Congruences for the Coefficients of Modular Forms and Applications to Number Theory

By

Karl Mahlburg

A dissertation submitted in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

(Mathematics)

at the

UNIVERSITY OF WISCONSIN – MADISON

2006

Abstract

In 1944, Freeman Dyson proposed the existence of a "crank" statistic that would give a combinatorial explanation for all three of the famous Ramanujan congruences for the partition function $p(n)$. There was a 40 year wait before Dyson's dream was realized by Andrews and Garvan in 1988, when they defined the crank and proved that it decomposed Ramanujan's congruences in a natural way. In 2000, there was another dramatic development in the subject of partition theory, as Ono proved that $p(n)$ satisfies infinitely many congruences in distinct arithmetic progressions. This again led to the question of how these new families might be explained combinatorially. One of the main theorems of this thesis proves that the same crank defined by Andrews-Garvan satisfies precisely the same type of congruences as those found by Ono for the partition function, and is thus a sort of "universal" statistic for partition congruences.

Ramanujan also studied the divisibility properties of the coefficients of the classical Eisenstein series $E_k(z)$. These coefficients are essentially divisor sums when properly normalized. The inverses of these series are not holomorphic, but the theory of ℓ-adic modular forms can be used to study the divisibility properties of quotients of Eisenstein series. The main result here is the existence of positive density sets of primes ℓ for which almost all of the coefficients of these quotients vanish modulo powers of ℓ.

These results demonstrate two important applications of modular forms in number theory, and the techniques used here naturally apply to more general classes of modular forms. The analytic modular transformation properties are a powerful tool for understanding the coefficients of these and many other number-theoretic functions.

Acknowledgements

I would like to thank my doctoral advisor Ken Ono for his support and guidance. I also thank the generous support of the National Science Foundation through both a Graduate Research Fellowship and a VIGRE Graduate Research Fellowship.

Contents

Chapter 1

Introduction

The applications of modular forms to modern number theory are as widespread as they are important. Some of the earliest developments in the subject include the study of theta functions, the generating functions for class numbers, representations by quadratic forms, the analytic properties modular L-functions, and elliptic functions. These areas have been driving forces in number theory since the 19th century, and continue to influence active research throughout the subject. More recently, modular forms have maintained their fundamental importance in the proofs of many groundbreaking results, including the works of Fields medalists Borcherds and Deligne on the connections between the coefficients of modular forms and Galois representations, and also in Wiles' proof of Fermat's Last Theorem. See [26] for more discussion of the breadth of number theory topics in which modular forms have made valuable contributions.

In many of these settings, modular forms arise as the generating functions of number theoretic functions, and thus the arithmetic of the coefficients of modular forms is very important. Loosely speaking, a modular form is a function on the complex upper-half plane that has a Fourier series and that satisfies certain analytic transformation properties. The power of modular forms in applications to number theory is in the modular transformation laws, which can "translate" the analytic properties of the function into remarkable combinatorial relationships among the coefficients.

The results of this thesis expand upon some of the author's previously published works that highlight the interplay between the analytic and combinatorial properties of two well-known examples of modular forms. First is the family of classical Eisenstein series, which have simple divisor sums as coefficients. In [22], the author considered simple quotients of Eisenstein series and proved divisibility properties for their coefficients for infinite families of primes. The second example is the partition function, whose generating function is very nearly the inverse of another important modular form, namely, Dedekind's eta-function. In [23], the author showed that a simple combinatorial statistic that was first envisioned by Dyson (the "crank") plays a fundamental role in explaining partition congruences of all types, not just those discovered by Ramanujan.

1.1 Congruences for quotients of Eisenstein series

The Eisenstein series are among the first examples of modular forms, and serve as canonical generators for many others. Recall the standard s-th divisor function, given by

$$\sigma_s(n) := \sum_{d|n,\, d>0} d^s,$$

and also the Bernoulli numbers B_n, which are defined by the Fourier expansion

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

Finally, for $z \in \mathcal{H}$, the complex upper-half plane, set $q := e^{2\pi i z}$ throughout this thesis.

Definition 1.1 *Let $k \geq 2$ be even. The* Eisenstein series of weight k *is*

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

For more background on divisor functions, Bernoulli numbers, and the Eisenstein series, see [17].

Ramanujan and Hardy [16] paid particular attention to the coefficients of the first three Eisenstein series:

$$E_2(q) = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n, \tag{1.1}$$
$$E_4(q) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n,$$
$$E_6(q) = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n.$$

In a recent paper, Berndt and Yee [10] proved congruences modulo small powers of 3 and 7 for seven different quotients of these Eisenstein series.

Theorem 1.2 (Berndt-Yee) *Let the functions $F_i(q) = \sum_{n\geq 0} a_i(n)q^n$ be given by the first two columns of the following table. Then the final two columns describe arithmetic progressions for which $a_i(n)$ satisfy congruences.*

i	F_i	$n \equiv 2 \pmod 3$	$n \equiv 4 \pmod 8$
1	$1/E_2(q)$	$a_1(n) \equiv 0 \pmod{3^4}$	
2	$1/E_4(q)$	$a_2(n) \equiv 0 \pmod{3^2}$	
3	$1/E_6(q)$	$a_3(n) \equiv 0 \pmod{3^3}$	$a_3(n) \equiv 0 \pmod{7^2}$
4	$E_2(q)/E_4(q)$	$a_4(n) \equiv 0 \pmod{3^3}$	
5	$E_2(q)/E_6(q)$	$a_5(n) \equiv 0 \pmod{3^2}$	
6	$E_4(q)/E_6(q)$	$a_6(n) \equiv 0 \pmod{3^3}$	
7	$E_2^2(q)/E_6(q)$	$a_7(n) \equiv 0 \pmod{3^5}$	$a_7(n) \equiv 0 \pmod 7$

The following theorem shows that the types of congruences in Theorem 1.2 are actually quite common, as there are infinite classes of primes for which almost every coefficient is divisible by arbitrary prime powers.

Theorem 1.3 *Let the coefficients $a_i(n)$ be defined as above.*

1. *If τ is any positive integer, then the set of non-negative integers n satisfying*

$$a_1(n) \equiv 0 \pmod{3^\tau}$$

has arithmetic density 1.

2. *If $i \in \{2, 4\}$, the prime ℓ is in the set $\{3\} \cup \{s \equiv 5 \text{ or } 11 \pmod{12}\}$, and τ is any positive integer, then the set of non-negative integers n satisfying*

$$a_i(n) \equiv 0 \pmod{\ell^\tau}$$

has arithmetic density 1.

3. *If $i \in \{3, 5, 6, 7\}$, the prime ℓ is in the set $\{3\} \cup \{s \equiv 7 \text{ or } 11 \pmod{12}\}$, and τ is any positive integer, then the set of non-negative integers n satisfying*

$$a_i(n) \equiv 0 \pmod{\ell^\tau}$$

has arithmetic density 1.

Remark 1.4 *In each of the cases in Theorem 1.3, there are infinitely many distinct arithmetic progressions of coefficients that satisfy linear congruences of the form found by Berndt and Yee. These can be found by using the theory of Hecke operators for integer weight modular forms in direct analog to the proof of Theorem 1.18 (see Chapter 3). In this way, Berndt and Yee's original congruences are all accounted for.*

The case of $\ell = 2$ was not addressed in [10], but the following theorem shows that all of the coefficients $a_i(n)$ also satisfy explicit congruences modulo arbitrary powers of 2.

Theorem 1.5 *If $1 \leq i \leq 7$ and τ is a positive integer, then the set of non-negative integers n satisfying*

$$a_i(n) \equiv 0 \pmod{2^\tau}$$

has arithmetic density 1. Furthermore, there exists some integer w such that

$$a_i(mn') \equiv 0 \pmod{2^\tau}$$

whenever m is a square-free odd integer that is the product of at least $w \cdot \tau$ distinct, odd prime factors, with $(m, n') = 1$.

The second part implies that there are numerous specific arithmetic sequences for which congruences hold, such as

$$a_3(1334025n + 1155) \equiv 0 \pmod{2^4}. \tag{1.2}$$

Remark 1.6 *The proof of this theorem follows from the nilpotency of the integral weight Hecke operators modulo 2, and appears in Section 3.1. Recent results of Khare and Boylan [11, 18] imply that the Hecke operators behave similarly modulo primes $\ell \leq 7$, and thus there are also analogs to Theorem 1.5 for these moduli (although the statements for the explicit congruences are slightly more complicated).*

1.2 Partitions

The theory of partitions can be traced back to basic results of Euler, and some of the earliest significant work by American mathematicians occurred in this subject [3]. In

the twentieth century, partition theory has matured greatly, and there are now numerous connections to other areas of mathematics, including combinatorics, representation theory, and even mathematical physics. Howeverr, despite these advancements, even seemingly innocent questions about the basic properties of partitions can be quite difficult, and the results of this section represent the culmination of over 60 years of study of questions first raised by Dyson (who was influenced by even earlier work of Ramanujan).

Definition 1.7 *A* partition *of an integer $n \geq 0$ is a non-increasing sequence of integers that sum to n. The partition function $p(n)$ counts the number of distinct partitions of n. If n is not a non-negative integer, then $p(n) := 0$.*

A partition of n is also frequently written as $\lambda_1 + \lambda_2 + \cdots + \lambda_k = n$, where $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 1$. The *weight* of such a partition is $|\lambda| = n$.

Example 1.8 *The partitions of* 4 *are:*

$$4, \qquad 3+1, \qquad 2+2,$$

$$2+1+1, \qquad 1+1+1+1,$$

and thus $p(4) = 5$.

1.2.1 Divisibility properties of the partition function

Partitions reflect fundamental additive properties of the integers (and might even be said to encode the "failure" of unique additive decompositions), so it is surprising to learn that $p(n)$ has divisibility properties as well. Indeed, some of the more famous results in the theory of partitions are Ramanujan's celebrated congruences for the partition function.

Theorem 1.9 (Ramanujan) *For all n,*

$$p(5n+4) \equiv 0 \pmod 5,$$
$$p(7n+5) \equiv 0 \pmod 7,$$
$$p(11n+6) \equiv 0 \pmod{11}.$$

There are many different proofs and generalizations of these formulae, and Ramanujan's original work influenced Watson and Atkin as they extended the congruences to arbitrary powers of $5, 7$ and 11. They achieved these results by using properties of theta functions, Eisenstein series, and other q-series identities (see [26] for more history). Sporadic progress was made in proving congruences for other small primes (largely by Atkin, who found many partition congruences for prime moduli up to 31 [8]), until a seminal paper by Ono revolutionized the subject in 2000 [24]. He developed aspects of the p-adic theory of half-integral weight modular forms and used this to prove the existence of infinite families of partition congruences modulo every prime $\ell \geq 5$.

Theorem 1.10 (Ono) *For any prime $\ell \geq 5$ there are infinitely many distinct arithmetic progressions $\{An+B\}$ such that*

$$p(An+B) \equiv 0 \pmod \ell \qquad \forall\, n \geq 0.$$

This result was then extended to classes of congruences for every modulus coprime to 6 through the continued works of Ahlgren and Ono [1, 2]. Unlike the original Ramanujan congruences, these results are typically quite complicated, as exhibited by the example

$$p(1977147619n + 815655) \equiv 0 \pmod{19}. \tag{1.3}$$

1.2.2 Partition statistics

Although the above results have a strikingly combinatorial flavor, the proofs of the preceding theorems do not provide great combinatorial insight as to why such congruences are true. However, there are simple statistics on partitions that do have an amazing relationship to the divisibility properties of the partition function.

Upon learning of the Ramanujan congruences, Dyson observed that a simple combinatorial statistic gives a tangible decomposition of the congruences modulo 5 and 7 [13]; this phenomenon was proven several years later by Atkin and Swinnerton-Dyer [9].

