})$. In particular, $j(\tau)$ is $SL_2(\mathbb{Z})$-invariant.*

*Proof.* ($\Rightarrow$) Suppose $j(\tau) = j(\tau')$. By definition of the $j$-function, and by Theorem 3.1.1, then the lattices $L := [1, \tau]$ and $L' := [1, \tau']$ are homothetic. That is, $[1, \tau'] = [\lambda, \lambda\tau]$ for some $\lambda \in \mathbb{C}$.

Hence, we can write

$$\lambda = r\tau' + s \text{ and } \lambda\tau = p\tau' + q,$$

with $p, q, r, s \in \mathbb{Z}$. We then have that

$$\tau = \frac{\lambda\tau}{\lambda} = \frac{p\tau' + q}{r\tau' + s} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \cdot \tau'.$$

Thus we just need to show that $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

We have that

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda\tau \\ \lambda \end{pmatrix}.$$

Similarly, since $[1, \tau'] = [\lambda, \lambda\tau]$, there exists a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with integer entries such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \lambda\tau \\ \lambda \end{pmatrix} = \begin{pmatrix} \tau' \\ 1 \end{pmatrix}.$$

But then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \begin{pmatrix} \tau' \\ 1 \end{pmatrix}.$$

Define the matrix

$$A := \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

So $A\left(\begin{smallmatrix} \tau' \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \tau' \\ 1 \end{smallmatrix}\right)$. Hence $a'\tau' + b' = \tau'$. Divide through by $\tau'$ and we get that $a' + b'\frac{1}{\tau'} = 1$. But $\frac{1}{\tau'} \notin \mathbb{R}$, since $[1, \tau']$ is a lattice. Hence, since $a'$ and $b'$ are integers, $b' = 0$ and $a' = 1$. Similarly, we have that $c'\tau' + d' = 1$, leading to the conclusion that $c' = 0$ and $d' = 1$. Thus we have that $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and so

$$\det(A) = 1 = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \det \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

Since the determinants on the right must be integers, then $\det\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) = \pm 1$. So now we just have to show that $\det\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) > 0$ .

Let $\tau' = a + bi$ for $a, b \in \mathbb{R}$. Then

$$\mathrm{Im}(\tau) = \mathrm{Im}\left(\frac{p\tau' + q}{r\tau' + s}\right) = \frac{b(ps - qr)}{|r\tau + s|^2} = \frac{\mathrm{Im}(\tau')(ps - qr)}{|r\tau + s|^2}.$$

Since $\tau$ and $\tau'$ are in $\mathbb{H}$, then $ps - qr = \det\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) > 0$, so

$$\det \begin{pmatrix} p & q \\ r & s \end{pmatrix} = 1,$$

and we have that $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

Now we prove the other direction of the implication, which proves to be a bit more straightforward:

($\Leftarrow$) Suppose $\tau' = \gamma\tau$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. That is,

$$\tau' = \frac{p\tau + q}{r\tau + s},$$

with $p, q, r, s \in \mathbb{Z}$, and $\det\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) = 1$.

Let $\lambda = r\tau + s$. Then we have that

$$\lambda[1, \tau'] = (r\tau + s)\left[1, \frac{p\tau + q}{r\tau + s}\right] = [r\tau + s, p\tau + q].$$

But we can write

$$-q(r\tau + s) + s(p\tau + q) = (ps - qr)\tau + (qs - qs) = \tau,$$

since $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Similarly,

$$p(r\tau + s) - r(p\tau + q) = (pr - pr)\tau + (ps - qr) = 1.$$

Thus $[1, \tau] \subseteq \lambda[1, \tau']$, and since clearly $\lambda[1, \tau'] \subseteq [1, \tau]$, we have that

$$[r\tau + s, p\tau + q] = \lambda[1, \tau'] = [1, \tau],$$

and hence $[1, \tau']$ is homothetic to $[1, \tau]$. It follows from Theorem 3.1.1 that $j(\tau) = j(\tau')$. $\square$

