Distribution Agreement

In presenting this thesis as a partial fulfillment of the requirements for a degree from Emory University, I hereby grant to Emory University and its agents the non-exclusive license to archive, make accessible, and display my thesis in whole or in part in all forms of media, now or hereafter now, including display on the World Wide Web. I understand that I may select some access restrictions as part of the online submission of this thesis. I retain all ownership rights to the copyright of the thesis. I also retain the right to use in future works (such as articles or books) all or part of this thesis.

Tessa Cotron April 20, 2017

Applications of Modular Forms to Elliptic Curves and Representation Theory

by

Tessa Cotron

Ken Ono
Adviser

Mathematics and Computer Science

Ken Ono

Adviser

John Duncan

Committee Member

Ajit Srivastava

Committee Member

2017

Applications of Modular Forms to Elliptic Curves and Representation Theory

By

Tessa Cotron

Ken Ono

Adviser

An abstract of
a thesis submitted to the Faculty of Emory College of Arts and Sciences
of Emory University in partial fulfillment
of the requirements of the degree of
Bachelor of Sciences with Honors

Tessa Cotron

2017

Abstract

Applications of Modular Forms to Elliptic Curves and Representation Theory

By Tessa Cotron

The theory of modular forms has many applications throughout number theory. In a recent paper [3], Bacher and de la Harpe study finitary permutation groups and the relations between their conjugacy growth series and $p(n)$, the partition function, and $p(n)_e$, a generalized partition function. The authors in [3] conjecture over 200 congruences for $p(n)_e$ which are analogous to the Ramanujan congruences for $p(n)$. Along with this, the study of asymptotics for these formulas is motivated by the group theory of [3]. We prove all of the conjectured congruences from [3] and give asymptotic formulas for all of the $p(n)_e$. Modular form congruences also play a role in the theory of elliptic curves. In [11], the authors look at modular forms and other polynomials which reduce modulo p to the supersingular polynomial $ss_p(j)$ for a given elliptic curve E over a field $\mathbf{F}_q$. We look at these results, which give four modular forms that reduce to the supersingular polynomial $ss_p(j)$. We also look at the Atkin orthogonal polynomials which give another way of finding polynomials that reduce modulo p to $ss_p(j)$, and we examine the hypergeometric properties of these polynomials and modular forms.

Applications of Modular Forms to Elliptic Curves and Representation Theory

By

Tessa Cotron

Ken Ono

Adviser

A thesis submitted to the Faculty of Emory College of Arts and Sciences
of Emory University in partial fulfillment
of the requirements of the degree of
Bachelor of Sciences with Honors

Mathematics and Computer Science

2017

Acknowledgements

I would first like to thank Ken Ono for serving as my advisor and mentor, and for his help and guidance on my thesis. I would also like to thank the Clare Booth Luce foundation for their support. Along with this, I would like to thank my thesis committee members John Duncan and Ajit Srivastava.

Table of Contents

List of Figures and Tables

1. Introduction

The theory of congruences arise in many different areas of math, and in particular all throughout number theory. Recall that two integers a and b are congruent modulo an integer n if n divides $a - b$. Although this is a rather simple concept, it proves to be an extremely useful tool with many applications. Two areas of number theory which rely heavily on the theory of congruences is the study of partition functions as well as the study of elliptic curves. This paper will focus on specific applications of the theory of congruences in regards to these two subjects. The first half of the paper will look at the arithmetic of supersingular elliptic curves, while the second half of the paper will focus on congruences which arise from finitary permutation groups.

1.1. **Elliptic Curves.** An elliptic curve over a field K is given by $y^2 = f(x)$ where $f(x)$ is a cubic without repeated roots. Finding the K-rational points on a given elliptic curve has long been a question of study. If one is given two points on the curve, there is a nice way of adding them to produce a third point. It turns out that the K-rational points on an elliptic curve form a group, and this nice way of adding two given points to produce a third will be defined as the group law in Section 3. For our purpose the field K will be taken to be a finite field, namely $K = \mathbb{F}_q$, for the first half of this paper. There are two useful numbers attached to a given elliptic curve E called the j-invariant and the discriminant of E. These will be defined in Section 3. The j-invariant is important in the study of elliptic curves for many reasons, one being that the j-invariant identifies an elliptic curve up to isomorphism.

There exists a special class of elliptic curves over a finite field known as supersingular elliptic curves. Given that the finite field has characteristic p prime, an elliptic curve can be identified as supersingular based on whether or not it has p-torsion over the algebraic closure of $\mathbb{F}_p$. This will be explained in more detail in Section 3. An elliptic curve over the rationals $\mathbb{Q}$ is supersingular modulo infinitely many primes.

However, the probability that an elliptic curve over a finite field $\mathbb{F}_q$ is supersingular is $\widetilde{O}(1/\sqrt{q})$, making them very rare. Whether or a not a given elliptic curve E is supersingular depends only on its j-invariant. It is a known fact that only finitely many supersingular j-invariants exist in the algebraic closure of a finite field of characteristic p. For a supersingular elliptic curve E, the j-invariant of E is contained in $\mathbb{F}_{p^2}$, and there are approximately $\frac{p}{12}$ supersingular j-invariants in $\mathbb{F}_{p^2}$. Using these j-invariants one can define the supersingular polynomial ss_p, which will be stated in Section 3. The first half of this paper will focus primarily on polynomials that reduce modulo p to the supersingular polynomial $ss_p(j)$.

The theory of modular forms will play a significant role in this process, and in the study of elliptic curves in general. Section 2 will give the necessary background on modular forms. Two very special functions in the theory of modular forms are the Delta function Δ and the modular j-invariant $j(\tau)$. Given a modular form f, it can be written in terms of the delta function and what will be defined as the divisor polynomial $\widetilde{f}$ of the modular form f with exponents in terms of δ and ϵ which will be determined by f. We will define in section 4 four special modular forms E_k, G_k, F_k, and H_k, which will give us the following theorem.

Theorem 1.1. *Let $k = p - 1$ where $p \geq 5$ is prime and let f be any of the four modular forms E_k, F_k, G_k, H_k, then the coefficients of the associated polynomial $\widetilde{f}$ are p-integral and*

$$ss_p(j) \equiv \pm j^{\delta}(j - 1728)^{\epsilon}\widetilde{f}(j) \pmod{p}. \tag{1.1}$$

In particular, for $p \geq 5$ prime, then we have that

$$\widetilde{E}_{p-1}(j) \equiv \widetilde{F}_{p-1}(j) \equiv (-1)^{\delta+\epsilon}\widetilde{G}_{p-1}(j) \equiv (-1)^{\delta+\epsilon}\widetilde{H}_{p-1}(j) \pmod{p}. \tag{1.2}$$

Example 1.2. Suppose that $p = 13$, then $k = 12$; for this k, we will get that $\epsilon = \delta = 0$. Therefore

$$ss_p(j) \equiv \widetilde{E}_{12}(j) \equiv \widetilde{F}_{12}(j) \equiv \widetilde{G}_{12}(j) \equiv \widetilde{H}_{12}(j) \pmod{p}.$$

Along with this, we will give in section 2 a way of showing that

$$\widetilde{E}_{12} = \frac{E_{12}}{\Delta}, \quad \widetilde{G}_{12} = \frac{G_{12}}{\Delta}, \quad \widetilde{H}_{12} = \frac{H_{12}}{\Delta}, \quad \widetilde{F}_{12} = \frac{F_{12}}{\Delta}.$$

Example 1.3. For $p = 23$, we have that $k = 22$, and $\epsilon = \delta = 1$, so

$$\begin{aligned} ss_p(j) &\equiv j(j-1728)\widetilde{E}_{22}(j) \equiv j(j-1728)\widetilde{G}_{22}(j) \\ &\equiv j(j-1728)\widetilde{H}_{22}(j) \equiv j(j-1728)\widetilde{F}_{22} \pmod{p}, \end{aligned}$$

and

$$\widetilde{E}_{22} = \frac{E_{22}}{\Delta E_4 E_6}, \quad \widetilde{G}_{22} = \frac{G_{22}}{\Delta E_4 E_6}, \quad \widetilde{H}_{22} = \frac{H_{22}}{\Delta E_4 E_6}, \quad \widetilde{F}_{22} = \frac{F_{22}}{\Delta E_4 E_6}.$$

In Section 2 we will revisit these examples to look at how to calculate the values of ϵ, δ, and $\widetilde{f}(j)$.

The Hecke operator will be defined in Section 2, and will be important for the next theorem. If one lets V be the space of polynomials in j where j is the modular j-invariant, then the following theorem and proposition are both true.

Theorem 1.4. *There is a unique function, up to a scalar multiple, ϕ on V for which all Hecke operators $T_n : V \to V$, $n \in N$, are self-adjoint with respect to the associated scalar product $(f, g) = \phi(fg)$, and a unique family of monic polynomials $A_n(j)$ of degree $n = 0, 1, 2, ...$ which are orthogonal with respect to this scalar product.*

Proposition 1.5. *The following definitions of a scalar product on V coincide:*

i) $(f, g) =$ *constant term of* fg *as a Laurent series in* V*;*

ii) $(f, g) =$ *constant term of* fgE_2E_4/E_6 *as a Laurent series in* j^{-1}

iii) $(f, g) =$ *constant term of* fgE_2 *as a Laurent series in* q*;*

iv) $(f,g) = \frac{6}{\pi}\int_{\pi/3}^{\pi/2} f(e^{i\theta})g(e^{i\theta})d\theta$

The A_n in Theorem 1.4 will be known as the Atkin polynomials, and will be discussed in detail in section 5. These polynomials can be described in several explicit ways given in the next theorem.

Theorem 1.6. *The Atkin polynomials A_n are defined as follows.*
i) Recursion Relation:

$$\begin{aligned} A_{n+1}(j) &= \Big(j - 24\frac{144n^2-29}{(2n+1)(2n-1)}\Big)A_n(j) \\ &\quad - 36\frac{(12n-13)(12n-7)(12n-5)(12n+1)}{n(n-1)(2n-1)^2}A_{n-1}(j) \end{aligned} \tag{1.3}$$

for $n \geq 2$ with $A_0(j) = 1$, $A_1(j) = j - 720$, and $A_2(j) = j^2 - 1640j + 269280$;
ii) Closed Formula:

(1.4)
$$A_n(j) = \sum_{m=0}^{n} 12^{3m}\Big[\sum_{j=0}^{m}(-1)^j\binom{-\frac{1}{12}}{m-j}\binom{-\frac{5}{12}}{m-j}\binom{n+\frac{1}{12}}{j}\binom{n-\frac{7}{12}}{j}]\binom{2n-1}{j}^{-1}\Big]j^{n-1};$$

iii) Differential Equation:

(1.5)
$$\begin{aligned} &j^2(j-c)^2(n^2j-144)A_n'''' + j(j-c)[6n^2j^2 - 144(36n^2+7)j + c^2/3]A_n''' \\ &\quad - [(2n^4-7n^2)j^3 - 48(72n^4-254n^2-30)j^2 - 4c(240n^2+413)j + 320c^2]A_n'' \\ &\quad - [(2n^4-n^2)j^2 - 24(72n^4-13n^2-12)j + 2c(192n^2-107)A_n'] \\ &\quad + [n^6j - 24(18n^4-n^2)]A_n \end{aligned}$$

where c=1728 and A_n is the unique polynomial solution of this equation.

The first five Atkin polynomials are listed below, and can be found using either the explicit formulas just given, or through the Gram-Schmidt orthogonalization

process, as will be shown in Section 5.

$$A_0(j) = 1,$$

$$A_1(j) = j - 720$$

$$A_2(j) = j^2 - 1640j + 269280,$$

$$A_3(j) = j^3 - \frac{12576}{5}j^2 + 1526958j - 107765856,$$

$$A_4(j) = j^4 - 3384j^3 + 3528552j^2 - 113263680j + 44184000960.$$

In general the coefficients of the Atkin polynomials A_n are rational, but for primes $p > 2n$ they are p-integral. It will be shown that there is a nice relation between the Atkin polynomials A_n and the supersingular polynomial ss_p, which is given by the following theorem.

Theorem 1.7. *Let p be prime, then $ss_p(j) \equiv A_{n_p}(j) \pmod{p}$ where $n_p \approx \frac{p}{12}$ is the degree of the supersingular polynomial, and $A_{n_p}(j)$ has p-integral coefficients.*

This theorem implies that one Atkin polynomial may work for as many as four supersingular polynomials.

