Modular Forms and Modular Congruences of the Partition Function

Shyam Narayanan

Advised by Professor Barry Mazur

Senior Thesis submitted in partial fulfillment for the honors requirements for the Bachelor of Arts degree in Mathematics

March 25, 2019

Contents

1 Introduction **4**
1.1 The Partition Function and Congruences 4
1.2 Modular Forms 5
1.3 This Thesis 5

2 An Introduction to the Theory of Modular Forms **7**
2.1 The Modular Group and Congruence Subgroups 7
2.2 The Fundamental Domain 8
2.3 Modular Forms over $SL_2(\mathbb{Z})$ 8
2.4 The Eisenstein Series 9
2.5 The Valence and Dimension Formulas 12
2.6 Modular Forms over Congruence Subgroups 13
2.7 The Hecke Operator 15
2.8 Half-Integral Weight Modular Forms 17

3 The Partition Function and The Ramanujan Congruences **19**
3.1 The Serre derivative 19
3.2 The Ramanujan Derivative Identities 21
3.3 The Ramanujan Congruences 22

4 Hecke Operators over $M_k(SL_2(\mathbb{Z}))$ and Another Family of Partition Function Congruences **25**
4.1 Preliminaries 25
4.2 Congruences of $F(\ell, k; z)$ modulo ℓ 28

4.3 The case $\ell = 13$ . . . 30
4.4 The case $\ell = 17$ . . . 30
4.5 The case $\ell = 19$ . . . 30
4.6 The case $\ell = 23$ . . . 31
4.7 The case $\ell = 29$ . . . 31
4.8 The case $\ell = 31$ . . . 31
4.9 Summary . . . 32

5 Background results on Modular Forms **33**
5.1 Computing Orders of Modular Forms . . . 33
5.2 Conversions of Modular Forms . . . 35
5.3 Eta Products and Modular Forms . . . 38
5.4 The Shimura Correspondence . . . 40
5.5 Half-integral Weight Hecke Operators over $\Gamma_1(N)$ . . . 41
5.6 Serre's Theorem on Hecke Operators . . . 41

6 General Modular Congruences for the Partition Function **42**
6.1 Proof of the General Modular Congruences . . . 42
6.2 Summary . . . 45

7 Computing Explicit Congruences **46**
7.1 Method to find Explicit Congruences . . . 46
7.2 Examples and Methods of Computation . . . 47

A Table of (ℓ, m) that Give Explicit Congruences **51**

Acknowledgements

First, I would like to thank my advisor, Professor Barry Mazur, for introducing me to the concept of modular forms and for all of his help throughout this thesis. I would also like to thank Professor Noam Elkies, Professor Ken Ono, Levent Alpoge, and Arnav Tripathy for answering some questions I had when writing my thesis, and William Chang for catching a few typos in my paper. I next wish to thank the inhabitants of the Harvard Math lounge, especially Patrick Guo, Davis Lazowski, Daniel Kim, and Ştefan Spătaru for their support and listening to all my complaints. Finally, I wish to thank my parents for all of their help and their encouragement of my pursuit of math.

1 Introduction

1.1 The Partition Function and Congruences

The integer partition function $p(n)$ equals the number of ways to write n as the sum of positive integers in nondecreasing order, with $p(0)$ defined to be 1. For instance, $p(5) = 7$ since 5 can be written as $5 = 5$, $5 = 1 + 4$, $5 = 2 + 3$, $5 = 1 + 2 + 2$, $5 = 1 + 1 + 3$, $5 = 1 + 1 + 1 + 2$, and $5 = 1+1+1+1+1$. Despite the simplicity of the partition function, no closed form expression for the partition function is known. However, there exists a known asymptotic formula

$$p(n) = \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right) \cdot (1 + o(1))$$

as $n \to \infty$, which was first proven by Hardy and Ramanujan.

Ramanujan also discovered that the partition function has surprising congruence patterns. For instance, he proved the following, now called the Ramanujan congruences [21]:

$$p(5n + 4) \equiv 0 \pmod 5 \tag{1}$$

$$p(7n + 5) \equiv 0 \pmod 7 \tag{2}$$

$$p(11n + 6) \equiv 0 \pmod{11}. \tag{3}$$

Ramanujan postulated that there are no equally simple congruences properties as the three listed above. This has now been proven, by which we mean that if ℓ is some prime, $0 \le \beta \le \ell - 1$ is some integer, and $p(\ell n + \beta) \equiv 0 \pmod{\ell}$ is true for all nonnegative integers n, then we must have (ℓ, β) equals either $(5, 4), (7, 5)$, or $(11, 6)$ [1]. However, this does not mean there are no other congruences of the partition function. Results of Watson [29] and Atkin [3] give us that if $24m \equiv 1 \pmod{5^a 7^b 11^c}$ for $a, b, c \ge 0$, then $p(m) \equiv 0 \pmod{5^a 7^{\lfloor (b+2)/2 \rfloor} 11^c}$. Moreover, there have been proven congruences modulo primes apart from $5, 7$, and 11, after results by authors including Atkin and O'Brien [4, 5], which proved results such as

$$p(11^3 \cdot 13n + 237) \equiv 0 \pmod{13}, \quad \text{and} \quad p(59^4 \cdot 13n + 111247) \equiv 0 \pmod{13}.$$

Yet, there was no general framework for proving these results, until papers by Ahlgren and Ono [18, 2] established that there exist congruences of the form $p(an+b) \equiv 0 \pmod m$ for all m relatively prime to 6. By this, we mean if $\gcd(6, m) = 1$, then there exist a, b such that $p(an+b) \equiv 0 \pmod m$ for all $n \ge 0$.

In addition to determining explicit congruences, people have studied the distribution and density of residues of $p(n)$ modulo primes m. For instance, Ono [18] proved that all primes $5 \le m \le 1000$,

$$\#\{0 \le n \le X : p(n) \equiv r \pmod m\} \gg_{r,m} \begin{cases} \sqrt{X}/\log X & 1 \le r \le m-1 \\ X & r = 0 \end{cases}.$$

What is remarkable about these results is that while the partition function is an inherently combinatorial object, these proofs have extensively required the theory of modular forms, which are certain classes of complex analytic functions. This strange relation between modular forms and the partition function is what motivates this thesis. In this thesis, we will investigate how the theory of modular forms can prove several astounding results about the partition function that do not have known purely combinatorial proofs.

1.2 Modular Forms

We will introduce the theory of modular forms in great detail in Section 2, so we just briefly define a modular form and explain some of their applications. A *modular form* is a holomorphic function on the upper half plane $\mathbb{H}$ that satisfies certain functional equations and boundedness conditions as we approach $i\infty$ or as we approach $\mathbb{Q}$ from certain directions. The simplest example of a modular form, which we will be dealing with significantly, is a modular form over $SL_2(\mathbb{Z})$, which is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ such that $|f(z)|$ is uniformly bounded in the region $\mathrm{Im}(z) > 1$ and

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

for all $z \in \mathbb{H}$ and all $a, b, c, d \in \mathbb{Z}$ such that $ad - bc = 1$.

Apart from studying the partition function, modular forms have been immensely useful in other areas. For instance, they have been used in determining congruences of other functions such as the Ramanujan tau function, which we will introduce (see [26] for examples of such congruences). In other areas of number theory, modular forms have proven useful in determining the number of ways to write an integer n as the sum of k squares [27], as well as in proving Fermat's Last Theorem [11]. Modular forms have also proven useful in understanding sphere packings, and were a key tool in the proofs that the famous E_8 lattice and Leech lattice provide optimal sphere packing in 8 and 24 dimensions, respectively [28, 10].

1.3 This Thesis

The goal of this thesis is to cover the background of modular forms and explain how they have been used to prove many strong results about partition function congruences. In section 2, we go over the background of modular forms, mainly focusing on modular forms over $SL_2(\mathbb{Z})$ but also introducing more general modular forms and half-integral weight modular forms. For the background, we will mainly follow the book Problems in the Theory of Modular Forms [15]. In our introduction, will skip certain sections and will often replace proofs with proof sketches for conciseness, but hope to provide sufficient intuition for how modular forms behave and why they are such a powerful tool. In section 3, we will give one proof of the Ramanujan congruences: i.e. Equations (1), (2), and (3). In section 4, we will show an additional family of congruences that can be proven using only the theory of modular forms over $SL_2(\mathbb{Z})$ as well as some computer-checkable computation, based on results of [18]. We note that in this section, we modify the methods of Ono [18] to give a more general framework of proof, which will allow us to straightforwardly extend the congruences Ono proves modulo $13, 17, 19$, and 23 to give similar congruences modulo 29 and 31.

In sections 5 and 6, we will reproduce the results of [2] to prove that for any integer m relatively prime to 6, there exists an infinite number of pairs $(a, b) \in \mathbb{N}^2$ such that $p(an + b) \equiv 0 \pmod{m}$ for all n. Section 6 will focus on the new ideas presented by Ahlgren and Ono in [2], whereas section 5 will focus on filling in details of [2] as well as either proving or stating many background results on general modular forms that Ahlgren and Ono use. While some of the background results will require more theory than we will be able to cover in this thesis, the way that Ahlgren and Ono use these strong results in modular forms to prove their families of partition functions is incredibly interesting. However, we note that Ahlgren and Ono's methods only give existence proofs of congruences but no explicit congruences. Therefore, we conclude with Section 7, in which we follow a paper of Weaver [30], which uses some of the methods of [2] as well as some other results to give several families of partition function congruences modulo primes $13 \leq m \leq 31$.

We finally describe the background one should have when reading this thesis. We do not assume any prior understanding of modular forms, but we assume prior knowledge of single variable complex analysis, such as knowledge of holomorphic and meromorphic functions, Taylor series, residue theorem, contour integration, and sum and product expansions of trigonometric functions. In addition, we will assume basic knowledge of analytic number theory, such as the definition of a Dirichlet character (i.e. a map χ from $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$) as well as the definition of an L-function and its Euler product formula

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

We will also assume some basic knowledge about algebra and algebraic number theory, such as familiarity with group actions and actions of $SL_2(\mathbb{Z})$, as well as understanding the definitions of number fields, ring of integers of a number field, and degrees of cyclotomic fields over $\mathbb{Q}$. We finally assume some basic knowledge of algorithms and Big O and little o notation, as we will require some computational tools and efficient algorithms to aid us in verifying certain partition function identities.

While modular forms have a lot of connections to geometry, we do not assume any background in algebraic geometry, and focus on the more analytic and combinatorial aspects of modular forms. For those interested in a more geometric approach to modular forms, we recommend [12] as an introductory book.

2 An Introduction to the Theory of Modular Forms

In this section we provide an exposition of the basic theory of modular forms, as well as provide motivation for how modular forms can be immensely useful in proving certain arithmetic identities. This section loosely follows [15], although we will skip some results and proofs, but include sketches of those related to arithmetic identities that demonstrate the power of modular forms. We end by briefly discussing half-integral weight modular forms, which are described in more detail in [24, 23].

2.1 The Modular Group and Congruence Subgroups

For some ring R, let $SL_2(R)$ be the group of 2×2 matrices with coefficients in R and determinant 1, and let $GL_2(R)$ be the group of invertible 2×2 matrices. Moreover, define the upper half plane $\mathbb{H}$ to be

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

It turns out that $GL_2(\mathbb{R})$ (and consequently, $SL_2(\mathbb{R})$ and $SL_2(\mathbb{Z})$) has a natural group action on the upper half plane $\mathbb{H}$. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{R})$, then γ acts on the upper half plane via the *Mobius transformation*:

$$\gamma z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} z := \frac{az+b}{cz+d} \in \mathbb{H}.$$

It is straightforward to verify that this indeed forms a group action, and this fact will be crucial in defining modular forms. We also note that the negative of the identity matrix, $-I$, performs a trivial action on $\mathbb{H}$. Therefore, it is sometimes natural to consider the group actions of $PSL_2(\mathbb{R}) = SL_2(\mathbb{R})/\{\pm I\}$ and $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$. The latter is often called the *modular group.*

We have the following well-known but important result about $SL_2(\mathbb{Z})$:

Theorem 2.1. *[15, Theorem 2.1.2] The group $SL_2(\mathbb{Z})$ is generated by the two matrices S and T, where*

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{4}$$

Modular forms are holomorphic functions on $\mathbb{H}$ which satisfy a certain functional equation with respect to a chosen discrete subgroup of $SL_2(\mathbb{R})$. For the purpose of this exposition, we will only look at the discrete subgroups $SL_2(\mathbb{Z})$ as well as certain types of *congruence subgroups.* These are finite index subgroups of $SL_2(\mathbb{Z})$, often represented by Γ, such that there exists some positive integer N such that $\ker(\phi_N) \subset \Gamma$ for $\phi_N : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ being the obvious map of reducing each element of the matrix modulo N. The most important congruence subgroups are

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : a, d \equiv 1 \pmod{N}, b, c \equiv 0 \pmod{N} \right\} = ker(\phi_N),$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : a, d \equiv 1 \pmod{N}, c \equiv 0 \pmod{N} \right\},$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

We remark that $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z})$, as well as that a congruence subgroup is any subgroup that contains $\Gamma(N)$ for some N. The *level* of a congruence subgroup Γ is defined as the smallest N such that $\Gamma(N) \subset \Gamma$. Thus, one can verify that $\Gamma_1(N)$ and $\Gamma_0(N)$ are both of level N.

2.2 The Fundamental Domain

If Γ is a discrete subgroup of $SL_2(\mathbb{R})$, we say that two points $z, z' \in \mathbb{H}$ are Γ-*equivalent* if $\gamma z = z'$ for some $\gamma \in \Gamma$. This definition allows us to define a *fundamental domain.* A closed set $\mathcal{F} \subset \mathbb{H}$ is called a *fundamental domain* for Γ if

1. $\mathcal{F}$ has connected interior.
2. Any $z \in \mathbb{H}$ is Γ-equivalent to some point in $\mathcal{F}$.
3. No two interior points in $\mathcal{F}$ are Γ-equivalent.
4. The boundary of $\mathcal{F}$ is piecewise smooth.

It turns out that $SL_2(\mathbb{Z})$ has a fundamental domain (in fact, several fundamental domains), but we will describe the *standard fundamental domain*:

Theorem 2.2. *[15, Theorem 3.2.2] The set*

$$\mathcal{F} = \left\{ z \in \mathbb{H} : |Re(z)| \leq \frac{1}{2}, |z| \geq 1 \right\}$$

is a fundamental domain for $SL_2(\mathbb{Z})$, and is often referred to as the standard fundamental domain.

We remark that if $\mathcal{F}$ is a fundamental domain for some discrete subgroup $\Gamma \subset SL_2(\mathbb{R})$, then $\gamma\mathcal{F}$ is also a fundamental domain for Γ for any $\gamma \in \Gamma$.

In addition, we remark that congruence subgroups of $SL_2(\mathbb{Z})$ often have fundamental domains as well. If we let $\mathcal{F}$ be the standard fundamental domain, then if $g_1, ..., g_r$ are right coset representatives and Γ is a congruence subgroup that contains the matrix $-I$, then $\mathcal{D} = \bigcup_{i=1}^{r} g_i\mathcal{F}$ is known to be a fundamental domain for Γ, assuming $\mathcal{D}$ has connected interior. As an example, one can verify that I, S, and ST are right coset representatives for $\Gamma_0(2) \subset SL_2(\mathbb{Z})$, and that $\mathcal{D} = \mathcal{F} \cup S\mathcal{F} \cup ST\mathcal{F}$ has a connected interior for S, T as defined in (4). Therefore, $\mathcal{D}$ is a fundamental domain for $SL_2(\Gamma_0(2))$.

Finally, we define a *cusp* of a congruence subgroup Γ as any point that is $SL_2(\mathbb{Z})$-equivalent to $i\infty$: namely the cusps are $i\infty$ and $\mathbb{Q}$. For a discrete subgroup Γ, two cusps α, α' are Γ-equivalent if $\Gamma\alpha = \alpha'$ for some $\gamma \in \Gamma$. It is clear that $i\infty$ and all rational numbers are $SL_2(\mathbb{Z})$-equivalent, but for congruence subgroups $\Gamma \subset SL_2(\mathbb{Z})$, the number of equivalence classes of cusps equals $[SL_2(\mathbb{Z}) : \Gamma]$.

2.3 Modular Forms over $SL_2(\mathbb{Z})$

We now are able to define a modular form over $SL_2(\mathbb{Z})$.

Definition 2.3. A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is a *modular form of weight k* if for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$,

$$f(\gamma z) := f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \tag{5}$$

and if $f(z)$ is uniformly bounded in the region $\mathrm{Im}(z) > 1$. The condition in (5) is often called the *modularity condition.*

We note that since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, we must have that $f(z+1) = f(z)$ which means that $f(z)$ is a holomorphic function on $q := e^{2\pi i z}$ for $z \in \mathbb{H}$, i.e. $f(z) = g(q)$ for g a holomorphic function on the punctured unit disk. However, since since $f(z)$ is uniformly bounded in the region $\mathrm{Im}(z) > 1$, we must have that $g(q)$ has a removable singularity around 0. Therefore, $f(z)$ must equal its Taylor series over $q = e^{2\pi i z}$ around $q = 0$. This gives us what is called a *q-series expansion* for f:

$$f = \sum_{n=0}^{\infty} a(n) e^{2\pi i n z} = \sum_{n=0}^{\infty} a(n) q^n. \tag{6}$$

As a result, we often say that f is *holomorphic at $i\infty$* if f is uniformly bounded in the $\mathrm{Im}(z) > 1$, as we can extend the q series to $q = 0$. Using our q-series expansion, we can define a *cusp form f* of weight k to be a modular form such that $a(0) = 0$, i.e. $\lim_{z \to i\infty} f(z) = 0$. We can thus define the following vector spaces of modular forms and cusp forms.

Definition 2.4. For $k \in \mathbb{Z}$, define $M_k(SL_2(\mathbb{Z}))$ to be the set of all modular forms of weight k over $SL_2(\mathbb{Z})$. Also, define $S_k(SL_2(\mathbb{Z}))$ to be the set of all cusp forms of weight k over $SL_2(\mathbb{Z})$.

It is straightforward to verify that $M_k(SL_2(\mathbb{Z}))$ and $S_k(SL_2(\mathbb{Z}))$ are $\mathbb{C}$-vector spaces. Moreover, we can also multiply modular forms, though the weights of the modular forms will add. Namely, if $f \in M_{k_1}(SL_2(\mathbb{Z}))$ and $g \in M_{k_1}(SL_2(\mathbb{Z}))$, it is easy to see that $fg \in M_{k_1+k_2}(SL_2(\mathbb{Z}))$. Moreover, if either f or g is a cusp form, then fg is also. All of these claims are part of [15, Exercise 4.1.5].

We also note that $M_k(SL_2(\mathbb{Z})) = S_k(SL_2(\mathbb{Z})) = \{0\}$ if k is odd. This is because the additive inverse of the identity matrix, $-I = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ means that by Equation (5), if f is a modular form of weight k, then $f(z) = f\left(\frac{-z}{-1}\right) = f(z) \cdot (-1)^k$, so either k is even or $f(z) = 0$ uniformly.

We will now define the *slash operator* for any function from $\mathbb{H}$ to $\mathbb{C}$, which is a very useful concept for modular forms.

Definition 2.5. Given any function $f : \mathbb{H} \to \mathbb{C}$ and some $\gamma \in GL_2(\mathbb{R})^+$ (i.e. γ is an invertible 2×2 real-valued matrix with positive determinant), we define the *slash operator* $f|_k\gamma$ to be the function

$$(f|_k\gamma)(z) = (\det \gamma)^{k/2}(cz+d)^{-k} f(\gamma z) \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

When the value of k equals the weight of the modular form, we drop the subscript on the slash.

Note that the modularity condition, i.e. Equation (5), is equivalent to $(f|\gamma)(z) = f(z)$ for all $\gamma \in SL_2(\mathbb{Z})$. Moreover, one can verify that the slash operator commutes [15, Exercise 4.1.3]; namely, if $\gamma_1, \gamma_2 \in GL_2(\mathbb{R})$, then $f|(\gamma_1\gamma_2) = (f|\gamma_1)|\gamma_2$. This means that since S, T defined in Theorem 2.1 generate $SL_2(\mathbb{Z})$, to verify the modular condition for some f, it suffices to show that $f|S = f|T = f$. In other words, we just need to verify that

$$f\left(-\frac{1}{z}\right) = z^k \cdot f(z) \text{ and } f(z+1) = f(z).$$

2.4 The Eisenstein Series

The Eisenstein series is a method of constructing modular forms of weight k for $k \geq 4$, k even. For $k \in \mathbb{N}, k > 2$, define

$$G_k(z) := \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(mz+n)^k} \tag{7}$$

for $z \in \mathbb{H}$. One can verify that this series converges absolutely and uniformly in some region bounded away from the real line as long as $k \geq 3$. The general idea to show that there are at most cn^2r^2 values of (m,n) such that $|mz+n| \leq r$, where c is a constant that may depend on z but is uniformly bounded in a region bounded away from the real line. See [15, Exercise 4.2.1] for more details. As a result, we have that $G_k(z)$ is a holomorphic function for $k \geq 3$, though if k is odd, we have $\frac{1}{(mz+n)^k} = -\frac{1}{(-mz+-n)^k}$, so $G_k(z) = 0$ for k odd. However, we have that $G_k(z)$ is a modular form of weight k for all even k. To verify the modular condition, note that

$$G_k(z+1) = \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(m(z+1)+n)^k} = \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(mz+(m+n))^k} = \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^k} = G_k(z),$$

and

$$G_k\left(\frac{1}{z}\right) = \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{1}{((m/z)+n)^k} = \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)\neq(0,0)}} \frac{z^k}{(m+nz)^k} = z^k G_k(z).$$

While the above is true for all $k \geq 3$, the fact that G_k is a modular form is uninteresting for odd k.

We will not fully prove $G_k(z)$ is holomorphic at $i\infty$, but it follows from the following theorem:

Theorem 2.6. *[15, Theorem 4.2.3] For any even $k \geq 4$,*

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

where $q = e^{2\pi i z}$, ζ represents the Riemann Zeta function, and $\sigma_s(n) = \sum_{d|n} d^s$.

To give some motivation for proving the above result, the way one can prove Theorem 2.6 is to first note that if we restrict to the case $m = 0$ in Equation (7), $\sum_{n\neq 0} \frac{1}{n^k} = 2\zeta(k)$, assuming k is even. Then, one can use the sum formula for cotangent,

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z+n} + \frac{1}{z-n} \right) \tag{8}$$

by successively differentiating (8) while writing $\cot(\pi z) = i\pi \frac{e^{2\pi i z}+1}{e^{2\pi i z}-1}$ to evaluate the sum in (7) for any fixed $m \neq 0$. Full details are provided in the proofs of Theorems 4.2.2 and 4.3.3 in [15].

The Eisenstein series E_k is simply a scaled version of G_k to force the first coefficient in the q-expansion to be 1. To more easily write out the series, we use the *Bernoulli numbers*:

Definition 2.7. Define the Bernoulli numbers B_k by the power series

$$\frac{x}{e^x - 1} =: \sum_{k=0}^{\infty} \frac{B_k x^k}{k!}, \tag{9}$$

which is a holomorphic function in a region around 0.

One can explicitly compute the values of the Bernoulli numbers. Also, by writing $\pi \cot(\pi z)$ in terms of $e^{2\pi i z}$, comparing (9) after dividing both sides by x to (8), and successively differentiating (8) in some region around $z = 0$, one can obtain the following:

Proposition 2.8. *[15, Exercise 4.2.4] For all even $k \geq 2$, we have*

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

Therefore, by dividing $G_k(z)$ by $2\zeta(k)$, we have that for all even k, we have the weight k modular form

$$E_k(z) := \frac{G_k(z)}{2\zeta(k)} = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n. \tag{10}$$

For examples of q-series for E_k, [15, Page 40] lists the expansions for $E_4, E_6, E_8, E_{10}, E_{12}$, and E_{14}.