Let us now think of Theorem 3.1.2 in the context of Theorem 1.2.4, what we aim to prove. The forward implication of Theorem 3.1.2 gives that $j(\tau)$, viewed as a map from $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ to $\mathbb{C}$, is well-defined. The backwards implication gives us that this map is one-to-one. Hence we already have half of Theorem 1.2.4 proved; namely, that $j(\tau)$ is one-to-one as a map from $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ to $\mathbb{C}$. Now we wish to show surjectivity. First, though, we must examine its behavior at the cusp, $i\infty$.

**Lemma 3.1.3.** *We have that*

$$\lim_{\mathrm{Im}(\tau)\to\infty} j(\tau) = \infty.$$

*Proof.* To start, consider

$$g_2(\tau) = 60 \sum_{m,n} \frac{1}{(m + n\tau)^4} = 60 \left( 2 \sum_{m=1}^{\infty} \frac{1}{m^4} + \sum_{m,n;n\neq 0} \frac{1}{(m + n\tau)^4} \right). \tag{3.1}$$

Let $\tau = a + bi$. But if we consider a single term in the right-hand sum, we find that

$$\lim_{\mathrm{Im}(\tau)\to\infty} \frac{1}{(m+n\tau)^4} = \lim_{\mathrm{Im}(\tau)\to\infty} \frac{1}{m^4 + 4m^3(n\tau) + 6m^2(n\tau)^2 + 4m(n\tau)^3 + (n\tau)^4}.$$

Because $n \neq 0$, then the $b^4$ term in $(n\tau)^4 = n^2(a^4 + 4a^3(bi) - 6a^2b^2 + 4a(bi)^3 - b^4)$ dominates the denominator as $b$ becomes arbitrarily large. Hence,

$$\lim_{\mathrm{Im}(\tau)\to\infty} \frac{1}{(m+n\tau)^4} = 0.$$

Since $g_2(\tau)$ is uniformly convergent by Lemma 2.2.3, then, in taking the limit, equation (3.1) becomes

$$\lim_{\mathrm{Im}(\tau)\to\infty} g_2(\tau) = 120 \sum_{m=1}^{\infty} \frac{1}{m^4}.$$

But this is a known infinite sum, with $\sum_{m=1}^{\infty} \frac{1}{m^4} = \frac{\pi^4}{90}$. Hence,

$$\lim_{\mathrm{Im}(\tau)\to\infty} g_2(\tau) = \frac{4}{3}\pi^4.$$

The limit behavior of $g_3(\tau)$ is shown similarly, with the sum $\sum_{m=1}^{\infty} \frac{1}{m^6} = \frac{\pi^6}{945}$ giving us that

$$\lim_{\mathrm{Im}(\tau)\to\infty} g_3(\tau) = \frac{8}{27}\pi^6.$$

Combining these two results, we get the limit of the denominator of the $j$-function:

$$\lim_{\mathrm{Im}(\tau)\to\infty} \left[g_2(\tau)^3 - 27g_3(\tau)^2\right] = \left(\frac{4}{3}\pi^4\right)^3 - 27\left(\frac{8}{27}\pi^6\right)^2 = 0. \tag{3.2}$$

Thus, it follows that

$$\lim_{\mathrm{Im}(\tau)\to\infty} j(\tau) = \infty.$$

□

**Remark:** Since, as shown in equation (3.2), $\Delta(\tau)$ has a simple zero at $\infty$, then $j(\tau)$ has a simple pole at $\infty$, and hence $j(\tau)$ is meromorphic at $\infty$. Combining this fact with Theorem 3.1.2, we have the following immediate corollary:

**Corollary 3.1.4.** *The function $j(\tau)$ is a modular function for $SL_2(\mathbb{Z})$.*

Now we can prove that $j(\tau)$ is, indeed, surjective.