Example 1.8. In the case that $12n-13$, $12n-7$, $12n-5$, and $12n+1$ are all prime, the supersingular polynomial for each of the four primes is the mod p reduction of the same Atkin polynomial. In particular, this will be the case for the primes $p = 23, 29, 31, 37$. For $p = 29$ one gets that $A_3(j) \equiv j^3 + 2j^2 + 21j \pmod{p}$.

1.2. **Partition Functions and Finitary Permutation Groups.** Bacher and de la Harpe, in [3], study infinite permutation groups that are locally finite. They investigate word length statistics for such groups with respect to various generating sets of transpositions. Given a nonempty set X and a permutation g of X, the *support* of g is $\sup(g) := \{x \in X : g(x) \neq x\}$. The group of permutations with finite support is called *finitary symmetric group of* X, denoted by $\mathrm{Sym}(X)$. The

subgroup of $\mathrm{Sym}(X)$ with even signature permutations is the *finitary alternating group* $\mathrm{Alt}(X)$. Given a group G and a generating set S, for $g \in G$, the *word length* $\ell_{G,S}(g)$ is the smallest non-negative integer n such that $g = s_1 s_2 \cdots s_n$ where $s_1, s_2, \ldots, s_n \in S \cup S^{-1}$. The smallest integer n such that there exists h in the conjugacy class of g where $\ell_{G,S}(h) = n$ is called the *conjugacy length* $\kappa_{G,S}(g)$. Denote the number of conjugacy classes in G made up of elements g where $\kappa_{G,S}(g) = n$ for $n \in \mathbb{N}$ by $\gamma_{G,S}(n) \in \mathbb{N} \cup \{0\} \cup \{\infty\}$. If $\gamma_{G,S}(n)$ is finite for all $n \in \mathbb{N}$ for a pair (G, S), then define the *conjugacy growth series* to be

$$C_{G,S}(q) := \sum_{n=0}^{\infty} \gamma_{G,S}(n) q^n. \tag{1.6}$$

By classical facts on symmetric groups, there exists a bijection between between conjugacy classes of $S_n(X)$ with sets of integer partitions. Recall that a *partition* of a positive integer n is a non-increasing sequence $\lambda := (\lambda_1, \lambda_2, \ldots)$ such that $\sum_{j \geq 1} \lambda_j = n$. The partition function $p(n)$ counts the number of partitions of n. This function has been studied both for its uses in number theory and combinatorics. The generating function for the partition function is given by

$$\sum_{n=0}^{\infty} p(n) q^n = \prod_{n=1}^{\infty} \frac{1}{1-q^n}. \tag{1.7}$$

Bacher and de la Harpe, motivated by their study of subgroups of $\mathrm{Sym}(X)$, define *generalized partition functions*, which are defined given a vector $\mathbf{e} := (e_1, e_2, \ldots, e_k) \in \mathbb{Z}^k$. Given such a vector, the corresponding *generalized partition function* $p(n)_{\mathbf{e}}$ is defined as the coefficients of the power series

$$\sum_{n=0}^{\infty} p(n)_{\mathbf{e}} q^n = \prod_{m=1}^{k} \prod_{n=1}^{\infty} \frac{1}{(1-q^{mn})^{e_m}} = \prod_{n=1}^{\infty} \frac{1}{(1-q^n)^{e_1} \cdots (1-q^{kn})^{e_k}}. \tag{1.8}$$

Observe that $p(n) = p(n)_{(1)}$. This function $p(n)_{\mathbf{e}}$ can be interpreted as multi-partition numbers with constraints on the parts.

The study of the asymptotics of these power series is motivated by the group theory in [3], while the classical work of Ramanujan motivates the study of their congruences.

Bacher and de la Harpe define the *exponential rate of conjugacy growth*, given a group G with generating set S, to be

$$H_{G,S}^{\mathrm{conj}} = \limsup_{n\to\infty} \frac{\log \gamma_{G,S}(n)}{n}.$$

The values of $H_{G,S}^{\mathrm{conj}}$ are 0 for the specific cases we study; thus, define the *modified exponential rate of conjugacy growth* to be

$$\widetilde{H}_{G,S}^{\mathrm{conj}} = \limsup_{n\to\infty} \frac{\log \gamma_{G,S}(n)}{\sqrt{n}}. \tag{1.9}$$

Let $S \subset \mathrm{Sym}(\mathbb{N})$ be a generating set such that $S_{\mathbb{N}}^{\mathrm{Cox}} \subset S \subset T_{\mathbb{N}}$, where

$$S_{\mathbb{N}}^{\mathrm{Cox}} = \{(i, i+1) : i \in \mathbb{N}\} \tag{1.10}$$

is such that $(\mathrm{Sym}(\mathbb{N}), S_{\mathbb{N}}^{\mathrm{Cox}})$ is a Coxeter system, and

$$T_{\mathbb{N}} = \{(x, y) \in \mathrm{Sym}(\mathbb{N}) : x, y \in \mathbb{N} \text{ are distinct}\} \tag{1.11}$$

is the conjugacy class of all transpositions in $\mathrm{Sym}(\mathbb{N})$. More information on Coxeter systems can be found in [5]. With S a generating set defined in this way, by Proposition 1 in [3], the generating function for $p(n)$ given by (1.7) corresponds to the conjugacy growth series $C_{\mathrm{Sym}(\mathbb{N}),S}(q)$ namely

$$C_{\mathrm{Sym}(\mathbb{N}),S}(q) = \prod_{n=1}^{\infty} \frac{1}{1-q^n}. \tag{1.12}$$

Given this conjugacy growth series of the finitary symmetric group, one has that the famous Hardy-Ramanujan asymptotic formula

$$p(n) \sim \frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}} \tag{1.13}$$

as $n \to \infty$ implies that the coefficients of the conjugacy growth series defined by a set S, $\gamma_{\mathrm{Sym}(\mathbb{N}),S}(n)$, approach the right-hand side of (1.13) as $n \to \infty$.

Now let $S' \subset \mathrm{Alt}(\mathbb{N})$ be a generating set of $\mathrm{Alt}(\mathbb{N})$ such that $S_{\mathbb{N}}^A \subset S' \subset T_{\mathbb{N}}^A$, where we define

$$S_{\mathbb{N}}^A := \{(i, i+1, i+2) \in \mathrm{Alt}(\mathbb{N}) : i \in N\} \tag{1.14}$$

and

$$T_{\mathbb{N}}^A := \cup_{g \in \mathrm{Alt}(\mathbb{N})} g S_{\mathbb{N}}^A g^{-1}. \tag{1.15}$$

By Proposition 11 in [3], the conjugacy growth series for the pair $(\mathrm{Alt}(\mathbb{N}), S')$ is given by

$$\begin{aligned} C_{\mathrm{Alt}(\mathbb{N}),S'}(q) &= \frac{1}{2}\sum_{n=0}^{\infty} p\left(\frac{n}{2}\right) q^n + \frac{1}{2}\sum_{n=0}^{\infty} p_2(n) q^n \\ &= \frac{1}{2}\prod_{n=1}^{\infty} \frac{1}{1-q^{2n}} + \frac{1}{2}\prod_{n=1}^{\infty} \frac{1}{(1-q^n)^2}, \end{aligned} \tag{1.16}$$

where $p\left(\frac{n}{2}\right) = 0$ for all odd n and $p_2(n)$ denotes the number of 2-colored partitions of n. By combining (1.12) and (1.16), one gets that

$$\begin{aligned} 2\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2n) &= p(n) + p_2(2n) \\ &= \gamma_{\mathrm{Sym}(\mathbb{N}),S}(n) + p_2(2n). \end{aligned} \tag{1.17}$$

In Section 7 we will define quantities δ and γ, which will give us the following theorem.

Theorem 1.9. *Given a nonzero vector $\boldsymbol{e} := (e_1, e_2, \ldots, e_k) \in \mathbb{Z}^k$ where $e_m \geq 0$ for all m, as $n \to \infty$, we have that*

$$p(dn)_{\boldsymbol{e}} \sim \frac{\lambda A^{\frac{1+\gamma}{4}}}{2\sqrt{\pi} n^{\frac{3+\gamma}{4}}} e^{2\sqrt{An}},$$

where

$$\lambda := \prod_{m=1}^{k} \left(\frac{m}{2\pi}\right)^{\frac{e_{dm}}{2}}$$

and

$$A := \frac{\pi^2 \delta}{6}.$$

Example 1.10. Let $\mathbf{e} = (1)$. Then $d = 1$, $\gamma = 1$, and $\delta = 1$, so $\lambda = \frac{1}{\sqrt{2\pi}}$ and $A = \frac{\pi^2}{6}$. Then as $n \to \infty$, we have that

$$p(n)_{(1)} \sim \frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}},$$

and our asymptotic coincides with (1.13).

Along with finding generalized asymptotic formulas, we study generalized forms of Ramanujan's congruences including those conjectured by Bacher and de la Harpe in [3]. The Ramanujan congruences are [4]:

$$p(5n+4) \equiv 0 \pmod 5$$

$$p(7n+5) \equiv 0 \pmod 7$$

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

Definition 1.11. With the definition of generalized partition numbers, Bacher and de la Harpe define a *generalized Ramanujan congruence* as:

(i) a nonzero integer vector $\mathbf{e} := (e_1, e_2, \ldots, e_k) \in \mathbb{Z}^k$,

(ii) an arithmetic progression $(An + B)_{n \geq 0}$ with $A \geq 2$ and $1 \leq B \leq A - 1$, and

(iii) a prime power ℓ^f with ℓ prime and $f \geq 1$

such that

$$p(An + B)_{\mathbf{e}} \equiv 0 \pmod{\ell^f}$$

for all $n \geq 0$.

Remark. Note that in Theorem 1.9 the e_m's must be nonnegative, whereas here the e_m's are allowed to take on negative values.

Bacher and de la Harpe conjectured over two hundred generalized Ramanujan congruences for $p(n)_{\mathbf{e}}$. They observe that the coefficients of conjugacy growth series satisfy congruence relations similar to the classic Ramanujan congruences for the partition function, then use these congruences to analyze the finitary alternating group.

Two types of congruences appear in [3], both of the form $p(\ell n+B)_{\mathbf{e}} \equiv 0 \pmod{\ell}$. The value of B is uniquely determined by the vector $\mathbf{e}$ for the first type of congruences. The second type consists of sets of congruences of the form $p(\ell n + B)_{\mathbf{e}} \equiv 0 \pmod{\ell}$ with varying values of B using the same values of ℓ and $\mathbf{e}$.

Example 1.12. One example of the first type of congruence is the conjectured congruence

$$p(5n + 2)_{(2,0,0,4)} \equiv 0 \pmod{5}$$

for all $n \geq 0$.

Example 1.13. A set of the second type of congruence is the pair of conjectured congruences

$$p(5n + 2)_{(2,0,0,2)} \equiv p(5n + 3)_{(2,0,0,2)} \equiv 0 \pmod{5}$$

for all $n \geq 0$.

In Section 8.2 we give an algorithm for determining the number of values of $p(n)_{\mathbf{e}}$ that must be computed in order to guarantee a congruence.

Given a vector $\mathbf{e} := (e_1, e_2, \ldots, e_k) \in \mathbb{Z}^k$ and a prime $\ell \geq 5$, we construct a vector of nonnegative integers $\mathbf{c_e} := (c_1, c_2, \ldots, c_k)$. Let $\mathbf{e}' := \mathbf{e} - \ell\mathbf{c_e}$. We then define

$$w := -\frac{1}{2}\sum_{m=1}^{k} e'_m \tag{1.18}$$

and

$$N := 24N_0 \gcd(24, \sum_{m=1}^{k} \frac{N_0}{m} e'_m)^{-1}, \tag{1.19}$$

where $N_0 := \operatorname{lcm}\{m : e'_m \neq 0\}$. The vector $\mathbf{e}'$ satisfies the following conditions:

(i) $e'_m \leq 0$ for all m,

(ii) $\sum_{m=1}^{k} m e'_m \equiv 0 \pmod{24}$,

(iii) $w \in \mathbb{Z}$, and

(iv) $\sum_{m=1}^{k} \frac{N}{m} e'_m \equiv 0 \pmod{24}$.