Definition 1.11 *If* $n = \lambda_1 + \lambda_2 + \cdots + \lambda_k$, *the* rank *of the partition* λ *is defined by*

$$\text{rank}(\lambda) := \lambda_1 - k. \tag{1.4}$$

The key result of [9] is that the rank function explains the Ramanujan congruences by dividing the partitions into classes of equal size.

Theorem 1.12 (Atkin, Swinnerton-Dyer) *Let* $\mathcal{N}(m, N, n)$ *denote the number of partitions* λ *of* n *such that* $\text{rank}(\lambda) \equiv m \pmod{N}$. *Then for any* $n \geq 0$,

$$\mathcal{N}(m, 5, 5n+4) = \frac{1}{5} \cdot p(5n+4) \qquad 0 \leq m \leq 4,$$
$$\mathcal{N}(m, 7, 7n+5) = \frac{1}{7} \cdot p(7n+5) \qquad 0 \leq m \leq 6.$$

However, one can easily check that even for the partitions of 6 the ranks do not follow this pattern modulo 11, so the Ramanujan congruence modulo 11 is not dissected by the rank.

Instead, Dyson conjectured the existence of an analogous "crank" function for the final Ramanujan congruence.

Conjecture 1.13 (Dyson) *There is a combinatorial statistic on partitions that explains the three Ramanujan congruences in the same manner as the rank dissection for the congruences modulo* 5 *and* 7 *found in Theorem 1.12.*

The existence of the crank remained unresolved for over forty years until Andrews and Garvan studied Ramanujan's so-called "Lost Notebook" and found that some peculiar q-series appeared near some computations related to $p(n)$ [4]. They defined the crank by combinatorially interpreting these series as generating functions, and then used a variety of q-series techniques to prove the congruences.

Definition 1.14 *If* $n = \lambda_1 + \lambda_2 + \cdots + \lambda_s + 1 + \cdots + 1$, *with exactly* r *ones, then let* $o(\lambda)$ *be the number of parts of* λ *that are strictly larger than* r. *The* crank *is given by*

$$\operatorname{crank}(\lambda) := \begin{cases} \lambda_1 & \text{if} \quad r = 0, \\ o(\lambda) - r & \text{if} \quad r \geq 1. \end{cases}$$

Andrews and Garvan proved Dyson's conjecture by verifying that the crank decomposes each of the Ramanujan congruences [5].

Theorem 1.15 *If the crank counting function is denoted by*

$$\mathcal{M}(m, N, n) := \#\left\{|\lambda| = n \ : \ \operatorname{crank}(\lambda) \equiv m \pmod{N}\right\},$$

then for $n \geq 0$,

$$\begin{aligned} \mathcal{M}(m, 5, 5n+4) &= \frac{1}{5} \cdot p(5n+4) \qquad 0 \leq m \leq 4, \\ \mathcal{M}(m, 11, 7n+5) &= \frac{1}{7} \cdot p(7n+5) \qquad 0 \leq m \leq 6, \\ \mathcal{M}(m, 11, 11n+6) &= \frac{1}{11} \cdot p(11n+6) \qquad 0 \leq m \leq 10. \end{aligned}$$

It is notable that the crank dissects the Ramanujan congruences modulo 5 and 7 in a different way than the rank.

Remark 1.16 *In [14], Garvan, Kim and Stanton also found "crank" functions of a different sort. They presented one such function for each of the original Ramanujan congruences, as well as one for the higher congruence* $p(25n+24) \equiv 0 \pmod{25}$. *These functions were constructed to encode explicit disjoint cycles of partitions; for example, the partitions of* $5n+4$ *were split into* $p(5n+4)/5$ *different* 5*-cycles, and one of the "crank" functions takes on* 5 *values corresponding to the cycle positions. The results of the present paper are based on Definition 1.14, and the term crank shall refer only to this for the remainder of the paper.*

It is clear that the set of partitions of n can be grouped by the crank,

$$p(n) = \sum_{m=0}^{N-1} \mathcal{M}(m, N, n). \tag{1.5}$$

Theorem 1.15 shows implies that in the special case of the Ramanujan congruences ($N = 5, 7$, or 11), all N terms on the right-hand side of (1.5) are equal. This clearly gives a combinatorial proof of the congruences. However, this is not the only useful way in which the crank might group partitions, and Ono speculated that a more general approach would lead to many more partition congruences.

Conjecture 1.17 (Ono) *For every prime* $\ell \geq 5$ *and integer* $\tau \geq 1$, *there are infinitely many non-nested arithmetic progressions* $An + B$ *for which*

$$M(m, \ell, An+B) = 0 \pmod{\ell^\tau}$$

for every $0 \leq m \leq \ell - 1$.

This can be viewed as a natural extension of Conjecture 1.13, as it is of great interest whether the new collection of congruences can also be explained combinatorially, and whether the crank function plays a similar role.

In particular, combining Ono's Conjecture with (1.5) would give a modified combinatorial proof that $p(An+B) \equiv 0 \pmod{\ell^\tau}$. The next theorem shows that this conjecture is true, and as such it represents the culmination of the study of questions first raised by Dyson in 1944. However, although the type of congruences in Conjecture 1.17 appear similar to those in Theorem 1.10, several technical problems intervene and complicate a naive application of Ono's methods to the crank function.

For a prime $\ell \geq 5$, set $\delta_\ell := (\ell^2-1)/24$, and define

$$\epsilon_\ell := \left(\frac{\delta_\ell}{\ell}\right) = \left(\frac{-6}{\ell}\right). \tag{1.6}$$

Finally, let

$$S_\ell := \left\{ 0 \leq \beta \leq \ell - 1 \;\middle|\; \left(\frac{\beta+\delta_\ell}{\ell}\right) = 0 \text{ or } -\epsilon_\ell \right\}. \tag{1.7}$$

Theorem 1.18 *Suppose that $\ell \geq 5$ is prime, τ and j are positive integers, and $\beta \in S_\ell$. Then a positive proportion of primes $Q \equiv -1 \pmod{24\ell}$ have the property that for every $0 \leq m \leq \ell^j - 1$,*

$$\mathcal{M}\left(m, \ell^j, \frac{Q^3 n + 1}{24}\right) \equiv 0 \pmod{\ell^\tau}$$

for all $n \equiv 1 - 24\beta \pmod{24\ell}$ that are not divisible by Q.

As developed by Ahlgren and Ono in [2], the most general known framework for congruences of $p(n)$ has a similar dependence on the set S_ℓ, and thus the crank congruences apparently hold in the most general possible setting. This makes the following natural corollaries of Theorem 1.18 all the more remarkable. Note that Corollary 1.19 is actually

a stronger result than Ono's Conjecture, as there is an additional degree of freedom in the exponents.

Corollary 1.19 *Suppose that $\ell \geq 5$ is prime and that τ and j are positive integers. Then there are infinitely many non-nested arithmetic progressions $An + B$ such that*

$$\mathcal{M}(m, \ell^j, An + B) \equiv 0 \pmod{\ell^\tau}$$

for every $0 \leq m \leq \ell^j - 1$.

Corollary 1.20 *Let $\ell \geq 5$ be prime, and j be a positive integer. Then there are infinitely many non-nested arithmetic sequences $An + B$ such that the crank underlies the congruence*

$$p(An + B) \equiv 0 \pmod{\ell^\tau}.$$

1.3 Structure of the thesis

Chapter 2 is devoted to the theory of modular forms, and contains all of the tools needed later. This includes the general theory of both integral and half-integral weight forms, data about the structure of spaces of modular forms, a variety of operators on these spaces and the connections to congruences for the coefficients. Specific examples of modular forms, such as Dedekind's eta-function and the Klein forms are also given, as they arise in the later proofs.

Chapter 3 contains the proofs of all of the main theorems. First, Theorems 1.3 and 1.5 are proven by relating the relevant quotients of Eisenstein series to ℓ-adic modular forms. Next comes more background on the crank function, leading to the proof of

Theorem 1.18. The generating functions that Andrews and Garvan found in Ramanujan's notebooks are closely related to Klein forms, which enables the application of the techniques from Chapter 2.

Finally, Chapter 4 concludes this thesis by discussing the context of the main theorems and their proofs, and offers some speculations for future and related work.

Chapter 2

Modular Forms

This chapter contains all of the relevant facts about one-variable modular forms that will be needed in the proofs of Chapter 3. See [26] for more details and a more exhaustive list of references for the subjects in this chapter.

2.1 Basic definitions

This section presents many of the fundamental objects and properties of modular forms. After the initial definitions, certain operators that map between spaces of modular forms are also defined; these types of manipulations will be important tools for understanding the coefficients of modular forms in later proofs.

2.1.1 Modular transformations

Let $\Gamma := SL_2(\mathbb{Z})$ denote the full modular group of 2-by-2 matrices with determinant 1. Γ acts on points z in the upper half-plane $\mathcal{H}$ by linear fractional transformations,

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

A *congruence subgroup* of level N is a subgroup $\Gamma' \leq \Gamma$ that also contains $\ker(\phi_N)$, where

$$\phi_N : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$$

is the projection map modulo N. For a given modulus N, denote the canonical congruence subgroups of level N by

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}, \tag{2.1}$$

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

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

The *cusps* of a subgroup $\Gamma' \leq \Gamma$ are the equivalence classes of $i\infty$ (also known as "the cusp at infinity") under the action of Γ'.

Definition 2.1 *Suppose that f is a meromorphic function on the upper half plane $\mathcal{H}$, and that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2^+(\mathbb{R})$. For $k \in \frac{1}{2}\mathbb{Z}$, the slash operator of weight k is defined by*

$$f(z) \Big|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} := (ad - bc)^{k/2}(cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right). \tag{2.2}$$

A key property of this operator is that it gives a group action on the ring of meromorphic functions on $\mathcal{H}$, as described in the next proposition.

Proposition 2.2 *If $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in GL_2^+(\mathbb{R})$, then*

$$f(z) \Big|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Big|_k \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = f(z) \Big|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

The convenient shorthand of the slash operator is very useful when computing a function's order of vanishing at cusps, as the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ maps $i\infty$ to the cusp a/c. The importance of these calculations is seen in the next definition; note that $q = e^{2\pi iz}$

is the uniformizer at $i\infty$, and thus a q-series can be viewed analytically as a Fourier expansion around $i\infty$.

Definition 2.3 *Let $k \in \frac{1}{2}\mathbb{Z}$, and let $\Gamma' \leq \Gamma$ be a congruence subgroup of level N, with $4 \mid N$ when $k - 1/2 \in \mathbb{Z}$. A meromorphic function f on the complex upper half plane is a* weakly holomorphic modular form *of weight k with respect to Γ' if it satisfies each of the following properties.*

1. *If $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, then*

$$f\left(\frac{az+b}{cz+d}\right) = \begin{cases} (cz+d)^k f(z) & \text{if} \quad k \in \mathbb{Z}, \\ \left(\frac{c}{d}\right)^{2k} \epsilon_d^{-2k} (cz+d)^k f(z) & \text{otherwise,} \end{cases} \tag{2.3}$$

   where $\left(\frac{c}{d}\right)$ is the generalized Legendre symbol (which is extended to negative c and d in the natural way), and $\epsilon_d := 1$ or i if $d \equiv 1$ or $3 \pmod 4$, respectively.