**Theorem 3.1.5.** *The function $j : \mathbb{H} \to \mathbb{C}$ is surjective.*

*Proof.* We know that $j(\tau)$ is nonconstant on $\mathbb{H}$, since there are values for $\tau$ that are distinct under the action of $\mathrm{SL}_2(\mathbb{Z})$ (each point in the fundamental region $F$ is $\mathrm{SL}_2(\mathbb{Z})$-distinct from every other point in $F$). Also, by Lemma 2.4.3, $j(\tau)$ is holomorphic on $\mathbb{H}$. Hence, by the

open mapping theorem, the image of $j(\tau)$ must be an open set in $\mathbb{C}$. Since the only set that is both open and closed in $\mathbb{C}$ is itself, it is sufficient to prove that $j(\mathbb{H})$ is closed.

Let $j(\tau_k)$ be a sequence in $j(\mathbb{H})$ converging to some $w \in \mathbb{C}$ (where $\tau_k \in \mathbb{H}$). Since $j(\tau)$ is invariant under $\mathrm{SL}_2(\mathbb{Z})$, then by only considering $\tau$ in our fundamental domain $F$, we may assume that each $\tau_k$ is such that

$$|\mathrm{Re}(\tau_k)| \leq \frac{1}{2} \text{ and } |\mathrm{Im}(\tau_k)| \geq \frac{\sqrt{3}}{2}.$$

Suppose the imaginary parts of the $\tau_k$'s are unbounded. But then, by Lemma 3.1.3, $j(\tau_k)$ contains a subsequence converging to $\infty$. Since $j(\tau_k)$ converges to $w$, this cannot happen. So the imaginary parts of the $\tau_k$'s are bounded, say by some $M \in \mathbb{R}$. Hence each $\tau_k$ lies in the region

$$R = \left\{ \tau \in \mathbb{H} : |\mathrm{Re}(\tau)| \leq \frac{1}{2}, \frac{\sqrt{3}}{2} \leq |\mathrm{Im}(\tau)| \leq \mathrm{M} \right\},$$

a compact subspace of $\mathbb{H}$. But this implies that $\tau_k$ has a subsequence converging to some $\tau_0 \in \mathbb{H}$. Since $j(\tau)$ is continuous and $j(\tau_k)$ converges to $w$, then $j(\tau_0) = w$, and hence $w \in j(\mathbb{H})$. Thus $j(\mathbb{H})$ is closed, and so $j(\mathbb{H}) = \mathbb{C}$.

□

Thus, through combining Theorem 3.1.2 and Theorem 3.1.5, we have proven Theorem 1.2.4, that $j(\tau)$ is a bijection between $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ and $\mathbb{C}$.

## 3.2 The Function $j(\tau)$ as a "Modular Function Generator"

Now we turn our sights to Theorem 1.2.5, namely showing that $j(\tau)$ generates all modular functions on $\mathrm{SL}_2(\mathbb{Z})$. Before the big results, we prove a quick lemma:

**Lemma 3.2.1.** *A modular function $f$ which is holomorphic at $\infty$ (i.e., its $q$-expansion has no negative powers of $q$) is constant.*

*Proof.* It suffices to show that $f(\mathbb{H} \cup \{\infty\})$ is compact in $\mathbb{C}$; the maximum modulus principle of complex analysis then tells us that $f$ must be constant. We do so by showing that $f(\mathbb{H} \cup \{\infty\})$ is sequentially compact, i.e., every sequence has a subsequence that converges to a point in $f(\mathbb{H} \cup \{\infty\})$. Since $\mathbb{C}$ is a metric space, compactness is equivalent to sequential compactness.

Let $\{f(\tau_k)\}$ be a sequence in $f(\mathbb{H} \cup \{\infty\})$. Since $f$ is modular and thus $\mathrm{SL}_2(\mathbb{Z})$-invariant, we can assume that each $\tau_k$ lies in our fundamental region $F$. If the imaginary parts of the $\tau_k$'s are unbounded, then there is a subsequence of $\{\tau_k\}$ converging to $i\infty$. But then there is a subsequence of $\{f(\tau_k)\}$ which converges to $f(\infty)$, which is a finite complex number since $f$ is holomorphic at $\infty$.