Now define

$$K_{\mathbf{e}} := \left\lfloor \frac{w}{12} N \prod_{p|N} \left(1 + \frac{1}{p}\right) \right\rfloor \tag{1.20}$$

where the product runs over all prime divisors of N.

For the first type of congruences conjectured in [3], the vector $\mathbf{e}$ determines the value of B as follows: define

$$\alpha := \sum_{m=1}^{k} m e_m \tag{1.21}$$

and

$$\delta_\ell := \begin{cases} \frac{\alpha}{24} \pmod{\ell} & \ell \nmid 24 \\ 0 & \ell \mid 24 \end{cases} \tag{1.22}$$

where $\frac{1}{24}$ is taken as the multiplicative inverse of $24 \pmod{\ell}$. Using this notation, we arrive at the following theorem:

Theorem 1.14. *Assume the notation above. Let $\ell \geq 5$ be prime. Then $p(\ell n+\delta_\ell)_{\boldsymbol{e}} \equiv 0 \pmod{\ell}$ for all n if and only if $p(\ell n + \delta_\ell)_{\boldsymbol{e}} \equiv 0 \pmod{\ell}$ for all $0 \leq n \leq K_{\boldsymbol{e}}$.*

The second type of congruence conjectured in [3] relies on a similar method, but requires using the Legendre symbol with respect to the prime ℓ. Define two sets as follows:

$$S_+ := \left\{\gamma_\ell \in \mathbb{Z} : \left(\frac{\gamma_\ell - \delta_\ell}{\ell}\right) = 1 \text{ and } 0 \leq \gamma_\ell \leq \ell - 1\right\} \tag{1.23}$$

and

$$S_- := \left\{\gamma_\ell \in \mathbb{Z} : \left(\frac{\gamma_\ell - \delta_\ell}{\ell}\right) = -1 \text{ and } 0 \leq \gamma_\ell \leq \ell - 1\right\}. \tag{1.24}$$

We then define

$$K'_{\mathbf{e}} := \left\lfloor \frac{w}{12} N\ell^2 \prod_{p \mid N\ell^2} \left(1 + \frac{1}{p}\right) \right\rfloor, \tag{1.25}$$

where the product runs over all prime divisors of $N\ell^2$.

Theorem 1.15. *Assume the notation above. Let $\ell \geq 2$ be prime where if $\ell = 2$ or 3, $\alpha \equiv 0 \pmod{\ell}$. Then $p(\ell n + \gamma_\ell)_{\boldsymbol{e}} \equiv 0$ (mod ℓ) for all n and all $\gamma_\ell \in S_+$ (resp. S_-) if and only if $p(\ell n+\gamma_\ell)_{\boldsymbol{e}} \equiv 0$ (mod ℓ) for all $0 \leq n \leq K'_{\boldsymbol{e}}$ and all $\gamma_\ell \in S_+$ (resp. S_-).*

With Theorems 1.14 and 1.15, we obtain the next corollary.

Corollary 1.16. *All of the conjectured congruences in* [3] *are true.*

It is natural to ask whether their are congruence relations between the coefficients of the conjugacy growth series of the finitary symmetric group and the finitary alternating group. By (1.17), there exist congruences modulo powers of primes between $2\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2n)$ and $\gamma_{\mathrm{Sym}(\mathbb{N}),S}(n)$ whenever the "discrepancy function," $p_2(2n)$, is congruent to 0. Using the previous theorem we get the following examples.

Example 1.17. For all $n \equiv 2, 3, 4 \pmod 5$, we have that

$$2\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2n) \equiv \gamma_{\mathrm{Sym}(\mathbb{N}),S}(n) \pmod 5.$$

Example 1.18. For all $n \equiv 17, 31, 38, 45 \pmod{49}$, we have that

$$2\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2n) \equiv \gamma_{\mathrm{Sym}(\mathbb{N}),S}(n) \pmod 7.$$

Ramanujan stated congruences for the partition function $p(n)$ modulo powers of 5, 7, and 11, which were proved by Watson in [18]. Atkin also proved the existence of congruences for the function $p_2(n)$ modulo powers of the primes 5, 7, and 13 in [2]. Using these results, we obtain congruences between the coefficients of the conjugacy growth series for these groups modulo powers of 5 and 7.

We will let $S \subset \mathrm{Sym}(\mathbb{N})$ be a generating set of $\mathrm{Sym}(\mathbb{N})$ such that $S_{\mathbb{N}}^{\mathrm{Cox}} \subset S \subset T_{\mathbb{N}}$, where $S_{\mathbb{N}}^{\mathrm{Cox}}$ and $T_{\mathbb{N}}$ are defined by (1.10) and (1.11), respectively. In addition, we let $S' \subset \mathrm{Alt}(\mathbb{N})$ be a generating set for $\mathrm{Alt}(\mathbb{N})$ such that $S_{\mathbb{N}}^{A} \subset S' \subset T_{\mathbb{N}}^{A}$, where $S_{\mathbb{N}}^{A}$ and $T_{\mathbb{N}}^{A}$ are defined by (1.14) and (1.15), respectively. Using this notation, we arrive at the following theorem.

Theorem 1.19. *Assume the notation above. Let $\ell = 5$ or 7 and let $j \geq 1$. Then for all $24n \equiv 1 \pmod{\ell^j}$, we have that*

$$\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2n) \equiv \gamma_{\mathrm{Sym}(\mathbb{N}),S}(n) \equiv 0 \pmod{\ell^{\lfloor j/2-1 \rfloor}}.$$

Example 1.20. For example, modulo 5, 25, and 125, we obtain for all $n \geq 0$ that

$$\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2 \cdot 5^4 n + 1198) \equiv 0 \pmod 5$$

$$\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2 \cdot 5^6 n + 29948) \equiv 0 \pmod{25}$$

$$\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2 \cdot 5^8 n + 748698) \equiv 0 \pmod{125}.$$

Likewise, modulo 7, 49, and 343, we obtain for all $n \geq 0$ that

$$\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2 \cdot 7^4 n + 4602) \equiv 0 \pmod 7$$
$$\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2 \cdot 7^6 n + 225494) \equiv 0 \pmod{49}$$
$$\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2 \cdot 7^8 n + 11049202) \equiv 0 \pmod{343}.$$

We would also like to ask what holds for general primes $\ell \notin \{5, 7\}$. Following the work of Treneer [17], we prove congruences between the coefficients of the conjugacy growth series for $(\mathrm{Alt}(\mathbb{N}), S')$ and $(\mathrm{Sym}(\mathbb{N}), S)$ modulo arbitrary powers of primes $\ell \geq 5$. Treneer's work gives general congruences for coefficients of various types of modular forms. We follow her method and make it explicit.

Let $\ell \geq 5$ be prime. We then define

$$m_\ell := \begin{cases} 2 & 5 \leq \ell \leq 23 \\ 1 & \ell \geq 29, \end{cases} \tag{1.26}$$

$$\delta_\ell := \frac{Q\ell^{m_\ell}\beta_\ell + 1}{24}, \tag{1.27}$$

and

$$\beta_\ell := \frac{23}{Q\ell^{m_\ell}} \pmod{24}. \tag{1.28}$$

Using this notation, we arrive at the following theorem.

Theorem 1.21. *Assume the above notation. Let $\ell \geq 5$ be prime and let $j \geq 1$. Then for a positive proportion of primes $Q \equiv -1 \pmod{144\ell^j}$, we have that*

$$2\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2Q\ell^{m_\ell} n + 2\delta_\ell) \equiv \gamma_{\mathrm{Sym}(\mathbb{N}),S}(Q\ell^{m_\ell} n + \delta_\ell) \pmod{\ell^j}$$

for all $24n + \beta_\ell$ coprime to $Q\ell$.

In Section 2 we will cover the necessary background on modular forms including Hecke operators, eta functions, and divisor polynomials. Section 3 covers the general background on elliptic curves and give a way of determining whether an elliptic curve is supersingular or not. We prove Theorem 1.1 in Section 4. Section 5 covers results on orthogonal polynomials, then we prove Theorem 1.4, Proposition 1.5, Theorem 1.6, and finally Theorem 1.7. In Section 6 we look at the hypergeometric properties of the modular form F_k from Theorem 1.1. We look at asymptotics for the generalized partition functions and prove Theorem 1.9 in Section 7. We give an algorithm for computing the vector $c_{\mathbf{e}}$ in Section 8 and then give proofs of Theorems 1.14 and 1.15. We prove Theorem 1.19 in Section 9. In Section 10 we use our results to look at congruences for $p_2(n)$ and give a proof of Theorem 1.21. The final section, Section 11, is an appendix with a list of the conjectured congruences from [3].

2. Modular Forms

Modular forms play an important role in the theory of elliptic curves. Here we will discuss the necessary background on modular forms. The information discussed here along with more on modular forms can be found in [13] and [12].

The group $\mathrm{SL}_2(\mathbb{Z})$ is the group of 2×2 matrices with integer entries and determinant equal to 1. This group is important in the study of modular forms, and is generated by the matrices

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

The standard fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ is given by

$$\mathfrak{F} = \{\tau : \frac{-1}{2} \leq \Re(\tau) \leq 0 \text{ and } |\tau| \geq 1\} \cup \{\tau : 0 < \Re(\tau) < \frac{1}{2} \text{ and } |\tau| > 1\}. \tag{2.1}$$

In order to give the definition of a modular form, we must first define the notion of a congruence subgroup.

Definition 2.1. For $N \in \mathbb{Z}^+$, the level N *congruence subgroups* $\Gamma_0(N)$, $\Gamma_1(N)$, and $\Gamma(N)$ are defined as

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : c \equiv 0 \pmod{N} \right\}$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ a \equiv d \equiv 1 \pmod{N}, \text{ and } c \equiv 0 \pmod{N} \right\}$$

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ a \equiv d \equiv 1 \pmod{N}, \text{ and } b \equiv c \equiv 0 \pmod{N} \right\}.$$

Given Γ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, then a *cusp of* Γ is an equivalence class in $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \infty$.

Example 2.2. If $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, then there is only one cusp; it is customary to choose the point at ∞ to be its representative.

We will need the following fact about congruence subgroups from [13, p. 2]:

Proposition 2.3. *If N is a positive integer, then*

$$[\Gamma_0(1) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

where the products are over the prime divisors of N.

Given $f(\tau)$ a meromorphic function on $\mathcal{H}$ and $k \in \mathbb{Z}$, the "slash" operator $|_k$ is defined by

$$(f|_k\gamma)(\tau) := (\det \gamma)^{k/2}(c\tau + d)^{-k} f(\gamma\tau),$$

for

$$\gamma\tau := \frac{a\tau + b}{c\tau + d}.$$

Using these notions we can now give the definition of a modular form, which will be essential to the rest of the paper.

Definition 2.4. Given a meromorphic function $f(\tau)$ on the upper half plane $\mathcal{H}$, $k \in \mathbb{Z}$, and Γ a congruence subgroup of level N, then $f(\tau)$ is a *modular form* if the following properties hold.

(1) For all $\tau \in \mathcal{H}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ one gets

$$f\Big(\frac{a\tau + b}{c\tau + d}\Big) = (c\tau + d)^k f(\tau).$$

(2) Given $\gamma_0 \in \mathrm{SL}_2(\mathbb{Z})$, then $(f|_k\gamma_0)(z)$ has a Fourier expansion of the form

$$(f|_k\gamma_0)(\tau) = \sum_{n \geq n_{\gamma_0}} a_{\gamma_0}(n) d_N^n,$$

where $q_N := e^{2\pi i z/N}$ and $a_{\gamma_0} \neq 0$.

2.1. **Eisenstein Series.** The *weight k Eisenstein series* $E_k(\tau)$ plays an important role in the theory of modular forms. Before giving the definition of $E_k(\tau)$, define B_k as the kth Bernoulli number, namely the kth coefficient given by the series

$$\sum_{k=0}^{\infty} B_k \cdot \frac{t^k}{k!} = \frac{t}{e^t - 1} = 1 - \frac{1}{2}t + \frac{1}{12}t^2 + ..., \tag{2.2}$$

Using this definition, we can now define $E_k(\tau)$ as follows.

Definition 2.5. For even k, the k^{th} *Eisenstein series* is defined by

$$E_k(\tau) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \Big(\sum_{d|n} d^{k-1} \Big) q^n, \tag{2.3}$$

where $q = e^{2\pi i \tau}$.