In the next subsection, we will note some fascinating results, such as $E_4^2 = E_8$ and $E_4E_8 = E_{10}$. However, by computing the first few terms of E_4 and E_6, we get $\frac{1}{1728}\cdot(E_4^3 - E_6^2) = q - 24q^2 + 252q^3 + ...$ This function is called the Δ function, its q-series coefficients are referred to as the τ function. Namely, we have

$$\Delta(z) := \frac{1}{1728}\cdot(E_4^3 - E_6^2) =: \sum_{n=1}^{\infty}\tau(n)q^n.$$

The Δ function is clearly a cusp form of weight 12, and as we will see in Section 3, has some very interesting relations to the partition function, which is one of several reasons why the Δ function and the τ function have been extensively studied.

Finally, although $G_k(z)$ does not converge absolutely for $k = 2$, there still exists a series $G_2(z)$ and a corresponding Eisenstein series $E_2(z)$. If we define

$$G_2(z) := \sum_{m=-\infty}^{\infty}\left(\sum_{\substack{n=-\infty \\ n\neq 0 \text{ if } m=0}}^{\infty}\frac{1}{(mz+n)^2}\right),$$

it can be shown that $G_2(z)$ converges and defines a holomorphic function, and for the same reason as for the higher G_k's, we will have

$$G_2(z) = 2\zeta(2) + \frac{2(-2\pi i)^2}{1!}\sum_{n=1}^{\infty}\sigma_1(n)q^n = \frac{\pi^2}{3} - 8\pi^2\sum_{n=1}^{\infty}\sigma_1(n)q^n.$$

Moreover, $G_2(z)$ will be an example of a "quasi-modular form" (see [15, Theorem 5.1.1]), meaning

$$G_2(z+1) = G_2(z), \;\; G_2\left(-\frac{1}{z}\right) = z^2G_2(z) - 2\pi iz. \tag{11}$$

Thus, by scaling G_2 by dividing by $2\zeta(2)$, we get the Eisenstein series E_2, which has the q-expansion

$$E_2(z) = 1 - \frac{4}{B_2}\sum_{n=1}^{\infty}\sigma_1(n)q^n = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n,$$

and by (11), satisfies

$$E_2(z+1) = E_2(z), \;\; E_2\left(-\frac{1}{z}\right) = z^2E_2(z) + \frac{6}{i\pi}z. \tag{12}$$

2.5 The Valence and Dimension Formulas

The valence formula gives us information about zeroes of a modular form and their orders, which can be used to determine the dimension of modular forms of weight k for all k. Given a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ that is not identically 0, recall that the *order* of f at some $z_0 \in \mathbb{H}$ is the largest integer n such that $f(z) \cdot (z - z_0)^{-n}$ is holomorphic in a neighborhood of z_0. We note that for a modular form f, the order of f at z_0 equals the order of f at γz_0, due to our modular condition and the fact that $cz_0 + d \neq 0$ if $z_0 \in \mathbb{H}$. If f has a Laurent series in $q = e^{2\pi iz}$ around $q = 0$, we define the order of f at $i\infty$ to be the largest n such that $f(z) \cdot q^{-n}$ is holomorphic around $q = 0$. We also define the order of f for any cusp $\alpha \in \mathbb{Q}$ as the order at $i\infty$ of the function $(f|\gamma)$, where $\gamma \in SL_2(\mathbb{Z})$ maps $i\infty$ to α. The order at α is well defined because $f(z+1)$ and $f(z)$ have the same order at $i\infty$ and because if $\gamma, \gamma' \in SL_2(\mathbb{Z})$ map $i\infty \mapsto \alpha$, then $\gamma = \pm\gamma' \cdot T^n$ for some n, where T is the Mobius transformation $z \mapsto z + 1$. We define $\text{ord}_z(f)$ to be the order of f for any $z \in \mathbb{H} \cup \mathbb{Q} \cup \{i\infty\}$.

Recall that $\mathcal{F}$, the standard fundamental domain of $SL_2(\mathbb{Z})$, is the closure of the set $\{z \in \mathbb{H} : |z| > 1, |\Re(z)| < \frac{1}{2}\}$. We will now state the valence formula:

Theorem 2.9. *[15, 4.3.1] Let f be a modular form in $M_k(SL_2(\mathbb{Z}))$, not identically 0. Then,*

$$ord_{i\infty}(f) + \frac{1}{2}ord_i + \frac{1}{3}ord_\rho(f) + \sum_{\substack{z\neq i,\rho \\ z\in\mathcal{F}'}} ord_z(f) = \frac{k}{12}.$$

Here, $\rho = e^{2\pi i/3}$ and $\mathcal{F}'$ equals $\mathcal{F}$, excluding all points in the boundary of $\mathcal{F}$ with negative real part.

While the full proof of the valence formula is tedious, we give a short outline of the main ideas. First, assume there are no zeroes along $\partial\mathcal{F}$, the boundary of $\mathcal{F}$, although there could be a zero at $i\infty$. We contour integrate $\frac{f'}{f}$ along $\mathcal{F} \cap \{\text{Im}(z) < N\}$ for some large N. The integral of $\frac{f'}{f}$ along $\partial\mathcal{F} \cap \{\Re(z) = \frac{1}{2}\}$ and $\partial\mathcal{F} \cap \{\Re(z) = -\frac{1}{2}\}$ will cancel out due to the orientation and since $\frac{f'(z+1)}{f(z+1)} = \frac{f'(z)}{f(z)}$. However, since $f(-1/z) = z^k \cdot f(z)$, the integral along $\partial\mathcal{F} \cap \{|z| = 1\} \cap \{\Re(z) > 0\}$ and $\partial\mathcal{F} \cap \{|z| = 1\} \cap \{\Re(z) < 0\}$ will not fully cancel out, but will equal $2\pi i \cdot \frac{k}{12}$. Assuming N is large enough so that there is no zero in $\mathcal{F} \cap \{Im(z) \geq N\}$, the integral along the top boundary $\{\text{Im}(z) = N, -\frac{1}{2} \leq \Re(z) \leq \frac{1}{2}\}$ will equal $2\pi i \cdot \text{ord}_{i\infty}(f)$. One can prove this by substituting $q = e^{2\pi iz}$ in the integral and applying the residue theorem over the variable q on a circle of radius $e^{-2\pi N}$.

To tackle the cases where there can be zeroes on $\partial\mathcal{F}$, we will have to slightly perturb our contour to avoid integrating over any poles of $\frac{f'}{f}$. However, since these points are shared between $\mathcal{F}$ and $\gamma\mathcal{F}$ for certain choices of $\gamma \in SL_2(\mathbb{Z})$, we will have to account for the "proportion" of the order that goes into our contour. We have this strange $\mathcal{F}'$ because for any $z \in \partial\mathcal{F}$ with real part $\frac{1}{2}$, $\text{ord}_f(z) = \text{ord}_f(z - 1)$, and for any $z \in \mathcal{F}$ with $|z| = 1$, $\text{ord}_f(z) = \text{ord}_f(-1/z)$.

Using the valence formula, we can also develop the dimension formula that gives us the dimension of $M_k(SL_2(\mathbb{Z}))$ and $S_k(SL_2(\mathbb{Z}))$ for all even integers k (we know the dimension is 0 for odd integers). Specifically, we will sketch a proof of the following:

Theorem 2.10. *[15, Corollary 4.4.2] For even $k \geq 0$,*

$$\dim M_k(SL_2(\mathbb{Z})) = \begin{cases} \lfloor \frac{k}{12} \rfloor & k \equiv 2 \pmod{12} \\ \lfloor \frac{k}{12} \rfloor + 1 & k \not\equiv 2 \pmod{12} \end{cases}.$$

Moreover, if $k < 0$, $\dim M_k(SL_2(\mathbb{Z})) = 0$, and $\dim S_k(SL_2(\mathbb{Z})) = \dim M_k(SL_2(\mathbb{Z})) - 1$ whenever $\dim M_k(SL_2(\mathbb{Z})) \geq 1$.

Proof Sketch. For $k < 0$, we cannot have any nonzero modular forms, due to Theorem 2.9 and the fact that f is holomorphic on $\mathbb{H}$ and is holomorphic at $i\infty$ means the order at all z must be nonnegative. We also cannot have $k = 2$ as there is no way to sum nonnegative multiples of $1, \frac{1}{2}$, and $\frac{1}{3}$ to get $\frac{1}{6}$. For $k = 0$, we know any constant is a modular form, but if there were a nonconstant modular form f, we can look at $f - c$ for some constant c to force a zero in the interior of $\mathcal{F}$, which will be a weight 0 modular form, contradicting Theorem 2.9. We can do similar things to show the dimension of $M_k(SL_2(\mathbb{Z}))$ for $k \in \{4, 6, 8, 10, 14\}$ is 1. We note there exists an Eisenstein series E_k, but if there existed some $f \in M_k(SL_2(\mathbb{Z}))$, then $f - cE_k$ for some c must have a root in the interior of $\mathcal{F}$, which will establish a contradiction with Theorem 2.9.

We next show for all nonnegative even k, $\dim S_{k+12}(SL_2(\mathbb{Z})) = \dim M_k(SL_2(\mathbb{Z}))$. First, note that we have an injective map $M_k(SL_2(\mathbb{Z})) \to S_{k+12}(SL_2(\mathbb{Z}))$ by multiplying with $\Delta(z)$, which is a weight 12 cusp form. However, Δ has no zeroes in $\mathcal{F}$ by Theorem 2.9 and as Δ has a zero at $i\infty$, so Δ has no zeroes in $\mathbb{H}$. Therefore, the map $M_k(SL_2(\mathbb{Z})) \to S_{k+12}(SL_2(\mathbb{Z}))$ is invertible, since we can just divide by Δ and do not have to worry about inducing any poles in $\mathbb{H}$ or at $i\infty$.

Finally, we must show $\dim M_k(SL_2(\mathbb{Z})) = \dim S_k(SL_2(\mathbb{Z})) + 1$ whenever $\dim M_k(SL_2(\mathbb{Z})) \geq 1$. This is true since there exists E_k which is a modular form that converges to 1 at $i\infty$, so $\dim M_k(SL_2(\mathbb{Z})) > \dim S_k(SL_2(\mathbb{Z}))$, but if $\dim M_k(SL_2(\mathbb{Z})) \geq \dim S_k(SL_2(\mathbb{Z})) + 2$, there must be two linearly independent modular forms in $M_k(SL_2(\mathbb{Z}))$ that cannot be combined to form a cusp form, which is clearly impossible. Combined, the above results prove our theorem. □

The dimension bound of modular forms is a crucial aspect of proving number theoretic identities. A general strategy for proving certain identities is to establish a certain q-series is a modular form, and then by finite dimensionality, show it must precisely equal some other modular form. For instance, note that $M_8(SL_2(\mathbb{Z}))$ and $M_{10}(SL_2(\mathbb{Z}))$ are 1-dimensional, which means that $E_4^2 = E_8$ and $E_4E_6 = E_{10}$, since E_4^2, E_4E_6 are nonzero modular forms with leading q^0-coefficient equal to 1. Using the q-series expansion of Eisenstein series (Equation (10)) and the fact that $B_4 = B_8 = -\frac{1}{30}$, $E_4^2 = E_8$ implies

$$\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^2 = 1 + 480\sum_{n=1}^{\infty}\sigma_7(n)q^n.$$

Thus, by evaluating the q^n-coefficient of both sides and dividing by 480, we get the following very strange result:

$$\sigma_7(n) = \sigma_3(n) + 120\sum_{m=1}^{n-1}\sigma_3(m)\sigma_3(n-m).$$

Such a result is astounding, as we used very little combinatorics or number theory, but predominantly complex analysis! This result, however, is just an introduction to the power that modular forms brings in proving combinatorial and number theoretic identities.

2.6 Modular Forms over Congruence Subgroups

Previously, we had been dealing exclusively with modular forms over $SL_2(\mathbb{Z})$. However, it is often useful to deal with modular forms over some congruence subgroup $\Gamma \subset SL_2(\mathbb{Z})$.

Definition 2.11. A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is a *modular form of weight k over* $\Gamma \subset$

$SL_2(\mathbb{Z})$ if for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$,

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

and if $f(z)$ is holomorphic all cusps, meaning for any $\gamma' \in SL_2(\mathbb{Z})$, $f|\gamma'$ is uniformly bounded in the region $\text{Im}(z) > 1$. We define $M_k(\Gamma)$ to be the set of weight k modular forms over Γ. Likewise, if $f|\gamma'$ vanishes at all cusps, i.e. $f|\gamma'$ converges to 0 as $\text{Im}(z) \to \infty$, then the we say f is a *cusp form of weight k over $\Gamma \subset SL_2(\mathbb{Z})$*. We define $S_k(\Gamma)$ to be the set of weight k cusp forms over Γ.

Note that in our definition of modular forms over $SL_2(\mathbb{Z})$, we did not force $f|\gamma$ to also be bounded towards $i\infty$, for all γ, because $f|\gamma = f$ for all γ. However, in this case, since we can have several orbits of Γ over $\mathbb{Q} \cup \{i\infty\}$, we need this additional condition.

Since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1(N)$, we have any modular form $f(z)$ over $\Gamma_1(N)$ just satisfy $f(z) = f(z+1)$, and therefore must have a q-series over f. For some more general congruence group $\Gamma(N) \subset \Gamma \subset SL_2(\mathbb{Z})$, we can still get a q-series, though perhaps with fractional coefficients. Let h be the smallest positive integer such that either $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$ or $\left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right) \in \Gamma$. (Note that if $-I$ is not in Γ, it is possible for one of these matrices to exist but not the other). Moreover, since $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma(N) \subset \Gamma$, we must have $h|N$. Then, $f(z) = f(z+h)$, which means that since f is holomorphic at $i\infty$, we must have that $f(z) = \sum_{n \geq 0} a(n) q^n$, where now $q = e^{2\pi i z/h}$.

Using the above q-series expansion, we define $\text{ord}_{i\infty}(f)$, the order of f at $i\infty$, to be $\frac{n}{h}$, where n is the smallest integer such that $a(n) \neq 0$. We can similarly define for any $\alpha \in \mathbb{Q}$, $\text{ord}_\alpha(f) := \text{ord}_{i\infty}(f|\gamma)$ for $\gamma \in SL_2(\mathbb{Z})$ sending $i\infty$ to α. We note that for any $\gamma' \in SL_2(\mathbb{Z}), \gamma \in \Gamma$, $(f|\gamma')|(\gamma'^{-1}\gamma\gamma') = (f|\gamma)|\gamma' = f|\gamma'$, which means that if $f \in M_k(\Gamma)$, then $f|\gamma \in M_k(\gamma'^{-1}\Gamma\gamma')$ and if $f \in S_k(\Gamma)$, then $f|\gamma \in S_k(\gamma'^{-1}\Gamma\gamma')$. Noting that $\Gamma(N)$ is a normal subgroup of $SL_2(\mathbb{Z})$, we have that if f is a modular form over $\Gamma \supset \Gamma(N)$, then so if $f|\gamma$, which means $\text{ord}_\alpha(f)$ is always a multiple of $\frac{1}{N}$.

Given our definition of modular forms over congruence subgroups, we also can define for any congruence subgroup the following vector space.

Definition 2.12. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. Then, define $M_k(\Gamma_0(N), \chi)$ to be the vector space of functions f such that for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, $f|\gamma = \chi(d) \cdot f$. We call this vector space the space of weight k modular forms over $\Gamma_0(N)$ with *Nebentypus character* χ.

First, note that since $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \Gamma_0(N)$, we must have that $f(z) = f(z) \cdot \chi(-1) \cdot (-1)^k$ for all $f \in M_k(\Gamma_0(N), \chi)$. Therefore, if $M_k(\Gamma_0(N), \chi)$ contains more than just the 0 function, χ is even, i.e. $\chi(-1) = 1$, if k is even and χ is odd, i.e. $\chi(-1) = -1$, if k is odd.

It is clear that if χ is the trivial character, then $M_k(\Gamma_0(N), \chi) = M_k(\Gamma_0(N))$. Moreover, since $\chi(d) = 1$ if $d \equiv 1 \pmod{N}$, we have $M_k(\Gamma_0(N), \chi) \subset M_k(\Gamma_1(N))$. In fact, we have the following:

Theorem 2.13. *[15, Theorem 8.2.5] We have the decomposition*

$$M_k(\Gamma_1(N)) = \bigoplus_\chi M_k(\Gamma_0(N), \chi).$$

Proof. First, we show any $f \in M_k(\Gamma_1(N))$ can be written as a sum $\frac{1}{\varphi(N)} \cdot \sum_\chi f_\chi$ for $f_\chi \in M_k(\Gamma_0(N), \chi)$. Let

$$f_\chi(z) = \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi^{-1}(d) \left(f \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right)(z)$$

for some choice a, b, c, d that forms a matrix in $\Gamma_0(N)$. We can always choose a, b, c, d by letting a be some multiplicative inverse of d mod N, $c = ad - 1$, and $b = 1$. Also, since $\Gamma_1(N)$ is a Normal subgroup of $\Gamma_0(N)$, the choice of a, b, c, d does not matter. Then, for any $\gamma = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma_0(N)$,

$$
\begin{aligned}
f_\chi(\gamma z) &= \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi^{-1}(d) f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} z\right)(c(\gamma z) + d)^{-k} \\
&= \chi(d') \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi^{-1}(dd') f\left(\begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} z\right) \frac{(c'z + d')^k}{((ca' + dc')z + (cb' + dd'))^k} \\
&= \chi(d') \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi^{-1}(d) f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} z\right)(cz + d)^{-k} \cdot (c'z + d')^k = f_\chi(z) \cdot (c'z + d')^k \chi(d').
\end{aligned}
$$

It is clear that $f(z) = \frac{1}{\varphi(N)} \sum_\chi f_\chi(z)$, where we sum over all Dirichlet characters. Moreover, $f_\chi(z)$ is holomorphic at all cusps, since $f|\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is holomorphic at all cusps.

To show we have a decomposition, we need to show our sum is unique. To show a function f cannot have two decompositions, by subtracting the decompositions it suffices to show that if $\sum_\chi f_\chi = 0$ for $f_\chi \in M_k(\Gamma_0(N), \chi)$ for each character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, then $f_\chi = 0$ for all χ. Note that if $\sum_\chi f_\chi = 0$, then $\sum_\chi f_\chi(\frac{az+b}{cz+d})(cz + d)^{-k} = 0$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. But $\sum_\chi f_\chi(\frac{az+b}{cz+d})(cz + d)^{-k} = \sum_\chi f_\chi(z) \cdot \chi(d)$, which means $\sum_\chi f_\chi(z) \cdot \chi(d) = 0$ for all $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. Thus, for any fixed character ψ,

$$
0 = \sum_d \psi^{-1}(d) \sum_\chi f_\chi(z)\chi(d) = \sum_\chi f_\chi(z) \sum_d \psi^{-1}(d)\chi(d) = \varphi(N) f_\psi(z),
$$

so we are done. □

Unlike the theory of modular forms over $SL_2(\mathbb{Z})$, the general theory of modular forms requires much more algebraic geometry, such as the Riemann-Roch theorem, as well as other theory that we will not develop. Therefore, for the purpose of this thesis, we will not prove some parts of this theory, in which case we will just state the important definitions and some results, either in the rest of this section or in Section 5. However, we will focus on how we can apply these results to prove theorems about congruences of the partition function, which is still very difficult, even if we cannot prove the results.

One example of a result that can be proven using the Riemann-Roch theorem is the corresponding valence and dimension formulas for any congruence subgroup $\Gamma \subset SL_2(\mathbb{Z})$. Even the statement will require understanding the geometry of the fundamental domain of Γ, and as we assume no knowledge of algebraic geometry, we will simply note that the dimension $\dim M_k(\Gamma)$ is finite for all integers k and congruence subgroups Γ. See [12, Sections 3.5-3.6] for a detailed proof.

2.7 The Hecke Operator

The Hecke operator is a key method that allows us to create new modular forms by modifying the q-series coefficients. While Hecke operators can be defined generally for all congruence subgroups, we will focus on Hecke operators over modular forms over $SL_2(\mathbb{Z})$ or $\Gamma_0(N)$ for some $N \in \mathbb{N}$.

Definition 2.14. Let m be a natural number. Then, define $\mathbf{X}_m$ to be the set of 2×2 matrices with integer coefficients with determinant m, and define $\mathbf{X}_m(N)$ to be the subset of $\mathbf{X}_m$ with bottom-left entry divisible by N.

Proposition 2.15. *The set of matrices of the form* $\left\{\left(\begin{smallmatrix} a & b \\ 0 & d\end{smallmatrix}\right) : ad = m, 0 \le b \le d-1\right\}$ *form cosets for left-multiplication of* $SL_2(\mathbb{Z})$ *on* $\boldsymbol{X}_m$. *In other words, every* $\alpha \in \boldsymbol{X}_m$ *can be uniquely written as* $\gamma \cdot \left(\begin{smallmatrix} a & b \\ 0 & d\end{smallmatrix}\right)$ *for some* $\gamma \in S_2(\mathbb{Z}), ad = m, 0 \le b \le d-1$. *The same set of matrices form cosets for left-multiplication of* $\Gamma_0(N)$ *on* $\boldsymbol{X}_m(N)$ *if* N, m *are relatively prime.*

Proof. We refer to [15, Theorem 5.2.1] where the case for $SL_2(\mathbb{Z})$ and $\mathbf{X}_m$ is proven, as it is quite computational. We show how one can use [15, Theorem 5.2.1] to deal with the case of $\Gamma_0(N)$ and $\mathbf{X}_m(N)$. Let $\alpha_1, ..., \alpha_r$ be the set of matrices $\left\{\left(\begin{smallmatrix} a & b \\ 0 & d\end{smallmatrix}\right) : ad = m, 0 \le b \le d-1\right\}$. Then, since $SL_2(\mathbb{Z})\alpha_i$ are disjoint, we also have $\Gamma_0(N)\alpha_i$ are disjoint. To show any element α in $\mathbf{X}_m(N)$ can be written as $\gamma\alpha_i$ for $\gamma \in \Gamma_0(N)$, we know from the first part that there is some $1 \le i \le r$ and $\gamma \in SL_2(\mathbb{Z})$ such that $\alpha = \gamma\alpha_i$. However, if we let $\gamma = \left(\begin{smallmatrix} a_1 & b_1 \\ c_1 & d_1\end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ and $\alpha_i = \left(\begin{smallmatrix} a & b \\ 0 & d\end{smallmatrix}\right)$, to have $\gamma\alpha_i \in \mathbf{X}_m(N)$ means the bottom-left entry of $\gamma\alpha_i$ must be a multiple of N. But this equals $c_1 a$, and since a, N are relatively prime, we must have $N|c_1$. Thus, $\alpha = \gamma\alpha_i$ for some i and some $\gamma \in \Gamma_0(N)$. □

Proposition 2.16. *Let* $\alpha_1, ..., \alpha_r$ *be the matrices* $\left\{\left(\begin{smallmatrix} a & b \\ 0 & d\end{smallmatrix}\right) : ad = m, 0 \le b \le d-1\right\}$. *Then, if* $f \in M_k(SL_2(\mathbb{Z}))$, $\sum_i (f|\alpha_i) \in M_k(SL_2(\mathbb{Z}))$ *and if* $f \in S_k(SL_2(\mathbb{Z}))$, $\sum_i (f|\alpha_i) \in S_k(SL_2(\mathbb{Z}))$. *Likewise, if* $f \in M_k(\Gamma_0(N), \chi)$, *then* $\sum_i \chi(d_i)^{-1}(f|\alpha_i) \in M_k(\Gamma_0(N), \chi)$, *and if* $f \in S_k(\Gamma_0(N), \chi)$, $\sum_i \chi(d_i)^{-1}(f|\alpha_i) \in S_k(\Gamma_0(N), \chi)$, *where* d_i *is the bottom-right entry of* α_i.

Proof Sketch. We sketch the more general case of $M_k(\Gamma_0(N), \chi)$ or $S_k(\Gamma_0(N), \chi)$. The case of $SL_2(\mathbb{Z})$ is done in [15, Theorem 5.2.2] and the general case is done in [15, Sections 8.1-8.2].