If the imaginary parts of the $\tau_k$'s are bounded, say $\mathrm{Im}(\tau_k) \leq M$ for some $M \in \mathbb{R}$, then each $\tau_k$ lies in the region $R := \{z \in \mathbb{C} : |z| \geq 1, -1/2 \leq \mathrm{Re}(z) \leq 1/2, \mathrm{Im}(z) \leq M\}$, which is closed and bounded and hence compact. Thus a subsequence of $\{\tau_k\}$ can be found which

converges to an element $\tau_0$ of $R$, and hence $f(\tau_k)$ converges to $f(\tau_0)$, since $f$ is continuous. Hence, $f(\mathbb{H} \cup \{\infty\})$ is compact and thus $f$ must be constant. □

**Lemma 3.2.2.** *Every holomorphic modular function for $SL_2(\mathbb{Z})$ is a polynomial in $j(\tau)$.*

*Proof.* Suppose $f(\tau)$ is a holomorphic modular function for $\mathrm{SL}_2(\mathbb{Z})$. Since $f$ is modular and thus meromorphic at the cusp $i\infty$, its $q$-expansion looks like

$$f(\tau) = \sum_{n=-m}^{\infty} a_n q^n,$$

where $m$ is some positive integer. But the only negative $q$-power term in $j(\tau)$'s $q$-expansion is simply $q^{-1}$. Hence, we can define a polynomial $A(x)$ such that $f(\tau) - A(j(\tau))$ has no terms with negative $q$ powers. So then $f(\tau) - A(j(\tau))$ is holomorphic at $\infty$ and hence must be constant by Lemma 3.2.1. Thus,

$$f(\tau) = k + A(j(\tau))$$

for some $k \in \mathbb{C}$ and hence $f(\tau)$ is a polynomial in $j(\tau)$. □

And now our goal for this section:

**Theorem 3.2.3.** *Every modular function for $SL_2(\mathbb{Z})$ is a rational function in $j(\tau)$.*

*Proof.* Suppose $f(\tau)$ is a modular function for $\mathrm{SL}_2(\mathbb{Z})$. Our goal is to find some polynomial $B(x)$ such that $B(j(\tau))f(\tau)$ is holomorphic. Then applying Lemma 3.2.2, we obtain the desired conclusion.

Because $f$ is modular, it only has a finite number of poles in our fundamental domain $F$. The idea is to find a polynomial of $j(\tau)$ for each pole that kills each pole of $f(\tau)$, making the resulting function holomorphic at that point.

Let $\tau_0$ be a pole of $f$ of order $m$. Suppose $j'(\tau_0) \neq 0$. Then consider

$$(j(\tau) - j(\tau_0))^m f(\tau).$$

If we write $j(\tau)$ and $f(\tau)$ as Laurent series about $\tau_0$, we get

$$j(\tau) = \sum_{n=0}^{\infty} a_n(\tau - \tau_0)^n \text{ and } f(\tau) = \sum_{n=-m}^{\infty} b_n(\tau - \tau_0)^n,$$

for some constants $a_n$ and $b_n$ since, at the point $\tau_0$, we know $j$ is holomorphic and $f$ has a pole of order $m$. Note that $a_0 = j(\tau_0)$.

Then consider

$$(j(\tau) - j(\tau_0))^m f(\tau) = \left( \left( \sum_{n=0}^{\infty} a_n(\tau - \tau_0)^n \right) - a_0 \right)^m f(\tau)$$

$$= \left( \sum_{n=1}^{\infty} a_n(\tau - \tau_0)^n \right)^m \sum_{n=-m}^{\infty} b_n(\tau - \tau_0)^n.$$

The resulting expansion will have no negative powers of $(\tau - \tau_0)$, and hence

$$(j(\tau) - j(\tau_0))^m f(\tau)$$

is holomorphic at $\tau_0$.