Proposition 2.6. *E_k is a modular form of weight k for $k \geq 4$ and k even. In the case $k = 2$, E_k is not modular.*

Proof. There is a classical calculation, which can be found in [12, pg. 110], that implies

$$2\zeta(k)E_k(\tau) = \sum_{(m,n)\in\mathbb{Z}^2-\{(0,0)\}} \frac{1}{(m\tau+n)^k}, \tag{2.4}$$

where $\zeta(s)$ is the Riemann zeta-function. The double sum given here must be absolutely convergent since $k \geq 4$, and in any compact subset of $\mathcal{H}$ is uniformly convergent. This gives that $E_k(\tau)$ is a holomorphic function on $\mathcal{H}$.

Along with this, observe that by (2.4) one gets that

$$\begin{aligned} E_k(\tau+1) &= \frac{1}{2\zeta(k)} \sum_{(m,n)\in\mathbb{Z}^2-\{(0,0)\}} \frac{1}{(m(\tau+1)+n)^k} \\ &= \frac{1}{2\zeta(k)} \sum_{(m,n)\in\mathbb{Z}^2-\{(0,0)\}} \frac{1}{(m\tau+(m+\tau))^k} \\ &= E_k(\tau) \end{aligned} \tag{2.5}$$

and

$$\begin{aligned} E_k(-\frac{1}{\tau}) &= \frac{1}{2\zeta(k)} \sum_{(m,n)\in\mathbb{Z}^2-\{(0,0)\}} \frac{1}{(m(-1/\tau)+n)^k} \\ &= \frac{1}{2\zeta(k)} \sum_{(m,n)\in\mathbb{Z}^2-\{(0,0)\}} \frac{\tau^k}{(n\tau-m)^k} \\ &= \tau^k E_k(\tau). \end{aligned} \tag{2.6}$$

This implies, since

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

generate $\mathrm{SL}_2(\mathbb{Z})$, that $E_k(\tau) \in M_k$. Therefore, for $k \geq 4$ and k even, E_k is a modular form.

In the case $k = 2$, observe that

$$E_2(\tau) = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n)q^n,$$

where

$$\sigma_{k-1}(n) := \sum_{1 \leq d|n} d^{k-1}.$$

For $\tau \in \mathcal{H}$,

$$\tau^{-2} E_2(-1/\tau) = E_2(\tau) + \frac{12}{2\pi i \tau}, \tag{2.7}$$

thus E_2 is not modular. □

Even though $E_2(\tau)$ is not a modular form, it does play an important role in the theory of modular forms, and is considered to be"nearly modular". More precisely this means

$$E_2\Big(\frac{a\tau + b}{c\tau + d}\Big) = (c\tau + d)^2 E_2(\tau) + \frac{6}{\pi i} c(c\tau + d), \tag{2.8}$$

for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$.

Along with this, define the *Delta-function* as

$$\Delta := \frac{E_4^3 - E_6^2}{1728} \tag{2.9}$$

and the *modular j-invariant* as

$$j(\tau) := \frac{E_4(\tau)^3}{\Delta(\tau)}. \tag{2.10}$$

The next proposition relates E_2, E_4, E_6 and Δ by their derivatives, but first recall that the theta operator is as follows

$$\Theta = q\frac{d}{dq} = \frac{1}{2\pi i}\frac{d}{d\tau}. \tag{2.11}$$

The following theorem and proof are also stated in [4], and more information on the special equations used in the proof can be found there.

Proposition 2.7. *The derivatives of E_2, E_4, E_6, Δ, and j are given by the following*

(2.12)
$$E_2^{'} = \frac{E_2^2 - E_4}{12}, \quad E_4^{'} = \frac{E_2E_4 - E_6}{3}, \quad E_6^{'} = \frac{E_2E_6 - E_4^2}{2}, \quad \Delta^{'} = E_2\Delta, \quad j' = \frac{-E_4^2E_6}{\Delta}.$$

Proof. Ramanujan defined the following equation

$$\Phi_{r,s}(q) := \sum_{(k,n)=1}^{\infty} k^r n^s q^{kn};$$

Eisenstein series are special cases of this function as is discussed in further detail in [4]. Now define the equation

$$S_r := \frac{-B_{r+1}}{2(r+1)} + \Phi_{0,r}(q) = \frac{-B_{r+1}}{2(r+1)} + \sum_{k=1}^{\infty} \frac{k^r q^k}{1-q^k}, \tag{2.13}$$

then

$$E_2(q) = -24S_1, \quad E_4(q) = 240S_3, \quad E_6(q) = -504S_5.$$

From this one can derive the three following equations

$$q\frac{dE_2(q)}{dq} = -24\Phi_{1,2}(q), \tag{2.14}$$

$$q\frac{dE_4(q)}{dq} = 240\Phi_{1,4}, \tag{2.15}$$

$$q\frac{dE_6(q)}{dq} = -504\Phi_{1,6}. \tag{2.16}$$

Recall the identity $\cot^2(\theta) = -(1 + \frac{d}{d\theta}\cot(\theta))$ and observe that

$$\begin{aligned}
\frac{x}{2}\cot\left(\frac{x}{2}\right) &= \frac{-ix}{2} - \frac{ix}{e^{-ix}-1} \\
&= \frac{-ix}{2} + \sum_{m=0}^{\infty} B_m \frac{(-ix)^m}{m!} \\
&= \sum_{n=0}^{\infty} \frac{(-1)^n B_{2n} x^{2n}}{(2n)!},
\end{aligned}$$

where the last step is possible due to the fact that $B_1 = -1/2$ and $B_{2n+1} = 0$ for $n \geq 1$.

Using these one can derive the following

$$\frac{1}{16}\cot^2\Big(\frac{1}{2}\theta\Big) = \frac{1}{4\theta^2} - \frac{1}{24} + \frac{1}{4}\sum_{n=1}^{\infty}\frac{(-1)^n B_{2n+2}(2n+1)\theta^{2n}}{(2n+2)!}.$$

Use the Maclaurin series for $\sin(x)$ and $\cos(x)$, namely

$$\sin(x) = \sum_{n=0}^{\infty}\frac{(-1)^n x^{2n+1}}{(2n+1)!}, \quad \cos(x) = \sum_{n=0}^{\infty}\frac{(-1)^n x^{2n}}{(2n)!},$$

and let x go to $k\theta$ to obtain

$$\begin{aligned}
&\Big(\frac{1}{2\theta} + \frac{1}{2}\sum_{n=1}^{\infty}\frac{(-1)^n B_{2n}\theta^{2n-1}}{(2n)!} + \sum_{k=1}^{\infty}\frac{q^k}{1-q^k}\sum_{n=0}^{\infty}\frac{(-1)^n k^{2n+1}\theta^{2n+1}}{(2n+1)!}\Big)^2 \\
&\quad = \frac{1}{4\theta^2} - \frac{1}{24} + \frac{1}{4}\sum_{n=1}^{\infty}\frac{(-1)^n B_{2n+2}}{(2n)!(2n+2)}\theta^{2n} + \sum_{k=1}^{\infty}\frac{q^k}{(1-q^k)^2}\sum_{n=0}^{\infty}\frac{(-1)^n k^{2n}\theta^{2n}}{(2n)!} \\
&\quad + \frac{1}{2}\sum_{k=1}^{\infty}\frac{kq^k}{1-q^k}\sum_{n=1}^{\infty}\frac{(-1)^{n-1}k^{2n}}{(2n)!}\theta^{2n}.
\end{aligned}$$

Collect common powers of θ, and use (2.13) and

$$\Phi_{1,2n}(q) = \sum_{m,k=1}^{\infty} mk^{2n}q^{mk} = \sum_{k=1}^{\infty}\frac{k^{2n}q^k}{(1-q^k)^2},$$

to get that

$$\begin{aligned}
&\Big(\frac{1}{2\theta} + \frac{S_1}{1!}\theta^3 - \frac{S_3}{3!}\theta + \frac{S_5}{5!}\theta^5 - ...\Big)^2 \\
&\qquad = \frac{1}{4\theta^2} + S_1 - \frac{\Phi_{1,2}}{2!}\theta^2 + \frac{\Phi_{1,4}}{4!}\theta^4 - ... + \frac{1}{2}\Big(\frac{S_3}{2!}\theta^2 - \frac{S_5}{4!}\theta^4 + \frac{S_7}{6!}\theta^6 - ...\Big).
\end{aligned}$$

Again equate coefficients, this time of θ^{2n} for $n \geq 1$, to get

$$\begin{aligned}
&\frac{(-1)^{n-1}}{2}\frac{S_{2n+1}}{(2n)!} + \frac{(-1)^n}{(2n)!}\Phi_{1,2n} \\
&\qquad = (-1)^{n-1}\Big(\frac{S_1}{1!}\frac{S_{2n-1}}{(2n-1)!} + \frac{S_3}{3!}\frac{S_{2n-3}}{(2n-3)!} + ... + \frac{S_{2n-1}}{(2n-1)!}\frac{S_1}{1!}\Big) + \frac{(-1)^n S_{2n+1}}{(2n+1)!},
\end{aligned}$$

which simplifies to

$$\frac{(2n+3)}{2(2n+1)}S_{2n+1} - \Phi_{1,2n} = \sum_{k=1}^{n} \binom{2n}{2k-1} S_{2n-2k+1}. \tag{2.17}$$

Set $n = 1$ in (2.17) to get

$$288\Phi_{1,2} = E_4(q) - E_2(q)^2; \tag{2.18}$$

set $n = 2$ in (2.17) to get

$$720\Phi_{1,4} = E_2(q)E_4(q) - E_6(q); \tag{2.19}$$

set $n = 3$ in (2.17) to get

$$1008\Phi_{1,6} = E_4(q)^2 - E_2(q)E_6(q). \tag{2.20}$$

Substitute (2.18) into (2.14) to get

$$q\frac{dE_2(q)}{dq} = \frac{E_2(q)^2 - E_4(q)}{12} \tag{2.21}$$

substitute (2.19) into (2.15) to get

$$q\frac{dE_4(q)}{dq} = \frac{E_2(q)E_4(q) - E_6(q)}{3}; \tag{2.22}$$

substitute (2.20) into (2.16) to get

$$q\frac{dE_6(q)}{dq} = \frac{E_2(q)E_6(q) - E_4(q)^2}{2}. \tag{2.23}$$

Now since Δ is defined as in (2.9), one gets that

$$\Delta' = \frac{3E_4^2E_4' - 2E_6E_6'}{1728},$$

substituting in for E_4' and E_6' we get

$$\frac{E_2(q)(E_4(q)^3 - E_6(q)^2)}{1728} = E_2(q)\Delta(q). \tag{2.24}$$

Recall j is define by (2.10) so

$$j' = \frac{\Delta 3E_4^2E_4' - E_4^3\Delta'}{\Delta^2},$$

by substituting in the equations for E_4' and Δ' this becomes

$$\frac{\Delta E_4^2(E_2E_4 - E_6) - E_4^3(E_2\Delta)}{\Delta^2} = \frac{-E_4^2E_6}{\Delta}.$$

□

2.2. **Eta Functions.** One modular form which will be important for the second half of this paper is *Dedekind's eta-function*, a weight 1/2 modular form defined as the infinite product

$$\eta(z) := q^{1/24}\prod_{n=1}^{\infty}(1-q^n),$$

where $q := e^{2\pi iz}$ and $z \in \mathbb{H}$. A useful fact about the eta-function is that it has the following transformation property as described in [13, p. 17]:

$$\eta\left(-\frac{1}{z}\right) = (-iz)^{\frac{1}{2}}\,\eta\,(z)\,. \tag{2.25}$$

Definition 2.8. An *eta-quotient* is a function $f(z)$ of the form

$$f(z) := \prod_{\delta|N}\eta(\delta z)^{r_\delta},$$

where $N \geq 1$ and each r_δ is an integer. If each $r_\delta \geq 0$, then $f(z)$ is known as an *eta-product*.

The following proposition regards properties of eta quotients.

Proposition 2.9. *If* $f(z) = \prod_{\delta|N}\eta(\delta z)^{r_\delta}$ *has integer weight* $k = \frac{1}{2}\sum_{\delta|N} r_\delta$, *with the additional properties that*

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

and

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

then $f(z)$ *satisfies*

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z) \tag{2.26}$$

for every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ *where the character* χ *is defined by* $\chi(d) := \left(\frac{(-1)^k s}{d}\right)$, *where* $s := \prod_{\delta|N} \delta^{r_\delta}$.