2. *There is some $n_0 \in \mathbb{Z}$ such that f has a Fourier expansion in $q_N := q^{1/N} = e^{2\pi i z/N}$ of the form*

$$f(z) = \sum_{n \geq n_0}^{\infty} c(n) q_N^n.$$

3. *$f(z)$ is holomorphic on the upper-half plane and meromorphic at the cusps of Γ'.*

If $f(z)$ is holomorphic at the cusps of Γ', then it is called a holomorphic modular form *(typically shortened to* modular form *in this work), and if $f(z)$ vanishes at the cusps, then it is a* cusp form*.*

The spaces of weakly holomorphic modular forms of weight k for the congruence subgroup Γ' (resp. holomorphic modular forms, cusp forms) are denoted by $M_k^!(\Gamma')$ (resp. $M_k(\Gamma'), S_k(\Gamma')$). The space of *modular functions* with respect to Γ' is defined to be $M_0^!(\Gamma')$.

In the special case that $\Gamma' = \Gamma_0(N)$, there is an additional definition.

Definition 2.4 *Suppose that χ is a Dirichlet character of conductor N and that $f(z)$ is a weakly holomorphic modular form of weight k with respect to $\Gamma_1(N)$ (resp. modular form, cusp form). Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma'$. If $f(\frac{az+b}{cz+d})$ is exactly $\chi(d)$ times the right side of (2.3), then $f(z)$ is a* weakly holomorphic modular form with character χ *(resp. modular form, cusp form).*

The spaces of weakly holomorphic modular forms of weight k with respect to $\Gamma_0(N)$ with character χ are denoted by $M_k^!(\Gamma_0(N), \chi)$ (resp. $M_k(\Gamma_0(N), \chi), S_k(\Gamma_0(N), \chi)$). There is a well-known decomposition of spaces of modular forms with respect to $\Gamma_1(N)$:

$$S_{\lambda+1/2}(\Gamma_1(N)) = \bigoplus_{\chi \text{ even}} S_{\lambda+1/2}(\Gamma_0(N), \chi). \tag{2.4}$$

2.1.2 Operators on modular forms

Now we review the Hecke operators for modular forms, which are crucial in finding congruences for the coefficients of such functions.

Definition 2.5 *Suppose that $f(z) = \sum_{n \geq 0} a(n) q^n \in M_k(\Gamma_0(N), \chi)$, and that $p \nmid N$ is a prime.*

1. *If $k \in \mathbb{Z}$, then the Hecke operator $T_p^{k,\chi}$ is defined by the action*

$$f(z) \mid T_p^{k,\chi} := \sum_{n \geq 0} \left(a(pn) + \chi(p) p^{k-1} a\left(\frac{n}{p}\right) \right) q^n.$$

2. *If $k - 1/2 \in \mathbb{Z}$, then the Hecke operator $T^{k,\chi}(p^2)$ is defined by*

$$f(z) \mid T^{k,\chi}(p^2) := \sum_{n \geq 0} \left(a(p^2 n) + \chi^*(p) \left(\frac{n}{p}\right) p^{k-3/2} a(n) + \chi^*(p^2) p^{2k-2} a\left(\frac{n}{p^2}\right) \right) q^n,$$

where $\chi^*(n) := \chi(n)\left(\frac{(-1)^{k-1/2}}{n}\right)$.

The superscripts k and χ are suppressed whenever the context is clear.

Another basic operation on modular forms is also described explicitly in terms of Fourier coefficients.

Definition 2.6 *Suppose that* $f = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(N), \chi)$, *and that* ψ *is a Dirichlet character. Then the twist of* f *by* ψ *is*

$$(f \otimes \psi)(z) := \sum_{n \geq 0} \psi(n)a(n)q^n.$$

The Hecke operators act on spaces of modular forms in an easily described manner, as does the operation of twisting by a character.

Proposition 2.7 *Suppose that* $f(z) \in M_k(\Gamma_0(N), \chi)$.

1. *For a prime* $p \nmid N$, *let* $T := T_p$ *if* k *is an integer, or* $T := T(p^2)$ *if* $k - 1/2 \in \mathbb{Z}$. *Then the action of* T *is space-preserving, i.e.,*

$$f(z) \mid T \in M_k(\Gamma_0(N), \chi).$$

2. *If* ψ *is a character with modulus* M, *then*

$$(f \otimes \psi)(z) \in M_k(\Gamma_0(NM^2), \chi\psi^2).$$

If ψ is a quadratic character, then this last part is especially simple.

It is a useful fact that the twist of a modular form by a quadratic character can also be written in terms of the slash operator. If p is a prime and

$$g := g_p = \sum_{v=1}^{p-1} \left(\frac{v}{p}\right) e^{2\pi i v/p}$$

is the standard Gauss sum, then

$$f(z) \otimes \left(\frac{\bullet}{p}\right) = \frac{g}{p} \sum_{v=1}^{p-1} \left(\frac{v}{p}\right) f(z) \Big|_k \begin{pmatrix} 1 & -v/p \\ 0 & 1 \end{pmatrix}. \tag{2.5}$$

This identity follows from the classical evaluation of the signs of Gauss sums. Note that the weight on the slash operator is irrelevant, as the above expression has no dependence on k.

Twisting a modular form by a character varies the coefficients in a periodic way (relative to the modulus of the character). An even simpler operation is to merely discard the coefficients that lie in certain arithmetic progressions, and this also acts functorially on spaces of modular forms.

Proposition 2.8 *Suppose that* $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_k(\Gamma_1(N))$, *where* k *is a half-integer. If* $t \geq 1$ *and* $0 \leq r \leq t-1$, *then*

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

The famous Shimura correspondence gives a means of embedding half-integral weight forms into spaces of even integral weight forms.

Theorem 2.9 (Shimura [30]) *Suppose that* $f(z) = \sum_{n \geq 1} c(n)q^n \in S_k(\Gamma_0(N), \chi)$, *with* $3/2 \leq k \notin \mathbb{Z}$, *and define a Dirichlet character by* $\psi_t := \chi(\bullet)\left(\frac{(-1)^{k-1/2}t}{\bullet}\right)$. *Let* $t > 0$ *be a square-free integer, and define the coefficients* $A_t(n)$ *by*

$$\sum_{n \geq 1} \frac{A_t(n)}{n^s} := L(s - k + 3/2, \psi_t) \cdot \sum_{n \geq 1} \frac{b(tn^2)}{n^s},$$

where the L-function is defined by

$$L(s, \chi) := \sum_{n \geq 1} \frac{\chi(n)}{n^s}.$$

There is then an integral weight form associated to f:

$$S_{t,k}(f(z)) := \sum_{n\geq 1} A_t(n)q^n \in M_{2k-1}(\Gamma_0(N), \chi^2).$$

Furthermore, if $k \geq 5/2$, then $S_{t,k}(f(z))$ is a cusp form.

The map $S_{t,k}$ is called the *Shimura lift*, and the next result states the important fact that it commutes with the Hecke operators. Note that the weight k is often suppressed when it is clear from context.

Proposition 2.10 *Suppose that $f(z) \in S_k(\Gamma_0(N), \chi)$ with $k \geq 3/2$. If $t > 0$ is square-free and $p \nmid Nt$ is a prime, then*

$$S_t(f(z) \mid T(p^2)) = S_t(f(z)) \mid T_p.$$

The action of the Hecke operators can also be understood from the perspective of Galois representations associated to modular forms, a subject which owes much to the work of Deligne and Serre [12].

2.1.3 Congruences for modular forms

The proofs in Section 3.1 require knowledge of the divisibility properties of the coefficients of integral weight modular forms. One of the most useful tools is Serre's work on divisibility of the coefficients of modular forms. His theorem implies that almost all of the coefficients will be divisible by M. The results in this section assume some familiarity with algebraic number theory and the properties of Hecke eigenforms, but the background material is thoroughly explained in the references mentioned.

Theorem 2.11 (Serre) *Let $f(z)$ be a holomorphic modular form of positive integer weight k, with Fourier expansion*

$$f(z) = \sum_{n=0}^{\infty} a(n)q^n, \tag{2.6}$$

where $a(n)$ are algebraic integers in some number field. If M is a positive integer, then there exists a positive constant α such that there are $O\left(\frac{x}{log^{\alpha} x}\right)$ integers $n \leq x$ where the $a(n)$ are not divisible by M.

Although this result determines the behavior modulo M of almost all of the coefficients of an integral weight modular form, the proofs in Section 3.2 rely on more specific knowledge of simultaneous congruences for multiple modular forms of different, non-integral weights and distinct levels. Fortunately, the ideas in Serre's proof actually provide much more information about precisely which coefficients vanish when reduced modulo M. Ono built on these arguments and determined when collections of integer modular forms will simultaneously vanish under the action of certain Hecke operators.

Theorem 2.12 (Ono [25]) *Let $f_1(z), f_2(z), \ldots, f_r(z)$ be integer weight cusp forms where*

$$f_i(z) = \sum_{n \geq 1} a_i(n)q^n \in S_{k_i}(\Gamma_0(N_i), \chi_i).$$

Suppose that the coefficients of every $f_i(z)$ and the values taken on by every χ_i are in $\mathcal{O}_K$, the ring of integers for some number field K. Finally, let v be a finite place of K with residue characteristic ℓ. If $p_0 \nmid \ell N_1 N_2 \cdots N_r$ is prime and $j \geq 1$, then there is a set of primes p with positive Frobenius density such that for every $1 \leq i \leq r$ the functions satisfy

$$\mathrm{ord}_v(f_i(z)|T_{p_0}^{k_i,\chi_i} - f_i(z)|T_p^{k_i,\chi_i}) > j.$$

A close inspection of the proof of Theorem 2.12 combined with Serre's observation that the coefficients of Hecke eigenforms arise as the traces of Frobenius elements under Galois representations imply two important special cases of the previous result. Specifically, the universal presence of complex conjugation and the identity map in the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ implies that there are always T_p with Hecke eigenvalues 0 and 2 modulo v^j for primes p in certain arithmetic progressions. A straightforward application of this phenomenon combined with Ono's proof of Theorem 2.12 gives the following corollary.

Corollary 2.13 *Suppose that k_i, N_i are integers, and that χ_i is a Dirichlet character for $1 \leq i \leq r$. Let $A_i := S_{k_i}(\Gamma_0(N_i), \chi_i) \cap \mathcal{O}_K[[q]]$, where $\mathcal{O}_K$ is the ring of integers in a fixed number field K. Suppose that $\mathfrak{m} \subset \mathcal{O}_K$ is an ideal with $\mathrm{Norm}_K(\mathfrak{m}) = M$. Then for $\theta \in \{\pm 1\}$, a positive proportion of primes $p \equiv \theta \pmod{N_1 \cdots N_r M}$ have the property that for each i,*

$$f_i(z) \mid T_p^{k_i,\chi_i} \equiv (1+\theta) f_i(z) \pmod{\mathfrak{m}}$$

for every $f_i(z) \in A_i$.

Finally, following a similar argument as the one found in Ahlgren and Ono's proof of Lemma 3.1 in [2], one can use Proposition 2.10 to obtain analogous congruence properties for the coefficients of half-integral weight modular forms. These follow from the commutativity of the Shimura correspondence and Hecke operators. These conclusions also hold for modular forms with respect to $\Gamma_1(N)$ due to the decomposition (2.4). Together with Corollary 2.13, this gives a result that plays a central role in the proof of Theorem 1.18 in Section 3.2.

Theorem 2.14 *Suppose that N_i is a positive integer and that $k_i \in 1/2 + \mathbb{Z}_{\geq 0}$ for $1 \leq i \leq r$, and let $g_1(z), \ldots, g_r(z)$ be half-integer weight cusp forms with algebraic integer*

coefficients such that $g_i(z) \in S_{k_i+1/2}(\Gamma_1(N_i))$. *If* $M \geq 1$, *then a positive proportion of primes* $p \equiv -1 \pmod{N_1 \cdots N_r M}$ *have the property that for every* i,

$$g_i(z) \mid T(p^2) \equiv 0 \pmod{M}.$$

A more general result for congruences modulo arbitrary ideals (in the style of Corollary 2.13) is also true for modular forms of half-integral weight, but only the setting of the above statement is relevant here.