Multiplying all such polynomials $(j(\tau) - j(\tau_k))^{m_k}$ corresponding to each of the $k$ poles of $f$ in $F$ yields the polynomial in $j(\tau)$

$$\prod_k (j(\tau) - j(\tau_k))^{m_k}$$

which, when multiplied by $f$, gives a function that is holomorphic at each pole $\tau_k$.

The only case we have omitted is if we have a pole $\tau_0$ such that $j'(\tau_0) = 0$. It turns out that this only happens at $i$ and $e^{2\pi i/3}$, and similar polynomials in $j(\tau)$ are easily obtained at each point so that their product with $f(\tau)$ gives a suitably holomorphic function. [Cox89]

Thus, multiplying all of our collected polynomials together to get some $B(j(\tau))$, we have that $B(j(\tau))f(\tau)$ is holomorphic, and hence by our previous theorem,

$$f(\tau) = \frac{A(j(\tau))}{B(j(\tau))}$$

for some polynomial $A(x)$.

□

Hence, in proving Theorem 1.2.5, we have shown that $j(\tau)$ can be thought of as the generator of all meromorphic modular functions. Such a function in general is called a **hauptmodul**, a term that will crop up in the statement of monstrous moonshine.

## 3.3 Denominator Formula

The connection between the $j$-function and the Monster that we alluded to in the Introduction is actually a specific case of the monstrous moonshine theorem. In fact, Borcherds uses yet another property of $j(\tau)$ to complete a portion of his argument in the proof of moonshine. This property is related to something called the denominator formula [Bor92], and takes the following form:

**Theorem 3.3.1.** *[Bor92] For $p = e^{2\pi i z}$ and $q = e^{2\pi i \tau}$ with $z, \tau \in \mathbb{H}$, we have that*

$$p^{-1} \prod_{m>0, n\in\mathbb{Z}} (1 - p^m q^n)^{c(mn)} = j(p) - j(q) \tag{3.3}$$

*where $j(q) - 744 = \sum_{n=-1}^{\infty} c(n) q^n = q^{-1} + 196884q + \cdots$, and $j(p) := j(z)$ and $j(q) := j(\tau)$.*

*Proof.* We begin by multiplying the left-hand side of equation (3.3) by $p$ and then taking the natural logarithm. So we have

$$\ln\left(\prod_{m>0, n\in\mathbb{Z}} (1 - p^m q^n)^{c(mn)}\right) = \sum_{m>0}\sum_{n\in\mathbb{Z}} \ln(1 - p^m q^n)^{c(mn)} = \sum_{m>0}\sum_{n\in\mathbb{Z}} c(mn)\ln(1 - p^m q^n)$$

by basic logarithm rules. Since $p^m q^n = e^{2\pi i(mz+n\tau)}$ and $c(mn) = 0$ for $n < -1$, then we have that

$$0 < |p^m q^n| < 1.$$

Hence we can use the Laurent expansion for the logarithm in our expression above, and we get

$$\sum_{m>0}\sum_{n\in\mathbb{Z}}\sum_{k>0} -c(mn)\frac{(p^m q^n)^k}{k} = -\sum_{m>0}\sum_{n\in\mathbb{Z}}\sum_{k>0} c(mn)\frac{p^{mk}q^{nk}}{k}.$$

Set $m_0 = mk$, and $n_0 = nk$. Then we have

$$-\sum_{m>0}\sum_{n\in\mathbb{Z}}\sum_{k>0} c(mn)\frac{p^{m_0}q^{n_0}}{k}.$$

By reindexing, and considering the sum over particular $m_0$'s and $n_0$'s instead of $k$'s, we get

$$-\sum_{m>0}\sum_{n\in\mathbb{Z}}\sum_{0<k|(m,n)} \frac{1}{k}c\left(\frac{mn}{k^2}\right)p^m q^n. \tag{3.4}$$