2.3. **Operators on Modular Forms.** Any modular form that is holomorphic (resp. vanishes) at all cusps of $\Gamma_0(N)$ and satisfies (2.26) is said to have Nebentypus character χ. The space of these forms is denoted $M_k(\Gamma_0(N), \chi)$ (resp. $S_k(\Gamma_0(N), \chi)$). If k is a positive integer and $f(z)$ satisfies the conditions of Proposition 2.9 and is holomorphic (resp. vanishes) at all of the cusps of $\Gamma_0(N)$, then $f(z) \in M_k(\Gamma_0(N), \chi)$ (resp. $S_k(\Gamma_0(N), \chi)$). If $f(z)$ satisfies the conditions of Proposition 2.9 but has poles at the cusps of $\Gamma_0(N)$, then call $f(z)$ a *weakly holomorphic modular form*; the space of such forms is denoted $M_k^!(\Gamma_0(N), \chi)$.

Definition 2.10. If $f(z) = \sum_{n=n_0}^{\infty} a(n)q^n$ is a weight k modular form, then the action of the *U-operator* $U(d)$ on $f(z)$ is defined by

$$f(z) \mid U(d) := d^{\frac{k}{2}-1} \sum_{v=0}^{d-1} f(z) \mid_k \sigma_{v,d} = \sum_{n=n_0}^{\infty} a(dn)q^n.$$

Likewise, the action of the *V-operator* $V(d)$ is defined by

$$f(z) \mid V(d) := d^{-\frac{k}{2}} f(z) \mid_k \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} = \sum_{n=n_0}^{\infty} a(n)q^{dn}.$$

Let V_k denote the space of holomorphic functions in $\mathcal{H}$ that transform like modular forms of weight k with at most exponential growth at infinity for $f \in V_k$. Define

the Hecke operators on V_k by

$$(f|_k T_n)(\tau) := n^{k/2} \sum_A \frac{1}{(c\tau+d)^k} f\Big(\frac{a\tau+b}{c\tau+d}\Big), \tag{2.27}$$

where $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \setminus \mathcal{M}_n$ for $n \in \mathbb{N}$ and $\mathcal{M}_n$ the set of 2×2 matrices with integral coefficients and determinant equal to n.

More precisely, we can define the Hecke operator in regards to the character χ of a modular form and a prime p as follows in the next definition.

Definition 2.11. If $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(N), \chi)$ and p is prime, then the action of the *Hecke operator* $T_{p,k,\chi}$ on $f(z)$ is defined by

$$f(z) \mid T_{p,k,\chi} := \sum_{n=0}^{\infty} (a(pn) + \chi(p)p^{k-1}a(n/p))q^n,$$

where $a(n/p) = 0$ if $p \nmid n$.

The Hecke operator only makes sense for $f \in V_k$, but for any 1-periodic function f, define the Hecke operator at infinty as

$$(f|_k T_n^{\infty}) := n^{k/2} \sum_{\substack{ad=n \\ a,d>0}} \sum_{b(mod)d} d^{-k} f\Big(\frac{a\tau+b}{d}\Big). \tag{2.28}$$

Since the matrices $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with $0 \leq b < d = \frac{n}{a}$ are set representatives for $\Gamma \setminus \mathcal{M}_n$, the operator at infinity agrees with $|_k T_n$ for $f \in V_k$.

Now recall the following result from [13, p. 21,28]:

Proposition 2.12. *Suppose that* $f(z) \in M_k(\Gamma_0(N), \chi)$.

(1) If $d \mid N$, *then*

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

(2) If d *is a positive integer, then*

$$f(z) \mid V(d) \in M_k(\Gamma_0(Nd), \chi).$$

(3) If p is prime, then

$$f(z) \mid T_{p,k,\chi} \in M_k(\Gamma_0(N), \chi).$$

Note that when one hits with the U and V operators, or multiplies by another modular form, that the character χ is apt to change. For more information on these operators see [13, pg. 28].

We now recall the notion of a "twist" of a modular form. Suppose that $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(N), \chi)$. If ψ is a Dirichlet character (mod m), then the *ψ-twist* of $f(z)$ is defined by

$$f_\psi(z) := \sum_{n=0}^{\infty} \psi(n)a(n)q^n.$$

Recall that $\psi(n) = 0$ if $\gcd(n, m) \neq 1$. We will use a property of "twists" from [13, p. 23]:

Proposition 2.13. *Suppose that $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(N), \chi)$. If ψ is a Dirichlet character with modulus m, then*

$$f_\psi(z) \in M_k(\Gamma_0(Nm^2), \chi\psi^2).$$

2.4. **Divisor Polynomials.** Now the notion of a divisor polynomial of a modular form will be defined as given in [13, p. 31]. Define $\widetilde{E}_k$ as

$$\widetilde{E}_k(\tau) := \begin{cases} 1 & \text{if } k \equiv 0 \pmod{12}, \\ E_4(\tau)^2 E_6(\tau) & \text{if } k \equiv 2 \pmod{12}, \\ E_4(\tau) & \text{if } k \equiv 4 \pmod{12}, \\ E_6(\tau) & \text{if } k \equiv 6 \pmod{12}, \\ E_4(\tau)^2 & \text{if } k \equiv 8 \pmod{12}, \\ E_4(\tau)E_6(\tau) & \text{if } k \equiv 10 \pmod{12}, \end{cases} \tag{2.29}$$

and $m(k)$ as

$$m(k) := \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor & \text{if } k \not\equiv 2 \pmod{12}, \\ \left\lfloor \frac{k}{12} \right\rfloor - 1 & \text{if } k \equiv 2 \pmod{12}. \end{cases} \tag{2.30}$$

Now given $f(\tau) \in M_k$ with $\widetilde{F}(f,x)$ the unique rational function in x such that

$$f(\tau) = \Delta(\tau)^{m(k)} \widetilde{E}_k(\tau) \widetilde{F}(f, j(z)),$$

then $\widetilde{F}(f,x)$ is a polynomial. Further, define the *divisor polynomial* of f by

$$F(f,x) := h_k(x) \widetilde{F}(f,x), \tag{2.31}$$

where $h_k(x)$ is given by

$$h_k(x) := \begin{cases} 1 & \text{if } k \equiv 0 \pmod{12}, \\ x^2(x-1728) & \text{if } k \equiv 2 \pmod{12}, \\ x & \text{if } k \equiv 4 \pmod{12}, \\ x - 1728 & \text{if } k \equiv 6 \pmod{12}, \\ x^2 & \text{if } k \equiv 8 \pmod{12}, \\ x(x-1728) & \text{if } k \equiv 10 \pmod{12}. \end{cases} \tag{2.32}$$

Now recall that in examples (1.2) and (1.3) found in section (1.1), we gave $F(f,x)$ and $\widetilde{F}(f, j(\tau))$ for $f = E_k, G_k, H_k, F_k$ without showing where we had obtained these values. In the following example we will work through the calculations for the case $p = 23$ using the definitions of $\widetilde{E}_k$, $m(k)$, and $h_k(x)$.

Example 2.14. In the case $p = 23$ we have that $k = 22 \equiv 10 \pmod{12}$, so we have that

$$\widetilde{E}_{22}(\tau) = E_4(\tau)E_6(\tau), \quad m(22) = \left\lfloor \frac{22}{12} \right\rfloor = 1, \quad h_{22}(j(\tau)) = j(\tau)(j(\tau) - 1728).$$

This gives that

$$E_{22}(\tau) = \Delta(\tau)E_4(\tau)E_6(\tau)\widetilde{F}(E_{22}, j(\tau)),$$
$$G_{22}(\tau) = \Delta(\tau)G_4(\tau)E_6(\tau)\widetilde{F}(G_{22}, j(\tau)),$$
$$H_{22}(\tau) = \Delta(\tau)E_4(\tau)E_6(\tau)\widetilde{F}(H_{22}, j(\tau)),$$
$$F_{22}(\tau) = \Delta(\tau)E_4(\tau)E_6(\tau)\widetilde{F}(F_{22}, j(\tau)),$$

where E_k is the Eisenstein series defined in this section, and G_k, H_k, F_k are modular forms that will be defined in section 4.

Using these equations we get that

$$\widetilde{F}(E_{22}, j(\tau)) = \frac{E_{22}(\tau)}{\Delta E_4(\tau)E_6(\tau)},$$
$$\widetilde{F}(G_{22}, j(\tau)) = \frac{G_{22}(\tau)}{\Delta E_4(\tau)E_6(\tau)},$$
$$\widetilde{F}(H_{22}, j(\tau)) = \frac{H_{22}(\tau)}{\Delta E_4(\tau)E_6(\tau)},$$
$$\widetilde{F}(F_{22}, j(\tau)) = \frac{F_{22}(\tau)}{\Delta E_4(\tau)E_6(\tau)},$$

which gives that the divisor polynomials for these modular forms are

$$F(E_{22}, j(\tau)) = j(\tau)(j(\tau) - 1728)\frac{E_{22}(\tau)}{\Delta(\tau)E_4(\tau)E_6(\tau)},$$
$$F(G_{22}, j(\tau)) = j(\tau)(j(\tau) - 1728)\frac{G_{22}(\tau)}{\Delta(\tau)E_4(\tau)E_6(\tau)},$$
$$F(H_{22}, j(\tau)) = j(\tau)(j(\tau) - 1728)\frac{H_{22}(\tau)}{\Delta(\tau)E_4(\tau)E_6(\tau)},$$
$$F(F_{22}, j(\tau)) = j(\tau)(j(\tau) - 1728)\frac{F_{22}(\tau)}{\Delta(\tau)E_4(\tau)E_6(\tau)}.$$

The divisor polynomial is important for reducing certain modular forms modulo p to the supersingular polynomial $ss_p(j)$, which will be defined in the next section.

3. Elliptic Curves

In [12], an *elliptic curve* over a field K is defined by a cubic polynomial $y^2 = f(x)$ with coefficients in K with distinct roots. The K' *points* of the elliptic curve are the solutions to the equation $y^2 = f(x)$. The fact that the curve has no multiple roots makes it a smooth curve, i.e. the partial derivatives do not vanish at any point on the curve. Along with this, an elliptic curve has what will be called the point at infinity. In order to properly define the point at infinity we will briefly discuss projective coordinates.

Given a curve $y^2 = f(x)$ we can rewrite it as $F(x, y) = 0$. Given a term $x^i y^j$, the total degree is $i + j$. If the maximum total degree of $F(x, y)$ is n, define the homogeneous polynomial $\widetilde{F}(x, y, z)$ to be the polynomial obtained by multiplying each monomial $x^i y^j$ in $F(x, y)$ by z^{n-i-j}. This brings the total degree in three variables x, y, z to n. More precisely one gets

$$\widetilde{F}(x, y, z) = z^n F(x, y).$$

Now, for any $\lambda \in K$ one has that

$$\widetilde{F}(\lambda x, \lambda y, \lambda z) = \lambda^n \widetilde{F}(x, y, z), \tag{3.1}$$

and for any nonzero $\lambda \in K$ we have $\widetilde{F}(\lambda x, \lambda y, \lambda z) = 0$ if and only if $\widetilde{F}(x, y, z) = 0$. More precisely, for $z \neq 0$, $\widetilde{F}(x, y, z) = 0$ if and only if $F(x/z, y/z) = 0$. This makes it natural to say that two points (x, y, z) and (x', y', z') are equivalent if there is a nonzero $\lambda \in K$ such that $(x', y', z') = \lambda(x, y, z)$. The projective plane $\mathbb{P}^2_K$ is then the set of equivalence classes of triples (x, y, z) under this relation and omitting the point $(0, 0, 0)$. Observe that every equivalence class (x, y, z), with nonzero z, has a unique point $(x, y, 1)$, thus one can think of such equivalence classes as points in the xy-plane. The left over points $(x, y, 0)$ form the line at infinity. This line at infinity can be taken as an ordinary line made up of the equivalence classes with nonzero y,

which must contain a unique point of the form $(x, 1, 0)$, along with the single point $(1, 0, 0)$ which is called the point at infinity. This allows one to think of $\mathbb{P}^2_K$ as the plane $(x, y, 1)$ with a projective line at infinity consisting of the line $(x, 1, 0)$ and its point at infinity $(1, 0, 0)$.