If f satisfies the modularity condition over $\Gamma_0(N)$, then $f|\gamma = f \cdot \chi(d)$ for any $\gamma \in \Gamma_0(N)$. Now, $\sum_i \chi(d_i)^{-1}(f|\alpha_i)|\gamma = \sum_i \chi(d_i)^{-1}(f|(\alpha_i\gamma))$. If $\Gamma_0(N)\alpha_i\gamma = \Gamma_0(N)\alpha_j\gamma$, then $\gamma'\alpha_i\gamma = \alpha_j\gamma$ for some $\gamma' \in \Gamma_0(N)$, which means α_i, α_j are in the same coset for left-multiplication by $\Gamma_0(N)$. Therefore, since $f|\gamma' = \chi(d')f$ for any $\gamma' \in \Gamma_0(N)$ and d' the bottom-right entry in γ', the set of functions $f|(\alpha_i\gamma)$ equals the set of functions $f|(\gamma_i'\alpha_i)$ for some $\gamma_i' \in \Gamma_0(N)$, so $\left(\sum_i \chi(d_i)^{-1}(f|\alpha_i)\right)|\gamma = \sum_i \chi(d_i)^{-1}(f|(\alpha_i\gamma)) = \sum_i \chi(d_i)^{-1} f|\alpha_i$. This verifies the modularity condition.

We have that

$$\sum_i f|\alpha_i = \sum_{ad=m, 0\le b\le d-1} f\left(\frac{az+b}{d}\right) \cdot m^{k/2} d^{-k}.$$

However, we note that $f\left(\frac{az+b}{d}\right)$ still being holomorphic or vanishing at all cusps follows from Corollary 5.4. While we are referencing a future section, we note that Proposition 5.1, Proposition 5.3, and Corollary 5.4, read in order, can be fully understood with the current background. □

We can now define the Hecke operator on modular forms using the above results.

Definition 2.17. The Hecke operator $T(m)$ is defined as follows. For $f \in M_k(SL_2(\mathbb{Z}))$ or $f \in M_k(\Gamma_0(N), \chi)$ with $\gcd(m, N) = 1$,

$$f|T(m) := m^{k/2-1} \sum_{ad=m, 0\le b\le d-1} \chi(a) \cdot f\Bigg|\begin{pmatrix} a & b \\ 0 & d\end{pmatrix} = \frac{1}{m} \sum_{ad=m, 0\le b\le d-1} \chi(a) \cdot a^k \cdot f\left(\frac{az+b}{d}\right).$$

If there is no Nebentypus character, we can drop the $\chi(d)$ term.

By Proposition 2.16, $T(m)$ is a map from $M_k(SL_2(\mathbb{Z}))$ to $M_k(SL_2(\mathbb{Z}))$ and from $S_k(SL_2(\mathbb{Z}))$ to $S_k(SL_2(\mathbb{Z}))$ (note that $\chi(a) = \chi(m) \cdot \chi(d)^{-1}$). We also have that if $\gcd(m, N) = 1$, $T(m)$ is a map from $M_k(\Gamma_0(N))$ to $M_k(\Gamma_0(N))$ and from $S_k(\Gamma_0(N))$ to $S_k(\Gamma_0(N))$.

As $f(\frac{az+b}{d})$ has a very simple q-expansion formula in terms of the q-expansion of f, it is quite easy to compute the q-series of $f|T(m)$ given the q-series of f. For $f(z) = \sum_{n\geq 0} \lambda(n)q^n$, it equals

$$f|T(m) = \sum_{n=0}^{\infty} \left(\sum_{a|\gcd(n,m)} \chi(a)a^{k-1}\lambda\left(\frac{mn}{a^2}\right) \right) q^n. \tag{13}$$

(See [15, Theorem 5.2.4] for proof in the case of forms in $M_k(SL_2(\mathbb{Z}))$ and [15, Exercise 8.2.6] for the general case). However, due to finite dimensionality of modular forms of fixed weight, we can express $f|T(m)$ as some linear combination of some known basis for the modular forms. As an example, since $S_{12}(SL_2(\mathbb{Z}))$ has dimension 1 and is spanned by Δ, we know that $\Delta|T(m) = c_m\Delta$ for some c_m. It turns out with this fact, and with Equation (13) to see how the Hecke operator acts on the q-series coefficients, one can show

$$\begin{aligned} \tau(mn) &= \tau(m)\tau(n) \text{ for } \gcd(m,n) = 1 \\ \tau(p^{a+1}) &= \tau(p)\tau(p^a) - p^{11}\tau(p^{a-1}) \text{ for } p \text{ prime}, a \in \mathbb{N}, \end{aligned}$$

where we recall that $\Delta(z) = \sum_{n\geq 1} \tau(n)q^n$ (see [15, Exercises 5.2.5-5.2.7]). We will, however, see several examples in Sections 4, 6, and 7 of how one can use Hecke operators to establish partition function congruences, and in Section 4 we will do so by explicitly establishing values of $f|T(m)$.

2.8 Half-Integral Weight Modular Forms

While we have been exclusively dealing with integral-weight modular forms, over the past 50 years, many results related to half-integral weight modular forms have arisen. The initial idea is to look at the classical theta function

$$\Theta(z) = \sum_{n\in\mathbb{Z}} e^{2\pi i n^2 z} = \sum_{n\in\mathbb{Z}} q^{n^2}.$$

It will turn out that Θ has the following transformation law that allows us to define it as a weight 1/2 modular form over $\Gamma_0(4)$. Let $\sqrt{z}$ for $z \in \mathbb{C}\backslash\{0\}$ be the branch of $\sqrt{z}$ with argument in the interval $(-\pi/2, \pi/2]$. Define ε_d to equal 1 if $d \equiv 1 \pmod 4$ and to equal i if $d \equiv 3 \pmod 4$. Finally, for d odd and $c \in \mathbb{Z}$, define the *Kronecker symbol* $\left(\frac{c}{d}\right)$ to equal the standard Jacobi symbol $\left(\frac{c}{|d|}\right)$ when at least one of c, d is nonnegative, and to equal $-\left(\frac{c}{|d|}\right)$ if both c, d are negative. Then, if we define

$$j(\gamma, z) := \begin{cases} \left(\frac{c}{d}\right)\varepsilon_d^{-1}\sqrt{cz+d} & c \neq 0 \\ 1 & c = 0 \end{cases}$$

with $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\left(\frac{c}{d}\right)$ representing the Kronecker symbol, it is known (see [24, 23]) that

$$\Theta(\gamma z) = j(\gamma, z)\Theta(z) \quad \forall \gamma \in \Gamma_0(4).$$

We now define a half-integral weight modular form as follows.

Definition 2.18. Let Γ be a congruence subgroup of level N. Moreover, let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. For k a nonnegative integer, a holomorphic function f on $\mathbb{H}$ is is in $M_{k+\frac{1}{2}}(\Gamma, \chi)$ if

$$f(\gamma z) = j(\gamma, z)^{2k+1} \cdot \chi(d) \cdot f(z) \quad \forall \gamma \in \Gamma$$

and f is holomorphic at all cusps, i.e. $f(\gamma z)/(cz+d)^{k+1/2}$ is holomorphic at $i\infty$ for all $\gamma \in SL_2(\mathbb{Z})$. If f vanishes at all cusps, then $f \in S_{k+\frac{1}{2}}(\Gamma, \chi)$. As in the integral weight case, if χ is the trivial character, we have the spaces $M_{k+\frac{1}{2}}(\Gamma)$ and $S_{k+\frac{1}{2}}(\Gamma)$, respectively.

Since Θ is a modular form in $M_{1/2}(\Gamma_0(4))$, we will usually require N to be a multiple of 4 for half-integral weight modular forms. For the purpose of this thesis, we will only be looking at half-integral weight modular forms over $\Gamma_0(N)$ and $\Gamma_1(N)$ for some $4|N$. We will not be delving much into the theory of half-integral weight modular forms, but will simply state some results needed about them later on and explain how they are valuable. For readers interested in learning about half-integral weight modular forms, we point to [7], which gives a good summary of [24, 23].

We will need to define Hecke operators on half-integral weight modular forms, though we will only need to look at the operator $T(p^2)$ for p prime on $S_{k+\frac{1}{2}}(\Gamma_0(N), \chi)$, for the case $p \nmid N$. We will later see a definition for the Hecke operator for $S_{k+\frac{1}{2}}(\Gamma_1(N))$, when $p \equiv -1 \pmod{N}$, and we will not need to deal with any other cases.

For any $f \in S_{k+\frac{1}{2}}(\Gamma_0(N), \chi) = \sum_{n \geq 1} a(n) q^n$, we define the Hecke operator $T_\chi(p^2)$ to satisfy

$$f|T_\chi(p^2) := \sum_{n=1}^{\infty} \left(a(p^2 n) + \chi(p) \left(\frac{(-1)^k n}{p} \right) p^{k-1} a(n) + \chi(p^2) p^{2k-1} a\left(\frac{n}{p^2} \right) \right) q^n, \tag{14}$$

where $a(n/p^2) := 0$ if $p^2 \nmid n$ [24, Theorem 1.7]. Like in the case of the integral weight modular form with Nebentypus character χ, we wish to sum $\chi(a) \cdot f|\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ for $ad = p^2, 0 \leq b \leq d-1$, though due to the weird sign issues when taking square roots and the functional equation of Θ, we will note that our Hecke operator will become (14).

3 The Partition Function and The Ramanujan Congruences

Recall that the partition function p is an arithmetic function such that $p(0) = 1$ and $p(n)$ for $n \in \mathbb{N}$ is the number of ways to represent n as the sum of at most n positive integers, where order does not matter. As a result, we can think of $p(n)$ as the number of ways to write $p(n) = a_1 \cdot 1 + a_2 \cdot 2 + a_3 \cdot 3 + \cdots$ for nonnegative integers $a_1, a_2, a_3, \ldots$ since all that matters is the number of times we have each integer in our sum. Therefore, we have the formal power series

$$\sum_{n=0}^{\infty} p(n) q^n = \prod_{i=1}^{\infty} \left(1 + q^i + q^{2i} + \cdots\right) = \prod_{i=1}^{\infty} \left(1 - q^i\right)^{-1}. \tag{15}$$

The right hand side of (15) can be seen to converge to a nonzero value for $|q| < 1$ by taking logarithms, so (15) is true for all $q = e^{2\pi i z}$, $z \in \mathbb{H}$. We also have the following theorem by Jacobi.

Theorem 3.1. *[15, Theorem 5.1.4] For $q = e^{2\pi i z}$, the cusp form $\Delta = \frac{1}{1728} \cdot \left(E_4^3 - E_6^2\right) \in S_{12}(SL_2(\mathbb{Z}))$ satisfies*

$$\Delta(z) = q \cdot \prod_{n=1}^{\infty} (1 - q^n)^{24} = q \cdot \left(\sum_{n=0}^{\infty} p(n) q^n\right)^{-24}. \tag{16}$$

This will allow us to define the following function.

Definition 3.2. Let $\eta(z)$ be the function such that $\eta^{24}(z) = \Delta(z)$. Specifically, we choose the root such that

$$\eta(z) = e^{i\pi z/12} \cdot \prod_{n=1}^{\infty} (1 - q^n) = e^{i\pi z/12} \cdot \left(\sum_{n=0}^{\infty} p(n) q^n\right)^{-1}.$$

The above results give a strong reason to suggest the theory of modular forms can be quite useful in understanding the partition function. In fact, many of the results that have been established on partition function congruences involve establishing that certain functions are modular forms and relating these functions to the partition function.

Our goal in this section is to prove three famous congruences proven by Ramanujan. Specifically, we will show that for all integers $n \geq 0$, we have

$$\begin{aligned} p(5n+4) &\equiv 0 \pmod{5} \\ p(7n+5) &\equiv 0 \pmod{7} \\ p(11n+6) &\equiv 0 \pmod{11}. \end{aligned}$$

There exist several known proofs of these congruences. We will show a proof of all three congruences which only requires the theory of modular forms over $SL_2(\mathbb{Z})$.

3.1 The Serre derivative

For a function $f(z)$ with q-series $\sum_{n \geq 0} a(n) q^n$ for $q = e^{2\pi i z}$, we define the D-operator and the Serre derivative as follows.

Definition 3.3. We define D as the differential operator such that

$$Df := q \cdot \frac{d}{dq} f = \sum_{n=0}^{\infty} na(n)q^n = \frac{1}{2\pi i}\frac{d}{dz} f.$$

Definition 3.4. For $f \in M_k(SL_2(\mathbb{Z}))$, we define the Serre derivative θ_k as

$$\theta_k(f) := Df - \frac{k}{12} E_2 f.$$

The Serre derivative is a useful operator for the following two reasons:

Proposition 3.5. *We have that θ_k is a linear operator and satisfies the product rule for modular forms $f \in M_k, g \in M_{k'}$.*

Proof. The fact that θ_k is linear is straightfoward to verify. To show the product rule, note that $fg \in M_{k+k'}(SL_2(\mathbb{Z}))$. Therefore,

$$\begin{aligned}
\theta_{k+k'}(fg) &= \frac{1}{2\pi i}\frac{d}{dz}(fg) - \frac{(k+k')}{12} E_2 \cdot (fg) \\
&= \frac{1}{2\pi i}\left(f\frac{d}{dz}g + g\frac{d}{dz}f\right) - \left(\frac{k}{12}E_2 f\right) g - \left(\frac{k'}{12}E_2 g\right) f \\
&= (\theta_k f)g + (\theta_{k'} g)f,
\end{aligned}$$

as desired. □

Proposition 3.6. *We have that θ_k maps $M_k(SL_2(\mathbb{Z})) \to M_{k+2}(SL_2(\mathbb{Z}))$ and $S_k(SL_2(\mathbb{Z})) \to S_{k+2}(SL_2(\mathbb{Z}))$.*

Proof. We know that $E_2(z)$ is holomorphic at $i\infty$, and we have that Df is holomorphic at $i\infty$ if f is, and Df vanishes at $i\infty$ if f does, by the q-series expansion of f. Therefore, we just need to verify the modular condition.

Let $f'(z)$ denote the derivative of f at z. Note that for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$,

$$f'(\gamma z) \cdot \frac{1}{(cz+d)^2} = \frac{d}{dz} f(\gamma z) = \frac{d}{dz}\Big((cz+d)^k \cdot f(z)\Big) = f'(z)(cz+d)^k + ckf(z)(cz+d)^{k-1}.$$

Therefore,

$$\frac{1}{2\pi i} f'(\gamma z) - \frac{k}{12}(E_2 f)(\gamma z) = \frac{1}{2\pi i}\Big(f'(z)(cz+d)^{k+2} + ckf(z)(cz+d)^{k+1}\Big) - \frac{k}{12}(E_2(\gamma z))f(z)(cz+d)^k.$$

For $\gamma = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\gamma z = z+1$, so we have $\theta_k f(z+1) = Df(z+1) - \frac{k}{12}E_2 f(z+1) = Df(z) - \frac{k}{12}E_2 f(z) = \theta_k f(z)$ by our q-series expansion. For $\gamma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, we have $\gamma z = -1/z$. Since $E_2(-1/z) = z^2 E_2(z) + \frac{6z}{\pi i}$, we have

$$\begin{aligned}
\theta_k f\left(-\frac{1}{z}\right) &= \frac{1}{2\pi i}\Big(f'(z)z^{k+2} + kf(z)z^{k+1}\Big) - \frac{k}{12}E_2(z)f(z)z^{k+2} - \frac{k}{12}f(z)z^{k+1} \cdot \frac{6}{\pi i} \\
&= \left(\frac{1}{2\pi i}f'(z) - \frac{k}{12}(E_2 f)(z)\right) z^{k+2} = \theta_k f(z) \cdot z^{k+2}.
\end{aligned}$$

□

3.2 The Ramanujan Derivative Identities

We define the functions P, Q, R as follows:

$$P = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n)q^n$$
$$Q = 1 + 240\sum_{n=1}^{\infty} \sigma_3(n)q^n$$
$$R = 1 - 504\sum_{n=1}^{\infty} \sigma_5(n)q^n.$$

Note that for $q = e^{2\pi iz}$ there are just the functions $E_2(z), E_4(z), E_6(z)$, respectively. The following identities involve the differential operator $D = q\frac{d}{dq}$ and P, Q, R and will be incredibly useful in establishing the Ramanujan congruences of the partition function.

Theorem 3.7. *We have*

$$DP = \frac{1}{12}(P^2 - Q)$$
$$DQ = \frac{1}{3}(PQ - R)$$
$$DR = \frac{1}{2}(PR - Q^2).$$

Proof. Note that by Proposition 3.6, we have that $\theta_4 E_4 \in M_6(SL_2(\mathbb{Z}))$ and $\theta_6 E_6 \in M_8(SL_2(\mathbb{Z}))$. We know that $M_6(SL_2(\mathbb{Z}))$ and $M_8(SL_2(\mathbb{Z}))$ are 1-dimensional vector spaces spanned by E_6 and E_8 respectively, so we have that $DQ - \frac{1}{3}E_2 Q = c_1 E_6 = c_1 R$ and $DR - \frac{1}{2}E_2 R = c_2 E_8 = c_2 Q^2$ for some $c_1, c_2 \in \mathbb{R}$. Comparing the q^0-coefficients tells us that $c_1 = -\frac{1}{3}$ and $c_2 = -\frac{1}{2}$. Thus, writing $E_2 = P$ gives us $DQ = \frac{1}{3}(PQ - R)$ and $DR = \frac{1}{2}(PR - Q^2)$.

We now just have to prove the first of the three identities. To show this, we prove that $\frac{1}{2\pi i}E_2'(z) - \frac{1}{12}E_2^2(z) \in M_4(SL_2(\mathbb{Z}))$. However, we know by Equation (12) that $E_2(z) = E_2(z+1)$ and $E_2(-1/z) = z^2 E_2(z) + \frac{6}{i\pi}z$, which means that

$$\frac{1}{2\pi i}E_2'(z+1) - \frac{1}{12}E_2^2(z+1) = \frac{1}{2\pi i}E_2'(z) - \frac{1}{12}E_2^2(z)$$

and

$$\begin{aligned}
\frac{1}{2\pi i}E_2'\left(\frac{-1}{z}\right) - \frac{1}{12}E_2^2\left(\frac{-1}{z}\right) &= \frac{z^2}{2\pi i}\left(\frac{d}{dz}E_2\left(-\frac{1}{z}\right)\right) - \frac{1}{12}\left(z^2E_2(z) + \frac{6}{i\pi}z\right)^2 \\
&= \frac{z^2}{2\pi i}\left(\frac{d}{dz}\left(z^2E_2(z) + \frac{6}{i\pi}z\right)\right) - \frac{1}{12}\left(z^2E_2(z) + \frac{6}{i\pi}z\right)^2 \\
&= \frac{z^2}{2\pi i}\left(2zE_2(z) + z^2E_2'(z) + \frac{6}{i\pi}\right) - \frac{1}{12}\left(z^2E_2(z) + \frac{6}{i\pi}z\right)^2 \\
&= \frac{z^4}{2\pi i}E_2'(z) - \frac{z^4}{12}E_2^2(z) = z^4\left(\frac{1}{2\pi i}E_2'(z) - \frac{1}{12}E_2^2(z)\right).
\end{aligned}$$

Therefore, we have $\frac{1}{2\pi i}E_2'(z) - \frac{1}{12}E_2^2(z) \in M_4(SL_2(\mathbb{Z}))$ as the modular relation is preserved under the two generators of $SL_2(\mathbb{Z})$ and we clearly have a holomorphic q-series expansion around $i\infty$. Therefore, $\frac{1}{2\pi i}E_2'(z) - \frac{1}{12}E_2^2(z) = DP - \frac{1}{12}P^2$ must equal $c_3 Q$ as $M_4(SL_2(\mathbb{Z}))$ has one dimension, and by comparing leading coefficients, we know $c_3 = -\frac{1}{12}$. Thus, $DP = \frac{1}{12}(P^2 - Q)$ as desired. $\square$

3.3 The Ramanujan Congruences

We now have the necessary toolkit to establish Ramanujan's congruence identities.

We first outline the general method of proving the Ramanujan congruences. First, for our prime $\ell \in \{5, 7, 11\}$, we will establish that $\Delta^{(\ell^2-1)/24}$ (which equals Δ for $\ell = 5$, Δ^2 for $\ell = 7$, and Δ^5 for $\ell = 11$) is congruent modulo ℓ to $D(f)$ for some f which is a polynomial of P, Q, and R. We will do this by looking at the q-series expansions of P, Q, R and using the Ramanujan derivative identities. This means that the $q^{\ell n}$ coefficients of $\Delta^{(\ell^2-1)/24}$ must be 0 modulo ℓ. Then, we note that $\Delta^{(\ell^2-1)/24} = q^{(\ell^2-1)/24} \cdot \prod(1-q^n)^{\ell^2} \cdot \prod(1-q^n)^{-1} \equiv \prod(1-q^{\ell n})^{\ell} \cdot \prod(1-q^n)^{-1} \pmod{\ell}$. We will use the fact that $\prod(1-q^{\ell n})^{\ell}$ is a power series in $q^{\ell n}$ to show we can divide by $\prod(1-q^{\ell n})^{\ell}$ to get that $q^{(\ell^2-1)/24} \cdot \prod(1-q^n)^{-1}$ must have all of the $q^{\ell n}$ coefficients congruent to 0 modulo ℓ. Finally, we recall that $\prod(1-q^n)^{-1} = \sum p(n)q^n$, which will mean $p(n) \equiv 0 \pmod{\ell}$ whenever $n \equiv -\frac{\ell^2-1}{24} \pmod{\ell}$, which will precisely be the Ramanujan congruences.

We now prove the Ramanujan congruences rigorously, following the method in [6].

Theorem 3.8. *For all integers $n \geq 0$, we have $p(5n+4) \equiv 0 \pmod 5$.*

Proof. Note that since $n \equiv n^5 \pmod 5$, we have that $\sigma_1(n) \equiv \sigma_5(n) \pmod 5$. Therefore, we have that $Q \equiv 1 \pmod 5$ and $P \equiv R \pmod 5$ when written as q-series, since $240 \equiv 0 \pmod 5$ and $-24 \equiv -504 \pmod 5$. Thus, we have that

$$1728\Delta = Q^3 - R^2 \equiv Q - P^2 \pmod 5$$

and by Theorem 3.7, we have

$$3DP \equiv Q - P^2 \pmod 5,$$

so as $1728 \equiv 3 \pmod 5$, we have $DP \equiv \Delta \pmod 5$. Now, using the product formula for Δ and the fact that $(1-q^n)^{25} \equiv (1-q^{25n}) \pmod 5$, we have

$$DP \equiv \Delta \equiv q\prod_{n=1}^{\infty}(1-q^n)^{24} \equiv q\prod_{n=1}^{\infty}\frac{(1-q^n)^{25}}{(1-q^n)} \equiv q\prod_{n=1}^{\infty}(1-q^n)^{-1}\prod_{n=1}^{\infty}(1-q^{25n}) \pmod 5.$$

Dividing the left and right by $\prod(1-q^{25n})$ and using the product formula for the partition generating function gives us

$$DP \cdot \prod_{n=1}^{\infty}(1-q^{25n})^{-1} \equiv q \cdot \prod_{n=1}^{\infty}(1-q^n)^{-1} = q \cdot \left(\sum_{n=0}^{\infty} p(n)q^n\right) = \sum_{n=1}^{\infty} p(n-1)q^n \pmod 5. \quad (17)$$

However, we know $DP = \sum_{n\geq 0} n\sigma_1(n)q^n$ and $n\sigma_1(n) \equiv 0 \pmod 5$ if $5|n$. Thus, since $\prod(1-q^{25n})^{-1}$ is a power series in q^5, we clearly have that the left hand side of (17) has all q^{5n} terms congruent to 0 modulo 5. Thus, (17) gives us $p(5n-1) \equiv 0 \pmod 5$ for all $n \geq 1$. $\square$

Theorem 3.9. *For all integers $n \geq 0$, we have $p(7n+5) \equiv 0 \pmod 5$.*

Proof. Note that $Q^2 = E_8 = 1 + 480\sum_{n\geq 1}\sigma_7(n)q^n$. Since $n^7 \equiv n \pmod 7$, we clearly have $\sigma_1(n) \equiv \sigma_7(n) \pmod 7$. Thus, as $480 \equiv -24 \pmod 7$, we have $Q^2 \equiv P \pmod 7$ when written as q-series. Also, since $7|504$, we have $R \equiv 1 \pmod 7$. Thus, by repeatedly using $Q^2 \equiv P, R \equiv 1 \pmod 7$, we have

$$(Q^3 - R^2)^2 \equiv (PQ-1)^2 \equiv PQ(PQ-1) - (PQ-1)$$
$$\equiv (P^2Q^2 - PQ) - (PQ - R) \equiv P(P^2 - Q) - (PQ - R) \pmod 7.$$

But noting that $P^2 - Q = 12DP$ and $PQ - R = 3DQ$ gives us

$$(Q^3 - R^2)^2 \equiv 12P \cdot DP - 3DQ = -q\frac{d(P^2)}{dq} - 3q\frac{dQ}{dq} \equiv -q\frac{d(P^2+3Q)}{dq} = -D(P^2+3Q) \pmod 7.$$

This means that $(Q^3-R^2)^2$ has q^{7n} coefficients congruent to 0 mod 7, since if $P^2+3Q = \sum a(n)q^n$, then $-D(P^2+3Q) = \sum -na(n)q^n$.