2.2 Modular forms modulo ℓ

We now return our attention to modular forms on Γ and consider the effects of reducing the q-series expansions modulo a prime ℓ. The space of modular forms of weight k with respect to Γ is denoted by M_k. For example, the Eisenstein series $E_k(z)$ from (1.1) is in M_k whenever $k \geq 4$ is even, and in fact all modular forms of level 1 are generated by E_4 and E_6.

Proposition 2.15 *If* E_4 *and* E_6 *are assigned the weights* 4 *and* 6, *respectively, then the spaces* M_k *form a graded algebra:*

$$\bigoplus_{\text{even } k \geq 4} M_k \simeq \mathbb{C}[E_4, E_6].$$

For a holomorphic function f, let $\operatorname{ord}_z(f)$ denote the order of zero of f at z. The definitions of modular forms and holomorphicity then imply a useful result.

Lemma 2.16 *If two modular forms* $f \in M_k$ *and* $f' \in M_{k'}$ *satisfy*

$$\operatorname{ord}_z(f) \geq \operatorname{ord}_z(f')$$

for all $z \in \mathcal{H}$, *then* $\frac{f}{f'} \in M_{k-k'}$.

The following basic facts are useful in understanding the divisors and congruence properties of Eisenstein series. For notational convenience, let $\omega := (-1 + i\sqrt{3})/2$ be the unique cube root of unity in the upper half plane.

Lemma 2.17 *Suppose that $k \geq 2$ is even. Then the following hold:*

1. $E_k(z) \equiv 1 \pmod{24}$ *for all k.*
2. *If ℓ is prime and $(\ell - 1) \mid k$, then $E_k(z) \equiv 1 \pmod{\ell^{\mathrm{ord}_\ell(2k)+1}}$.*
3. *If $k \geq 4$ and $k \not\equiv 0 \pmod{6}$, then $E_k(\omega) = 0$. In particular, E_4 has a simple zero at ω.*
4. *If $k \geq 4$ and $k \not\equiv 0 \pmod{4}$, then $E_k(i) = 0$. In particular, E_6 has a simple zero at i.*

This lemma follows from the definitions of modular forms and the Eisenstein series, and from classical congruences for the denominators of Bernoulli numbers (see [17], [26]).

2.2.1 The structure of $\widetilde{M_k}$

For the purpose of understanding the divisibility properties of the coefficients of modular forms, consider now the algebra of modular forms whose coefficients have been reduced modulo ℓ, where ℓ is a fixed prime for the duration of this development. Modular forms here are identified with their coefficients as formal power series, and the reduction modulo ℓ applies to each coefficient individually.

Definition 2.18 *The space of modular forms of weight k reduced modulo ℓ is*

$$\widetilde{M_k} := \left\{ \widetilde{f}(z) = \sum_{n \geq 0} a(n) q^n \pmod{\ell} \ : \ f(z) = \sum_{n \geq 0} a(n) q^n \in M_k \cap \mathbb{Z}_\ell[[q]] \right\}.$$

Swinnerton-Dyer showed that the only non-trivial relation that is introduced when reducing modular forms modulo ℓ comes from the congruences of Lemma (2.17) [31] (compare with Proposition 2.15).

Proposition 2.19 *The graded algebra of modular forms modulo ℓ has the structure:*

$$\bigoplus_{\text{even } k \geq 4} M_k \simeq \mathbb{C}[E_4, E_6]/E_{\ell-1}.$$

Finally, Fermat's Little Theorem implies a simple result that relates congruences modulo ℓ^m to congruences modulo ℓ^{m+1}.

Lemma 2.20 *If $f(q) \equiv g(q) \pmod{\ell^m}$ as formal power series, then*

$$f(q)^\ell \equiv g(q)^\ell \pmod{\ell^{m+1}}.$$

2.2.2 Integer weight ℓ-adic modular forms

Theorem 2.11 of Serre would directly imply Theorem 1.3 if each $F_i(q)$ were a modular form of positive integer weight. However, these functions are not even holomorphic, so this argument does not succeed. Instead, Lemmas 2.16 and 2.17 will lead to the construction of modular forms that are congruent to $F_i(q)$ modulo ℓ^τ for those τ specified in Theorem 1.3. This is equivalent to the fact that $F_i(q)$ are "ℓ-adic holomorphic modular forms", which will be explained shortly.

Before that, recall the construction of $\mathbb{Q}_\ell$ as the inverse limit of finite field extensions of $\mathbb{Q}$. The space of ℓ-adic modular forms is similarly defined as the inverse limit of spaces of modular forms under the ℓ-adic metric for power series, where series convergence requires uniform convergence across all coefficients.

Definition 2.21 *Let ℓ be a prime number. An* ℓ-adic modular form *is a function $f(q) = \sum_{n\geq 0} a(n)q^n$, with coefficients $a(n) \in \mathbb{Q}_\ell$ for which there exists a sequence $\{f_i(q)\}_{i\geq 1}$ of modular forms with respect to Γ with rational coefficients that satisfy*

$$\lim_{i\to\infty} f_i(q) = f(q).$$

The weight *of $f(q)$ is then defined by*

$$k = \lim_{i\to\infty} k_i,$$

where k_i is the weight of $f_i(q)$.

A key fact is that the value of k does not depend on the f_i, and thus the weight of a ℓ-adic modular form is well-defined.

The only remaining hurdle in proving Theorem 1.3 is the fact that $E_2(z)$ is not a modular form, but a result of Serre shows that $E_2(z)$ does behave well ℓ-adically.

Proposition 2.22 (Serre [29]) *For all positive, even integers k, and for any prime ℓ that doesn't divide the numerator of B_k, the Eisenstein series E_k (possibly re-normalized) is an ℓ-adic modular form of weight k.*

Remark 2.23 *Re-normalizing may be necessary to ensure ℓ-integral coefficients.*

This implies that modulo ℓ^τ, an Eisenstein series E_k may always be replaced by a modular form of integral weight, which is also true for generic ℓ-adic modular forms by Definition 2.21.

Definition 2.24 *Fix a prime ℓ. If $f(q)$ is an ℓ-adic modular form and $\tau \geq 1$, then let $f^*(\tau; q)$ denote a holomorphic modular form such that*

$$f^*(\tau; q) \equiv f(q) \pmod{\ell^\tau}.$$

Note that $E_k^*(\tau; q)$ may be taken as $E_k(q)$ itself if $k \geq 4$ (again, up to possible renormalizations).

2.2.3 Nilpotency modulo 2

The situation modulo 2 (and other primes $\ell \leq 7$) is somewhat different, as there is additional structure afforded by the action of the Hecke operators. Tate proved a conjecture of Serre for modular forms modulo 2 [32] and showed that the action of the Hecke operators is locally nilpotent modulo 2. In other words, if $f \in M_k$, there exists $w \leq \dim M_k \leq \frac{k}{12} + 1$ such that for any collection of distinct odd primes $m_1, \ldots, m_w$,

$$f \mid T(m_1) \mid \cdots \mid T(m_w) \equiv 0 \pmod 2.$$

Combined with (2.5), this leads to the following fact.

Lemma 2.25 *If $f = \sum_{n=0}^{\infty} a(n)q^n$ is a modular form of integral weight, and $m_1, \ldots, m_w$ are distinct odd primes such that*

$$f \mid T(m_1) \mid \cdots \mid T(m_w) \equiv 0 \pmod 2,$$

then $a(nm_1 \cdots m_w) \equiv 0 \pmod 2$ for any n that is coprime to $m_1 m_2 \cdots m_w$.

Proof. By induction on Definition 2.5 (as in [26]), we obtain

$$f(q) \mid T(m_1) \mid \cdots \mid T(m_w) \equiv \sum_{n=0}^{\infty} q^n \sum_{d \mid m} a\left(\frac{nm}{d^2}\right) \pmod 2, \tag{2.7}$$

where $m = m_1 \cdots m_w$. The conclusion follows, as $a(nm)$ is the only non-zero term in the coefficient of q^n whenever n is coprime to m. $\square$

2.3 Modular forms with infinite product expansions

Thus far modular forms have been viewed in terms of their q-expansions, and the coefficients have been discussed from an additive perspective. However, some of the most natural number-theoretic generating functions, such as those associated with partitions, are infinite q-series products. There are two special classes of such products that also satisfy modular transformation properties.

2.3.1 Dedekind's eta-function

Recall the definition of Dedekind's eta-function,

$$\eta(z) := q^{1/24} \prod_{n \geq 1} (1 - q^n). \tag{2.8}$$

This function has an explicit multiplier system under modular transformations as proved by Petersson [27]. For notational convenience, set $\exp(x) := e^{2\pi i x}$.

Proposition 2.26 *If* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, *then the modular transformations for* $\eta(z)$ *are given by*

$$\eta(z) \Big|_{1/2} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \varepsilon(a,b,c,d) \cdot \eta(z),$$

where

$$\varepsilon(a,b,c,d) := \begin{cases} \left(\frac{d}{c}\right) \exp\left(\frac{(a+d-bdc-3)c+bd)}{24}\right) & \text{if} \quad 2 \nmid c, \\ \left(\frac{c}{d}\right) \exp\left(\frac{(a+d-bdc-3d)c+bd+3d-3}{24}\right) & \text{if} \quad 2 \mid c. \end{cases}$$

The preceding formulas show that $\eta(z) \in M_{1/2}(\Gamma(24))$, and in fact, properties of classical modular forms show that it is actually a cusp form [7]. Proposition 2.26 also implies modularity properties for many other more complicated infinite products that arise in practice, which are encapsulated in the next result about eta-quotients [15].

Proposition 2.27 *Suppose that there is some $N \geq 1$ such that $f(z) = \prod_{\delta|N} \eta^{r_\delta}(\delta z)$, with the additional properties that $k := \frac{1}{2}\sum_{\delta|N} \in \mathbb{Z}$ and*

$$\sum_{\delta|N} \delta \cdot r_\delta \equiv \sum_{\delta|N} \frac{N}{\delta} \cdot r_\delta \equiv 0 \pmod{24}.$$

If the expression

$$\frac{N}{24} \sum_{\delta|N} \frac{(c,\delta)^2 \cdot r_\delta}{(c, \frac{N}{c}) \cdot c\delta}$$

is non-negative (resp. vanishes) for each divisor $c \mid N$ then

$$f(z) \in M_k(\Gamma_0(N), \chi) \quad (\text{resp. } S_k(\Gamma_0(N), \chi).$$

The character here is $\chi := \left(\frac{(-1)^k s}{\bullet}\right)$, where $s := \prod \delta^{r_\delta}$.

The formula preceding the cusp condition is the order of a cusp $\frac{a}{c}$, which is calculated in a similar manner to the modular transformations that are found in Section 3.2.3.

Remark 2.28 *If $f(z)$ is an eta-quotient, then the order at a cusp $\frac{a}{c}$ only depends on the denominator c.*

2.3.2 Siegel functions and Klein forms

While developing the theory of modular units, Kubert and Lang [20] studied the transformation properties of certain modular functions that generalize $\eta^2(z)$ and that are closely connected to the crank generating function found by Andrews and Garvan (see Section 3.2.1).

The Siegel functions and Klein forms have an implicit dependence on a fixed modulus N, and for such a modulus, set $\zeta := e^{2\pi i/N}$.

Definition 2.29 *Let $1 \leq s \leq N-1$.*

1. *The $(0,s)$–Siegel function has the q-expansion*

$$\eta_{0,s}(z) := q^{1/12}\omega_s \prod_{n\geq 1}(1-\zeta^s q^n)(1-\zeta^{-s}q^n),$$

where $\omega_s := \zeta^{s/2}(1-\zeta^{-s})$.