Therefore given $\widetilde{F}(x, y, z)$ with $x, y, z \in K$ one can look at the solutions (x, y, z) in $\mathbb{P}^2_K$ to the equation $\widetilde{F}(x, y, z) = 0$. The solutions to this equation with $z \neq 0$ are the points $(x, y, 1)$ such that $\widetilde{F}(x, y, 1) = F(x, y) = 0$. The left over points are on the line at infinity.

Example 3.1. Let $f(x) = x^3 - n^2x$, then the elliptic curve $y^2 = x^3 - n^2x$ corresponds to the equation $y^2z = x^3 - n^2xz^2$. So using this we have

$$F(x, y) = y^2 - x^3 + n^2x \text{ and } \widetilde{F}(x, y, z) = y^2z - x^3 + n^2xz^2.$$

The points at infinity for this curve are the equivalence classes $(x, y, 0)$ where $0 = \widetilde{F}(x, y, 0) = -x^3$, namley $x = 0$. This in turn gives the equivalence class $(0, 1, 0)$.

Note that any elliptic curve $y^2 = f(x)$ will have exactly one point at infinity and it will be the same point seen in the example: $(0, 1, 0)$. For more information on this see [12].

Every elliptic curve E over K can be written in terms of an affine equation, i.e. a nonhomogeneous linear equation, of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_0, \tag{3.2}$$

where each a_i is in K. This equation is the *generalized Weierstrass equation* of E.

The characteristic of K, denoted $\text{char}(K)$, is the minimal $m \in \mathbb{Z}$ such that m times the identity element of K equals zero. When $\text{char}(K) \neq 2$ or 3, the curve E can be written, through a change of variables, in a reduced version of this equation

known as the *Weierstrass equation*. The Weierstrass equation of E is of the form

$$y^2 = x^3 + ax + b$$

with $a, b \in K$. For more on the Weierstrass equations of an elliptic curve, see [7].

Example 3.2. The equation $y^2 = x^3 + 1$ is an elliptic curve since it has no multiple roots. The graph of this curve is given in the following figure.

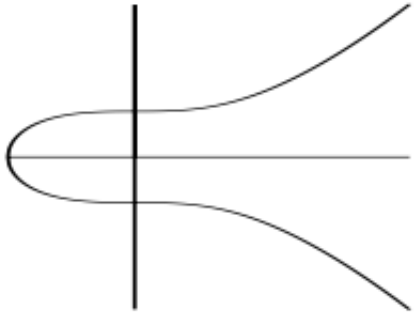

FIGURE 1. $y^2 = x^3 + 1$

Example 3.3. The equation $y^2 = x^3 - 3x + 2 = (x-1)^2(x+2)$ is not an elliptic curve since 1 is a multiple root of the equation.

There exists a group law under which the points with coordinates in K on an elliptic curve E over K in union with the point at infinity form an abelian group which is denoted $E(K)$. Suppose you are given two points already on the curve, $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, then there exists a group law which will give you a third point $P_3 = (x_3, y_3)$. Begin by looking at the line which connects P_1 and P_2. This line is as follows

$$y = \lambda x + v, \text{ where } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } v = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

Now substitute $y = \lambda x + v$ into the equation for the curve to get

$$y^2 = (\lambda x + v)^2 = x^3 + ax^2 + bx + c,$$

which becomes

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda v)x + (c - v^2).$$

The three roots x_1, x_2, x_3 of this cubic equation give the x-coordinates of the three intersection points of the line with the curve, therefore

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda v)x + (c - v^2) = (x - x_1)(x - x_2)(x - x_3).$$

By equating coefficients of x^2 on either side, one gets

$$a - \lambda^2 = -x_1 - x_2 - x_3,$$

thus

$$x_3 = \lambda^2 - a - x_1 - x_2 \text{ and } y_3 = \lambda x_3 + v.$$

This construction and the following example come from [16, p. 23-27].

Example 3.4. Let our elliptic curve be given by the following equation

$$y^2 = x^3 + 17,$$

and our initial points be

$$P_1 = (-1, 4) \text{ and } P_2 = (2, 5).$$

The line through these points along with λ and v are given by

$$y = \frac{1}{3}x + \frac{13}{3} \text{ with } \lambda = \frac{1}{3} \text{ and } v = \frac{13}{3}.$$

Therefore using the equations for x_3 and y_3 we get

$$x_3 = -\frac{8}{9} \text{ and } y_3 = \frac{109}{27},$$

so $P_3 = (-\frac{8}{9}, \frac{109}{27})$.

Two important quantities related to elliptic curves are the j-invariant and discriminant of E. Given that E is written in the form $y^2 = x^3 + ax + b$, the *j-invariant* and *discriminant* of E are defined in [14] as

$$j(E) := \frac{(-48a)^3}{\Delta(E)}, \quad \Delta(E) := -16(4a^3 + 27b^2). \tag{3.3}$$

The j-invariant identifies E up to isomorphism over $\bar{\mathbb{F}}_q$. More precisely, if E_1 and E_2 are two elliptic curves over the field K, then there is an isomorphism from E_1 to E_2 over the algebraic closure $\overline{K}$ if and only if their j-invariants are the same, i.e. $j(E_1) = j(E_2)$. See [15, p. 45-47] for a proof of this.

3.1. **Supersingular Elliptic Curves.** From here on out it is assumed that the field K is of the form $\mathbb{F}_q$ for $q = p^r$ where p is prime, i.e. the field K will be taken to be a finite field of characteristic p.

Definition 3.5. Given an elliptic curve E over $\mathbb{F}_q$, the N-torsion of E is defined in [14] as

$$E[N] := \{P \in E(\bar{\mathbb{F}}_q) : NP = O_E\}.$$

Definition 3.6. An elliptic curve E over a field $\mathbb{F}_q$, where $q = p^r$ for some prime p, is *supersingular* if any of the following equivalent statements are true [14]:

i) $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$,

ii) $E(\bar{\mathbb{F}}_q)$ has no p-torsion,

iii) $\mathrm{End}(\mathbb{F}_q)$ is non-commutative.

If E is not supersingular, then it is called *ordinary*.

Note that supersingularity depends on the j-invariant of E, and if E is supersingular then the j-invariant of E is contained in $\mathbb{F}_{p^2}$ [15, pg. 148]. There are approximately $\frac{p}{12}$ supersingular j-invariants in $\mathbb{F}_{p^2}$.

Let $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ be the set of automorphisms of $\mathbb{F}_q$ that map every element of $\mathbb{F}_p$ to itself, then

$$N_{\mathbb{F}_q/\mathbb{F}_p}(x) := \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)} \sigma(x).$$

Using these notations, the following proposition gives a way to determine whether an elliptic curve E is supersingular or not.

Proposition 3.7. *Take E to be an elliptic curve over $\mathbb{F}_q$ defined by the equation $y^2 = f(x)$ for $f(x) \in \mathbb{F}_q[x]$ of degree 3. Let a_p be the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$, then $|E(\mathbb{F}_q)| \equiv 1 - N_{\mathbb{F}_q/\mathbb{F}_p}(a_p)$.*

Proof. For $x \in \mathbb{F}_q$, observe that

$$f(x)^{(q-1)/2} = \left(\frac{f(x)}{p}\right) = \begin{cases} -1 & \text{if } f(x) \notin (\mathbb{F}_q)^2 \\ 0 & \text{if } f(x) = 0 \\ 1 & \text{if } f(x) \in (\mathbb{F}_q^\times)^2. \end{cases}$$

Therefore the number of solutions to $y^2 = f(x)$ given such an $x \in \mathbb{F}_q$ equals

$$1 + f(x)^{(q-1)/2} = \begin{cases} 0 & \text{if } f(x) \notin (\mathbb{F}_q)^2 \\ 1 & \text{if } f(x) = 0 \\ 2 & \text{if } f(x) \in (\mathbb{F}_q^\times)^2. \end{cases}$$

Counting the point at infinity this gives

$$|E(\mathbb{F}_q)| = 1 + \sum_{x \in \mathbb{F}_q} (1 + f(x)^{(q-1)/2}) \quad \text{in } \mathbb{F}_q.$$

Now define the sum over elements in $\mathbb{F}_q$ to the j^{th} power by $S^n := \sum_{x \in \mathbb{F}_q} x^n$. If $n = 0$, then $S^n = p^n \cdot 1 = 0$. If $n \geq 1$ with $(q-1)|n$ then $0^n = 0$ and $x^n = 1$ for $x \neq 1$, thus $S^n = (q-1) \cdot 1 = -1$. If $n \geq 1$ but $(q-1) \nmid n$ then there exists some $y \in \mathbb{F}_q$ such

that $y^n \neq 1$, but

$$y^n S^n = y^n \sum_{x \in \mathbb{F}_q} x^n = \sum_{x \in \mathbb{F}_q} y^n x^n = \sum_{x \in \mathbb{F}_q} (yx)^n.$$

Since yx ranges over the field when x does, this gives that the last sum is equal to S^n, thus

$$y^n S^n = S^n,$$

which implies that in this case $S^n = 0$. Therefore, the sum $\sum_{x \in \mathbb{F}_q} x^n$ is equal to -1 when $n|(q-1)$ and $n \neq 0$, otherwise the sum is equal to 0.

Since $f(x)$ is a polynomial of degree 3, in the expansion of $f(x)^{(q-1)/2}$ every term is of the form x^n for $0 \leq n \leq \frac{3}{2}(q-1)$. This implies that

$$\sum_{x \in \mathbb{F}_q} (1 + f(x)^{(q-1)/2}) = -a_q,$$

where a_q is the coefficient of $x^{(q-1)}$ in the sum, thus

$$|E(\mathbb{F}_q)| = 1 - a_q \quad \text{in } \mathbb{F}_q.$$

On the other hand, for $q = p^r$, the expansion

$$f(x)^{\frac{q-1}{2}} = f(x)^{\frac{p-1}{2}(1+p+\ldots+p^r)} = f(x)^{\frac{p-1}{2}} f^{(p)}(x^p)^{\frac{p-1}{2}} \ldots f^{(p^{r-1})}(x^{p^{r-1}})^{\frac{p-1}{2}},$$

where $f^{(p^n)}$ is the polynomial obtained by raising the coefficients of f to the p^nth power, implies that

$$a_q = a_p^{1+p+\ldots+p^r} = \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)} \sigma(a_p) = N_{\mathbb{F}_q/\mathbb{F}_p}(a_p),$$

which completes the proof of the proposition. □

Corollary 3.8. *E is supersingular if and only if $a_p = 0$.*

Proof. If $a_p = 0$ then $|E(\mathbb{F}_q)| \equiv 1 \pmod{p}$, thus E has no p-torsion over $\bar{\mathbb{F}}_p$ and is supersingular. On the other hand if $a_p \neq 0$ then $|E(\mathbb{F}_{q^n})| \equiv 1 - (N_{\mathbb{F}_q/\mathbb{F}_p}(a_p))^n$. If the order of $N_{\mathbb{F}_q/\mathbb{F}_p}(a_p)$ divides n, then $1-(N_{\mathbb{F}_q/\mathbb{F}_p}(a_p))^n$ is divisible by p. Therefore $1 - (N_{\mathbb{F}_q/\mathbb{F}_p}(a_p))^n \equiv 0 \pmod{p}$, so E does have p-torsion and is ordinary. □

Example 3.9. Take $E : y^2 = x^3 - x$, and assume $p \equiv 3 \pmod{4}$ for p prime, then $a_p = 0$ for a_p as in Proposition 3.7. This gives that $|E(\mathbb{F}_{p^r})| \equiv 1 \pmod{p}$, which gives that E is supersingular over $\mathbb{F}_{p^2}$.

Given an elliptic curve E over $\mathbb{F}_q$ of characteristic p, the supersingular polynomial is given by

$$ss_p(j) = \prod_{\substack{E/\bar{\mathbb{F}}_p \\ E\ supersingular}} (j - j(E)) \quad \in \mathbb{F}_p[j]. \tag{3.4}$$

Majority of the first half of this paper will focus on ways of reducing polynomials to ss_p modulo p prime.