Now, very similarly to Theorem 3.8, we have

$$(Q^3-R^2)^2 = 1728^2\Delta^2 \equiv \Delta^2 = q^2\left(\sum_{n=0}^{\infty} p(n)q^n\right)\prod_{n=1}^{\infty}(1-q^n)^{49} \equiv \left(\sum_{n=2}^{\infty} p(n-2)q^n\right)\prod_{n=1}^{\infty}(1-q^{49n}) \pmod 7,$$

and therefore,

$$(Q^3 - R^2)^2 \cdot \prod_{n=1}^{\infty}(1-q^{49n})^{-1} \equiv \sum_{n=2}^{\infty} p(n-2)q^n \pmod 7. \tag{18}$$

Again, since $\prod(1-q^{49n})^{-1}$ is a power series in q^7, the left hand side of (18) has all q^{7n} terms congruent to 0 modulo 7, as $(Q^3 - R^2)^2$ does. Thus, $p(7n-2) \equiv 0 \pmod 7$ for all $n \geq 1$. □

Finally, we prove the congruence modulo 11.

Theorem 3.10. *For all integers $n \geq 0$, we have $p(11n+6) \equiv 0 \pmod{11}$.*

Proof. First, since $11|264$, by using the q-series expansion of E_{10}, we have that

$$QR = E_{10} \equiv 1 \pmod{11} \tag{19}$$

Next, note that $E_{12} = 1 + \frac{65520}{691}\sum_{n\geq 1}\sigma_{11}(n)q^n$. Also, $M_{12}(SL_2(\mathbb{Z}))$ has dimension 2 and contains Δ, which is a cusp form and has a nonzero q^1 coefficient, which means $f, g \in M_{12}(SL_2(\mathbb{Z}))$ are equal if their q^0 and q^1 coefficients are the same. Thus, one can verify that

$$441Q^3 + 250R^2 = 691E_{12} = 691 + 65520\sum_{n\geq 1}\sigma_{11}(n)q^n.$$

Noting that $n^{11} \equiv n \pmod{11}$ and thus $\sigma_{11}(n) = \sigma_1(n)$, we have that

$$Q^3 - 3R^2 \equiv 441Q^3 + 250R^2 \equiv 691 + 65520\sum_{n\geq 1}\sigma_{11}(n)q^n \equiv -2 + 2\sum_{n\geq 1}\sigma_1(n)q^n = -2P \pmod{11}. \tag{20}$$

By writing $R \equiv Q^{-1}$ and $P \equiv \frac{-1}{2}(Q^3 - 3Q^{-2}) \equiv 5Q^3 - 4Q^{-2} \pmod{11}$, we have that

$$\begin{aligned}P^5 - 3P^3Q - 4P^2R + 6QR &\equiv (5Q^3 - 4Q^{-2})^5 - 3(5Q^3 - 4Q^{-2})^3Q - 4(5Q^3 - 4Q^{-2})^2Q^{-1} + 6\\ &= 3125Q^{15} - 12875Q^{10} + 20800Q^5 - 16554 + 6258Q^{-5} - 1024Q^{-10}\\ &\equiv Q^{15} - 5Q^{10} + 10Q^5 - 10 + 5Q^{-5} - Q^{-10} \pmod{11}\end{aligned} \tag{21}$$

and

$$(Q^3 - R^2)^5 \equiv (Q^3 - Q^{-2})^5 = Q^{15} - 5Q^{10} + 10Q^5 - 10 + 5Q^{-5} - Q^{-10} \pmod{11}. \tag{22}$$

Thus, $(Q^3 - R^2)^5 \equiv P^5 - 3P^3Q - 4P^2R + 6QR \pmod{11}$. Next, note that by Theorem 3.7,

$$\begin{aligned} D(3P^4 - 4P^2Q + 5PR) &\equiv (P^3 + 3PQ + 5R)DP - 4P^2dQ + 5PdR \\ &\equiv (P^3 + 3PQ + 5R) \cdot \frac{1}{12}(P^2 - Q) - 4P^2 \cdot \frac{1}{3}(PQ - R) + 5P \cdot \frac{1}{2}(PR - Q^2) \\ &\equiv P^5 - 3P^3Q - 4P^2R + 6PR \pmod{11}, \end{aligned} \tag{23}$$

where in the final line of (23), the equivalence is true simply by expanding as a polynomial in P, Q, and R. Therefore, we have that $(Q^3 - R^2)^5 \equiv D(3P^4 - 4P^2Q + 5PR) \pmod{11}$, so we have the q^{11n} coefficients of $(Q^3 - R^2)^5$ are divisible by 11.

We finish similarly to Theorems 3.8 and 3.9. Note that

$$(Q^3 - R^2)^5 \equiv \Delta^5 = q^2 \left(\sum_{n=0}^{\infty} p(n)q^n\right) \prod_{n=1}^{\infty}(1 - q^n)^{121} \equiv \left(\sum_{n=2}^{\infty} p(n-5)q^n\right) \prod_{n=1}^{\infty}(1 - q^{121n}) \pmod{11},$$

and therefore,

$$(Q^3 - R^2)^5 \cdot \prod_{n=1}^{\infty}(1 - q^{121n})^{-1} \equiv \sum_{n=2}^{\infty} p(n-5)q^n \pmod{11}. \tag{24}$$

Again, since $\prod(1 - q^{121n})^{-1}$ is a power series in q^{11}, the left hand side of (24) has all q^{7n} terms congruent to 0 modulo 7, as $(Q^3 - R^2)^5$ does. Thus, $p(11n - 5) \equiv 0 \pmod{11}$ for all $n \geq 1$. □

What is perhaps the hardest part of proving the Ramanujan congruences, even given the general outline, is to find some polynomial f of P, Q, and R such that $Df \equiv \Delta^{(\ell^2-1)/24} \pmod{\ell}$. In fact, one may wonder how one may come up with taking $P^5 - 3P^3Q - 4P^2R + 6QR$ and trying to show is congruent to Δ^5. One way is to note that if P, Q, and R are viewed as weight $2, 4$, and 6 modular forms (where P is really a quasi-modular form) then since $QR \equiv 1 \pmod{11}$ is weight 10 and $(Q^3 - R^2)^5$ is weight 60, it is reasonable for some weight 10 quasi-modular form in terms of P, Q, and R to be congruent to $(Q^3 - R^2)^5$, and by playing with the first few q-series coefficients, there are not too many options.

Perhaps a more natural way is to show that $\Delta^{(\ell^2-1)/24}$ has its $q^{\ell n}$ coefficients congruent to 0 modulo ℓ is using the Hecke operator, though we chose not to use this method as we will see this method repeatedly used in the next section. The idea is to show that $\Delta^{(\ell^2-1)/24}|T(\ell) \equiv 0 \pmod{\ell}$ by noting that $\Delta^{(\ell^2-1)/24}|T(\ell)$ is a cusp form of weight $\frac{\ell^2-1}{2}$, and the dimension of cusp forms of this weight is $\frac{\ell^2-1}{24}$. It is thus possible to show that if the first few coefficients of $\Delta^{(\ell^2-1)/24}|T(\ell)$ are congruent to 0 modulo ℓ, then $\Delta^{(\ell^2-1)/24}|T(\ell) \equiv 0 \pmod{\ell}$. We can use this fact and the way the Hecke operator changes the q-series expansion to show $\Delta^{(\ell^2-1)/24}$ has its $q^{\ell n}$ coefficients congruent to 0 modulo ℓ.

4 Hecke Operators over $M_k(SL_2(\mathbb{Z}))$ and Another Family of Partition Function Congruences

In this section, we will show another family of congruences relating to the partition function that can be established solely using the theory of modular forms in $M_k(SL_2(\mathbb{Z}))$. While many more general congruences can be established using the more general theory of modular forms (such as half-integral weight forms or forms with Nebentypus character), we will primarily deal with such congruences in Section 6. We mostly follow several of the results in [18] that only require the theory of modular forms in $M_k(SL_2(\mathbb{Z}))$, and will see that we can still prove many fascinating congruences. These congruences will primarily deal with primes from 13 through 31, and all follow a very similar set of calculations. Specifically, we will get congruences which give us information about

$$p\left(\frac{\ell^k \cdot (24n + r_{\ell,k}) + 1}{24}\right) \pmod{\ell},$$

for primes $13 \leq \ell \leq 31$ and all positive integers k, where $r_{\ell,k}$ is the unique integer between 0 and 23 such that $\ell^k r_{\ell,k} \equiv -1 \pmod{24}$.

The method followed generally follows that presented in Section 4 of [18], though we significantly change the way this is presented to explain a more general theory behind the congruences we are proving. We also note that the cases $13, 17, 19, 23$ are done in [18], and although the cases $\ell = 29, 31$ were not done, they follow from the same approach.

4.1 Preliminaries

We start with the following simple but crucial result, proven in [26, 25].

Proposition 4.1. *Suppose that $f_1, f_2 \in M_k(SL_2(\mathbb{Z}))$. Then, for any prime ℓ, $f_1 \equiv f_2 \pmod{\ell}$ if and only if for all $n \leq \frac{k}{12}$, the coefficients of q^n in f_1 and f_2 are congruent modulo ℓ.*

Proof. The only if direction is trivial. For the if direction, we prove this via induction on k.

Let $a_1(n), a_2(n)$ represent the q^n-coefficient of f_1, f_2, respectively. If $k \in \{0, 4, 6, 8, 10, 14\}$, then $f_1 = a_1(0)E_k$ and $f_2 = a_2(0)E_k$, where E_k is the normalized Eisenstein series for $k > 0$ and $E_k = 1$ if $k = 0$. We know that E_k has integral coefficients as E_4, E_6 do, and since $a_1(0) \equiv a_2(0) \pmod{\ell}$, we have $f_1 \equiv f_2 \pmod{\ell}$.

Now, for $k = 12$ or $k > 14$, choose some $a, b \in \mathbb{N} \cup \{0\}$ such that $4a + 6b = k$. Then, defining $f_1' = f_1 + (a_2(0) - a_1(0))E_4^a E_6^b$, we have that $f_1' \equiv f_1 \pmod{\ell}$ and $f_1' - f_2 \in S_k(SL_2(\mathbb{Z}))$, which means $\frac{f_1' - f_2}{\Delta} \in S_{k-12}(SL_2(\mathbb{Z}))$ as Δ has no zeroes in $\mathbb{H}$. However, since $\Delta = q + 1728q^2 + ...$, we have that if $a_1(n) \equiv a_2(n) \pmod{\ell}$ for all $n \leq \frac{k}{12}$, then the q^n-coefficient of $\frac{f_1' - f_2}{\Delta}$ is congruent to 0 modulo ℓ for all $n \leq \frac{k-12}{12} = \frac{k}{12} - 1$. By our induction hypothesis, this means $\frac{f_1' - f_2}{\Delta} \equiv 0 \pmod{\ell}$, and thus $f_1' - f_2 \equiv 0 \pmod{\ell}$ and $f_1 \equiv f_1' \equiv f_2 \pmod{\ell}$. □

We also will need the following important fact about the Bernoulli numbers to prove a stronger version of Proposition 4.1.

Proposition 4.2. *[26, Lemma 4] Let ℓ be a prime and v be a nonnegative integer. Then:*

(a) If $(\ell - 1) | 2v$, then ℓB_{2v} is an integer and $\ell B_{2v} \equiv -1 \pmod{\ell}$.

(b) *If* $(\ell-1) \nmid 2v$, *then* $\frac{B_{2v}}{2v}$ *is* ℓ*-integral, i.e., when reduced,* ℓ *does not divide the denominator. Moreover,* $\frac{B_{2v}}{2v}$ *reduced modulo* ℓ *only depends on* $2v$ *modulo* $\ell-1$.

Given these two results, we can prove the following corollary which strengthens 4.1.

Corollary 4.3. *Suppose that* $f_1 \in M_k$ *and* $f_2 \in M_{k'}$ *where* $k \equiv k' \pmod{\ell-1}$. *Then, they are congruent modulo* ℓ *iff for all* $n \leq \max\left(\frac{k}{12}, \frac{k'}{12}\right)$, *the coefficients of* q^n *in* f_1 *and* f_2 *are congruent modulo* ℓ.

Proof. Note that by Theorem 4.2a, we know that

$$E_{\ell-1}(z) = 1 - \frac{2(\ell-1)}{B_{\ell-1}} \sum_{n=1}^{\infty} \sigma_{\ell-2}(n) q^n = 1 - \ell \cdot \frac{2(\ell-1)}{\ell B_{\ell-1}} \sum_{n=1}^{\infty} \sigma_{\ell-2}(n) q^n.$$

While $E_{\ell-1}$ may not have integer q-series coefficients, the denominators all divide the numerator of $B_{\ell-1}$, which means that there is some integer a_ℓ such that $a_\ell \equiv 1 \pmod{\ell}$ and $a_\ell E_{\ell-1}$ has integer q-series coefficients. This clearly implies $a_\ell E_{\ell-1} \equiv 1 \pmod{p}$, as ℓ does not divide the numerator of $\ell B_{\ell-1}$. Now, assuming WLOG that $k \leq k'$, if $k'-k = r(\ell-1)$, then $f_1 \cdot (a_\ell \cdot E_{\ell-1})^r \equiv f_1 \pmod{\ell}$ and $f_1 \cdot (a_\ell \cdot E_{\ell-1})^r, f_2 \in M_{k'} \cap \mathbb{Z}[[q]]$, so we can apply Proposition 4.1 on $f_1 \cdot (a_\ell \cdot E_{\ell-1})^r$ and f_2. □

Next, we define the following operators:

Definition 4.4. We define U and V as operators that act on formal power series in q such that for all positive integers M,

$$\left(\sum_{n\geq 0} a(n) q^n\right)\Bigg| U(M) = \sum_{n \geq 0} a(Mn) q^n$$

and

$$\left(\sum_{n\geq 0} a(n) q^n\right)\Bigg| V(M) = \sum_{n \geq 0} a(n) q^{Mn}.$$

We note that for primes ℓ, $U(\ell)$ corresponds closely to the Hecke operator, as we show below, and $V(\ell)$ corresponds to replacing z with ℓz.

Proposition 4.5. *For* ℓ *prime and* $f = \sum a(n) q^n \in M_k(SL_2(\mathbb{Z}))$ *for* $k \geq 2$, $f|U(\ell) \equiv f|T(\ell) \pmod{\ell}$.

Proof. As ℓ is prime, we use Equation (13) to get

$$f|T(\ell) = \sum_{n=0}^{\infty} \left(\sum_{d |\gcd(n,\ell)} d^{k-1} a\left(\frac{\ell \cdot n}{d^2}\right)\right) q^n.$$

Since ℓ is prime, d can only be 1 or ℓ. We do not care about the $d = \ell$ case since $\ell^{k-1} \equiv 0 \pmod{\ell}$. Therefore, modulo ℓ, this equals

$$\sum_{n=0}^{\infty} a(\ell \cdot n) q^n = f|U(\ell).$$
□

We also note the following, which follows immediately from the fact that $e^{2\pi i(\ell z)n} = q^{\ell n}$.

Proposition 4.6. $f(z)|V(\ell) = f(\ell z)$.

Next, we define the following two functions:

Definition 4.7. For $\ell \geq 5$ prime and $k, n \in \mathbb{Z}$, define $F(\ell, k; z)$ as a power series over q with coefficients in $\mathbb{Z}/\ell\mathbb{Z}$ such that

$$F(\ell, k; z) := \sum_{\substack{n \geq 0 \\ 24 | \ell^k n + 1}} p\left(\frac{\ell^k n + 1}{24}\right) q^n \pmod{\ell}$$

Definition 4.8. For $\ell \geq 5$ prime and k, n are positive integers, define $a(\ell, k, n) \in \mathbb{Z}/\ell\mathbb{Z}$ such that

$$\sum_{n=0}^{\infty} a(\ell, k, n) q^n :\equiv \frac{\left(\Delta^{(\ell^{2k}-1)/24}(z) | U(\ell^k)\right) | V(24)}{\eta^{\ell^k}(24z)} \pmod{\ell}$$

We now prove a few results which will be key preliminaries in our main theorems of this section.

Theorem 4.9. *[18, Theorem 6] If $\ell \geq 5$ is prime and $k, n \in \mathbb{N}$, then*

$$p\left(\frac{\ell^k n + 1}{24}\right) \equiv a(\ell, k, n) \pmod{\ell}.$$

Proof. First, note that

$$\frac{\eta^{\ell^k}(\ell^k z)}{\eta(z)} = q^{(\ell^{2k}-1)/24} \cdot \prod_{n \geq 1} \frac{\left(1 - q^{\ell^k n}\right)^{\ell^k}}{(1 - q^n)} = \left(\sum_{n=0}^{\infty} p(n) q^{n + (\ell^{2k}-1)/24}\right) \cdot \prod_{n \geq 1} \left(1 - q^{\ell^k n}\right)^{\ell^k},$$

where we used the product formula for the partition generating function. Applying the $U(\ell^k)$ operator to both sides and simplifying the right hand side gives us

$$\begin{aligned} \frac{\eta^{\ell^k}(\ell^k z)}{\eta(z)} \bigg| U\left(\ell^k\right) &= \left(\sum_{n=0}^{\infty} p(n) q^{n + (\ell^{2k}-1)/24}\right) \bigg| U(\ell^n) \cdot \prod_{n \geq 1} (1 - q^n)^{\ell^k} \\ &= \left(\sum_{n=0}^{\infty} p\left(\ell^k n + \beta(\ell^k)\right) q^{n + \frac{(\ell^{2k}-1)/24 + \beta(\ell^k)}{\ell^k}}\right) \cdot \prod_{n \geq 1} (1 - q^n)^{\ell^k} \end{aligned}$$

where $\beta(\ell^k)$ is the unique positive integer less than ℓ^k such that $24\beta(\ell, k) \equiv 1 \pmod{\ell^k}$.

Since ℓ is prime, we have that $(1 - q^{\ell^k})^{\ell^k} \equiv (1 - q)^{\ell^{2k}} \pmod{\ell}$, so

$$\frac{\eta^{\ell^k}(\ell^k z)}{\eta(z)} \equiv \frac{\eta^{\ell^{2k}}(z)}{\eta(z)} \equiv \Delta^{(\ell^{2k}-1)/24}(z) \pmod{\ell},$$

and thus,

$$\Delta^{(\ell^{2k}-1)/24}(z) \bigg| U\left(\ell^k\right) \equiv \left(\sum_{n=0}^{\infty} p\left(\ell^k n + \beta(\ell^k)\right) q^{n + \frac{(\ell^{2k}-1)/24 + \beta(\ell^k)}{\ell^k}}\right) \cdot \prod_{n \geq 1} (1 - q^n)^{\ell^k} \pmod{\ell}.$$

We can divide both sides by $\prod_{n\geq 1}(1-q^n)^{\ell^k}$ and preserve congruence modulo ℓ as the denominator's leading coefficient is 1, which is relatively prime to ℓ. Thus,

$$\frac{\Delta^{(\ell^{2k}-1)/24}(z)\big|U\left(\ell^k\right)}{\prod\limits_{n\geq 1}(1-q^n)^{\ell^k}} \equiv \sum_{n=0}^{\infty} p\left(\ell^k n+\beta(\ell^k)\right) q^{n+\frac{(\ell^{2k}-1)/24+\beta(\ell^k)}{\ell^k}} \pmod{\ell}.$$

We replace q with q^{24} (or equivalently take the $V(24)$ operator of both sides) and divide both sides by q^{ℓ^k} to get

$$\frac{\left(\Delta^{(\ell^{2k}-1)/24}(z)\big|U\left(\ell^k\right)\right)\Big|V(24)}{q^{\ell^k}\prod\limits_{n\geq 1}(1-q^{24n})^{\ell^k}} \equiv \sum_{n=0}^{\infty} p(\ell^k n+\beta(\ell^k))q^{24n+\frac{24\beta(\ell^k)-1}{\ell^k}} \pmod{\ell}.$$

However, it is clear that the left hand side equals $\sum a(\ell,k,n)q^n$ and that the right hand side equals

$$\sum_{\substack{n\geq 0\\ 24|\ell^k n+1}} p\left(\frac{\ell^k n+1}{24}\right) q^n \equiv F(\ell,k;z) \pmod{\ell}$$

since $\ell^k n \equiv -1 \pmod{24}$ is clearly equivalent to n being of the form $24n'+(24\beta(\ell^k)-1)/\ell^k$ for some $n'\geq 0$. This concludes the proof. □

Proposition 4.10. *[18, Proposition 7] If $\ell \geq 5$ is prime and k is a positive integer, then*

$$F(\ell,k+1;z) \equiv F(\ell,k;z)|U(\ell) \pmod{\ell}.$$

Proof. By definition of $F(\ell,k;z)$,

$$F(\ell,k;z)|U(\ell) \equiv \left(\sum_{\substack{n\geq 0\\ 24|\ell^k n+1}} p\left(\frac{\ell^k n+1}{24}\right) q^n\right)\Bigg|U(\ell) = \sum_{n\geq 0} p\left(\frac{\ell^{k+1}n+1}{24}\right) q^n$$

where we let $p(a)=0$ if a is not a nonnegative integer. Therefore, this equals

$$\sum_{\substack{n\geq 0\\ 24|\ell^{k+1} n+1}} p\left(\frac{\ell^{k+1} n+1}{24}\right) q^n \equiv F(\ell+1,k;z) \pmod{\ell}.$$

□

4.2 Congruences of $F(\ell,k;z)$ modulo ℓ

For all primes $\ell \geq 5$, we provide a general framework that, under certain conditions, will allow us to prove that $F(\ell,k;z)$ is congruent modulo ℓ to $\frac{f(24z)}{\eta^r(24z)}$ for some integral-weight modular form f over $SL_2(\mathbb{Z})$. We will show in later subsections of this section that the primes $\ell = 13, 17, 19, 23, 29$, and 31 satisfy the necessary conditions, allowing us to prove many congruences relating to the partition function modulo these primes only using the theory of modular forms in $M_k(SL_2(\mathbb{Z}))$ that we have already established.