2. *The $(0,s)$–Klein form is given by*

$$t_{0,s}(z) := \frac{-i}{2\pi}\cdot\frac{\eta_{0,s}(z)}{\eta^2(z)} = \frac{-i\omega_s}{2\pi}\prod_{n\geq 1}\frac{(1-\zeta^s q^n)(1-\zeta^{-s}q^n)}{(1-q^n)^2}.$$

Remark 2.30 *The Siegel functions and Klein forms are also defined for arbitrary integer pairs* $(r,s) \pmod N$*, although the general definition is unnecessary in the present development. The complete set of Siegel functions over all pairs modulo N comprises the modular units in the modular function field for* $\Gamma(N)$*. These functions were also studied extensively by Schoeneberg [28].*

Kubert and Lang studied Klein forms from the perspective of modular forms on lattices, and their work helps characterize the transformations for the Klein forms that are used in Section 3.2. In the following, let $\overline{d}$ denote the reduction of d modulo N.

Proposition 2.31 *If* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$*, then*

$$t_{0,s}(z)\,\Big|_{-1}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \beta(s,c,d)\cdot t_{0,\overline{ds}}(z),$$

where the multiplier is

$$\beta(s,c,d) := \exp\left(\frac{cs+(ds-\overline{ds})}{2N} - \frac{cds^2}{2N^2}\right). \tag{2.9}$$

Proof. The Klein form $t_{0,s}$ is closely related to the Weierstrass σ-function on lattices, and thus for any $\gamma \in \Gamma$,

$$t_{0,s}(Az) = t_{(0,s)\cdot A}(z). \tag{2.10}$$

Formula **K2** in Kubert and Lang [20] states that

$$t_{a_1+b_1,a_2+b_2}(z) = \varepsilon_0(a_1, a_2, b_1, b_2) \cdot t_{a_1,a_2}(z), \tag{2.11}$$

where

$$\varepsilon_0(a_1, a_2, b_1, b_2) := \exp\left(\frac{b_1b_2 - b_1a_2 - b_2a_1}{2N^2} + \frac{b_1 + b_2}{N}\right).$$

Combining (2.10) and (2.11) leads to an expression for the general multiplier system for the collection of $t_{0,s}(z)$. In the specific case that $N \mid c$, the proposition statement is recovered:

$$t_{0,s}(z)\,\Big|_{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = t_{cs,\,ds}(z) = t_{(0,\,\overline{ds})\,+\,(cs,\,ds-\overline{ds})}(z) \tag{2.12}$$

$$= \varepsilon_0(0,\ \overline{ds},\ cs,\ ds - \overline{ds}) \cdot t_{0,\overline{ds}}(z) \tag{2.13}$$

$$= \exp\left(\frac{cs + (ds - \overline{ds})}{2N} - \frac{cds^2}{2N^2}\right) \cdot t_{0,\overline{ds}}(z), \tag{2.14}$$

which is the desired transformation. □

While it is true that $t_{r,s}(z)$ is a modular form of weight -1 with respect to $\Gamma(2N^2)$ for any pair (r, s) [20], Proposition 2.31 shows that the Klein forms comprise a set of "vector-valued modular forms" with respect to Γ, as the function index can change under transformations. However, the Klein forms $t_{0,s}(z)$ are actually modular for a larger subgroup, as the expression for the roots of unity are always trivial and $t_{0,s} = t_{0,\overline{ds}}$ for matrices in $\Gamma_1(2N^2)$.

Corollary 2.32 *If* $1 \le s \le N-1$, *then* $t_{0,s}(z) \in M^!_{-1}(\Gamma_1(2N^2))$.

Chapter 3

Proofs of Theorems

This chapter presents proofs of the main theorems from Chapter 1, making heavy use of the theory of modular forms from Chapter 2.

3.1 Quotients of Eisenstein series

3.1.1 Inverse power series expansions

The congruences of Theorem 1.2 provide certain arithmetic progressions such that $a_i(n) \equiv 0 \pmod{\ell^a}$, where $\ell \in \{3, 7\}$ and a is a small, positive integer. Berndt and Yee's proof relies on the fact that each of the series in (1.1) has the form

$$F(q) = 1 + M \sum_{n=1}^{\infty} a(n) q^n, \tag{3.1}$$

where M is some rational number. Setting $G(q) := 1/F(q)$ and observing that $G(q)F(q) = 1$ leads to a simple functional equation for the power series of $G(q)$, namely

$$G(q) = 1 - G(q) \left(M \sum_{n=1}^{\infty} a(n) q^n \right). \tag{3.2}$$

This can then be iterated to give an "M-adic" expansion

$$\begin{aligned} G(q) &= 1 - M \sum_{n_1=1}^{\infty} a(n_1) q^{n_1} + M^2 \sum_{n_1=1}^{\infty} \sum_{n_2=1}^{\infty} a(n_1) a(n_2) q^{n_1+n_2} + \dots \\ &= 1 + \sum_{k=1}^{\infty} (-1)^k M^k \sum_{n_1,\dots,n_k=1}^{\infty} a(n_1) \cdots a(n_k) q^{n_1+\cdots+n_k}. \end{aligned} \tag{3.3}$$

For primes $\ell \mid M$, this formula simplifies drastically when considered modulo powers of ℓ. In the specific cases examined by Berndt and Yee, the value of M is always divisible by 3 in the expansion of $1/E_2(q)$, $1/E_4(q)$, and $1/E_6(q)$, and is additionally divisible by 7 in the case of $1/E_6(q)$. By using both new and known identities involving divisor functions, they obtained the stated congruences.

The present author also used a similar inverse series expansion to study the overpartition function $\bar{p}(n)$ modulo small powers of 2 in [21] and conclude that $\bar{p}(n) \equiv 0 \pmod{64}$ for a set of n with density 1. An *overpartition* is a partition in which the first occurrence of each distinct part may or may not be overlined. The *overpartition function* $\bar{p}(n)$ counts the number of distinct overpartitions of n, and this is effectively a convolution product between standard partitions and partitions into distinct parts. The generating function for overpartitions is

$$\sum_{n\geq 0} \bar{p}(n) = \prod_{n\geq 1} \frac{1+q^n}{1-q^n} = \left(1 + 2\sum_{n\geq 0} (-1)^n q^{n^2}\right)^{-1}.$$

This means that there is an inverse series expansion of the form (3.1) with $M = 2$. The density then follow from asymptotics and parity properties for the number of representations of integers by simple diagonal quadratic forms.

However, in both of the settings just described the method was clearly restricted to primes that divide the leading factor M, and a different approach is required to obtain divisibility properties for infinite classes of primes. It is here that the theory of modular forms modulo ℓ can be applied.

3.1.2 Proof of Theorem 1.3

The proof of Theorem 1.3 uses the theory of ℓ-adic modular forms to relate the quotients of Eisenstein series to holomorphic modular forms. The proof is subdivided into the same cases as the theorem statement.

(1) Suppose that $i = 1$, and consider the function $F_1(q) = 1/E_2(q)$. By Proposition 2.22, E_2 is a 3-adic modular form of weight 2. Recall Definition 2.24, so that $E_2^*(\tau; q)$ is a modular form of positive weight $k \equiv 2 \pmod{3^\tau}$ with the property that

$$E_2^*(\tau; q) \equiv E_2(q) \pmod{3^\tau}.$$

From equation (1.1), it is clear that $E_2(q) \equiv 1 \pmod 3$, and thus Lemma 2.20 yields

$$E_2(q)^{3^{\tau-1}} \equiv 1 \pmod{3^\tau}.$$

To complete this section of the proof, apply Theorem 2.11 to

$$\frac{1}{E_2(q)} \equiv \frac{1}{E_2(q)} \cdot (E_2(q))^{3^{\tau-1}} \equiv (E_2(q))^{3^{\tau-1}-1} \equiv (E_2^*(\tau; q))^{3^{\tau-1}-1} \pmod{3^\tau}. \tag{3.4}$$

(2) Now suppose that $i \in \{2, 4\}$, so that the function $F_i(q)$ has the form $G(q)/E_4(q)$ for some G. When $\ell = 3$, equation (1.1) again shows that $E_4(q) \equiv 1 \pmod 3$. Then Serre's theorem applies to

$$\frac{G(q)}{E_4(q)} \equiv \frac{G^*(\tau; q)}{E_4(q)} \cdot (E_4(q))^{3^{\tau-1}} \equiv G^*(\tau; q) \cdot (E_4(q))^{3^{\tau-1}-1} \pmod{3^\tau}. \tag{3.5}$$

The remaining cases are when $\ell \equiv 5$ or $11 \pmod{12}$. By Lemma 2.17,

$$E_{(\ell-1)\ell^{\tau-1}}(q) \equiv 1 \pmod{\ell^\tau}, \tag{3.6}$$

and therefore

$$\frac{G(q)}{E_4(q)} \equiv \frac{G^*(\tau;q)}{E_4(q)} \cdot E_{(\ell-1)\ell^{\tau-1}}(q) \equiv G^*(\tau;q) \cdot \frac{E_{(\ell-1)\ell^{\tau-1}}(q)}{E_4(q)} \pmod{\ell^\tau}. \tag{3.7}$$

A simple calculation shows that

$$(\ell-1)\ell^{\tau-1} \equiv \begin{cases} 4 \cdot 5^{\tau-1} \pmod{12} & \text{if} \quad \ell \equiv 5 \pmod{12}, \\ 10 \cdot (-1)^{\tau-1} \pmod{12} & \text{if} \quad \ell \equiv 11 \pmod{12}. \end{cases}$$

Thus $(\ell-1)\ell^{\tau-1} \not\equiv 0 \pmod{6}$, and therefore Lemmas 2.16 and 2.17 demonstrate that $E_{(\ell-1)\ell^{\tau-1}}(q)/E_4(q)$ is a modular form of weight $(\ell-1)\ell^{\tau-1}-4$. This is a positive value unless $\ell = 5$ and $\tau = 1$, but in this case the quotient becomes $E_4/E_4 = 1$, and the congruences in the statement of the Theorem hold trivially.

(3) Finally, consider the cases where $i \in \{3,5,6,7\}$. Here the functions $F_i(q)$ all have the form $G(q)/E_6(q)$, and as $E_6(q) \equiv 1 \pmod{3}$, an equation similar to (3.5) holds, which proves the theorem for $\ell = 3$.

Now suppose that $\ell \equiv 7$ or $11 \pmod{12}$. A direct analog to equation (3.7) holds, so the proof is complete so long as $E_{(\ell-1)\ell^{\tau-1}}(q)/E_6(q)$ is a modular form of integer weight. The weight of the numerator is

$$(\ell-1)\ell^{\tau-1} \equiv \begin{cases} 6 \cdot 7^{\tau-1} \pmod{12} & \text{if} \quad \ell \equiv 7 \pmod{12}, \\ 10 \cdot (-1)^{\tau-1} \pmod{12} & \text{if} \quad \ell \equiv 11 \pmod{12}, \end{cases}$$

and in either case, $(\ell-1)\ell^{\tau-1} \not\equiv 0 \pmod{4}$. Lemmas 2.16 and 2.17 again imply that $E_{(\ell-1)\ell^{\tau-1}}/E_6$ is a modular form of positive weight, with a single exception when $\ell = 7$ and $\tau = 1$, which is the trivial case $E_6/E_6 = 1$. $\square$

Remark 3.1 *Note that the expressions for the weights of each $F_i(q)$ converge ℓ-adically, which verifies the conditions of Definition 2.21.*

3.1.3 Proof of Theorem 1.5

Theorem 1.5 requires analysis of the coefficients of Eisenstein series modulo 2. For any i, the series $F_i(q)$ has the form $F(q)/G(q)$, and both F and G may be replaced by integer weight modular forms $F^*(\tau;q)$ and $G^*(\tau;q)$ when reduced modulo 2^τ. Also, since $G(q) \equiv 1 \pmod 8$ in all cases by (1.1),

$$\frac{F(q)}{G(q)} \equiv \frac{F(q)}{G(q)} \cdot (G(q))^{2^{\tau-3}} \equiv F^*(\tau;q) \cdot (G^*(\tau;q))^{2^{\tau-3}-1} \pmod{2^\tau}, \tag{3.8}$$

where the final term is a modular form of some integral weight k. This modular form is denoted by

$$H_0(q) := \sum_{n=0}^{\infty} b(n)q^n = F^*(\tau;q)G^*(\tau;q)^{2^{\tau-3}-1}. \tag{3.9}$$

Theorem 2.11 then immediately implies the desired density result.