But, by Lemma 2.3.3, we know that, for fixed $m > 0$,

$$\sum_{0<k|(m,n)}\sum_{n\in\mathbb{Z}} \frac{1}{k}c\left(\frac{mn}{k^2}\right)p^m q^n = T_m\left(\sum_{n\in\mathbb{Z}} c(n)q^n\right)p^m,$$

where $T_m$ is the $m$-th Hecke operator. Hence, expression (3.4) now becomes

$$-\sum_{m>0} T_m\left(\sum_{n\in\mathbb{Z}} c(n)q^n\right)p^m = -\sum_{m>0} T_m(j(q) - 744)p^m.$$

As each $T_m$ is a linear operator on the space of holomorphic modular functions, then this expression can be written

$$\sum_{m>0} f_m(q)p^m,$$

where each $f_m$ is a holomorphic modular function. Now recall that we began by multiplying the left hand side of equation 3.3 by $p$ and taking the logarithm. Hence we have shown that

$$\ln\left(\prod_{m>0,n\in\mathbb{Z}}(1-p^m q^n)^{c(mn)}\right) = \sum_{m>0} f_m(q)p^m.$$

If we exponentiate our expression and multiply by $p^{-1}$, then, we get that

$$p^{-1}\prod_{m>0,n\in\mathbb{Z}}(1-p^m q^n)^{c(mn)} = p^{-1}e^{\sum_{m>0} f_m(q)p^m}.$$

Since $e^z$ is an analytic function with a nice Fourier expansion with respect to $p$, then this expression becomes

$$p^{-1}\sum_{m\geq 0} h_m(q)p^m,$$

where each $h_m$ is some holomorphic modular function. By Lemma 3.2.2, each $h_m(q)$ can be written as a polynomial in $j(q)$. Thus we get that the left hand side of equation (3.3) is equal to

$$\sum_{m\geq -1} g_m(j(q))p^m,$$

where each $g_m$ is a polynomial. Now we compare this sum with the right hand side of (3.3),

$$j(p) - j(q) = \frac{1}{p} + 744 + \sum_{m\geq 1} c(m)p^m - j(q),$$

clearly a polynomial in $j(q)$. Hence, we have shown that each side of (3.3) can be written as a polynomial of $j(q)$. But, as Borcherds notes in [Bor92], if we know the coefficients of $q_n$ for $n \leq 0$ in a polynomial of $j(q)$, we can determine the polynomial entirely. So it will suffice to show that, in the left hand expansion of (3.3) the coefficient on $\frac{1}{q}$ is $-1$, the constant term is $j(p) - 744$, and the coefficients for $q^n$, $n < -1$ are all 0.

First, note that $c(mn)$ is zero whenever $n \leq 0$ and $m > 1$. Hence, the left hand side of (3.3) becomes

$$\begin{aligned} p^{-1}(1-p^1q^{-1})^1 \prod_{m>0,n>0}(1-p^mq^n)^{c(mn)} &= (p^{-1}-q^{-1}) \prod_{m>0,n>0}(1-p^mq^n)^{c(mn)} \\ &= p^{-1}\prod_{m>0,n>0}(1-p^mq^n)^{c(mn)} - q^{-1}\prod_{m>0,n>0}(1-p^mq^n)^{c(mn)}. \end{aligned} \tag{3.5}$$

Since $n \geq 1$ in the product, the only $\frac{1}{q}$ term will come from the right-hand product in expression (3.5), multiplying the only constant term in the product, 1. Hence, the coefficient on $\frac{1}{q}$ is, indeed, $-1$.