For any prime $\ell \geq 5$, define $\delta_\ell := \frac{\ell^2-1}{24}$. Note that $\Delta^{\delta_\ell}(z)|T(\ell)$ is a cusp form over $SL_2(\mathbb{Z})$ with weight $\frac{\ell^2-1}{2}$, and the smallest n such that the q^n-coefficient of $\Delta^{\delta_\ell}(z)|T(\ell)$ is nonzero is at least $\lceil \frac{\delta_\ell}{\ell} \rceil = \lceil \frac{\ell^2-1}{24\ell} \rceil = \lceil \frac{\ell}{24} \rceil$. Let $r = \lceil \frac{\ell}{24} \rceil$ and assume that for some $k' \in \mathbb{N}$ and some cusp form $f(z) \in S_{k'}(SL_2(\mathbb{Z}))$ with integer coefficients, we have $\Delta^{\delta_\ell}(z)|U(\ell) \equiv f(z) \pmod{\ell}$. Next, suppose that

$$f(z)|U(\ell) \equiv g(z) \pmod{\ell} \tag{25}$$

and that

$$(\Delta^{\delta_\ell}(z) \cdot g(z))|U(\ell) \equiv cf(z) \pmod{\ell} \tag{26}$$

for some $k'' \in \mathbb{N}$, $c \in \mathbb{Z}/\ell\mathbb{Z}$ and cusp form $g(z) \in S_{k''}(SL_2(\mathbb{Z}))$ with integer coefficients. Then, we will have that by Definition 4.8 and Theorem 4.9,

$$F(\ell, 1; z) \equiv \frac{\left(\Delta^{\delta_\ell}(z)|U(\ell)\right)\big|V(24)}{\eta^\ell(24z)} \equiv \frac{f(z)|V(24)}{\eta^\ell(24z)} = \frac{f(24z)}{\eta^\ell(24z)} \pmod{\ell}.$$

Now, if $F(\ell, 2k+1; z) \equiv c' \cdot \frac{f(24z)}{\eta^\ell(24z)} \pmod{\ell}$ for some $c' \in \mathbb{Z}/\ell\mathbb{Z}$, then note that

$$\eta^\ell(24z) = q^\ell \cdot \prod_{n=1}^{\infty} \left(1 - q^{24n}\right)^\ell \equiv q^\ell \cdot \prod_{n=1}^{\infty} \left(1 - q^{24\ell n}\right) \equiv \eta(24\ell z) \pmod{\ell}.$$

Therefore, we have $F(\ell, 2k+2; z) \equiv F(\ell, 2k+1; z)|U(\ell) \pmod{\ell}$ by Proposition 4.10, and since $\eta^\ell(24z) \equiv \eta(24\ell z)$, which is a power series in q^ℓ,

$$F(\ell, 2k+2; z) \equiv c' \cdot \frac{f(24z)}{\eta^\ell(24z)}\Bigg|U(\ell) \equiv c' \frac{f(24z)|U(\ell)}{\eta(24z)} \equiv c' \frac{g(24z)}{\eta(24z)} \pmod{\ell},$$

using (25) and the fact that $24, \ell$ are relatively prime in the last congruence. Similarly, we have $F(\ell, 2k+3; z) \equiv F(\ell, 2k+2; z)|U(\ell)$ by Proposition 4.9 and $\eta^{\ell^2}(2rz) \equiv \eta(24\ell^2 z)$ which is a power series in q^ℓ. These equations mean

$$F(\ell, 2k+3; z) \equiv c' \cdot \frac{g(24z)}{\eta(24z)}\Bigg|U(\ell) = c' \cdot \frac{g(z) \cdot \eta^{\ell^2-1}(24z)}{\eta(24z) \cdot \eta^{\ell^2-1}(24z)}\Bigg|U(\ell) = c' \cdot \frac{g(z) \cdot \Delta^{\delta_\ell}(24z)}{\eta^{\ell^2}(24z)}\Bigg|U(\ell)$$

$$\equiv c' \cdot \frac{\left(g(z) \cdot \Delta^{\delta_\ell}(24z)\right)|U(\ell)}{\eta^\ell(24z)} \equiv c \cdot c' \cdot \frac{f(z)}{\eta^\ell(24z)} \equiv c \cdot F(\ell, 2k+1; z) \pmod{\ell}.$$

As a result, by inducting on k, we get for all integers $k \geq 0$,

$$F(\ell, 2k+1, z) \equiv c^k \cdot \frac{f(24z)}{\eta^\ell(24z)} \pmod{\ell} \tag{27}$$

$$F(\ell, 2k+2, z) \equiv c^k \cdot \frac{g(24z)}{\eta(24z)} \pmod{\ell}. \tag{28}$$

In the next 6 subsections, we use these results to prove congruences for primes ℓ between 13 and 31. We note that the general framework is to find modular forms f, g such that $\Delta^{\delta_\ell}(z)|U(\ell) \equiv f(z) \pmod{\ell}$ that satisfy equations 25 and 26, so that we can apply equations (27) and (28) to find our desired congruences.

4.3 The case $\ell = 13$

For $\ell = 13$, we have $\delta_\ell = 7$. One can verify that $\Delta^7|U(13) \equiv 11\Delta(z) \pmod{13}$. Since $\Delta^7|T(13)$ and Δ are weight 84 and 12 cusp forms over $SL_2(\mathbb{Z})$, and $84 \equiv 12 \pmod{12}$, by Proposition 4.5 and Corollary 4.3, we only need to verify the coefficients of q^n for $n \leq 7$. Thus, $f(z) = 11\Delta(z)$. We can similarly verify that $\Delta(z)|U(13) \equiv \Delta(z)|T(13) \equiv 8\Delta(z)$ by checking only the terms of q^n for $n \leq 1$, and $\Delta^8(z)|U(13) \equiv \Delta^8(z)|T(13) \equiv 4\Delta(z)$ by checking only the terms of q^n for $n \leq 8$. Thus, we can set $g(z) = 10\Delta(z) \equiv 8 \cdot 11\Delta(z) \pmod{13}$, and $c = 6 \equiv 8 \cdot 4 \pmod{13}$. By (27) and (28), we get

$$F(13, 2k+1; z) \equiv 11 \cdot 6^k \cdot \frac{\Delta(24z)}{\eta^{13}(24z)} \equiv 11 \cdot 6^k \cdot \eta^{11}(24z) \pmod{13}, \tag{29}$$

$$F(13, 2k+2; z) \equiv 10 \cdot 6^k \cdot \frac{\Delta(24z)}{\eta(24z)} \equiv 10 \cdot 6^k \cdot \eta^{23}(24z) \pmod{13}. \tag{30}$$

Therefore, by using Definition 4.7 to define $F(13, k; z)$, using Equations (29) and (30), dividing by q^{11} for the $2k+1$ case and q^{23} for the $2k+2$ case, and then replacing z with $z/24$, we have

$$\sum_{n=0}^{\infty} p\left(\frac{13^{2k+1}(24n+11)+1}{24}\right) q^n \equiv 11 \cdot 6^k \cdot \prod_{n=1}^{\infty} (1-q^n)^{11} \pmod{13}, \tag{31}$$

$$\sum_{n=0}^{\infty} p\left(\frac{13^{2k+2}(24n+23)+1}{24}\right) q^n \equiv 10 \cdot 6^k \cdot \prod_{n=1}^{\infty} (1-q^n)^{23} \pmod{13}. \tag{32}$$

4.4 The case $\ell = 17$

For $\ell = 17$, we have $\delta_\ell = 12$. One can verify that $\Delta^{12}|U(17) \equiv 7\Delta(z)E_4(z) \pmod{17}$, by using Proposition 4.5 and Corollary 4.3 and verifying the coefficients of q^n for $n \leq 12$. Thus, $f(z) = 7\Delta(z)E_4(z)$. We can similarly verify that $(\Delta(z)E_4(z))|U(17) \equiv 7\Delta(z)E_4(z)$ by checking only the terms of q^n for $n \leq 1$, and $(\Delta^{13}(z)E_4(z))|U(17) \equiv 13\Delta(z)E_4(z)$ by checking only the terms of q^n for $n \leq 13$. Thus, we can set $g(z) = 15\Delta(z)$, and $c = 6$. By (27) and (28), we get

$$F(17, 2k+1; z) \equiv 7 \cdot 6^k \cdot \frac{\Delta(24z)E_4(24z)}{\eta^{17}(24z)} \equiv 7 \cdot 6^k \cdot \eta^{7}(24z)E_4(24z) \pmod{17}, \tag{33}$$

$$F(17, 2k+2; z) \equiv 15 \cdot 6^k \cdot \frac{\Delta(24z)E_4(24z)}{\eta(24z)} \equiv 15 \cdot 6^k \cdot \eta^{23}(24z)E_4(24z) \pmod{17}. \tag{34}$$

Therefore, by using Definition 4.7 to define $F(17, k; z)$, using Equations (33) and (34), dividing by q^7 for the $2k+1$ case and q^{23} for the $2k+2$ case, and then replacing z with $z/24$, we have

$$\sum_{n=0}^{\infty} p\left(\frac{17^{2k+1}(24n+7)+1}{24}\right) q^n \equiv 7 \cdot 6^k \cdot E_4(z) \prod_{n=1}^{\infty} (1-q^n)^{11} \pmod{17}, \tag{35}$$

$$\sum_{n=0}^{\infty} p\left(\frac{17^{2k+2}(24n+23)+1}{24}\right) q^n \equiv 15 \cdot 6^k \cdot E_4(z) \prod_{n=1}^{\infty} (1-q^n)^{23} \pmod{17}. \tag{36}$$

4.5 The case $\ell = 19$

For $\ell = 19$, we have $\delta_\ell = 15$. One can verify that $\Delta^{15}|U(19) \equiv 5\Delta(z)E_6(z) \pmod{19}$, by using Proposition 4.5 and Corollary 4.3 and verifying the coefficients of q^n for $n \leq 15$. Thus, $f(z) =$

$5\Delta(z)E_6(z)$. We can similarly verify that $(\Delta(z)E_6(z))|U(19) \equiv 6\Delta(z)E_6(z)$ by checking only the terms of q^n for $n \leq 1$, and $(\Delta^{16}(z)E_6(z))|U(19) \equiv 8\Delta(z)E_6(z)$ by checking only the terms of q^n for $n \leq 16$. Thus, we can set $g(z) = 11\Delta(z)E_6(z)$, and $c = 10$.

Via an almost identical set of calculations to subsections 4.3 and 4.4, we have

$$\sum_{n=0}^{\infty} p\left(\frac{19^{2k+1}(24n+5)+1}{24}\right) q^n \equiv 5 \cdot 10^k \cdot E_6(z) \prod_{n=1}^{\infty} (1-q^n)^5 \pmod{19}, \tag{37}$$

$$\sum_{n=0}^{\infty} p\left(\frac{19^{2k+2}(24n+23)+1}{24}\right) q^n \equiv 11 \cdot 10^k \cdot E_6(z) \prod_{n=1}^{\infty} (1-q^n)^{23} \pmod{19}. \tag{38}$$

4.6 The case $\ell = 23$

For $\ell = 23$, we have $\delta_\ell = 22$. One can verify that $\Delta^{22}|U(23) \equiv \Delta(z)E_{10}(z) \pmod{23}$, by using Proposition 4.5 and Corollary 4.3 and verifying the coefficients of q^n for $n \leq 22$. Thus, $f(z) = \Delta(z)E_{10}(z)$. We can similarly verify that $(\Delta(z)E_{10}(z))|U(23) \equiv 5\Delta(z)E_{10}(z)$ by checking only the terms of q^n for $n \leq 1$, and $(\Delta^{23}(z)E_{10}(z))|U(23) \equiv \Delta(z)E_{10}(z)$ by checking only the terms of q^n for $n \leq 23$. Thus, we can set $g(z) = 5\Delta(z)E_{10}(z)$, and $c = 5$.

Via an almost identical set of calculations to subsections 4.3 and 4.4, we have

$$\sum_{n=0}^{\infty} p\left(\frac{23^{2k+1}(24n+1)+1}{24}\right) q^n \equiv 5^k \cdot E_{10}(z) \prod_{n=1}^{\infty} (1-q^n) \pmod{23}, \tag{39}$$

$$\sum_{n=0}^{\infty} p\left(\frac{23^{2k+2}(24n+23)+1}{24}\right) q^n \equiv 5^{k+1} \cdot E_{10}(z) \prod_{n=1}^{\infty} (1-q^n)^{23} \pmod{23}. \tag{40}$$

4.7 The case $\ell = 29$

For $\ell = 29$, we have $\delta_\ell = 35$. One can verify that $\Delta^{35}|U(29) \equiv 8\Delta^2(z)E_4(z) \pmod{29}$, by using Proposition 4.5 and Corollary 4.3 and verifying the coefficients of q^n for $n \leq 35$. Thus, $f(z) = 8\Delta^2(z)E_4(z)$. We can similarly verify that $(\Delta^2(z)E_4(z))|U(29) \equiv 6\Delta^2(z)E_4(z) + 3\Delta(z)E_4^4(z)$ by checking only the terms of q^n for $n \leq 2$, and $((6\Delta^2(z)E_4(z) + 3\Delta(z)E_4^4(z)) \cdot \Delta^{35}(z))|U(29) \equiv 3\Delta^2(z)E_4(z)$ by checking the terms of q^n for $n \leq 23$. Thus, we can set $g(z) = 8 \cdot (6\Delta^2(z)E_4(z) + 3\Delta(z)E_4^4(z))$ and $c = 3$.

We again do a similar calculation as in subsections 4.3 and 4.4 to get

$$\sum_{n=0}^{\infty} p\left(\frac{29^{2k+1}(24n+19)+1}{24}\right) q^n \equiv 8 \cdot 3^k \cdot E_4(z) \prod_{n=1}^{\infty} (1-q^n)^{19} \pmod{29}, \tag{41}$$

$$\sum_{n=0}^{\infty} p\left(\frac{29^{2k+2}(24n+23)+1}{24}\right) q^n \equiv 8 \cdot 3^k \cdot E_4(z)(6\Delta(z) + 3E_4^3(z)) \prod_{n=1}^{\infty} (1-q^n)^{23} \pmod{29}. \tag{42}$$

4.8 The case $\ell = 31$

For $\ell = 31$, we have $\delta_\ell = 40$. One can verify that $\Delta^{40}|U(31) \equiv 10\Delta^2(z)E_6(z) \pmod{31}$, by using Proposition 4.5 and Corollary 4.3 and verifying the coefficients of q^n for $n \leq 40$. Thus, $f(z) = 10\Delta^2(z)E_6(z)$. We can similarly verify that $(\Delta^2(z)E_6(z)|U(31) \equiv -(\Delta^2(z)E_6(z) + 2\Delta(z)E_6^3(z))$ by checking the terms of q^n for $n \le 2$, and $((\Delta^2(z)E_4(z)+2\Delta(z)E_6^3(z))\cdot\Delta^{40}(z))|U(31) \equiv \Delta^2(z)\cdot E_6(z)$ by checking the coefficients of q^n for $n \le 42$. Thus, we can set $g(z) = -10(\Delta^2(z)E_6(z)+2\Delta(z)E_6^3(z))$ and $c = -1$.

We again do a similar calculation as in subsections 4.3 and 4.4 to get

$$\sum_{n=0}^{\infty} p\left(\frac{31^{2k+1}(24n+17)+1}{24}\right) q^n \equiv 10\cdot(-1)^k \cdot E_6(z)\prod_{n=1}^{\infty}(1-q^n)^{17} \pmod{31}, \tag{43}$$

$$\sum_{n=0}^{\infty} p\left(\frac{31^{2k+2}(24n+23)+1}{24}\right) q^n \equiv 10\cdot(-1)^{k+1} \cdot E_6(z)(\Delta(z)+2E_6^2(z))\prod_{n=1}^{\infty}(1-q^n)^{23} \pmod{31}. \tag{44}$$

4.9 Summary

The functions such as $E_6(z)\cdot\prod_{n\ge1}(1-q^n)^{17} \pmod{31}$ may seem strange, so Equation (43) seemingly does not give much information about the partition function modulo 31. However, we will see in Section 5 that $E_4(24z), E_6(24z)$, and $\eta(24z) = q\prod(1-q^{24n})$ are all modular forms over $\Gamma_0(576)$. Therefore, if we were to replace n with $24n$, we get an interesting family of relations connecting the partition function with modular forms over $\Gamma_0(576)$.

However, we can also get much simpler relations which are perhaps even more interesting. For instance, if we set $n = 0$, Equations (43) and (44) give us

$$p\left(\frac{31^{2k+1}\cdot 17+1}{24}\right) \equiv 10(-1)^k \pmod{31}$$

and

$$p\left(\frac{31^{2k+2}\cdot 23+1}{24}\right) \equiv 20(-1)^{k+1} \pmod{31}$$

for all $k \ge 0$. We can repeat this for all primes from 13 to 31, as well as replace $n = 0$ with some other small n to get various similar congruences.

Finally, we briefly explain how one can do the required computations, such as verifying the q^n-coefficients of $((\Delta^2(z)E_4(z)+2\Delta(z)E_6^3(z))\cdot\Delta^{40}(z))|U(31)$ modulo 31 for all $n \le 42$ (which is probably the hardest verification to compute). First, we note that by our Eisenstein q-series formula (see Equation (10)), we can compute the first n coefficients of E_{2k} in $O(n\log n)$ time by computing $\sigma_{2k-1}(n)$ modulo ℓ for all n. This is done by adding $(r)^{2k+1}$ to the t^{th} coefficient for all $r|t, t \le n$. Moreover, it is easy to multiply any power series over q by $\eta(z)$ for the first n coefficients in $O(n\sqrt{n})$ time with the the following well-known theorem, called Euler's pentagonal number theorem:

Theorem 4.11. *[15, Exercise 1.2.2] We have*

$$\prod_{n=1}^{\infty}(1-q^n) = \sum_{k=-\infty}^{\infty}(-1)^k q^{k(3k-1)/2}. \tag{45}$$

Thus, there are only $O(\sqrt{n})$ nonzero coefficients of $\eta(z)$ that we have to worry about, and multiplying by $\Delta^{40}(z)$ only requires us to multiply by $\eta(z)$ 40×24 times. We also only need to calculate the q^n coefficients for $(\Delta^2(z)E_4(z)+2\Delta(z)E_6^3(z))\cdot\Delta^{40}(z)$ for $n \le 31\times 42 = 1302$.

5 Background results on Modular Forms

While the theory of modular forms in $M_k(SL_2(\mathbb{Z}))$ for even integers k gives us many interesting partition function congruences, this theory can only get us so far. To establish a more general set of congruences, we will need to look at a more general theory of modular forms. In this section, we provide several results which do not represent any of the main ideas in [2], but represent important facts the authors claim that must be established for their results to be true. Some of these are computational results which are stated or assumed but not explicitly cited, so we provide proofs or proof sketches of them here. Some of the computations are very straightforward but may not be included in standard textbooks, so we cannot cite them and we therefore prove them.

Unfortunately, some of the other results stated (mainly in Subsections 5.4 and 5.6) require theory far beyond the scope of this thesis to prove. However, these required results can be stated quite easily given an understanding of the previous sections as well as basic knowledge of L-functions, so we content ourselves with the statements and provide references for the interested reader.

5.1 Computing Orders of Modular Forms

Our goal here is to compute the order at each of the cusps of modular forms that scaled or shifted by some rational number. This will allow us to verify in later subsections that certain functions are either modular forms or cusp forms. As we will see in Section 6, these verifications will allow Ahlgren and Ono in [2] to use the theory of modular forms to establish congruences.

Recall that for any holomorphic function $f : \mathbb{H} \to \mathbb{C}$ and any real number c, the order of f at $i\infty$ equals c if $\lim_{z\to i\infty} f(z) \cdot e^{-2\pi i c z}$ is well defined, finite, and nonzero. Moreover, for any $\alpha \in \mathbb{Q}$, we say the order of f at α equals c if the order of $f|_k\gamma$ is c at $i\infty$ for $\gamma \in SL_2(\mathbb{Z})$ sending $i\infty$ to α.

Proposition 5.1. *Suppose $f : \mathbb{H} \to \mathbb{C}$ is holomorphic and has well-defined order at all cusps. Then, for any positive integer N, $f(Nz)$ has well-defined order at all cusps. We can also explicitly compute the order of $f(Nz)$ at a cusp α in terms of only N, α, and the order of $f(z)$ at $N\alpha$.*

Proof. To compute the order of $f(Nz)$ for some $\alpha \in \mathbb{Q}$, let $\gamma_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ and $\gamma_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in SL_2(\mathbb{Z})$ be matrices sending $i\infty$ to α and $N \cdot \alpha$, respectively. Note that $\frac{a_1}{c_1} = \alpha$ and $\frac{a_2}{c_2} = N\alpha$. Then, the order of $f(Nz)$ at α equals

$$\begin{aligned} \mathrm{ord}_{i\infty}\left(f(N\cdot\gamma_1 z)\cdot(c_1z+d_1)^{-k}\right) &= \mathrm{ord}_{i\infty}\left(f(\gamma_2\circ\gamma_2^{-1}(N\gamma_1 z))\cdot(c_1z+d_1)^{-k}\right) \\ &= \mathrm{ord}_{\gamma_2(i\infty)}\left(f(\gamma_2^{-1}(N\gamma_1 z))\cdot\left(\frac{c_2\cdot\gamma_2^{-1}(N\gamma_1 z)+d_2}{c_1z+d_1}\right)^k\right). \end{aligned} \tag{46}$$

Now, note that

$$\gamma_2^{-1}(N\cdot\gamma_1 z) = \begin{pmatrix} d_2 & -b_2 \\ -c_2 & a_2 \end{pmatrix} \cdot \begin{pmatrix} Na_1 & Nb_1 \\ c_1 & d_1 \end{pmatrix} z = \begin{pmatrix} Na_1d_2 - c_1b_2 & Nb_1d_2 - d_1b_2 \\ c_1a_2 - Na_1c_2 & d_1a_2 - Nb_1c_2 \end{pmatrix} z.$$

Since $\frac{a_1}{c_1} = \alpha$ and $\frac{a_2}{c_2} = N\alpha$, we have $c_1a_2 - Na_1c_2 = 0$. Moreover, we have $Na_1d_2 - c_1b_2 = (a_2d_2 - b_2c_2)\cdot\frac{Na_1}{a_2} = \frac{Na_1}{a_2}$ and $d_1a_2 - Nb_1c_2 = (a_1d_2 - b_1c_1)\cdot\frac{a_2}{a_1}$. If $\alpha \neq 0$, then $a_1, a_2 \neq 0$, so

$$\gamma_2^{-1}(N\cdot\gamma_1(z)) = \begin{pmatrix} \frac{Na_1}{a_2} & Nb_1d_2 - d_1b_2 \\ 0 & \frac{a_2}{a_1} \end{pmatrix} z = \frac{Na_1^2}{a_2^2}\cdot z + \beta$$

for some rational number β. If $\alpha = 0$, then $a_1 = a_2 = 0$, $c_1, c_2 \in \{\pm 1\}$, $b_1 = -c_1$, and $b_2 = -c_2$. This means

$$\gamma_2^{-1}(N \cdot \gamma_1(z)) = \begin{pmatrix} -c_1 b_2 & -d_1 b_2 \\ 0 & -N b_1 c_2 \end{pmatrix} z = \frac{z}{N} + \beta$$

for some $\beta \in \mathbb{Q}$. We know that γ_1, γ_2 are well defined up to multiplication by $\pm I$ for fixed α, so if we define $h(\alpha) := \frac{N a_1^2}{a_2^2}$ for $\alpha \neq 0$ and $h(\alpha) := \frac{1}{N}$ for $\alpha = 0$, we have

$$\lim_{z \to i\infty} \left(\frac{c_2 \cdot \gamma_2^{-1}(N \cdot \gamma_1 z) + d_2}{c_1 z + d_1} \right)^k = \left(\frac{c_2}{c_1} \cdot h(\alpha) \right)^k$$

is some nonzero rational number, so plugging into Equation (46) gives us

$$\mathrm{ord}_\alpha(f(Nz)) = \mathrm{ord}_{\gamma_2(i\infty)} f(z) \cdot h(\alpha) = \mathrm{ord}_{(N\alpha)} f(z) \times \begin{cases} 1/N & \alpha = 0 \\ N \cdot (a_1/a_2)^2 & \alpha \neq 0 \end{cases}.$$

Finally, it is clear that $f(Nz)$ clearly has order $N \cdot \mathrm{ord}_{i\infty} f(z)$ at $\alpha = i\infty$. □

Proposition 5.2. *For a prime ℓ and a positive integer t, define $E_{\ell,t}(z) := \frac{\eta^{\ell^t}(z)}{\eta(\ell^t z)}$. Then, $E_{\ell,t}$ has positive order at all cusps of $\Gamma_0(\ell^t)$ not $\Gamma_0(\ell^t)$-equivalent to $i\infty$, which are precisely the rational numbers α such that ℓ^t does not divide the denominator of α when written as a reduced fraction.*

Proof. If $\alpha \in \mathbb{Q}$ is $\Gamma_0(\ell^t)$-equivalent to $i\infty$, then $\alpha = \gamma(i\infty)$, where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell^t)$. This means $\ell^t | c$ so $\alpha = \frac{a}{c}$, where $\ell^t | c$ which means $\ell \nmid a$ since a, c must be relatively prime. Thus, any reduced fraction of the form $\frac{a}{c}$ where $\ell^t \nmid c$ cannot be $\Gamma_0(\ell^t)$-equivalent to $i\infty$. Conversely, if $\alpha = \frac{a}{c}$ where a, c are relatively prime and $\ell^t | c$, one can show by Bezout's identity (using the Euclidean algorithm) that $\exists b, d \in \mathbb{Z}$ such that $ad - bc = 1$. Thus, any such α is $\Gamma_0(\ell^t)$-equivalent to $i\infty$.