To prove the specific congruences, observe that the discussion in Section 2.2.3 shows that H_0 has some degree of nilpotency that is bounded by $w = \left[\frac{k}{12}\right] + 1$, which also bounds the degree of nilpotency of the image of H_0 under any Hecke operator. Let $m_1, \ldots, m_w$ be distinct odd primes, and define

$$H_1'(q) := H_0(q) \mid T(m_1) \mid \cdots \mid T(m_w). \tag{3.10}$$

By the definition of nilpotency, $H_1'(q) \equiv 0 \pmod 2$, so we may set $H_1(q) := H_1'(q)/2$, which is again a modular form of weight k with integer coefficients.

Now iterate the above process to construct $H_i(q)$ for each $1 \le i \le \tau - 1$. For each i, choose primes $m_{wi+1}, \ldots, m_{w(i+1)}$ that are coprime to $m_1, \ldots, m_{wi}$, and then define

$$H_{i+1}(q) := \frac{1}{2}\Big[H_i(q) \mid T(m_{wi+1}) \mid \cdots \mid T(m_{w(i+1)})\Big]. \tag{3.11}$$

The end result of this is the function $H_\tau(q)$, which is a modular form with integer

coefficients. Expanding (3.10) and (3.11), this means that

$$2H_\tau(q) = \frac{1}{2^{\tau-1}}\Big[H_0(q) \mid T(m_1) \mid \cdots \mid T(m_{w\tau})\Big] \equiv 0 \pmod 2. \tag{3.12}$$

Lemma 2.25 leads to the conclusion that

$$\frac{b(n)}{2^{\tau-1}} \equiv 0 \pmod 2$$

for any n that is coprime to $m_1 \cdots m_{w\tau}$, which completes the proof, as the above arguments hold for every set of distinct primes. $\square$

It bears noting that in the cases $i = 2, 3, 6$, neither $F(q)$ nor $G(q)$ are equal to $E_2(q)$, and thus $F^*(\tau; q) = F(q)$ and $G^*(\tau; q) = G(q)$. Thus the weight of $H_0(q)$ can be calculated explicitly to obtain bounds on the weights of the modular forms in (3.8), which in turn gives bounds on the nilpotency degree w in the statement of Theorem 1.5.

For example, if $i = 3$, then $F_3(q) = 1/E_6(q)$ and

$$H_0(q) = \frac{1}{E_6(q)} \equiv \frac{1}{E_6(q)} \cdot (E_6(q))^{2^{\tau-3}} \equiv (E_6(q))^{2^{\tau-3}-1} \pmod{2^\tau}.$$

This has weight $6(2^{\tau-3} - 1) = 12 \cdot 2^{\tau-4} - 6$, and thus the nilpotency degree w is at most $2^{\tau-4}$. Set m to be the product of the first $\tau \cdot 2^{\tau-4}$ primes. Since $mn + 1$ is prime to m for any integer n,

$$a_3(m^2 n + m) \equiv 0 \pmod{2^\tau}. \tag{3.13}$$

In particular, when $\tau = 4$ and 5, then m is the product of the first 4 and 10 primes, respectively, and (3.13) becomes

$$a_3\left((3 \cdot 5 \cdot 7 \cdot 11)^2 n + 3 \cdot 5 \cdot 7 \cdot 11\right) \equiv 0 \pmod{2^4}$$

$$a_3\left((3 \cdot 5 \cdots 31)^2 n + (3 \cdot 5 \cdots 31)\right) \equiv 0 \pmod{2^5}.$$

3.2 The proof of Theorem 1.18

3.2.1 Crank generating functions

Definition 3.2 *The refined crank counting function is*

$$\mathcal{M}(m,n) := \#\left\{|\lambda| = n \ : \ \mathrm{crank}(\lambda) = m\right\}.$$

This is indeed a refinement of the crank counting functions from Chapter 1, as

$$\mathcal{M}(m,N,n) = \sum_{k=-\infty}^{\infty} \mathcal{M}(m+kN,n). \tag{3.14}$$

It is the generating function for $\mathcal{M}(m,n)$ that Andrews and Garvan studied when defining the crank [5]. This two-variable generating function has a nice infinite product representation

$$\begin{aligned} F(x,z) &:= \sum_{m=-\infty}^{\infty}\sum_{n\geq 0}\mathcal{M}(m,n)x^m q^n = \sum_{\lambda} x^{\mathrm{crank}(\lambda)}q^{|\lambda|} \\ &= \prod_{n\geq 1}\frac{1-q^n}{(1-xq^n)(1-x^{-1}q^n)}, \end{aligned} \tag{3.15}$$

which is clearly related to the Siegel functions and Klein forms seen in Section 2.3.2.

Standard techniques in q-series and character sums now relate these generating functions to those for $\mathcal{M}(m,N,n)$. Consider a positive integer N and a residue class $m \pmod N$, and define a primitive root of unity by $\zeta := e^{2\pi i/N}$. Elementary manipulations of power series involving the orthogonality of primitive characters then show that

$$\begin{aligned} \frac{1}{N}\sum_{s=0}^{N-1}F(\zeta^s,z)\zeta^{-ms} &= \frac{1}{N}\sum_{s=0}^{N-1}\sum_{\lambda}\zeta^{\mathrm{crank}(\lambda)s-ms}q^{|\lambda|} \\ &= \sum_{\lambda} q^{|\lambda|}\left(\frac{1}{N}\sum_{s=0}^{N-1}\zeta^{s(\mathrm{crank}(\lambda)-m)}\right) = \sum_{\lambda'} q^{|\lambda'|} \\ &= \sum_{n\geq 0}\mathcal{M}(m,N,n)q^n, \end{aligned} \tag{3.16}$$

where the summation in the penultimate expression is over all partitions λ' such that $\text{crank}(\lambda') \equiv m \pmod{N}$. Combining (3.15) and (3.16) gives the generating function for the cranks modulo N:

$$\sum_{n\geq 0} \mathcal{M}(m,N,n)q^n = \frac{1}{N}\sum_{s=0}^{N-1}\left(\prod_{n\geq 1}\frac{(1-q^n)\zeta^{-ms}}{(1-\zeta^{-s}q^n)(1-\zeta^s q^n)}\right). \tag{3.17}$$

The specialization to roots of unity completes the connection to the Klein forms, so that the crank generating function can be rewritten in terms of modular forms.

Proposition 3.3 *If $1 \leq s \leq N$, then*

$$F(\zeta^s, z) = \frac{q^{1/24}}{\eta(z)t_{0,s}(z)} \cdot \frac{-i\omega_s}{2\pi}.$$

The $s = 0$ term in (3.17) is just the partition generating function

$$\sum_{n\geq 0} p(n)q^n = \prod_{n\geq 1}\frac{1}{1-q^n} = \frac{q^{1/24}}{\eta(z)},$$

so the relationship between the crank function and partition function is now much clearer.

Proposition 3.4

$$\sum_{n\geq 0}\mathcal{M}(m,N,n)q^n = \frac{-i}{2\pi N}\sum_{s=1}^{N-1}\frac{\omega_s\zeta^{-ms}}{\eta(z)t_{0,s}(z)}\cdot q^{1/24} + \frac{1}{N}\sum_{n\geq 0}p(n)q^n.$$

Remark 3.5 *Theorem 1.15 and the ensuing discussion show that the summand in Proposition 3.4 involving Klein forms is identically zero in the special cases of the Ramanujan partition congruences. In general, the difference between the crank function $\mathcal{M}(m,N,n)$ and $p(n)/N$ is evidently the coefficient of a modular form, so understanding the divisibility properties of these coefficients is of fundamental import.*

3.2.2 Crank generating functions and modular forms

Throughout the rest of this section, let $N := \ell^j$ be a fixed power of a fixed prime $\ell \geq 5$. This will be the modulus for the crank functions, and the reader should understand that many of the auxiliary functions defined in this section implicitly depend on N.

The results of Chapter 2 require modular forms of positive weight with algebraic coefficients, so define

$$\begin{aligned} g_m(z) &:= \left(\sum_{n \geq 0} N \cdot \mathcal{M}(m, N, n) q^{n+\delta_\ell} \right) \prod_{n \geq 1} (1 - q^{\ell n})^\ell \\ &= \frac{-i}{2\pi} \sum_{s=1}^{N-1} \frac{\eta^\ell(\ell z)}{\eta(z)} \cdot \frac{\omega_s \zeta^{-ms}}{t_{0,s}(z)} + \frac{n^\ell(\ell z)}{\eta(z)}. \end{aligned} \tag{3.18}$$

Let $G_m(z)$ and $P(z)$, respectively, denote the two summands in the final line of (3.18). The modularity properties of eta-quotients and Klein forms described in Proposition 2.27 and Corollary 2.32 show that

$$P(z) = \frac{\eta^\ell(\ell z)}{\eta(z)} \in M_{\frac{\ell-1}{2}} \left(\Gamma_0(\ell), \left(\frac{\bullet}{\ell} \right) \right), \quad \text{and} \tag{3.19}$$

$$G_m(z) \in M^!_{\frac{\ell+1}{2}}(\Gamma_1(2N^2)). \tag{3.20}$$

Although $G_m(z)$ has poles at many cusps (the orders are calculated explicitly later), many of them can be cancelled by subtracting a certain quadratic twist (see Theorem 3.10).

Definition 3.6 *For any function $f(z) = \sum a(n) q^n$, define*

$$\widetilde{f}(z) := f(z) - \epsilon_\ell \left(f \otimes \left(\frac{\bullet}{\ell} \right) \right)(z).$$

Remarkably, this same quadratic twist was applied to $\widetilde{P}(z)$ in [2] in order to prove congruences for $p(n)$. This was necessary because the analog of Theorem 2.14 used by

Ahlgren and Ono also applies only to cusp forms. In fact, there were still some non-vanishing cusps even after subtracting a quadratic twist of $P(z)$, so they eliminated the other cusps by using ℓ-adic properties of certain modular forms.

Specifically, they used the facts recorded in Proposition 2.27 to construct an eta-quotient that behaves simply modulo ℓ^τ and that vanishes at many cusps.

Proposition 3.7 *If t is a positive integer, and $\chi_{\ell,t}$ is the Dirichlet character defined by*

$$\chi_{\ell,t}(n) := \left(\frac{(-1)^{\frac{\ell^t-1}{2}}\ell^t}{n}\right),$$

then the modular form

$$E_t(z) := \frac{\eta^{\ell^t}(z)}{\eta(\ell^t z)} \in M_{\frac{\ell^t-1}{2}}(\Gamma_0(\ell^t), \chi_{\ell,t})$$

vanishes at every cusp $\frac{a}{c}$ with ℓ^t not dividing c.

Remark 3.8 *By Lemma 2.20, this function also satisfies $E_t(z)^{\ell^\tau} \equiv 1 \pmod{\ell^{\tau+1}}$ for any $\tau \geq 0$. Also note that the weights of these functions converge ℓ-adically as t increases.*

A modified version of the arguments in [2] now produce a cusp form from $P(z)$.