4. Polynomials That Reduce to the Supersingular Polynomial

In [11] the authors are interested in ways of computing the supersingular polynomials for elliptic curves, which was defined in equation (3.4). Zagier and Kaneko describe several ways of constructing canonical polynomials in $\mathbb{Q}[j]$ that reduce modulo p to $ss_p(j)$. They begin by showing that there exists a family of polynomials that come from special modular forms of weight $p-1$ that reduce to ss_p.

Let M_k be the space of modular forms of weight k on $\Gamma = PSL(2,\mathbb{Z})$. Then k can be written uniquely as

$$k = 12m + 4\delta + 6\epsilon, \quad m \in \mathbb{Z}_{\geq 0}, \quad \delta \in \{0,1,2\}, \quad \epsilon \in \{0,1\}. \tag{4.1}$$

The dimension of M_k $\dim M_k$ is equal to $m+1$ and the modular forms in M_k can be uniquely written as

$$f(\tau) = \Delta(\tau)^m E_4(\tau)^\delta E_6(\tau)^\epsilon \widetilde{f}(j(\tau)) \tag{4.2}$$

where $\widetilde{f}$ is a polynomial of degree $\leq m$ in $j(\tau)$, and the coefficient of j^m in $\widetilde{f}$ is equal to the constant term of the Fourier expansion of f. Note that the values of m, δ, ϵ and $\widetilde{f}$ can be found using (2.29) and (2.30), (2.31), and (2.32). For each k, define the four modular forms E_k, G_k, H_k, F_k as follows:

- $E_k :=$ the normalized Eisenstein series of weight k;
- $G_k :=$ the coefficient of X^k in $(1 - 3E_4(\tau)X^4 + 2E_6(\tau)X^6)^{-1/2}$;
- $H_k :=$ the coefficient of X^k in $(1 - 3E_4(\tau)X^4 + 2E_6(\tau)X^6)^{k/2}$;
- F_k, for $k \not\equiv 2 \pmod 3$, is the unique normalized solution in M_k of the differential equation $\vartheta_{k+1}\vartheta_k F_k = \frac{k(k+2)}{144} E_4 F_k$. Let $\vartheta_k : M_k \to M_{k+2}$ given by $f \to f' - kE_2 f/12$ with $f' = (2\pi i)^{-1} df/d\tau = q df/dq$. Note, E_2 is the nearly modular Eisenstein series of weight 2.

Definition 4.1. Given a prime p, and a nonzero $t \in \mathbb{Q}$, then t can be written uniquely in the form $t = \frac{a}{b}p^r$ for some $a, b, r \in \mathbb{Z}$ with $b > 0$, and $\gcd(p, ab) = \gcd(a, b) = 1$. The *p-adic norm* of t is then given by

$$|t|_p := \begin{cases} p^{-r} & t \neq 0 \\ 0 & t = 0. \end{cases} \tag{4.3}$$

Using the the p-adic norm, one can define the notion of p-integrality as follows.

Definition 4.2. Given $t \in \mathbb{Q}$, call t *p-integral* if $|t|_p \leq 1$, and call a polynomial $f(x) \in \mathbb{Q}[x]$ *p-integral* if all of the coefficients of $f(x)$ are p-integral.

Following the notations just given we get Theorem 1.1, which we will now prove.

4.1. **Proof of Theorem 1.1.** Recall that (2.12) gives E_2', E_4', E_6', and Δ', and note that more generally one gets that $\vartheta_k(f) = f' - \frac{k}{12}E_2 f \in M_{k+2}$ for all $f \in M_k$, and where $'$ denotes differentiation with respect to $2\pi i\tau$. With k as in (4.1), any $f \in M_k$ has a zero of multiplicity $\geq \delta$ at $\tau = e^{\pi i/3}$ and a zero of multiplicity $\geq \epsilon$ at $\tau = e^{\pi i/2}$. This gives that $E_4^\delta E_6^\epsilon$ divides f, and that there exists a polynomial $\widetilde{f}$ of degree $\leq m$ as in (4.2) which represents f. If $k \not\equiv 0 \pmod 3$, then E_4 divides every element of M_{k+4}. This implies that there exists an endomorphism ϕ_k of M_k defined by $\phi_k(f) = E_4^{-1}\vartheta_{k+2}(\vartheta_k(f))$. However, $\kappa_k := \frac{k(k+2)}{144}$ times the constant term of f is the constant term of $\phi_k(f)$, thus the map preserves the codimension 1 subspace of cusp forms and induces the map multiplication by κ_k on the quotient space. Therefore, κ_k is an eigenvalue of ϕ_k. Let F_k be a corresponding eigenvector; the other eigenvectors are then the modular forms $\Delta^i F_{k-12i}$ for $i \in [1, m]$ with the eigenvalues $\kappa_{k-12i} \neq \kappa_k$ since $\vartheta_k \cdot \Delta^i = \Delta^i \cdot \vartheta_{k-12i}$. This gives that F_k, up to a normalizing factor, is unique.

Now let $p \geq 5$ be prime, then for any elliptic curve E over $\mathbb{F}_q$ of characteristic p, E can be written in Weirstrass form as

$$E:\ y^2 = x^3 - 3Qx + 2R.$$

If Q has degree four and R has degree six, define a graded homogeneous polynomial $H_{p-1}(Q, R)$ of degree $p-1$ as the coefficient of x^{p-1} in $(x^3 - 3Qx + 2R)^{(p-1)/2}$. Note that if $Q = E_4(\tau)$ and $R = E_6(\tau)$, then $H_{p-1}(E_4(\tau), E_6(\tau))$ is equal to $H_{p-1}(\tau)$ defined at the beginning of Section 4.

As was noted at the beginning of Section 4, $H_{p-1}(Q, R)$ can be written as

$$H_{p-1}(Q, R) = \Delta^m Q^\delta R^\epsilon \widetilde{H}_{p-1}(j)$$

for some $\widetilde{H}_{p-1} \in \mathbb{Z}[j]$. Using equations (2.29) and (2.30) for $H_{p-1}(Q,R)$ one gets that for $k = p-1$,

$$m = \left\lfloor \frac{p}{12} \right\rfloor, \quad \delta = \begin{cases} 0 & \text{if } p \equiv 1 \pmod 3, \\ 1 & \text{if } p \equiv 2 \pmod 3, \end{cases} \quad \epsilon = \begin{cases} 0 & \text{if } p \equiv 0 \pmod 4, \\ 1 & \text{if } p \equiv 1 \pmod 4. \end{cases}$$

Along with this, a_p from Corollary 3.8 is given by the divisor polynomial, found using (2.31), thus E is supersingular if and only if $j^\delta(j-1728)^\epsilon \widetilde{H}_{p-1}(j) = 0$. If this is the case, then

$$ss_p(j) | j^\delta (j-1728)^\epsilon \widetilde{H}_{p-1}(j).$$

Since ss_p and $j^\delta(j-1728)^\epsilon \widetilde{H}_{p-1}(j)$ have the same zeros, it suffices to show that $j^\delta(j-1728)^\epsilon \widetilde{H}_{p-1}(j)$ has no multiple roots since ss_p is by definition square free.

By the expansion

$$(x^3 - 3Qx + 2R) = (x^3+2R)^{(p-1)/2} - 3\frac{p-1}{2} Qx (x^3+2R)^{(p-3)/2} + O(Q^2)$$

one gets that

$$H_{p-1}(x) = \begin{cases} \binom{\frac{p-1}{2}}{\frac{p-1}{3}} + O(Q) & \text{if } p \equiv 1 \pmod 3 \\ -3\frac{p-1}{2}\binom{\frac{p-3}{2}}{\frac{p-2}{3}} 2R^{\frac{p-5}{6}} Q + O(Q^2) & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

This implies that $\widetilde{H}_{p-1}(0) \not\equiv 0 \pmod p$ and by a similar argument $\widetilde{H}_{p-1}(1728) \not\equiv 0 \pmod p$. Along with this, since $H_{p-1}(Q,R)$ satisfies a second order linear differential equation with polynomial coefficients and leading coefficient $j(j-1728)$, no $x \in \bar{\mathbb{F}}_p$ is a multiple zero. Namely a common zero in $\bar{\mathbb{F}}_p \setminus \{0, 1728\}$ of $\widetilde{H}_{p-1}$ and its first derivative would be a zero of every higher derivative, and thus would have infinite order, but this is not possible.

More precisely, it will now be shown that

$$ss_p \equiv (-1)^{\delta+\epsilon} j^\delta (j-1728)^\epsilon \widetilde{H}_{p-1}(j) \pmod p. \tag{4.4}$$

To get the constant factor $(-1)^{\delta+\epsilon}$, since ss_p is monic, it suffice to compute the leading coefficient of $\widetilde{H}_{p-1}$. For all $f \in M_k$ the leading the coefficient of $\widetilde{f}(j)$ is the constant term of the Fourier expansion of f, namely the limiting value of f as q goes to 0. Since E_4 and E_6 both go to 1 as q goes to 0, the required value for $\widetilde{H}_{p-1}$ is just the coefficient of x^{p-1} in $(1-3x^4+2x^6)^{(p-1)/2}$.

Observe that $1-3x^4+2x^6$ factors as $(1-x)^2(1+x)^2(1+2x^2) = (1-x^2)^2(1+2x^2)$. Recursively it is then shown that

$$\begin{aligned}(1-3x^4+2x^6)^n &= (1-x)^{2n}(1+x)^{2n}(1+2x^2)^n \\ &= (1-x^2)^{2n}(1+2x^2)^n,\end{aligned}$$

which gives $(1-3x^4+2x^6)^{(p-1)/2} = (1-x^2)^{(p-1)}(1+2x^2)^{(p-1)/2}$. Along with this, $(1-x^2)^{p-1} = (1-x^2)^p(1-x^2)^{-1} \equiv \frac{1-x^{2p}}{1-x^2}$, thus

(4.5)

$$\begin{aligned}(1-x^2)^{p-1}(1+2x^2)^{(p-1)/2} &\equiv \frac{1-x^{2p}}{1-x^2}\Big[(1+2x^2)^{(p-1)/2} - 3^{\frac{p-1}{2}} + 3^{\frac{p-1}{2}}\Big] \\ &\equiv (1-x^{2p})\Big[(1+cx^{p-1})(1-x^{-2}) - 3^{\frac{p-1}{2}}(1-x^{-2})\Big] + \Big(\frac{3}{p}\Big)\frac{1-x^{2p}}{1-x^2} \\ &\equiv (1-x^{2p})(\text{poly. of degree } 3) + \Big(\frac{3}{p}\Big)\frac{1-x^{2p}}{1-x^2} \pmod p,\end{aligned}$$

where, in line 2, c is some coefficient. This gives that the desired coefficient is congruent to $\left(\frac{3}{p}\right) = (-1)^{\delta+\epsilon}$ modulo p. Therefore, as claimed,

$$ss_p \equiv (-1)^{\delta+\epsilon} j^\delta (j-1728)^\epsilon \widetilde{H}_{p-1}(j) \pmod p.$$

To show that $\widetilde{G}_{p-1} \equiv \widetilde{H}_{p-1}$ recall that

$$\begin{aligned}G_k &= \text{the coefficient of } x^k \text{ in } (1-3E_4x^4+2E_6x^6)^{-1/2} \\ H_k &= \text{the coefficient of } x^k \text{ in } (1-3E_4x^4+2E_6x^6)^{k/2}.\end{aligned}$$

By this, H_k and G_k differ by a facotr of $(1-3E_4x^4+2E_6x^6)^{p/2}$ since in the case we are looking at $k=p-1$. However

$$\begin{aligned}(1-3E_4x^4+2E_6x^6)^{p/2} &\equiv 1-(3E_4)^{p/2}x^{2p}+(2E_6)^{p/2}x^{3p} \pmod p \\ &\equiv 1+O(x^p) \pmod p,\end{aligned}$$

which implies the desired congruence.

Now the congruence between $\widetilde{G}_p-1$ and $\widetilde{E}_p-1$ will be shown. Take $E: y^2=x^3-3E_4x+2E_6$ over $\mathbb{C}$. This can be parameterized by the Weierstrass $\wp$ function in order to keep the coefficients rational. More details on this function and the parameterization process can be found in [12, p. 16].