As for terms which are constant in $q$, in the left-hand product in expression (3.5) we just have $p^{-1}$. In the right-hand product, the constant terms arise when $n = 1$, since then the $q^{-1}$ distributes through and cancels out the $q$ term. So we wish to find the coefficients on the $q$ terms in the product

$$\prod_{m>0}(1-p^mq)^{c(m)}. \tag{3.6}$$

By the binomial theorem, $(1-p^mq)^{c(m)} = 1 - c(m)p^mq + \cdots$ for each $m > 1$. So then expression (3.6) looks like

$$\prod_{m>0}(1-c(m)p^mq+\cdots),$$

so the only $q$ term in our product occurs when that second term multiplies with all the 1's in the other product terms. Thus if we collect all our q terms together, we get

$$q\sum_{m>0} c(m)p^m = q\left(j(p) - \frac{1}{p} - 744\right).$$

But then the $q^{-1}$ knocks out the $q$, and the only $q$-constant term we get from our left hand product in (3.5) is $\frac{1}{p}$, so the constant term in the left-hand side of (3.3) is $j(p) - 744$, the same as the $q$-constant term in the right-hand side.

Thus, the left and right hand sides of (3.3) are equal as polynomials in $j(q)$ and are hence equal.

□

# Chapter 4

# Monstrous Moonshine

We at last return to the conjecture that connects this wondrous function $j$ to the wondrous group $\mathbb{M}$. As you might imagine, the result is quite wondrous. First, though, we need just one more object before we can actually state the theorem which Borcherds proved.

## 4.1 The Moonshine Module $V\natural$

Now that we've introduced the Monster and Representation Theory, we can briefly introduce the Moonshine Module $V\natural$. In 1988, Igor Frenkel, James Lepowsky, and Arne Meurman constructed the $\mathbb{M}$-module $V\natural$ (that is, the monster group $\mathbb{M}$ has a group action on $V\natural$) [FLM88]. The pivotal property of $V\natural$ is the fact that it can be considered an infinite-dimensional, graded representation of $\mathbb{M}$. This is not a representation in the strict sense (it is infinite dimensional!); rather, $V\natural$ can be expressed as a direct sum of representations of the Monster, like so:

$$V\natural = \bigoplus_{n=-1}^{\infty} V_n,$$

where each $V_n$ is a finite representation of the Monster. The construction of $V\natural$ takes up much of a mathematical tome of 508 pages [FLM88], and will not explicitly be covered here. Suffice to say, the authors constructed $V\natural$ such that the respective dimensions of each $V_n$ correspond with the coefficients of the $j$-function's $q$-expansion. So this representation helps to shed light on the observation noted in the Introduction. Hence $V\natural$ was named the Moonshine Module, after Conway and Norton's famous conjecture that this representation helped to prove.

## 4.2 Once Conjecture, Now Theorem

The monstrous moonshine conjecture of Conway and Norton coalesced over the years since they first posed it, reflecting the new discoveries of various algebraic structures. Eventually the conjecture was transformed into something general enough and clear enough to prove. Here is the actual statement of the theorem which Borcherds proved in [Bor92]:

**Theorem 4.2.1.** *[Bor92] Let $V = V_\natural = \bigoplus_{n\in\mathbb{Z}}^{\infty} V_n$ be the Moonshine Module constructed by Frenkel, Lepowsky, and Meurman. Then, for any $g \in \mathbb{M}$, the McKay-Thompson series*

$$T_g(q) = \sum_{n=-1}^{\infty} tr(g|V_n)q^n$$

*is a hauptmodul for a genus 0 subgroup of $\mathrm{SL}_2(\mathbb{R})$.*

As mentioned in Chapter 3, a Hauptmodul is, in essence, an analogue to the $j$-function in that a Hauptmodul generates all modular functions for a particular modular subgroup $G$ of $SL_2(\mathbb{R})$. "Genus 0" describes the topological genus of the resulting surface when we take $\mathbb{H}$ and mod out by the action of our group $G$, then compactify. For example, with $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, then $\Gamma\backslash\mathbb{H}$ can be viewed as the Riemann sphere missing the point at infinity. For a visualization, look at the fundamental region $F$. The left-hand side is identified with the right-hand side, so "roll up" one side to the other, then tape the bottom edges together. This gives us the Riemann sphere missing infinity. So if we just add in the point at infinity, we get the Riemann sphere, which is a genus 0 topological space.