Proposition 3.9 *If τ is sufficiently large, then there is some integer $\lambda' \geq 1$, and some character χ such that*

$$\frac{\widetilde{P}(24z)}{\eta^\ell(24\ell z)} \cdot E_{j+1}(24z)^{\ell^\tau} \in S_{\lambda'+1/2}(\Gamma_0(576\ell^{\max\{3,j+1\}}), \chi).$$

This somewhat complicated modular form still encodes a great deal of information about $p(An+B)$ modulo $\ell^{\tau+1}$ for certain arithmetic progressions $An+B$, and it is this form that can be used to prove the congruences. Arguing in a similar way with $\widetilde{G_m}(z)$ gives another important cusp form (see Lemma 3.11), which, once combined with (3.18) and

Proposition 3.9, implies the existence of a crucial decomposition of the crank generating function into what is essentially a sum of ℓ-adic modular forms (which can also be defined for half-integral weights).

Theorem 3.10 *For any $\tau \geq 0$ and $0 \leq m \leq N-1$, there is a character χ, positive integers λ and λ', and modular forms with algebraic integer coefficients*

$$F_m(z) \in S_{\lambda+1/2}(\Gamma_1(576\ell^2N^2)),$$
$$F'(z) \in S_{\lambda'+1/2}(\Gamma_0(576\ell^{\max\{3,j+1\}}), \chi)$$

such that

$$\frac{\widetilde{g_m}(24z)}{\eta^\ell(24\ell z)} \equiv F_m(z) + F'(z) \pmod{\ell^\tau}.$$

The existence of $F'(z)$ is clear from Proposition 3.9, whereas the existence of $F_m(z)$ is the content of Lemma 3.11 in the next section. After that, Theorem 1.18 follows as a consequence of Theorem 3.10.

3.2.3 The existence of $F_m(z)$

The existence of a suitable $F_m(z)$ is the final piece needed in the proof of Theorem 3.10).

Lemma 3.11 *If τ is sufficiently large, then there is some $\lambda \geq 1$ such that*

$$\frac{\widetilde{G_m}(24z)}{\eta^\ell(24\ell z)} \cdot E_{j+1}(24z)^{\ell^\tau} \in S_{\lambda+1/2}(\Gamma_1(576\ell^2N^2)). \tag{3.21}$$

Proof. Basic facts about modular forms along with Proposition 2.7, Definition 3.6, and (3.20) imply that $\widetilde{G_m}(24z) \in M^!_{(\ell+1)/2}(\Gamma_1(48\ell^2N^2))$. Combining this with the eta-product factors makes it clear that $\Gamma_1(576\ell^2N^2)$ is the appropriate congruence subgroup.

Because of Proposition 3.7, we know that $E_{j+1}(z)$ vanishes at each cusp $\frac{a}{c}$ where $\ell N \nmid c$. Once τ is taken to be sufficiently large, it only remains to be shown that $\widetilde{G_m}(z)/\eta^\ell(\ell z)$ vanishes at each cusp $\frac{a}{c}$ with $\ell N \,|\, c$, as replacing z by $z/24$ does not affect the signs of the cusp orders. Such a cusp $\frac{a}{c}$ is associated with a matrix of the form

$$A_{a,c} := \left(\begin{smallmatrix} \bar{a} & -b \\ -c & a \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^{-1} \in \Gamma_0(\ell N),$$

since $e^{2\pi i(A_{a,c}z)}$ vanishes as $z \to \frac{a}{c}$. However, since the behavior at $\frac{a}{c}$ is completely determined by the value of c for the relevant modular forms, a slight abuse of notation can be adopted whereby the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is used to compute the order at $\frac{a}{c}$ (even though this latter matrix is actually $A_{\bar{a},c}$).

The expansion of the denominator function at the cusp $\frac{a}{c}$ with $\ell N | c$ is

$$\frac{1}{\eta^\ell(\ell z)} \Big|_{\ell/2} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = q^{\ell^2/24} + \dots \tag{3.22}$$

up to a root of unity. Thus the proof of the lemma hinges on showing that the expansion of $\widetilde{G_m}(z)$ at $\frac{a}{c}$ is $(*q^h + \dots)$ for some $h > \ell^2/24$, where the $*$ represents a non-zero constant. To determine this expansion, recall (3.19) and calculate

$$\begin{aligned} G_m(z) \Big|_{\frac{\ell+1}{2}} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \frac{-i}{2\pi} \left(\sum_{s=1}^{N-1} \frac{\eta^\ell(\ell z)}{\eta(z)} \cdot \frac{\omega_s \zeta^{-ms}}{t_{0,s}(z)} \right) \Big|_{\frac{\ell+1}{2}} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= \frac{-i}{2\pi} \left(\frac{d}{\ell}\right) \frac{\eta^\ell(\ell z)}{\eta(z)} \sum_{s=1}^{N-1} \frac{\omega_s \zeta^{-ms}}{t_{0,s}(z)} \Big|_1 \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= \frac{-i}{2\pi} \left(\frac{d}{\ell}\right) \frac{\eta^\ell(\ell z)}{\eta(z)} \sum_{s=1}^{N-1} \frac{\omega_s \zeta^{-ms}}{\beta_s t_{0,\overline{ds}}(z)}. \end{aligned} \tag{3.23}$$

Here the β_s are the roots of unity described in Proposition 2.31, so that

$$t_{0,s}(z) \Big|_{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \beta_s \cdot t_{0,\overline{ds}}(z). \tag{3.24}$$

To find the expansion of $G_m(z) \otimes (\frac{\bullet}{\ell})$, first observe that for any $v' \equiv d^2 v \pmod{\ell}$ there is a commutation relation

$$\begin{pmatrix} 1 & -v/\ell \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} 1 & -v'/\ell \\ 0 & 1 \end{pmatrix}, \tag{3.25}$$

where

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} := \begin{pmatrix} a - cv/\ell & b - cvv'/\ell^2 + (av' - dv)/\ell \\ c & d + cv'/\ell \end{pmatrix} \in \Gamma_0(\ell N). \tag{3.26}$$

Recall the twist of a modular form by a quadratic character from (2.5), and set $g := g_\ell$. Taken together with the expansion in (3.23) and the identities (3.25) and (3.26), this implies that

$$\begin{aligned} &\left(G_m(z) \otimes \left(\frac{\bullet}{\ell}\right)\right) \Big|_{\frac{\ell+1}{2}} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= \frac{g}{\ell} \sum_{v=1}^{\ell-1} \left(\frac{v}{\ell}\right) G_m(z) \Big| \begin{pmatrix} 1 & -v/\ell \\ 0 & 1 \end{pmatrix} \Big|_{\frac{\ell+1}{2}} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= \frac{g}{\ell} \sum_{v=1}^{\ell-1} \left(\frac{v}{\ell}\right) G_m(z) \Big|_{\frac{\ell+1}{2}} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \Big| \begin{pmatrix} 1 & -v'/\ell \\ 0 & 1 \end{pmatrix} \\ &= \frac{-ig}{2\pi\ell} \sum_{v=1}^{\ell-1} \left(\frac{v}{\ell}\right) \left(\sum_{s=1}^{N-1} \frac{\eta^\ell(\ell z)}{\eta(z)} \cdot \frac{\omega_s \zeta^{-ms}}{t_{0,s}(z)} \right) \Big|_{\frac{\ell+1}{2}} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \Big| \begin{pmatrix} 1 & -v'/\ell \\ 0 & 1 \end{pmatrix}. \end{aligned} \tag{3.27}$$

Now this can be evaluated using the modular transformation properties of $t_{0,s}(z)$ and $\eta^\ell(\ell z)/\eta(z)$.

$$\begin{aligned}
&\left(G_m(z) \otimes \left(\frac{\bullet}{\ell}\right)\right) \Big|_{\frac{\ell+1}{2}} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad (3.28)\\
&= \frac{-ig}{2\pi\ell} \sum_{v=1}^{\ell-1} \left(\frac{v}{\ell}\right) \left(\frac{d'}{\ell}\right) \sum_{s=1}^{N-1} \frac{\eta^\ell(\ell z)}{\eta(z)} \cdot \frac{\omega_s \zeta^{-ms}}{\beta'_s t_{0,\overline{d's}}(z)} \Big| \begin{pmatrix} 1 & -v'/\ell \\ 0 & 1 \end{pmatrix}\\
&= \frac{-ig}{2\pi\ell} \left(\frac{d'}{\ell}\right) \sum_{s=1}^{N-1} \sum_{v=1}^{\ell-1} \left(\frac{v}{\ell}\right) \frac{\eta^\ell(\ell z)}{\eta(z)} \cdot \frac{\omega_s \zeta^{-ms}}{\beta'_s t_{0,\overline{d's}}(z)} \Big| \begin{pmatrix} 1 & -v'/\ell \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

Here β'_s is defined just as β_s was in (3.24). The next goal is to find the relationship between (3.23) and (3.28). Since $d' \equiv d \pmod N$ and $\ell N \mid c$, a short computation involving Proposition 2.31 shows that $\beta'_s = \beta_s$. Thus the expansion of (3.23) begins as

$$\frac{-i}{2\pi} \left(\frac{d}{\ell}\right) \left(\sum_{s=1}^{N-1} \frac{\omega_s \zeta^{-ms}}{\omega_{\overline{ds}} \cdot \beta_s} q^{\delta_\ell} + \dots \right), \qquad (3.29)$$

and (3.28) begins with

$$\begin{aligned}
&\frac{-ig}{2\pi\ell} \left(\frac{d}{\ell}\right) \left(\sum_{s=1}^{N-1} \frac{\omega_s \zeta^{-ms}}{\omega_{\overline{ds}} \cdot \beta_s} \sum_{v=1}^{\ell-1} \left(\frac{v}{\ell}\right) q^{\delta_\ell} \Big| \begin{pmatrix} 1 & -v'/\ell \\ 0 & 1 \end{pmatrix} + \dots \right) \qquad (3.30)\\
&= \frac{-ig}{2\pi\ell} \left(\frac{d}{\ell}\right) \left(q^{\delta_\ell} \sum_{s=1}^{N-1} \frac{\omega_s \zeta^{-ms}}{\omega_{\overline{ds}} \cdot \beta_s} \sum_{v=1}^{\ell-1} \left(\frac{v}{\ell}\right) e^{-2\pi i v' \delta_\ell/\ell} + \dots \right).
\end{aligned}$$

Multiplying the first term of the above equation by $-\epsilon_\ell$ gives precisely the negative of the displayed term in (3.29), and hence they cancel in $\widetilde{G_m}(z)$. The cusp expansion has only integral powers of q due to the series expansion of the Klein forms and eta-quotient in (3.23) and (3.28), and therefore must have the form $(*q^{\delta_\ell+1} + \dots)$. Since $\delta_\ell + 1 > \ell^2/24$, the proof is complete. $\square$

3.2.4 Proof of Theorem 1.18 from Theorem 3.10

Armed with the existence of $F_m(z)$ and $F'(z)$, Theorem 2.14, and other results from Section 2.1.3, we can now prove the congruences for the crank generating functions. On the one hand, the definition of $g_m(z)$ in (3.18) shows that

$$\frac{\widetilde{g_m}(24z)}{\eta^\ell(24\ell z)} = \sum_{n\equiv 0 \pmod{\ell}} N\mathcal{M}(m,N,n-\delta_\ell)q^{24n-\ell^2} + 2\sum_{(\frac{n}{\ell})=-\epsilon_\ell} N\mathcal{M}(m,N,n-\delta_\ell)q^{24n-\ell^2}. \tag{3.31}$$

If $\beta \in S_\ell$, then restricting the above sum to those indices $n' \equiv \beta + \delta_\ell \pmod{\ell}$ gives a new series

$$\begin{aligned} h_{m,\beta}(z) :=& \gamma_\beta \sum_{n'=\beta+\delta_\ell+\ell n} N\mathcal{M}(m,N,n'-\delta_\ell)q^{24n'-\ell^2} \qquad (3.32)\\ &= \gamma_\beta \sum_{n\geq 0} N\mathcal{M}(m,N,\ell n+\beta)q^{24\ell n+24\beta-1} \\ &= \gamma_\beta \sum_{n\equiv 24\beta-1 \pmod{24\ell}} N\mathcal{M}\left(m,N,\frac{n+1}{24}\right)q^n, \qquad (3.33) \end{aligned}$$

where

$$\gamma_\beta := \begin{cases} 1 & \text{if} \quad \beta \equiv -\delta_\ell \pmod{\ell}, \\ 2 & \text{otherwise.} \end{cases} \tag{3.34}$$

On the other hand, Theorem 3.10 implies that

$$h_{m,\beta}(z) \equiv F_{m,\beta}(z) + F'_\beta(z) \pmod{\ell^\tau}, \tag{3.35}$$

where the q-expansion of $F_{m,\beta}(z)$ is defined by restricting $F_m(z)$ to only those indices with $n' \equiv \beta+\delta_\ell \pmod{\ell}$, and the q-expansion of $F'_\beta(z)$ is defined by a similar restriction.