Now, suppose that $\frac{a}{c} \in \mathbb{Q}$ with $\ell^t \nmid c$. Then, the order of $\eta^{\ell^t}(z)$ at $\frac{a}{c}$ is just $\frac{1}{2} \cdot \ell^t$, since Δ has order 12 at all cusps and $\eta^{12} = \Delta$. Moreover, by Proposition 5.1, we can compute the order of $\eta(\ell^t z)$ at $\alpha = \frac{a}{c}$. If $\alpha = 0$, then the order is $\mathrm{ord}_{\ell^t \cdot 0} \eta(z) \cdot \frac{1}{\ell^t} = \frac{1}{2} \cdot \frac{1}{\ell^t}$. Otherwise, if $\ell^t \alpha = \frac{a'}{c'}$, then if $\ell^r | c$ but $\ell^{r+1} \nmid c$ for some $0 \leq r < t$, then $c' = \frac{c}{\ell^r}$ and $a' = a \cdot \ell^{t-r}$. Thus, we have the order of $\eta(\ell^t z)$ at α is $\frac{1}{2} \cdot \frac{\ell^t \cdot a^2}{(a')^2} \leq \frac{1}{2} \cdot \ell^{t-2}$. Taking the quotient clearly gives us that

$$\mathrm{ord}_\alpha \frac{\eta^{\ell^t}(z)}{\eta(\ell^t z)} \geq \frac{1}{2} \cdot \ell^t - \frac{1}{2} \cdot \ell^{t-2} > 0,$$

as desired. □

Proposition 5.3. *Suppose $f : \mathbb{H} \to \mathbb{C}$ is holomorphic and has well-defined order at all cusps. Then, for any rational number r, $f(z+r)$ has well-defined order at all cusps. We can also explicitly compute the order of $f(z+r)$ at a cusp α in terms of only r, α, and the order of $f(z)$ at $\alpha + r$.*

Proof. To compute the order of $f(z+r)$ for some $\alpha \in \mathbb{Q}$, let $\gamma_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ and $\gamma_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in SL_2(\mathbb{Z})$ be matrices sending $i\infty$ to α and $\alpha + r$, respectively. Similarly to in Proposition 5.1, $\frac{a_1}{c_1} = \alpha$, $\frac{a_2}{c_2} = \alpha + r$, and the order of $f(z+r)$ at α equals

$$\mathrm{ord}_\alpha f(z+r) = \mathrm{ord}_{\alpha+r} \left(f(\gamma_2^{-1}(r + \gamma_1 z)) \cdot \left(\frac{c_2 \cdot \gamma_2^{-1}(r + \gamma_1 z) + d_2}{c_1 z + d_1} \right)^k \right). \tag{47}$$

We will not be computing the order explicitly, but we note that since $\gamma_2^{-2}(r+\gamma_1 z)$ is a map in $SL_2(\mathbb{Q})$ mapping $i\infty$ to $i\infty$, it must be of the form $\gamma_2^{-2}(r+\gamma_1 z) = \begin{pmatrix} a_3 & b_3 \\ 0 & d_3 \end{pmatrix} z = \frac{a_3 z + b_3}{d_3}$, where $a_3, b_3, d_3 \in \mathbb{Q}$ and $a_3 d_3 = 1$, and the matrix is unique up to multiplication by $\pm I$. Then, we have

$$\lim_{z\to i\infty} \left(\frac{c_2 \cdot \frac{a_3 z + b_3}{d_3} + d_2}{c_1 z + d_1} \right)^k = \left(\frac{c_2 \cdot a_3}{c_1 \cdot d_3} \right)^k,$$

which is a nonzero rational number. Therefore, using Equation (47) gives us

$$\mathrm{ord}_\alpha(f(z+r)) = \mathrm{ord}_{\alpha+r} f\left(\begin{pmatrix} a_3 & b_3 \\ 0 & d_3 \end{pmatrix} z \right) = \mathrm{ord}_{\alpha+r} f\left(\frac{a_3 z + b_3}{d_3} \right) = \frac{a_3}{d_3} \cdot \mathrm{ord}_{\alpha+r}(f(z)).$$

Finally, it is clear that $f(z+r)$ and $f(z)$ have the same order at $\alpha = i\infty$. □

Corollary 5.4. *The three statements $f(z)$, $f(Nz)$, and $f(z+r)$ are holomorphic at all cusps are equivalent for $N, \in \mathbb{Z}, r \in \mathbb{Q}$. Likewise, the three statements $f(z)$, $f(Nz)$, and $f(z+r)$ vanishing at all cusps are equivalent.*

Proof. To check the order of $f(z+r)$ at each cusp, we use Proposition 5.3 and note that at $i\infty$, the order of f remains constant and at any $\alpha \in \mathbb{Q}$, $\mathrm{ord}_\alpha f(z+r) = \frac{a_3}{d_3} \cdot \mathrm{ord}_{\alpha+r} f(z)$, where a_3, d_3 are some rational numbers such that $a_3 d_3 = 1$, as in the proof of Proposition 5.3. This means that $\frac{a_3}{d_3}$ is a positive rational number. Therefore, f has nonnegative order for all cusps if and only if $f(z+r)$ does, and f has positive order for all cusps if and only if $f(z+r)$ does.

To check the order of $f(Nz)$, we know from Proposition 5.1, which tells us $\mathrm{ord}_\alpha(f(Nz))$ either equals $\mathrm{ord}_0(f(z))/N$ for the case $\alpha = 0$, $\mathrm{ord}_{(N\alpha)} f(z) \cdot N \cdot (a_1/a_2)^2$ for some $a_1, a_2 \in \mathbb{Z}\backslash\{0\}$ if $\alpha \in \mathbb{Q}\backslash\{0\}$, and $\mathrm{ord}_{i\infty} f(z) \cdot N$ if $\alpha = i\infty$. Therefore, f has nonnegative order for all cusps if and only if $f(Nz)$ does and if f has positive order for all cusps if and only if $f(Nz)$ does. □

5.2 Conversions of Modular Forms

In this section, we prove a few propositions under a similar theme. Namely, we show that given some modular form f, possibly half-integral, after some change to the q-series of f or replacement of z with a linear transformation of z, we will get another modular form.

Proposition 5.5. *Let $r \in \mathbb{Z}$, $t, N \in \mathbb{N}$ and $2k \in \mathbb{N}$ such that if $k \notin \mathbb{N}$, then $4|N$. Then, if $f(z) \in S_k(\Gamma_1(Nt))$, then $f(z+\frac{r}{t}) \in S_k(\Gamma_1(Nt^2))$.*

Proof. Define $g(z) = f(z+\frac{r}{t})$. For any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(Nt^2)$, $g(\gamma z)$ equals

$$f\left(\frac{az+b}{cz+d} + \frac{r}{t} \right) = f\left(\frac{\left(a+\frac{rc}{t}\right)z + \left(b+\frac{rd}{t}\right)}{cz+d} \right) = f\left(\frac{\left(a+\frac{rc}{t}\right)\left(z+\frac{r}{t}\right) + \left(b+\frac{rd}{t} - \frac{r}{t}\left(a+\frac{rc}{t}\right)\right)}{c\left(z+\frac{r}{t}\right) + \left(d-\frac{rc}{t}\right)} \right).$$

Let $a' = a + \frac{rc}{t}$, $b' = b + \frac{rd}{t} - \frac{r}{t}\left(a+\frac{rc}{t}\right)$, $c' = c$, and $d' = d - \frac{rc}{t}$. Since $a \equiv b \equiv 1 \pmod{Nt^2}$ and $c \equiv 0 \pmod{Nt^2}$, we have that a' is an integer and $a' \equiv 1 \pmod{Nt}$, b' is an integer, $c' = c \equiv 0 \pmod{Nt^2}$, and d' is an integer such that $d' \equiv 1 \pmod{Nt}$. Also, $a'd' - b'c' = 1$. Thus,

$$g(\gamma z) = f\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \left(z+\frac{r}{t}\right) \right) = f\left(z+\frac{r}{t}\right) \cdot j\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}, z+\frac{r}{t} \right) = g(z) \cdot j(\gamma, z).$$

To show the last equality, we have $c'\left(z+\frac{r}{t}\right)+d' = cz+d$. This proves the equality if $k \in \mathbb{N}$. If $k \notin \mathbb{N}$, then $\varepsilon_d = \varepsilon_{d'} = 1$ as $d, d' \equiv 1 \pmod N$ and $4|N$. Thus we need to show $\chi_c(d) = \left(\frac{c}{d}\right)$ (representing Kronecker symbol) equals $\chi_c(d') = \left(\frac{c}{d'}\right)$. To prove the last statement, note that for any odd prime $p|c$, $p|\frac{c}{t}$ as $Nt^2|c$. Thus, $d \equiv d' \pmod{4p}$ so if $p \equiv 1 \pmod 4$, $\left(\frac{p}{d}\right) = \left(\frac{d}{p}\right) = \left(\frac{d'}{p}\right) = \left(\frac{p}{d'}\right)$, which is true even if d or d' are negative. Likewise, if $p \equiv 3 \pmod 4$, $\left(\frac{p}{d}\right) = (-1)^{(d-1)/2}\left(\frac{d}{p}\right) = (-1)^{(d'-1)/2}\left(\frac{d'}{p}\right) = \left(\frac{p}{d'}\right)$. Also, $\left(\frac{-1}{d}\right) = (-1)^{(d-1)/2}$ even if d is negative, so $\left(\frac{-1}{d}\right) = \left(\frac{-1}{d'}\right)$. Finally, for $p = 2$, note that $\left(\frac{2}{d}\right) = 1$ for $d \equiv \pm 1 \pmod 8$ and $\left(\frac{2}{d}\right) = -1$ for $d \equiv \pm 3 \pmod 8$. If $8|c$, then $\left(\frac{2}{d}\right) = \left(\frac{2}{d'}\right)$ as $|d| \equiv |d'| \pmod 8$ or $|d| \equiv -|d'| \pmod 8$. Else, since $N|c$, $4|c$ and $\left(\frac{4}{d}\right) = 1 = \left(\frac{4}{d'}\right)$. Therefore, we have that by definition of Kronecker symbol, $\left(\frac{c}{d}\right) = \left(\frac{c}{d'}\right)$.

Finally, we know $f(z+\frac{r}{t})$ vanishes at all cusps by Corollary 5.4. □

Proposition 5.6. *Let $r, t, N \in \mathbb{N}$ and $2k \in \mathbb{N}$ such that if $k \notin \mathbb{N}$, then $4|N$. Then, if*

$$f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_k\left(\Gamma_1(Nt)\right),$$

we have

$$\sum_{n \equiv r \pmod t} a(n)q^n \in S_k\left(\Gamma_1(Nt^2)\right).$$

Proof. Note that because

$$f\left(z+\frac{r}{t}\right) = \sum_{n=0}^{\infty} a(n)e^{2\pi i rn/t}q^n,$$

we have that

$$\sum_{n \equiv r \pmod t} a(n)q^n = \frac{1}{t}\sum_{j=0}^{t-1} e^{-2\pi i rj/t} f\left(z+\frac{j}{t}\right).$$

Since $f\left(z+\frac{j}{t}\right) \in S_k(\Gamma_1(Nt^2))$ by Proposition 5.5, the result is immediate. □

Proposition 5.7. *For any prime ℓ, any nonnegative integer k, and any function $f(z) = \sum_{n\geq 0} a(n)q^n$ in $M_k\left(\Gamma_0(\ell), \left(\frac{\cdot}{\ell}\right)\right)$, we have that $\sum_{n\geq 0}\left(\frac{n}{\ell}\right)a(n)q^n \in M_k\left(\Gamma_0(\ell^3), \left(\frac{\cdot}{\ell}\right)\right)$, where $\left(\frac{n}{\ell}\right)$ represents the Legendre symbol.*

Proof. First, note that

$$\sum_{r=0}^{\ell-1}\left(\frac{r}{\ell}\right) f\left(z+\frac{r}{\ell}\right) = \sum_{n=0}^{\infty}\left(\sum_{r=0}^{\ell-1}\left(\frac{r}{\ell}\right)e^{2\pi i rn/\ell}\right)a(n)q^n. \tag{48}$$

To evaluate the inner sum, note that if $\ell|n$, it becomes $\sum_{r=0}^{\ell-1}\left(\frac{r}{\ell}\right) = 0$, and otherwise, it equals

$$\sum_{r=0}^{\ell-1}\left(\frac{n}{\ell}\right)\left(\frac{rn}{\ell}\right)e^{2\pi i rn/\ell} = \left(\frac{n}{\ell}\right)\cdot\sum_{r=0}^{\ell-1}\left(\frac{r}{\ell}\right)e^{2\pi i r/\ell} = \left(\frac{n}{\ell}\right)\cdot\begin{cases}\sqrt{\ell} & \text{if } \ell \equiv 1 \pmod 4 \\ i\sqrt{\ell} & \text{if } \ell \equiv 3 \pmod 4\end{cases}.$$

The last equality comes from the quadratic Gauss sum formula, but we actually just need to show that the inner sum equals $\left(\frac{n}{\ell}\right)\cdot c_\ell$ for some nonzero constant c_ℓ independent of n. We can show

$c_\ell \neq 0$ more easily by showing the Gauss sum has magnitude $\sqrt{\ell}$ (see [14, Theorem 5.3.3]), or by using the fact that $\mathbb{Q}[e^{2\pi i/\ell}]$ has dimension $\ell - 1$ with the only nontrivial linear dependence between $1, e^{2\pi i/\ell}, ..., e^{2\pi i(\ell-1)/\ell}$ being $\sum_{r=0}^{\ell-1} e^{2\pi i r/\ell} = 0$. What is important, however, is that the right hand side of (48) equals

$$c_\ell \cdot \sum_{n=0}^{\infty} \left(\frac{n}{\ell}\right) a(n) q^n$$

for $c_\ell \neq 0$, which means it suffices to prove that the left hand side of (48) is in $M_k(\Gamma_0(\ell^3), (\frac{\cdot}{\ell}))$.

We first verify the functional equation. For any $\gamma = \begin{pmatrix} a & b \\ \ell^2 c & d \end{pmatrix} \in \Gamma_0(\ell^2)$, choose $0 \le s \le \ell - 1$ so that $as \equiv dr \pmod{\ell}$ (note s is unique for fixed γ, r), and define $z' = z + \frac{s}{\ell}$. Then,

$$f\left(\gamma z + \frac{r}{\ell}\right) = f\left(\frac{az+b}{\ell^2 cz + d} + \frac{r}{\ell}\right) = f\left(\frac{a(z' - s/\ell) + b + r\ell c(z' - s/\ell) + dr/\ell}{\ell^2 c(z' - s/\ell) + d}\right)$$

$$= f\left(\frac{(a + r\ell c)z' + (b - rsc + (dr - as)/\ell)}{(\ell^2 c)z' + (d - s\ell c)}\right) = f\left(\begin{pmatrix} a + r\ell c & b - rsc + \frac{dr - as}{\ell} \\ \ell^2 c & d - s\ell c \end{pmatrix} z'\right)$$

$$= f(z')(\ell^2 cz' + d - s\ell c)^k \cdot \left(\frac{d - s\ell c}{\ell}\right) = f\left(z + \frac{s}{\ell}\right) \cdot (\ell^2 cz + d)^k \cdot \left(\frac{d}{\ell}\right).$$

For a fixed γ, since $\ell \nmid a, d$, we have a bijection between values of $s \in \{0, 1, ..., \ell - 1\}$ and $r \in \{0, 1, ..., \ell - 1\}$. Moreover, since $ad \equiv 1 \pmod{\ell}$, we have that $(\frac{r}{\ell}) = (\frac{s}{\ell})$ for corresponding values of r, s. Therefore, we have that

$$\sum_{r=0}^{\ell-1} \left(\frac{r}{\ell}\right) f\left(\gamma z + \frac{r}{\ell}\right) = \sum_{s=0}^{\ell-1} \left(\left(\frac{s}{\ell}\right) f\left(z + \frac{s}{\ell}\right) (\ell^2 c + d)^k \left(\frac{d}{\ell}\right)\right) = \left(\sum_{r=0}^{\ell-1} \left(\frac{r}{\ell}\right) f\left(z + \frac{r}{\ell}\right)\right) \cdot (\ell^2 c + d)^k \left(\frac{d}{\ell}\right),$$

which verifies our functional equation.

Finally, we know the left hand side of (48) has no poles at any of the cusps by Corollary 5.4. □

Proposition 5.8. *Let $m, N \in \mathbb{N}$ and $2k \in \mathbb{N}$ such that if $k \notin \mathbb{N}$, then $4|N$. Then, $f(z) \in M_k(\Gamma_0(N), \chi)$ or $S_k(\Gamma_0(N), \chi)$, then $f(mz) \in M_k(\Gamma_0(m \cdot N), \chi')$ or $S_k(\Gamma_0(m \cdot N), \chi')$, where $\chi' = \chi$ if $k \in \mathbb{N}$ and $\chi'(d) = \chi(d) \cdot \left(\frac{m}{d}\right)$ if $k \notin \mathbb{N}$.*

Proof. To verify the modular condition, first choose $\gamma = \left(\begin{smallmatrix} a & b \\ mNc & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. If k is an integer,

$$f(m \cdot \gamma z) = f\left(m \cdot \frac{az + b}{mNcz + d}\right) = f\left(\begin{pmatrix} a & mb \\ Nc & d \end{pmatrix} (mz)\right) = f(mz) \cdot (mNcz + d)^k \cdot \chi(d).$$

If k is a half integer, then

$$f(m \cdot \gamma z) = f\left(m \cdot \frac{az + b}{mNcz + d}\right) = f\left(\begin{pmatrix} a & mb \\ Nc & d \end{pmatrix} (mz)\right) = f(mz) \cdot j\left(\begin{pmatrix} a & mb \\ Nc & d \end{pmatrix}, mz\right)^{2k} \cdot \chi(d).$$

If $c = 0$, then the matrix is $\pm I$, so there is nothing to verify. Otherwise, this equals

$$f(mz) \cdot \left(\left(\frac{Nc}{d}\right) \epsilon_d^{-1} \sqrt{mNcz + d}\right)^{2k} \cdot \chi(d) = f(mz) \cdot j\left(\begin{pmatrix} a & b \\ Nmc & d \end{pmatrix}, z\right)^{2k} \cdot \left(\frac{m}{d}\right)^{2k} \cdot \chi(d).$$

Since $2k$ is odd, we have the modular condition is satisfied.

Finally, verifying the order at each cusp is done by Corollary 5.4. □

Proposition 5.9. *[2] For any nonnegative integer k and N a positive multiple of 4, we have a decomposition*

$$S_{k+\frac{1}{2}}(\Gamma_1(N)) = \bigoplus_{\chi \text{ even}} S_{k+\frac{1}{2}}(\Gamma_0(N), \chi).$$

Moreover, if $f \in S_{k+\frac{1}{2}}(\Gamma_1(N))$ has coefficients in $\mathcal{O}_K$ for some number field K, then f can be written as $\sum a_\chi f_\chi$, where a_χ are algebraic numbers, and $f_\chi \in S_{k+\frac{1}{2}}(\Gamma_0(N), \chi)$ has coefficients in $\mathcal{O}_{K'}$ for some possibly larger number field K'.

Proof Outline. The first part of the proof is very similar to the proof of Theorem 2.13. The idea is to look the function $g := \frac{f}{\Theta^{2k+1}}$ and define

$$g_\chi(z) := \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi^{-1}(d) g\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} z\right).$$

As done in Theorem 2.13, one can exploit the symmetry behind this sum to show that $g_\chi(\gamma z) = \chi(d) g_\chi(z)$ for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ and $g = \frac{1}{\varphi(N)} \cdot \sum_\chi g_\chi$. We can thus define $f_\chi = \Theta^{2k+1} \cdot g_\chi$ so that $\frac{1}{\varphi(N)} \sum f_\chi = f$. Checking holomorphy at the cusps is straightforward, since if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, then $g(\gamma z) \cdot \Theta(\gamma z)^{2k+1}$ equals $f(\gamma z) \cdot (cz + d)^{k+1/2}$ times a root of unity. We can assume our decomposition only has even χ, since $g(\gamma z) = g(z)$ for $\gamma = -I$ will force $\chi(-1) = 1$ if $g \not\equiv 0$.

We will not be able to prove the second part with our current background, but we note that the result comes from known decomposition theorems of f into algebraic linear combinations of Hecke eigenforms [20, 19]. □

5.3 Eta Products and Modular Forms

We will require three claims about certain Eta products being modular forms, where Eta products are functions of the form $\prod \eta(n_i z)^{r_i}$, $n_i \in \mathbb{N}, r_i \in \mathbb{Z}$. These are claimed in [2] without proof or citation, as they are perhaps folklore results. We prove these lemmas using results from [16, 24].

Lemma 5.10. *For any prime ℓ and positive integer t,*

$$\frac{\eta^{\ell^t}(z)}{\eta(\ell^t z)} \in M_{(\ell^t-1)/2}\left(\Gamma_0(\ell^t), \left(\frac{(-1)^{(\ell^t-1)/2}\ell^t}{\cdot}\right)\right).$$

Remark. We note that as Jacobi symbols, $\left(\frac{(-1)^{(\ell^t-1)/2}\ell^t}{n}\right) = \left(\frac{n}{\ell^t}\right)$ by Jacobi reciprocity, but we use the left symbol as we intend to use the *Kronecker symbol*.