How does this theorem tie into the $j$-function, you ask? Well, if we let $g = 1$, the identity element of the Monster, then because each representation $V_n$ has dimension corresponding to the coefficients of the Fourier expansion of $j(\tau)$, we have that

$$T_1(q) = \frac{1}{q} + 196884q + 2149360q^2 + \cdots = j(\tau) - 744.$$

Of course, we can construct a Thompson series for every element $g \in \mathbb{M}$. Since $\mathbb{M}$ has 194 conjugacy classes, then Theorem 2.1.6 tells us that we can expect at most 194 Thompson-Mckay series $T_g$. In fact, there are only 171 distinct series [Gan04], and, by the moonshine theorem, every one is a Hauptmodul for some genus 0 subgroup of $\mathrm{SL}_2(\mathbb{R})$.

## 4.3 The Future

The discovery of this fascinating connection between $\mathbb{M}$ and modular functions has led to a wide range of related research. For instance, the question has been asked, "Are there any similar connections between other groups and modular functions?" In 1987, even before monstrous moonshine was actually proved, Conway and Norton synthesized a generalized moonshine conjecture which essentially explores similar connections while generalizing the characters with respect to $V_n$ (see [Car08]). As it is, this conjecture is still unproven, but many other relevant results have been proved along the way.

The exploration of moonshine has led to the creation and examination of various algebraic objects, including vector operator algebras, Kac-Moody algebras, genus 0 functions, and $V_\natural$ itself. Monstrous moonshine has even found purchase in the realm of physics, where it is used to explore something called conformal field theory, a particular quantum field theory on 2-dimensional space-time (see [Gan04] for a brief overview).

Though moonshine now delves ever deeper into strange, new algebraic objects, none of it would be possible without Jay and his monstrous friend.

# Bibliography


[Apo90] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*. Springer-Verlag New York, Inc., New York, NY, 1990.

[Arm] John Armstrong. Billiards 2. http://unapologetic.wordpress.com/2007/02/12/billiards-2/.

[BB87] J.M. Borwein and P.B. Borwein. *Pi & the AGM: A Study in Analytic Number Theory and Computational Complexity*. Wiley, New York, NY, 1987.

[Bor92] Richard Borcherds. Monstrous moonshine and monstrous lie superalgebras. *Invent. Math.*, 109:405–444, 1992.

[Car08] Scott Carnahan. Generalized moonshine i: Genus zero functions. *arXiv:0812.3440v2 [math.RT]*, 2008.

[CN79] J. H. Conway and S. P. Norton. Monstrous moonshine. *Bull. Lond. Math. Soc.*, 11:308–339, 1979.

[Cox89] David A. Cox. *Primes of the Form $x^2 + ny^2$*. John Wiley & Sons, Inc, Hoboken, NJ, 1989.

[FH91] William Fulton and Joe Harris. *Representation Theory: A First Course*. Springer-Verlag New York, Inc., New York, NY, 1991.

[FLM88] Igor Frenkel, James Lepowsky, and Arne Meurman. *Vertex Operator Algebras and the Monster*. Harcourt Brace Jovanovich, San Diego, CA, 1988.

[Gan04] Terry Gannon. Monstrous moonshine: The first twenty-five years. *arXiv:math/0402345v2 [math.QA]*, 2004.

[Ser73] Jean-Pierre Serre. *A Course in Arithmetic*. Springer-Verlag New York, Inc., New York, NY, 1973.

[Sol01] Ronald Solomon. A brief history of the classification of the finite simple groups. *Bulletin of the American Mathematical Society*, 38(3):315–352, 2001.