Proposition 2.8 implies that

$$F_{m,\beta}(z) \in S_{\lambda+1/2}(\Gamma_1(576\ell^4N^2)), \tag{3.36}$$
$$F'_{\beta}(z) \in S_{\lambda'+1/2}(\Gamma_0(576\ell^{2+\max\{3,j+1\}}), \chi).$$

Applying Theorem 2.14 to $F_{m,\beta}(z)$ and $F'_{\beta}(z)$ and appealing to Dirichlet's density theorem about primes in arithmetic progressions shows that a positive proportion of primes $Q \equiv -1 \pmod{24\ell}$ have the property that

$$F_{m,\beta}(z) \mid T^{\lambda+1/2,1}(Q^2) \equiv F'_{\beta}(z) \mid T^{\lambda+1/2,\chi}(Q^2) \equiv 0 \pmod{\ell^\tau} \tag{3.37}$$

for all m. This in turn gives that $h_{m,\beta}(z) \mid T(Q^2) \equiv 0 \pmod{\ell^\tau}$ for all m. Replace n by Qn in Definition 2.5 to see that

$$\gamma_\beta N\mathcal{M}\left(m, N, \frac{Q^3n+1}{24}\right) \equiv 0 \pmod{\ell^\tau} \tag{3.38}$$

for all $n \equiv 1 - 24\beta \pmod{24\ell}$ that are not divisible by Q. Since N is fixed and τ is arbitrary, dividing by N proves the congruences of Theorem 1.18. $\square$

Chapter 4

Conclusion

The divisibility properties of the coefficients of Eisenstein series and the partition function are primary examples of the importance of the arithmetic of modular forms in number theory, and the results of this thesis exhibit the ongoing development of this field. Holomorphic modular forms are very special analytic objects, and therefore it's not surprising that many of the modular forms that arise as generating functions of natural number-theoretic objects lie in spaces of modular forms with fewer analytic conditions. However, the ℓ-adic properties of these functions are often still quite nice, and because the theory of ℓ-adic modular forms also encompasses a wider class of functions, the arithmetic of their coefficients have become more accessible to study, as seen in Section 2.1.3.

4.1 Quotients of Eisenstein series

The proofs in Section 3.1 suggest that the $F_i(q)$ satisfy no such pervasive congruences for any other moduli, as Lemma 2.17 and Section 2.2.1 completely characterize the Eisenstein series modulo prime powers. It is also clear that many other quotients of Eisenstein series will have similar infinite families of congruences for primes in certain arithmetic progressions.

However, the techniques used here are not limited to only quotients where the denominator has the form of equation (3.1). Indeed, any quotient of modular forms that is congruent to an ℓ-adic modular form can be studied in this way. For example, consider the modular j-function, $j(z) = q^{-1} + 744 + 196884q + \ldots$, which is clearly not of this form [19]. Nonetheless, the coefficients of $1/j(z)$ can still be shown to satisfy all of the properties stated in Theorem 1.3, part (2), as we can write

$$\frac{1}{j(z)} = \frac{(Q(q))^3 - (R(q))^2}{1728(Q(q))^3} \equiv \frac{(Q(q))^3 - (R(q))^2}{1728(Q(q))^3} \cdot (E_{(p-1)p^l}(q))^3 \pmod{p^l}.$$

The arguments of Section 3.1 show that the appropriate holomorphicity and modularity conditions are met, so the asserted congruences hold.

The theory developed in Section 2.1.3 actually allows for much more general functions, including sums of meromorphic modular forms with distinct weights and levels. Conclusions can be made about the asymptotic behavior of the distribution of the coefficients of these functions modulo algebraic ideals in all cases.

4.2 Cranks and partition congruences

The partition function has often acted as a perfect "test case" for new techniques in modular forms, as its generating function is associated with a negative, half-integral weight modular form. The theory of half-integral weight modular forms, the Shimura correspondence, the theory of ℓ-adic modular forms, and the theory of Hecke operators and Galois representations have all been successfully applied in the study of the partition function. Of particular interest is the interplay between the combinatorics of partitions and the divisibility properties of the associated modular forms. The crank function arose from the happy situation that the coefficients of the modular units afford a simple

combinatorial interpretation in terms of partitions and q-series, and thus the important analytic properties of these functions meshes nicely with the combinatorial realm.

A natural question to ask is whether the crank function might provide an equinumerous decomposition for any partition congruences apart from Ramanujan's congruences modulo $5, 7$ and 11, and thus if there are any direct analogs to Theorem 1.15 for other primes.

In [6], Andrews and Lewis studied the behavior of $\mathcal{M}(m, N, n)$ for $N = 2, 3, 4$, and found that not only are they unequal for different m, they also display a certain alternating phenomenon. For example, when $N = 2$, they proved that

$$\mathcal{M}(0, 2, 2n) > \mathcal{M}(1, 2, 2n) \tag{4.1}$$
$$\mathcal{M}(1, 2, 2n + 1) > \mathcal{M}(0, 2, 2n + 1)$$

for all $n \geq 0$. This sort of distribution is not surprising after viewing the expansion in Proposition 3.4. The crank functions modulo N differ from $p(n)/N$ by a meromorphic modular form, and it is reasonable to expect that with the exception of finitely many small primes and arithmetic progressions (which will perhaps turn out to include only those for Ramanujan's congruences), this difference is never zero. As a consequence, Theorem 1.18 would then be the best possible result, in the sense that there are no infinite families of partition congruences that are grouped into equal classes by the crank.

It is also important to observe that the techniques used to prove congruences for the crank generating functions also apply to a large class of modular forms. The essential properties of the crank generating function are apparent in Theorem 3.10. The main results followed from the fact that the crank functions can be written as finite linear

combinations of ℓ-adic cusp forms. The conditions of Theorem 2.14 are then met, and the combinatorics of the Hecke operators led to linear congruences for the coefficients. There are many other natural families of number-theoretic functions whose generating functions are also closely related to weakly holomorphic and/or negative weight modular forms, and similar results are likely to hold. Of particular interest are the number-theoretic interpretations of the modular units, as their role in number theory has been explored much less thoroughly than more classical functions such as the Eisenstein series and eta-function.

Bibliography

[1] S. Ahlgren, *Distribution of the partition function modulo composite integers m*, Math. Ann., 318 (2000), pp. 795–803.

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

[3] G. Andrews, *The theory of partitions*, Cambridge University Press, Cambridge, 1998.

[4] G. Andrews and B. Berndt, *Ramanujan's lost notebook I*, Springer, New York, 2005.

[5] G. Andrews and F. Garvan, *Dyson's crank of a partition*, Bull. Amer. Math. Soc., 18 (1988), pp. 167–171.

[6] G. Andrews and R. Lewis, *The ranks and cranks of partitions moduli 2, 3, and 4*, Journal of Number Theory, 85 (2000), pp. 74–84.

[7] T. Apostol, *Modular functions and dirichlet series in number theory*, Springer-Verlag, New York, 1990.

[8] A. Atkin, *Multiplicative congruence properties and density problems for $p(n)$*, Proc. London Math. Soc. (3), 18 (1968), pp. 563–576.

[9] A. Atkin and P. Swinnerton-Dyer, *Some properties of partitions*, Proc. London Math. Soc. (3), 4 (1954), pp. 84–106.

[10] B. Berndt and A. Yee, *Congruences for the coefficients of quotients of eisenstein series*, Acta Arithmetica, 104 (2002), pp. 297–308.

[11] M. Boylan, *Non-vanishing of the partition function modulo small primes*. preprint.

[12] P. Deligne and J.-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. cole Norm. Sup., 7 (1975), pp. 507–530.

[13] F. Dyson, *Some guesses in the theory of partitions*, Eureka, 8 (1944), pp. 10–15.

[14] F. Garvan, D. Kim, and D. Stanton, *Cranks and t-cores*, Invent. Math., 101 (1990), pp. 1–17.

[15] B. Gordon and K. Hughes, *Multiplicative properties of η-products ii*, in A tribute to Emil Grosswald: number theory and related analysis, vol. 143 of Contemp. Math., Providence, RI, 1993, Amer. Math. Soc., pp. 415–430.

[16] G. Hardy, *Ramanujan*, Cambridge University Press, London, 1940.

[17] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, vol. 84 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1990.

[18] C. Khare, *Serre's modularity conjecture: the level one case*. to appear in Duke Math. Journal.

[19] N. Koblitz, *Introduction to elliptic curves and modular forms*, vol. 97 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1984.

[20] D. Kubert and S. Lang, *Modular units*, vol. 244 of Grundlehren der mathematischen Wissenschaften, Springer-Verlag, New York, 1981.

[21] K. Mahlburg, *The overpartition function modulo small powers of 2*, Discrete Mathematics, 286 (2004), pp. 263–267.

[22] ——, *More congruences for the coefficients of quotients of eisenstein series*, Journal of Number Theory, 115 (2005), pp. 89–99.

[23] ——, *Partition congruences and the andrews-garvan-dyson crank*, Proc. Nat. Acad. Sci., 102 (2005), pp. 15373–15376.

[24] K. Ono, *Distribution of the partition function modulo m*, Ann. of Math., 151 (2000), pp. 293–307.

[25] ——, *Nonvanishing of quadratic twists of modular l-functions and applications to elliptic curves*, J. Reine Angew. Math., 533 (2001), pp. 81–97.

[26] ——, *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, vol. 102 of CBMS Regional Conference Series in Mathematics, American Mathematical Society, Providence, RI, 2004.

[27] H. Petersson, *Über die arithmetischen eigenschaften eines systems multiplikativer modulfunktionen von primzahlstufe*, Acta Math., 95 (1956), pp. 57–110.

[28] B. Schoeneberg, *Elliptic modular functions: an introduction*, Springer-Verlag, New York-Heidelberg, 1974.

[29] J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, in Modular functions of one variable, III, vol. 350 of Lecture Notes in Math., Berlin, 1973, Springer, pp. 191–268.

[30] G. Shimura, *On modular forms of half integral weight*, Ann. Math., 97 (1973), pp. 440–481.

[31] H. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms*, in Modular Forms in One Variable III, vol. 350 of Springer Lect. Notes, Berlin, 1973, Springer, pp. 1–55.

[32] J. Tate, *The non-existence of certain galois extensions of $\mathbb{Q}$ unramified outside 2*, in Arithmetic Geometry (Tempe, Az., 1993), vol. 174 of Contemp. Math., Providence, RI, 1994, Amer. Math. Soc., pp. 153–156.