Proof. We will use the method and cite some results from [16]. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, where $c > 0$, $\gcd(c, 6) = 1$, then

$$\eta(\gamma z) = \varepsilon(\gamma) \left(-i(cz + d)\right)^{1/2} \eta(z)$$

with

$$\varepsilon(\gamma) = \exp\left(-\pi i \left(-\frac{1}{12} c(a + d) + \frac{3}{4}(c + 1) + \frac{1}{2} c \left(\frac{a}{c}\right)\right)\right),$$

by [16, Lemma 1]. Here, $(-i(cz + d))^{1/2}$ is the branch with positive real part. The proof requires a complicated formula for $\varepsilon(\gamma)$ called the *Dedekind sum.* One can also prove (see [16, Lemma 2]) that $\Gamma_0(\ell^t)$ can be generated by $-I$ and all matrices of the form $\left(\begin{smallmatrix} a & b \\ \ell^t c & d \end{smallmatrix}\right) \in \Gamma_0(\ell^t)$ where $c > 0$ and $\gcd(6, c) = 1$, whenever $\ell \geq 5$. For a matrix γ of this form, we have

$$\eta^{\ell^t}(\gamma z) = \eta^{\ell^t}(z) \cdot \left(-i(\ell^t cz + d)\right)^{\ell^t/2} \cdot \exp\left(-\pi i \ell^t \left(-\frac{1}{12}\ell^t c(a+d) + \frac{3}{4}(\ell^t c + 1) + \frac{1}{2}\ell^t c\left(\frac{a}{\ell^t c}\right)\right)\right) \quad (49)$$

Next, note that

$$\eta(\ell^t \cdot \gamma z) = \eta\left(\ell^t \cdot \frac{az+b}{\ell^t cz + d}\right) = \eta\left(\begin{pmatrix} a & \ell^t b \\ c & d \end{pmatrix}(\ell z)\right),$$

so

$$\eta(\ell^t \gamma z) = \eta(\ell^t z) \cdot \left(-i(\ell^t cz + d)\right)^{1/2} \cdot \exp\left(-\pi i\left(-\frac{1}{12}c(a+d) + \frac{3}{4}(c+1) + \frac{1}{2}c\left(\frac{a}{c}\right)\right)\right). \quad (50)$$

Since $\ell^{2t} \equiv 1 \pmod{24}$ and $e^{2\pi i} = 1$, we have a lot of cancellation if we divide (49) by (50). If we use the fact that $\ell^{2t} c\left(\frac{a}{c}\right)$ and $c\left(\frac{a}{c}\right)$ are odd integers congruent modulo 4, and that $\left(\frac{a}{\ell^t}\right) \in \{\pm 1\}$, a straightforward computation of dividing (49) by (50) yields

$$\frac{\eta^{\ell^t}(\gamma z)}{\eta(\ell^t \gamma z)} = \frac{\eta^{\ell^t}(z)}{\eta(\ell^t z)} \cdot (-i(\ell^t c + d))^{(\ell^t - 1)/2} \exp\left(-\frac{3}{4}\pi i(\ell^t - 1)\right) \cdot \exp\left(\frac{\pi i}{2}\left(\left(\frac{a}{\ell^t}\right) - 1\right)\right).$$

It is clear that $\exp\left(\frac{\pi i}{2}\left(\left(\frac{a}{\ell^t}\right) - 1\right)\right) = \left(\frac{a}{\ell^t}\right)$. Also, since $-i = \exp\left(-\frac{1}{2}\pi i\right)$ and $(\ell^t - 1)/2 \in \mathbb{Z}$, we have that

$$(-i(\ell^t c + d))^{(\ell^t - 1)/2} \exp\left(-\frac{3}{4}\pi i(\ell^t - 1)\right) = 1.$$

Thus, we have

$$\frac{\eta^{\ell^t}(\gamma z)}{\eta(\gamma(\ell^t z))} = \frac{\eta^{\ell^t}(z)}{\eta(\ell^t z)} \cdot \left(\frac{a}{\ell^t}\right)$$

for any such matrix γ with $\gcd(6, c) = 1, c > 0$. We know these matrices generate, and that $\gamma(-Iz) = \gamma(z)$, which one can check will agree with the Nebentypus character regardless of ℓ^t modulo 4, so we are done. □

Lemma 5.11. *For any prime ℓ,*

$$\frac{\eta^{\ell}(\ell z)}{\eta(z)} \in M_{(\ell-1)/2}\left(\Gamma_0(\ell), \left(\frac{\cdot}{\ell}\right)\right).$$

Lemma 5.11 is proven essentially the same way as Lemma 5.10. We will not do the computations.

Lemma 5.12. *We have*

$$\eta(24z) \in S_{1/2}\left(\Gamma_0(576), \chi_{12}\right) := S_{1/2}\left(\Gamma_0(576), \left(\frac{12}{\cdot}\right)\right).$$

Proof. To prove fully will be difficult, but we prove it given some facts. First, recall Euler's pentagonal number theorem (see Theorem 4.11), which tells us

$$\prod_{n=1}^{\infty}(1 - q^n) = \sum_{k=-\infty}^{\infty} (-1)^k q^{k(3k-1)/2}. \quad (51)$$

Using Equation (51), it is straightforward to verify that

$$\eta(24z) = q\prod_{n=1}^{\infty}(1-q^{24n}) = \sum_{k=-\infty}^{\infty}(-1)^k q^{(6k-1)^2} = \frac{1}{2}\sum_{n\in\mathbb{Z}}\chi_{12}(n)q^{n^2}.$$

We will now use [24, Proposition 2.2], which tells us for any even character χ of conductor N, $\sum_{n\in\mathbb{Z}}\chi(n)q^{n^2} \in M_{1/2}(\Gamma_0(4N^2),\chi)$. In our case, $N = 12$, so we are done. □

5.4 The Shimura Correspondence

The Shimura correspondence gives a fascinating relationship between half-integral weight modular forms and even integer weight modular forms. To describe the relationship, we first define the Shimura lift on cusp forms of weight $k+\frac{1}{2}$, where k is a positive integer.

Definition 5.13. Let $f(z) = \sum_{n\geq 1} a(n)q^n \in S_{k+\frac{1}{2}}(\Gamma_0(N),\chi)$, where $4|N$ and χ is a character modulo N. Then, for each squarefree integer t, let $A_t(n)$ for $n \geq 1$ be the algebraic integers so that

$$\sum_{n=1}^{\infty}\frac{A_t(n)}{n^s} := L(s-k+1, \chi\cdot\chi_{-1}^k\chi_t)\cdot\sum_{n=1}^{\infty}\frac{a(t\cdot n^2)}{n^s}$$

as Dirichlet series, where $\chi_t(n)$ is the Kronecker character $\left(\frac{t}{n}\right)$ if $n \equiv 1 \pmod 4$ and $\left(\frac{4t}{n}\right)$ otherwise (so $\chi_{-1}(n) = \left(\frac{-4}{n}\right)$). Finally, define the *Shimura lift* $S_t(f(z))$ to have the series expansion $\sum_{n\geq 1} A_t(n)q^n$.

We will need a few simple results to make sense of this Shimura lift.

Proposition 5.14. *$S_t(f)$ has algebraic integer coefficients for all t if and only if f has algebraic integer coefficients. Moreover, if f has its coefficients all in $\mathcal{O}_K$, the ring of integers in some number field, then $S_t(f)$ has its coefficients in $\mathcal{O}_{K'}$ for some potentially larger number field K'. K' is independent of $f, k,$ and t but is possibly dependent on K and N.*

Proof. For any character χ,

$$L(s-k+1,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^{s-k+1}} = \sum_{n=1}^{\infty}\frac{\chi(n)\cdot n^{k-1}}{n^s},$$

which means $L(s-k+1,\chi)$ is a Dirichlet series over s with algebraic integer coefficients. Thus, $A_t(n)$ is the Dirichlet convolution of the functions $(\chi\chi_{-1}^k\chi_t)(n)\cdot n^{k-1}$ and $a(t\cdot n^2)$, and clearly is an algebraic integer for all n if $a(n)$ is for all n. Moreover, $(\chi\chi_{-1}^k\chi_t)(n)$ is an algebraic integer in some cyclotomic field containing all characters modulo N, since $\chi_{-1}(n), \chi_t(n) \in \{\pm 1\}$. Therefore, $A_t(n) \in O_{K'}$ for all n, where K' is the smallest number field containing K and the cyclotomic field.

Now, suppose that $A_t(n)$ is an algebraic integer for all t and n. Then for any fixed t,

$$L(s-k+1,\chi) = \prod_{\ell \text{ prime}}\left(1-\frac{\chi(\ell)}{\ell^{s-k+1}}\right)^{-1} = \prod_{\ell \text{ prime}}\left(1-\frac{\chi(\ell)\cdot\ell^{k-1}}{\ell^s}\right)^{-1}$$

$$\Rightarrow L(s-k+1,\chi)^{-1} = \prod_{\ell \text{ prime}}\left(1-\frac{\chi(\ell)\cdot\ell^{k-1}}{\ell^s}\right),$$

where we are using the Euler product of L-functions. Since $\chi(\ell) \cdot \ell^{k-1}$ is an algebraic integer,

$$\sum_{n=1}^{\infty} \frac{a(t \cdot n^2)}{n^s} = \sum_{n=1}^{\infty} \frac{A_t(n)}{n^s} \cdot \prod_{\ell \text{ prime}} \left(1 - \frac{(\chi \cdot \chi_{-1}^k \cdot \chi_t)(\ell) \cdot \ell^{k-1}}{\ell^s}\right)$$

is a Dirichlet series that must have algebraic integer coefficients, so $a(t \cdot n^2)$ is an algebraic integer for all t and n. Writing any integer $m \geq 1$ as $t \cdot n^2$ for t squarefree and $n \in \mathbb{N}$, we are done. □

Corollary 5.15. *For any integer M, $S_t(f) \equiv 0 \pmod{M}$ (i.e. every q-series coefficient of $S_t(f)$ is an algebraic integer divisible by M) if and only if $f \equiv 0 \pmod{M}$.*

Proof. Note that $S_t(f)/M = S_t(f/M)$, so the result is immediate from Proposition 5.14. □

Most importantly, we will need the famous Shimura correspondence. The original result was proven by Shimura in [24], but we will require a slightly stronger version, proven by Cipra and Niwa [9, 17]. The proof is far beyond the scope of this thesis, so we will only state the theorem.

Theorem 5.16. *For $f(z) \in S_{k+\frac{1}{2}}(\Gamma_0(N), \chi)$ for $4|N$, if $k \geq 2$, then $S_t(f(z)) \in S_{2k}(\Gamma_0(N), \chi^2)$. Moreover, we have what is called the commutativity of the correspondence, i.e. if $p \nmid N$ is prime, then*

$$S_t(f|T(p^2)) = S_t(f)|T(p).$$

5.5 Half-integral Weight Hecke Operators over $\Gamma_1(N)$

We can define half-integral Hecke operators over $\Gamma_1(N)$ in certain cases. If $\ell \equiv -1 \pmod{N}$ is prime and $f \in S_{k+\frac{1}{2}}(\Gamma_1(N))$, we can define $f|T(\ell^2)$ similarly to how we did it for forms in $S_{k+\frac{1}{2}}(\Gamma_0(N), \chi)$. Recall from Proposition 5.9 that f can be written as $\sum_{\chi \text{ even}} f_\chi$, where $f_\chi \in S_{k+\frac{1}{2}}(\Gamma_0(N), \chi)$. Therefore, $\chi(\ell) = 1$, so we can apply linearity to $f_\chi|T_\chi(\ell^2)$ (see Equation (14)) to define

$$f|T(\ell^2) := \sum_{n=1}^{\infty} \left(a(\ell^2 n) + \left(\frac{(-1)^k n}{\ell}\right) \ell^{k-1} a(n) + \ell^{2k-1} a\left(\frac{n}{\ell^2}\right)\right) q^n. \tag{52}$$

Since $f_\chi|T_\chi(\ell^2) \in S_{k+\frac{1}{2}}(\Gamma_0(N), \chi)$, we clearly have $f|T(\ell^2) \in S_{k+\frac{1}{2}}(\Gamma_1(N))$.

5.6 Serre's Theorem on Hecke Operators

Finally, we have the following theorem due to Serre, whose proof requires some theory of Galois representations associated to modular forms, so we do not have the background to prove it. However, it is an important tool in the main results of Ahlgren and Ono [2] and can be stated easily.

Theorem 5.17. *[22, 2] Let M, N be positive integers, and let $\mathcal{O}_K$ be the ring of integers in some number field K. Then, a positive density of primes $p \equiv -1 \pmod{MN}$ satisfy the following property: for all characters χ and functions $F_\chi \in S_k(\Gamma_0(N), \chi)$ with coefficients in $\mathcal{O}_K$,*

$$F_\chi(z)|T(p) \equiv 0 \pmod{M}.$$

We remark that while Serre only proved the result for an individual χ, Ahlgren and Ono [2] noted that Serre's proof can be straightforwardly modified to tackle the case of all χ simultaneously.

6 General Modular Congruences for the Partition Function

In this section, we use much of the theory developed on integral weight and half-integral weight modular forms to establish the existence of a large family of partition function congruences, as first done in [2]. Specifically, for any power of a prime that is at least 5, we will establish an infinite series of congruences modulo that prime power. While we have not developed much theory of half-integral weight modular forms and have merely stated results, we believe that the way that one proves these partition function congruences given the theory as a black box is still quite enlightening.

We briefly summarize the general method of proof. The first goal is to find some half-integral weight modular form F that has its coefficients congruent to values of the partition function modulo some prime power, which we do in Lemma 6.1. To do this, we will have to use many of the results in Subsections 5.1 and 5.2 to verify that certain functions we are defining verify the modular identity and are holomorphic/vanish at the cusps. Next, we use the Shimura correspondence to associate the form F we create in Lemma 6.1 to some integral weight modular forms, and use Serre's result on congruences of Hecke operators over integral weight modular forms to establish that $F|T(\ell^2) \equiv 0$ for infinitely many primes ℓ. Finally, we can look at how $T(\ell^2)$ acts on the q-series coefficients of F to get our desired result.

6.1 Proof of the General Modular Congruences

We first introduce some essential notation. Recall that for each prime $\ell \geq 5$, we had defined $\delta_\ell := \frac{\ell^2-1}{24}$. Moreover, we define $\mathbb{Z}[[q]]$ to be the ring of power series in $q = e^{2\pi i z}$, and we define $\varepsilon_\ell := (\frac{-6}{\ell}) = (\frac{\delta_\ell}{\ell})$ be the Legendre character. Finally, define

$$A_\ell := \left\{\beta \in \{0, 1, ..., \ell-1\} : \left(\frac{\beta + \delta_\ell}{\ell}\right) \neq \varepsilon_\ell\right\}.$$

Lemma 6.1. *Fix a prime $\ell \geq 5$ and positive integer r. If $\beta \in A_\ell$, then there is a integer $k \geq 2$ and a modular form $F(z) \in S_{k+\frac{1}{2}}(\Gamma_1(576\ell^4)) \cap \mathbb{Z}[[q]]$ such that*

$$F(z) \equiv \sum_{n=0}^{\infty} p(\ell n + \beta) q^{24\ell n + 24\beta - 1} \pmod{\ell^r}.$$

Proof. First, note that by Lemma 5.10, we have for all $t \in \mathbb{N}$,

$$E_{\ell,t}(z) := \frac{\eta^{\ell^t}(z)}{\eta(\ell^t z)} \in M_{(\ell^t-1)/2}\left(\Gamma_0(\ell^t), \left(\frac{(-1)^{(\ell^t-1)/2} \cdot \ell^t}{\cdot}\right)\right).$$

We define $\chi_{\ell,t}$ to be the above character. By Proposition 5.2, we have that $E_{\ell,t}$ vanishes (i.e. has positive order) at all cusps of $\Gamma_0(\ell^t)$ that are not $\Gamma_0(\ell^t)$-equivalent to $i\infty$.

Moreover, note that

$$E_{\ell,t} = \prod_{n\geq 1} \frac{(1-q^n)^{\ell^t}}{(1-q^{n\cdot\ell^t})} \equiv 1 \pmod{\ell}$$

since $(1-X)^{\ell^t} \equiv (1-X^{\ell^t}) \pmod{\ell}$ by the Frobenius endomorphism theorem. Note that for any q-series $f \equiv 1 \pmod{\ell^s}$, we have that if $f = 1 + \ell^s \cdot g$, $f^n = (1+\ell^s \cdot g)^\ell = 1 + \ell^{s+1} g + \ell^{2s}\binom{\ell^s}{2} g^2 + ... \equiv 1 \pmod{\ell^{s+1}}$. Thus, by inducting on s, we have that for all $s, t \in \mathbb{N}$,

$$E_{\ell,t}^{\ell^s} \equiv 1 \pmod{\ell^{s+1}}. \tag{53}$$

Next, define

$$f_\ell(z) := \frac{\eta^\ell(\ell z)}{\eta(z)} \in M_{(\ell-1)/2}\left(\Gamma_0(\ell), (\tfrac{\bullet}{\ell})\right) \tag{54}$$

which is true by Lemma 5.11. Letting $f_\ell = \sum_{n\geq 0} a(n)q^n$, Equation (54) and the product formula for the partition function (see Equation (15)) give us

$$\sum_{n=0}^{\infty} a(n)q^n = q^{(\ell^2-1)/24} \cdot \prod_{n=1}^{\infty} \frac{\left(1-q^{\ell n}\right)^\ell}{(1-q^n)} = \left(\sum_{n=0}^{\infty} p(n)q^{n+\delta_\ell}\right) \cdot \prod_{n=1}^{\infty}\left(1-q^{\ell n}\right)^\ell. \tag{55}$$

Next, define $\tilde{f}_\ell(z)$ by

$$\tilde{f}_\ell(z) := \sum_{n=0}^{\infty}\left(1-\varepsilon_\ell\left(\frac{n}{\ell}\right)\right)a(n)q^n, \tag{56}$$

for $(\frac{n}{\ell})$ representing the Legendre symbol. By Proposition 5.7, we have that $\sum\left(\frac{n}{\ell}\right)a(n)q^n \in M_{(\ell-1)/2}\left(\Gamma_0(\ell^3), (\frac{\bullet}{\ell})\right)$, which implies $\tilde{f}_\ell(z) \in M_{(\ell-1)/2}\left(\Gamma_0(\ell^3), (\frac{\bullet}{\ell})\right)$. By Equation (55), we know that $a(n) = 0$ for all $n < \delta_\ell$. Moreover, since $\varepsilon_\ell \cdot \left(\frac{\delta_\ell}{\ell}\right) = 1$, by (56), we have that $\tilde{f}$ has order at least $\delta_\ell + 1$ at $i\infty$. Now, if we define $f_{\ell,s}(z) := E_{\ell,3}^{\ell^s}(z) \cdot \tilde{f}_\ell(z)$, then $f_{\ell,s}(z)$ is a cusp form for $s \geq 1$ since $E_{\ell,3}$ vanishes at all cusps not equivalent to $i\infty$ in $\Gamma_0(\ell^3)$ by Proposition 5.2, so

$$f_{\ell,s}(z) \in S_{s\cdot(\ell^3-1)/2+(\ell-1)/2}\left(\Gamma_0(\ell^3), \chi_{\ell,t}^{\ell^s}\cdot\left(\frac{\bullet}{\ell}\right)\right) = S_{s'}\left(\Gamma_0(\ell^3), \chi_{\ell,t}\cdot\left(\frac{\bullet}{\ell}\right)\right)$$

for $s' = \frac{1}{2}\left(s(\ell^3-1)+(\ell-1)\right)$. Moreover, $\mathrm{ord}_{i\infty}(f_{\ell,s}(z)) \geq \delta_\ell + 1$ and if s is sufficiently large, $\mathrm{ord}_\alpha(f_{\ell,s}(z)) > \mathrm{ord}_\alpha(\eta^\ell(\ell z))$ for all $\alpha \in \mathbb{Q}$ not $\Gamma_0(\ell^3)$-equivalent to $i\infty$. Finally, by Equation (53), we have that $f_{\ell,s}(z) \equiv \tilde{f}_\ell(z) \pmod{\ell^r}$ if $s \geq r-1$.

Therefore, for sufficiently large $s \in \mathbb{N}$, we have that $f_{\ell,s}(z)/\eta^\ell(\ell z)$ vanishes at all cusps, since $\eta^\ell(\ell z)$ has order $\frac{\ell^2}{24} = \delta_\ell + \frac{1}{24}$ at $i\infty$. Therefore, $f_{\ell,s}(24z)/\eta^\ell(24\ell z)$ must also vanish at all cusps by Corollary 5.4. Moreover, since $f_{\ell,s}(z) \in S_{s'}(\Gamma_0(\ell^3), \chi)$ for some χ and $\eta(24z) \in S_{1/2}(\Gamma_0(576), \chi_{12})$ by Proposition 5.12, we have $f_{\ell,s}(24z)/\eta^\ell(24\ell z) \in S_{s'-\ell/2}(\Gamma_0(576\ell^3), \chi')$ for some χ' by Proposition 5.8. Now, since $f_{\ell,s}(z) \equiv \tilde{f}\ell(z) \pmod{\ell^r}$, by Equations (55) and (56) and by replacing z with $24z$,

$$\begin{aligned}\frac{f_{\ell,s}(24z)}{\eta^\ell(24\ell z)} &\equiv \left(\sum_{n=0}^{\infty} p(n)\left(1-\varepsilon_\ell\left(\frac{n+\delta_\ell}{\ell}\right)\right)q^{24(n+\delta_\ell)}\right)\cdot\prod_{n=1}^{\infty}\left(1-q^{24\ell n}\right)^\ell \cdot q^{-\ell^2}\prod_{n=1}^{\infty}\left(1-q^{24\ell n}\right)^{-\ell} \\ &\equiv \sum_{n\equiv -\delta_\ell \pmod{\ell}} p(n)q^{24n-1} + 2\sum_{(\frac{n+\delta_\ell}{\ell})=-\varepsilon_\ell} p(n)q^{24n-1} \pmod{\ell^r}.\end{aligned}$$

The Lemma follows by looking at the terms with q^n where $n \equiv 24\beta - 1 \pmod{24\ell}$ and using Proposition 5.5 and the definition of A_ℓ. □

Lemma 6.2. *Suppose that $f(z) = \sum_{n\geq 1} a(n)q^n$ is a cusp form in $S_{k+\frac{1}{2}}(\Gamma_1(N))$ for some $k \geq 2$ such that $a(n)$ is an algebraic integer for all $n \geq 1$. Then, for all $m \in \mathbb{N}$, a positive proportion of the primes $\ell \equiv -1 \pmod{m \cdot N}$ have the property that $f(z)|T(\ell^2) \equiv 0 \pmod{m}$.*

Proof. By Proposition 5.9, since $f \in \mathbb{Z}[[q]]$, we can write $f(z) = \sum_{\chi \text{ even}} a_\chi f_\chi(z)$ for a_χ algebraic numbers and $f_\chi \in S_{k+\frac{1}{2}}(\Gamma_0(N), \chi)$ having algebraic integer coefficients in $\mathcal{O}_K$, the ring of integers of some number field K, for all χ. There exists some integer r such that $r \cdot a_\chi$ is an algebraic integer for all χ, so replacing f with $r \cdot f$ and m with $r \cdot m$, we can assume a_χ is an algebraic integer for all χ. Thus, it suffices to show that a positive proportion of primes $\ell \equiv -1 \pmod{m \cdot N}$ satisfy $f_\chi(z)|T(\ell^2) \equiv 0 \pmod{m}$ for all $f_\chi \in S_{k+\frac{1}{2}}(\Gamma_0(N), \chi)$. This is because the Hecke operator $T(\ell^2)$ over $S_{k+\frac{1}{2}}(\Gamma_1(N))$ is just defined as a linear combination of the corresponding Hecke operators over $S_{k+\frac{1}{2}}(\Gamma_0(N), \chi)$ by Equation (52), since $\ell \equiv -1 \pmod{N}$.

We know by Theorem 5.17 that a positive proportion of primes $\ell \equiv -1 \pmod{m \cdot N}$ satisfy the following: all $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ and all $F(z) \in S_{2k}(\Gamma_0(N), \chi)$ with coefficients in $\mathcal{O}_K$ satisfy

$$F|T(\ell) \equiv 0 \pmod{m}. \tag{57}$$

Now, by Theorem 5.16, we have that $S_t(f_\chi) \in S_{2k}(\Gamma_0(N), \chi^2)$ for all χ, and by Proposition 5.14, $S_t(f_\chi)$ has algebraic integer coefficients in some number field $K' \supseteq K$ for all t. Therefore, for a positive proportion of primes $\ell \equiv -1 \pmod{m \cdot N}$,

$$S_t(f_\chi)|T(\ell) \equiv 0 \pmod{m} \text{ for all } \chi, t. \tag{58}$$

Therefore, by the commutativity of the correspondence in Theorem 5.16, we have $S_t(f_\chi|T(\ell^2)) \equiv 0 \pmod{m}$ for all χ, t and any ℓ satisfying (58), which means that by Corollary 5.15, $f_\chi|T(\ell^2) \equiv 0 \pmod{m}$ for any ℓ satisfying (58), which is precisely what we wished to show. □

We can now establish general partition function congruences using Lemmas 6.1 and 6.2.

Theorem 6.3. *Let $m \geq 5$ be prime, r be a positive integer, and suppose $0 \leq \beta \leq m-1$ is in A_m. Then, a positive proportion of primes $\ell \equiv -1 \pmod{24m}$ satisfy*

$$p\left(\frac{\ell^3 n + 1}{24}\right) \equiv 0 \pmod{m^r}$$

for all $n \equiv 1 - 24\beta \pmod{24m}$ such that $\ell \nmid n$.

Proof. We apply Lemma 6.2 to the modular forms $F(z)$ in Lemma 6.1 as follows. For our prime m and integer β, let $F_{m,r,\beta}(z)$ to be our form $F \in S_{k+\frac{1}{2}}(\Gamma_1(576m^4)) \cap \mathbb{Z}[[q]]$ such that

$$F_{m,r,\beta}(z) \equiv \sum_{n=0}^{\infty} p(mn+\beta) q^{24mn+24\beta-1} = \sum_{\substack{n=0 \\ n \equiv (24\beta-1) \pmod{24m}}}^{\infty} p\left(\frac{n+1}{24}\right) q^n \pmod{m^r}.$$

Therefore, a positive proportion of primes $\ell \equiv -1 \pmod{576m^4 \cdot m^r}$, and thus, a positive proportion of primes $\ell \equiv -1 \pmod{24m}$, satisfy $F_{m,r,\beta}(z)|T(\ell^2) \equiv 0 \pmod{m^r}$.

Using the definition of the Hecke operator for weight $k + \frac{1}{2}$ modular forms, if we define $a(n)$ such that $F_{m,r,\beta}(z) =: \sum_{n \geq 1} a(n) q^n$, then

$$F_{m,r,\beta}|T(\ell^2) = \sum_{n=1}^{\infty} \left(a(\ell^2 n) + \left(\frac{(-1)^k n}{\ell}\right) \ell^{k-1} + \ell^{2k-1} a\left(\frac{n}{\ell^2}\right) \right) q^n.$$

Define $n' := \ell \cdot n$. If $\ell \nmid n$, we have the $q^{n'}$-coefficient of $F_{m,r,\beta}|T(\ell^2)$ modulo m^r equals

$$a(\ell^3 n) + \left(\frac{(-1)^k n\ell}{\ell}\right) \ell^{k-1} + \ell^{2k-1} a\left(\frac{n}{\ell}\right) = a(\ell^3 n) = p\left(\frac{\ell^3 n + 1}{24}\right) \equiv 0 \pmod{m^r},$$

assuming that $\ell^3 n \equiv (24\beta - 1) \pmod{24m}$. However, since $\ell \equiv -1 \pmod{24m}$, we have this congruence whenever $n \equiv 1 - 24\beta \pmod{24m}$ and $\ell \nmid n$. □

This implies the following incredible result.

Corollary 6.4. *For any integer m such that $\gcd(6, m) = 1$, there exists integers $a \in \mathbb{N}, 0 \le b \le a-1$ such that $p(an + b) \equiv 0 \pmod{m}$ for all nonnegative integers n.*

Proof. Write $m = \prod m_i^{r_i}$ where $r_i \in \mathbb{N}$ and m_i are primes. For each m_i, by Theorem 6.3, there exists infinitely many primes $\ell \equiv -1 \pmod{24m_i}$ and some integer $0 \le \beta \le m-1$ such that

$$p\left(\frac{\ell^3(24m_i n + 1 - 24\beta) + 1}{24}\right) = p\left(\ell^3 m_i n + \frac{\ell^3 + 1}{24} - \ell^3\beta\right) \equiv 0 \pmod{m_i^{r_i}},$$

as long as $\ell \nmid (24m_i n + 1 - 24\beta)$. Since ℓ, m_i, and 24 are pairwise relatively prime, we can choose $0 \le \kappa \le \ell - 1$ such that $\ell \nmid (24m_i n + 1 - 24\beta)$ whenever $n \equiv \kappa \pmod{\ell}$. Thus, for infinitely many primes $\ell \equiv -1 \pmod{24m_i}$, there exist $0 \le \beta \le m-1, 0 \le \kappa \le \ell - 1$ such that

$$p\left(\ell^4 m_i n + \ell^3 m_i \kappa + \frac{\ell^3 + 1}{24} - \ell^3\beta\right) \equiv 0 \pmod{m_i^{r_i}}.$$

To finish, for each m_i choose $\ell_i = \ell$ such that all m_i's and ℓ_i's are distinct (which can be done as there are infinitely many choices for ℓ for each m_i). Finally, apply Chinese Remainder theorem. □

6.2 Summary

The previous result is incredibly powerful, as it not only develops a framework to explain most previously known congruences modulo primes $m \le 31$, but also allows us to show there are congruences modulo all prime powers except for powers of 2 and 3 and even all integers modulo any integer relatively prime to 6! One weakness of this method, however, is that we are using Serre's theorem on Hecke operators to establish that there is a positive density of primes ℓ such that $F|T(\ell^2) \equiv 0 \pmod{m^r}$, but we do not get any explicit primes ℓ. Therefore, to find more explicit congruences, we may need use slightly different constructions of functions F which are already known to satisfy $F|T(\ell^2) \equiv 0$. This is what we will do in Section 7, which will give us a large number of congruences, though only modulo primes which are at most 31.

7 Computing Explicit Congruences

As we noted in Subsection 6.2, the results of [2] do not give us explicit congruences of the partition function. In this section, we follow the results of [30] to give explicit partition function congruences.

7.1 Method to find Explicit Congruences

Definition 7.1. For primes $13 \le m \le 31$, define $f_m(z)$ as

$$f_m(z) := \begin{cases} 11\eta^{11}(24z) & m = 13 \\ 7\eta^{7}(24z)E_4(24z) & m = 17 \\ 5\eta^{5}(24z)E_6(24z) & m = 19 \\ \eta(24z)E_{10}(24z) & m = 23 \\ 8\eta^{19}(24z)E_4(24z) & m = 29 \\ 10\eta^{17}(24z)E_6(24z) & m = 31 \end{cases}.$$

We have the following, although we have not built the theory required to prove the second part.

Theorem 7.2. *[13, Proposition 6] For all primes $13 \le m \le 31$, we have $f_m(z) \in S_{\frac{m-2}{2}}(\Gamma_0(576), \chi_{12})$. Moreover, $f_m(z)$ is an eigenform of of the Hecke operator $T(\ell^2)$ for all primes ℓ.*

Proof. The first part is true since $\eta(24z) \in S_{1/2}(\Gamma_0(576), \chi_{12})$ by Proposition 5.12, and since $E_4(z) \in M_4(SL_2(\mathbb{Z}))$ and $E_6(z) \in M_6(SL_2(\mathbb{Z}))$, we have that $E_4(24z) \in M_4(\Gamma_0(576))$ and $E_6(24z) \in M_6(\Gamma_0(576))$ by Proposition 5.8. The second part requires a deeper understanding of the theory of half-integral weight *newforms*, which we have not introduced, so we do not prove it here. □

We note that the above result means we do not have to use Theorems 5.16 or 5.17 to convert to the integral weight case, as done in Section 6.

Proposition 7.3. *For primes $13 \le m \le 31$, we have*

$$\sum_{n=\lfloor m/24 \rfloor}^{\infty} p(mn + m - \delta_m)q^{24n+(24-m)} \equiv f_m(z) \pmod{m}.$$

Proof. Recall from Definition 4.7 that $F(m, 1; z) = \sum_{24|(mn+1)} p\left(\frac{mn+1}{24}\right) q^n \pmod{m}$. As $m^2 \equiv 1 \pmod{24}$, we have $mn+1 \equiv 0$ if and only if $n \equiv -m \pmod{24}$. Thus, writing $n = 24n' + (24-m)$, we have $p\left(\frac{mn+1}{24}\right) = p(mn' + m - \delta_m)$, so we clearly have $\sum p(mn+m-\delta_m)q^{24n+(24-m)} = F(m, 1; z)$. Therefore, Equations (29) and (33) for $k = 0$ have already proven the proposition for the cases $m = 13$ and $m = 17$. We note that we used the same logic to arrive at the cases $m = 19, 23, 29, 31$ to attain equations (37), (39), (41), and (43), so the proposition is true for all primes $13 \le m \le 31$. We start the summation from $n = \lfloor m/24 \rfloor$ so that $mn+m-\delta_m$ and $24n+(24-m)$ are nonnegative. □

Using Theorem 7.2 and Proposition 7.3, we can prove the main theorem of this section.

Theorem 7.4. *Let $m, \ell \ge 5$ be primes and suppose that $f_m(z)$ satisfies $f|T(\ell^2) \equiv \lambda_{\ell,m} f \pmod{m}$ for some integer $\lambda_{\ell,m}$. If $\lambda_{\ell,m} \equiv 0 \pmod{m}$, then for all n such that $\ell \nmid n$ and $n \equiv -(\ell m) \pmod{24}$,*

$$p\left(\frac{m\ell^3 n + 1}{24}\right) \equiv 0 \pmod{m}.$$

If $\lambda_{\ell,m} \equiv \omega \cdot \ell^{(m-5)/2} \pmod{m}$ *for* $\omega \in \{\pm 1\}$, *then for all* n *such that* $\ell \nmid n$, $n \equiv -m \pmod{24}$, *and* $\chi_{12}(\ell)\left(\frac{(-1)^{(m-3)/2}n}{\ell}\right) = \omega$,

$$p\left(\frac{m\ell^2 n + 1}{24}\right) \equiv 0 \pmod{m}.$$

Proof. Let $a_m(n)$ represent the q^n-coefficient in f_m. Then, we have

$$\sum_{n=0}^{\infty} a_m(n)q^n \equiv \sum_{\substack{n \geq 0 \\ 24|(mn+1)}} p\left(\frac{mn+1}{24}\right) q^n \pmod{m}.$$

Since f_m is a half-integral weight modular form, we can apply the $T(\ell^2)$ Hecke operator to $f(z)$ to get that if $f_m(z)|T(\ell^2) \equiv \lambda_m f(z) \pmod{m}$, then for all $n \geq 0$,

$$\lambda_{\ell,m} a_m(n) \equiv a_m(\ell^2 n) + \chi_{12}(\ell)\left(\frac{(-1)^{\frac{m-3}{2}} n}{\ell}\right) \ell^{\frac{m-5}{2}} a_m(n) + \chi_{12}(\ell^2)\ell^{m-4} a_m(n/\ell^2) \pmod{m}. \quad (59)$$

Suppose first that $\lambda_{\ell,m} \equiv 0 \pmod{m}$. If we assume $\ell \nmid n$ and define $n' := \ell \cdot n$, we get $a_m(n'/\ell^2) = 0$ and $\left(\frac{(-1)^{(m-3)/2}n'}{\ell}\right) = 0$ (as a Kronecker symbol) as $\ell | n'$ but $\ell^2 \nmid n'$. Therefore, evaluating the $q^{n'}$-coefficient and using (59) gives us

$$0 \equiv \lambda_{\ell,m} a_m(n') \equiv \lambda_{\ell,m} a_m(\ell n) \equiv a_m(\ell^3 n) \pmod{m}$$

for all $\ell \nmid n$ and $24|(m\ell^3 n + 1)$. Since $2, 3 \nmid \ell, m$, we have that for all $n \equiv -\ell m \pmod{24}$ and $\ell \nmid n$,

$$p\left(\frac{m\ell^3 n + 1}{24}\right) \equiv 0 \pmod{m}.$$

Next, suppose that $\lambda_{\ell,m} \equiv \omega \ell^{(m-5)/2} \pmod{m}$, where $\omega \in \{\pm 1\}$. If we choose n so that $\ell \nmid n$ but $\chi_{12}(\ell)\left(\frac{(-1)^{(m-3)/2}n}{\ell}\right) = \omega$, then we have $a_m(n/\ell^2) = 0$ and therefore, we have

$$\omega \ell^{\frac{m-5}{2}} a_m(n) \equiv \lambda_{\ell,m} a_m(n) \equiv a_m(\ell^2 n) + \omega \ell^{\frac{m-5}{2}} a_m(n) \pmod{m} \Rightarrow 0 \equiv a_m(\ell^2 n) \pmod{m}.$$

Therefore, if we additionally have $24|m(\ell^2 n) + 1$, i.e. $n \equiv -m \pmod{24}$, we get

$$p\left(\frac{m\ell^2 n + 1}{24}\right) \equiv 0 \pmod{m}. \qquad \square$$

7.2 Examples and Methods of Computation

Weaver [30] used Theorem 7.4 and some computation to show numerous explicit congruences modulo primes $13 \leq m \leq 31$ (see [30, Theorems 1-2]). We will give examples and explain how one can determine all the congruences she did with explicit computation.

First, suppose we can compute the partition function $p(n)$ modulo m for all primes $13 \leq m \leq 31$ and all $n \leq 7.5 \times 10^6$ (as done in [30]). We know from Proposition 7.3 (or our definition of f_m) that the first nonzero q^n-coefficient modulo m of $f_m(z)$ is at $24(\lfloor \frac{m}{24} \rfloor + 1) - m$. Defining

$r_m = 24(\lfloor \frac{m}{24} \rfloor + 1) - m$, since $r_m \ell^2 \equiv -m \pmod{24}$ and since r_m is squarefree and therefore isn't divisible by ℓ^2, we can use (7.2) to get

$$\begin{aligned}\lambda_{\ell,m} &\equiv \frac{a_m(\ell^2 r_m)}{a_m(r_m)} + \chi_{12}(\ell)\left(\frac{(-1)^{(m-3)/2} r_m}{\ell}\right)\ell^{(m-5)/2} \\ &\equiv \frac{p(m\ell^2\lfloor\frac{m}{24}\rfloor + m\delta_\ell(24-m) + m - \delta_m)}{p(m\lfloor\frac{m}{24}\rfloor + m - \delta_m)} + \chi_{12}(\ell)\left(\frac{(-1)^{(m-3)/2} r_m}{\ell}\right)\ell^{(m-5)/2} \pmod{m}.\end{aligned}$$

Thus, we can use Proposition 7.3 to find the value of $\lambda_{\ell,m}$ as long as $m\ell^2\lfloor\frac{m}{24}\rfloor + m\delta_\ell(24-m) + m - \delta_m \le 7.5 \times 10^6$), and then verify if $\lambda_{\ell,m} \equiv 0$ or $\lambda_{\ell,m} \equiv \pm\ell^{(m-5)/2} \pmod{m}$, which can be done extremely quickly since ℓ will never exceed 10^4, even if we replace 7.5×10^6 with 1.5×10^7.

We in fact ran the algorithm until 1.5×10^7 to find potentially new congruences, of which there were several. (See Appendix A, where we list all pairs (ℓ, m) that we find with $\lambda_{\ell,m} \in \{0, \pm\ell^{(m-5)/2}\} \pmod{m}$). For instance, one can show $\lambda_{3881,23} \equiv 0 \pmod{23}$. Therefore, for all n such that $3881 \nmid n$ and $n \equiv 17 \pmod{24}$, we get $p\left(\frac{23(3881)^3 n+1}{24}\right) \equiv 0 \pmod{23}$. If we were to choose $n' = 24 \cdot n + 17$ and replace n with n', we would get that for all n such that $24n \not\equiv -17 \pmod{3881}$,

$$p\left(\frac{23 \cdot 3881^3 \cdot (24 \cdot n + 17) + 1}{24}\right) = p\left(23 \cdot 3881^3 n + \frac{23 \cdot 3881^3 \cdot 17 + 1}{24}\right) \equiv 0 \pmod{23}. \quad (60)$$

As an example of the second case, one can show that $\lambda_{727,31} \equiv 727^{13} \equiv 28 \pmod{31}$, so $\omega = 1$ as per the notation of Theorem 7.4. As $31 \equiv 3 \pmod 4$ and $727 \equiv 7 \pmod{12}$, we have for all n such that $(\frac{n}{727}) = -1$ and $n \equiv 17 \pmod{24}$, $p\left(\frac{31 \cdot 727^2 \cdot n+1}{24}\right) \equiv 0 \pmod{31}$. If we choose $n' = 24 \cdot 727 \cdot n + 41$, for instance, since $(\frac{41}{727}) = -1$, and replace n with n', we get the congruence

$$p\left(\frac{31 \cdot 727^2 \cdot (24 \cdot 727n + 41)}{24}\right) = p\left(31 \cdot 727^3 n + \frac{31 \cdot 727^2 \cdot 41 + 1}{24}\right) \equiv 0 \pmod{31}. \quad (61)$$

We can replace 41 with several other numbers, so the pair $(\ell, m) = (727, 31)$ will give numerous congruences that we haven't listed.

We finally note how to efficiently compute the values of $p(n)$ modulo m for all $n \le 1.5 \times 10^7$, $13 \le m \le 31$. Recall Euler's pentagonal number theorem, which tells us

$$\prod_{n=1}^{\infty}(1 - q^n) = \sum_{k=-\infty}^{\infty}(-1)^k q^{k(3k-1)/2}. \quad (62)$$

Therefore, to compute the partition function, we just have to compute the inverse of the right hand side of (51) modulo m. However, since the sum has $O(\sqrt{n})$ nonzero terms less than n and has leading coefficient 1, we can compute $p(n)$ in $O(\sqrt{n})$ time given $p(1), ..., p(n-1)$ by forcing the q^n-term of $\left(\sum_{n\ge 0} p(n)q^n\right) \cdot \left(\sum_{k\in\mathbb{Z}}(-1)^k q^{k(3k-1)/2}\right)$ to be 0 for all $n \ge 1$. Therefore, computing the partition function modulo m for all $n \le N$ takes $O(N^{3/2})$ time. If we define $M = 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31$, $M < 10^8$, so we can do the computations modulo M, and therefore, modulo all primes simultaneously, with 32-bit integers. (The runtime in my simulation in Java, for instance, took slightly over 10 minutes). We end by making a quick note that the partition function can actually be computed even faster asymptotically modulo certain primes, using Fast Fourier Transform methods [8], though this will not help in our case.

References

[1] S. Ahlgren and M. Boylan. Arithmetic properties of the partition function. *Invent. math.* 153: 487–502, 2003.

[2] S. Ahlgren and K. Ono. Congruence properties for the partition function. *Proc. Natl. Acad. Sci.* 98(23): 12882–12884, 2001.

[3] A. O. L. Atkin. Proof of a Conjecture of Ramanujan. *Glasgow Math. J.* 8: 14–32, 1967.

[4] A. O. L. Atkin. Multiplicative congruence properties and density problems for $p(n)$. *Proc. London Math. Soc.* 3: 563–576, 1968.

[5] A. O. L. Atkin and J. N. O'Brien. Some properties of $p(n)$ and $c(n)$ modulo powers of 13. *Trans. Amer. Math. Soc.* 126: 442–459, 1967.

[6] B. C. Berndt. Ramanujan's congruences for the partition function modulo 5, 7, and 11. *Int. J. Number Theory*, 3: 349-–354, 2007.

[7] K. Buzzard. Notes on modular forms of half-integral weight. 2013.

[8] N. Calkin, J. Davis, K. James, E. Perez, and C. Swannack. Computing the integer partition function. *Math. Comput.* 76(259): 1619–1638, 2007.

[9] B. Cipra. On the Niwa-Shintani theta kernel lifting of modular forms, *Nagoya Math. J.* 91: 49–117, 1983.

[10] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko, and M. Viazovska. The sphere packing problem in dimension 24. *Ann. Math.* 185: 1017–1033, 2017.

[11] G. Cornell, J. H. Silverman, and G. Stevens. Modular Forms and Fermat's Last Theorem. Springer, 1997.

[12] F. Diamond and J. Shurman. A First Course in Modular Forms. Springer New York, 2005.

[13] L. Guo and K. Ono. The partition function and the arithmetic of certain modular L-functions. *Int. Math. Res. Notices* 21: 1179–1197, 1999.

[14] R. Murty. Problems in Analytic Number Theory, 2nd ed. Springer, 2008.

[15] R. Murty, M. Dewar, and H. Graves. Problems in the Theory of Modular Forms. Springer, 2016.

[16] M. Newman. Construction and application of a certain class of modular functions. *Proc. London Math. Soc.* 7 (3): 334–350, 1956.

[17] S. Niwa. Modular forms of half integral weight and the integral of certain theta functions, *Nagoya Math. J.* 56: 147–161, 1975.

[18] K. Ono. Distribution of the partition function modulo m. *Ann. Math.* 151: 293–307, 2000.

[19] K. Ono. Private Communication. 2019.

[20] K. Ono and C. Skinner. Fourier coefficients of half-integral weight modular forms modulo ℓ. *Ann. Math.* 147 (2), 453–470, 1998.

[21] S. Ramanujan. Congruence properties of partitions, *Proc. London Math. Soc.* 19: 207–210, 1919.

[22] J.-P. Serre. Divisibilité de certaines fonctions arithmétiques, *L'Ensein. Math.* 22: 227–260, 1976.

[23] J.-P. Serre and H. M. Stark. Modular forms of weight 1/2. In *Modular functions of one variable, VI* (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Lecture Notes in Math 627: 27–67, 1977.

[24] G. Shimura. On modular forms of half integral weight. *Ann. Math.* 97: 440–481, 1973.

[25] J. Sturm. On the congruence of modular forms. In *Number Theory, Lecture Notes in Mathematics* 1240: 275–280, 1987.

[26] H. P. F. Swinnerton-Dyer. On ℓ-adic representations and congruences for coefficients of modular forms. In *Modular Functions of One Variable III*: 1–55, 1972.

[27] I. Varma. Sums of squares, modular forms, and Hecke characters (Master's dissertation). 2010.

[28] M. S. Viazovska. The sphere packing problem in dimension 8. *Ann. Math.* 185: 991–1015, 2017.

[29] G. N. Watson. Ramanujans Vermutung über Zerfällungsanzahlen. *J. Reine Angew. Math.* 179: 97–128, 1938.

[30] R. Weaver. New congruences for the partition function. *Ramanujan J.* 5: 53–63, 2001.

A Table of (ℓ, m) that Give Explicit Congruences

Here, we list all pairs of primes (ℓ, m) such that $13 \le m \le 31$, $m\ell^2\lfloor \frac{m}{24} \rfloor + m\delta_\ell(24-m) + m - \delta_m \le 1.5 \times 10^7$, and $\lambda_{\ell,m}$, as defined in Theorem 7.4, is congruent modulo m to 0, $\ell^{(m-5)/2}$, or $-\ell^{(m-5)/2}$. By Theorem 7.4, we can establish interesting congruences for all such ℓ, m that we have listed.

Note that we are including all pairs listed in [30, Theorems 1-2], and that the $\epsilon \in \{\pm 1\}$ defined in [30, Theorem 2] is different from the $\omega \in \{\pm 1\}$ such that $\lambda_{\ell,m} \equiv \omega \ell^{(m-5)/2} \pmod{m}$.

m	ℓ: $\lambda_{\ell,m} \equiv 0 \pmod{m}$	ℓ: $\lambda_{\ell,m} \equiv \ell^{(m-5)/2} \pmod{m}$	ℓ: $\lambda_{\ell,m} \equiv -\ell^{(m-5)/2} \pmod{m}$
13	59, 73, 131, 167, 389, 433, 479, 563, 587, 673, 691, 719, 859, 1091, 1297, 1319, 1549, 1579	97, 109, 191, 251, 397, 463, 769, 823, 839, 991, 1223, 1229, 1231, 1291, 1307, 1361, 1367	103, 241, 283, 409, 439, 727, 751, 809, 1063, 1259, 1277, 1321, 1409, 1543
17	41, 89, 103, 433, 571, 607, 677, 701, 743, 887, 1013, 1109, 1187, 1283, 1301, 1487 1667	23, 67, 107, 191, 293, 359, 373, 587, 641, 1093, 1511	127, 151, 709, 929, 1031, 1123, 1249, 1279, 1381, 1409, 1429, 1499, 1619, 1669
19	101, 191, 211, 337, 349, 739, 1129, 1193, 1249, 1381, 1511, 1637, 1777, 1823, 1933	61, 109, 193, 269, 631, 647, 673, 857, 929, 977, 1103, 1373, 1663, 1667, 1783	13, 23, 97, 103, 137, 271, 431, 571, 827, 919, 1093, 1153, 1217, 1277, 1291, 1549, 1657, 1753
23	5, 19, 37, 47, 67, 179, 239, 353, 599, 761, 853, 997, 1319, 1493, 1553, 1789, 1997, 2239, 2731, 3319, 3541, 3547, 3881	587, 593, 673, 757, 769, 1823, 2503, 2549, 2687, 2749, 2803, 2897, 3001, 3413	107, 421, 503, 661, 857, 911, 1049, 1277, 1381, 1531, 1663, 1753, 1847, 1933, 1993, 3307, 3461, 3571, 3793
29	331	17, 139, 193, 443, 631, 691, 701, 773	41, 137, 227, 229, 347, 367, 431, 439, 509, 577
31	107, 229, 283, 383, 463	101, 193, 271, 587, 727	179, 181, 239

Table 1: Table of (ℓ, m) depending on the comparison of $\lambda_{\ell,m}$ to $\ell^{(m-5)/2} \pmod{m}$.