There exists a map $\psi:\mathbb{C}\to E$ by $\psi(u)=(P(u),-1/2P(u))$ where

$$P(u)=\frac{1}{u^2}+\sum_{\substack{n\geq 4\\ n \text{ even}}}\frac{12^{n/2}B_n}{n(n-2)!}E_n(\tau)u^{n-2}. \tag{4.6}$$

Since G_k equals the coefficient of x^k in $(1-3E_4x^4+2E_6x^6)^{-1/2}$, this implies G_k equals the coefficient of x^{-1} in $x^{-k-1}(1-3E_4x^4+2E_6x^6)^{-1/2}$. But this is equal to

$$\operatorname{Res}_{x=0}\frac{dx}{x^{k+1}\sqrt{1-3E_4x^4+2E_6x^6}}.$$

Letting x equal $P(u)^{-1/2}$ this gives

$$\begin{aligned}&\operatorname{Res}_{u=0}\frac{d(P(u)^{-1/2})}{P(u)^{\frac{-(k+1)}{2}}\sqrt{1-3E_4P(u)^{-2}+2E_6P(u)^{-3}}}\\ &=\operatorname{Res}_{u=0}P(u)^{\frac{k+1}{2}}\\ &=\text{coeff. of } u^k \text{ in } \left(1-\sum_{\substack{n\geq 4\\ n \text{ even}}}\frac{12^{n/2}B_n}{n(n-2)!}E_nu^n\right)^{\frac{k+1}{2}}.\end{aligned}$$

For $n < p-1$, one gets that $\frac{B_n E_n}{n!}$ is a polynomials in E_4 and E_6 with p-integral coefficients. Along with this, $\frac{pB_{p-1}}{(p-1)!} \equiv 1 \pmod{p}$, therefore with $k = p-1$,

$$\left(1 - \sum_{\substack{n \geq 4 \\ n \text{ even}}} \frac{12^{n/2} B_n}{n(n-2)!} E_n u^n\right)^{p/2} \equiv 1 + 12^{\frac{p-1}{2}} E_{p-1} u^{p-1} + O(u^p) \pmod{p}.$$

However, $12^{\frac{p-1}{2}} \equiv \left(\frac{12}{p}\right) = (-1)^{\delta+\epsilon}$, thus the congruence for G_{p-1} is obtained.

Recall that F_k was defined up to a constant as the unique modular form annihilated by the operator $\vartheta_{k+1}\vartheta_k - \kappa_k E_4$. If $k = p-1$, the eigenvalues κ_{k-12r} for $f \in [0, k/12]$ of the operator $E_4^{-1}\vartheta_{k+1}\vartheta_k$ are still distinct after reducing modulo p. Therefore this characterization is still valid in characteristic p. Applying the definition of ϑ_k and using (2.12) one gets that

(4.7)

$$\begin{aligned}
\vartheta_{k+2}\vartheta_k f - \kappa_k E_4 f &= \vartheta_{k+2}\Big(f_k' - kE_2\frac{f_k}{12}\Big) - \frac{k(k+2)}{144} \\
&= f'' - kE_2\frac{f'}{12} - kE_2'\frac{f}{12} - (k+2)E_2\Big(\frac{f'}{12} - kE_2\frac{f}{144}\Big) - \frac{k(k+2)}{144}E_4 f \\
&= f'' - f'E_2\frac{k+1}{6} - kf\frac{E_2^2 - E_4}{144} + f\frac{k(k+2)E_2^2}{144} - f\frac{k(k+2)E_4}{144} \\
&= f'' - \frac{k+1}{6}E_2 f' + \frac{k(k+1)}{12}E_2' f,
\end{aligned}$$

but if $k = p-1$ and f is E_{p-1}, this vanishes modulo p since the Fourier expansion of f reduces to 1 modulo p. This then gives the proportionality of E_{p-1} and F_{p-1} modulo p.

The exact constant of proportionality in (1.2) is found by normalizing F_k. This is done by

(4.8) constant term of the Fourier expansion of $F_k(\tau) = (-1)^m \binom{\frac{k-5}{6}}{m}$

for m defined as in (4.1). The reasoning behind this will be shown in Section 6. The right hand side of (4.8) is congruent to 1 modulo p if $k = p - 1$, thus we get the desired constant of proportionality.

5. The Atkin Orthogonal Polynomials

Several results of Atkin are discussed by the authors in [11]. Atkin defines a sequence of orthogonal polynomials $A_n(j) \in \mathbb{Q}[j]$, one in each degree n, with respect to a special scalar product.

5.1. **Orthogonal Polynomials.** Given a vector space V over a field K and $(\ ,\ )$ a scalar product on V such that $(f, g) = \phi(fg)$ for $\phi : V \to K$ a linear functional. Let ϕ have the form $\phi(f) = \int_a^b f(X)w(X)dX$ for a, b real numbers such that $a < b$, and w a positive function on (a, b). Given a basis $\{X^n\}_{n\geq 0}$ of V, by applying the Gram-Schmidt process a unique basis of monic orthogonal polynomials P_n are found by

$$P_n(X) = X^n - \sum_{m=0}^{n-1} \frac{(X^n, P_m)}{(P_m, P_m)} P_m(X) \tag{5.1}$$

as long as the scalar product (P_n, P_n) is not zero. Assuming that the non-degeneracy condition holds, the following proposition is true.

Proposition 5.1. *Assuming the notation above, the following are true:*
i) The polynomials P_n satisfy a three term recursion of the form

$$P_{n+1}(X) = (X - a_n)P_n(X) - b_n P_{n-1}(X) \tag{5.2}$$

for a_n, $b_n \in K$, $b_n = \frac{(P_n,P_n)}{(P_{n-1},P_{n-1})} \neq 0$.
ii) Define a second sequence of polynomials $\{Q_n\}_{n\geq 0}$ in $K[X]$ by the same recurrence as in i), but with $Q_0 = 0$ and $Q_1 = \phi(1)$. Then

$$\frac{Q_n(X)}{P_n(X)} = \Phi(X) + O(X^{-2n-1}) \in K[[X^{-1}]] \tag{5.3}$$

where

$$\Phi(X) = \sum_{n=0}^{\infty} g_n X^{-n-1} \in K[[X^{-1}]], \quad g_n = (X^n, 1) = \phi(X^n). \tag{5.4}$$

This property characterizes P_n and Q_n uniquely.

iii) Define $\lambda_n \in K$ $(n \geq 1)$ by the continued fraction expansion

$$g_0 + g_1 x + g_2 x^2 + ... = \cfrac{g_0}{1 - \cfrac{\lambda_1 x}{1 - \cfrac{\lambda_2 x}{\ddots}}} \in K[[X]]. \tag{5.5}$$

Then all λ_n are non-zero and $a_n = \lambda_{2n} + \lambda_{2n+1}$, $b_n = \lambda_{2n-1}\lambda_{2n}$ for $n \geq 1$.

Proof. i) Since all of the $P_n(x)$ are monic, this gives $XP_n = P_{n+1} + a_{nn}P_n + a_{nn-1}P_{n-1} + ... + a_{n0}P_0$ where each $a_{ij} \in K$. By the orthogonality of the P_n and the fact that the scalar product of two polynomials only depends on their product, this gives

$$a_{nm}(P_m, P_m) = (a_{nm}P_m, P_m) = (XP_n, P_m) = (P_n, XP_m) = \begin{cases} 0 & \text{if } m \leq n-2 \\ (P_n, P_n) & \text{if } m = n-1. \end{cases}$$

Taking $a_{nn} = a_n$ and $a_{nn-1} = b_n$ this gives that $XP_n = P_{n+1} + a_n P_n + b_n P_{n-1}$, and thus that $P_{n+1} = (X - a_n)P_n - b_n P_{n-1}$.

ii) Since P_n is orthogonal to all monomials of degree less than n,

$$\begin{aligned} P_n(X)\Phi(X) &= P_n(X) \sum_{m \geq 0} \phi(X^m) X^{-m-1} \\ &= \sum_{m \geq 0} X^{-m-1} P_n \int_a^b X^m w(X) dX \\ &= \sum_{m \geq 0} X^{-m-1} \int_a^b P_n X^m w(X) dx \\ &= \sum_{m \geq} X^{-m-1} (P_n, X^m), \end{aligned} \tag{5.6}$$

thus the coefficient of $X^{-m-1} = 0$ for $m \in [0, n-1]$. This gives that

$$P_n(X)\Phi(X) = Q_n(X) + O(X^{-n-1}) \quad \in K[X, X^{-1}]] \tag{5.7}$$

where $Q_n(X)$ is a polynomial of degree $n-1$ and $K[X, X^{-1}]]$ is the ring of Laurent series in X^{-1}, namely sums of polynomials in X and power series in X^{-1}. Furthermore, this gives that

$$\frac{Q_n(X)}{P_n(X)} = \Phi(X) + O(X^{-2n-1}.$$

On the other hand, given $P_n(X)\Phi(X) = Q_n(X) + O(X^{-n-1})$ for Q_n a polynomial of degree $n-1$, by the same work done in (5.6), one gets that for $m \in [0, n-1]$ the coefficient of x^{-m-1} vanishes, namely that $(P_n, X^m) = 0$, thus P_n is orthogonal to all monomials of lower degree. Thus (5.7) characterizes P_n completely.

Along with this, using (5.2) one gets that

$$Q_{n+1} + O(x^{-n-2}) = [(x - an)P_n - b_n P_{n-1}]\Phi(X),$$

which by (5.7) gives

$$\begin{aligned} Q_{n+1}(X) &= \Phi(X)\left[(X - a_n)\frac{Q_n(X) + O(X^{-n-1})}{\Phi(X)} - b_n\frac{Q_{n-1}(X) + O(X^{-n})}{\Phi(X)}\right] + O(x^{-n-2}) \\ &= (x - a_n)Q_n(X) - b_n Q_{n-1}(X) + O(x^{-n}), \end{aligned}$$

which must vanish for $n \geq 1$. Therefore the polynomials Q_n satisfy the same recursion as the P_n with $Q_0 = 0$ and $Q_1 = g_0$.

iii) Define the vector space V^* as $K[Y]$ with a scalar product $(f, g) = \psi(fg)$, where

$$\psi(Y^n) = \begin{cases} 0 & \text{if } n \text{ odd} \\ g_{n/2} & \text{if } n \text{ even.} \end{cases}$$

By the same construction used for P_n, we get a family of orthogonal polynomials $P_n^*(Y)$. Since odd and even polynomials in Y are orthogonal to each other, $P+n^*(Y)$

has parity n for all n, namely even indexed polynomials are even and odd indexed polynomials are odd. By part i) if the proposition applied to (V^*, Y),

$$P^*_{n+1} = YP^*_n(Y) - \lambda_n P^*_{n-1} \tag{5.8}$$

for nonzero constant $\lambda_n = \frac{(P^*_n, P^*_n)}{(P^*_{n-1}, P^*_{n-1})} \in K$. Part ii) of the proposition gives that there are companion polynomials Q^*_n to P^*_n of degree $n-1$, thus opposite parity, and that the Q^*_n satisfy the recursion $Q^*_{n+1} = YQ^*_n - \lambda_n Q^*_{n-1}$. Along with this, $\frac{Q^*_n}{P^*_n}$ are the best approximations to $\sum g_k Y^{-2k-1}$ at infinity.

By induction on n the following equation is derived

$$\begin{pmatrix} Q^*_{n+1} & Q^*_n \\ P^*_{n+1} & P^*_n \end{pmatrix} = \begin{pmatrix} g_0 & 0 \\ Y & 1 \end{pmatrix} \begin{pmatrix} Y & 1 \\ -\lambda_1 & 0 \end{pmatrix} \cdots \begin{pmatrix} Y & 1 \\ -\lambda_n & 0 \end{pmatrix}. \tag{5.9}$$

This in turn gives that

$$\cfrac{g_0 Y^{-1}}{1 - \cfrac{\lambda_1 Y^{-2}}{1 - \cfrac{\lambda_2 Y^{-2}}{\ddots \cfrac{}{1 - \lambda_n Y^{-2}}}}} = \frac{Q^*_{n+1}}{P^*_{n+1}} = \frac{g_0}{Y} + \frac{g_1}{Y^3} + \cdots + \frac{g_n}{Y^{2n+1}} + O(\frac{1}{y^{2n+3}}).$$

By setting $X = Y^{-2}$ and letting n go to infinity this gives (5.5). Along with this, the recursion of P^*_n implies the recursion

$$P^*_{n+2} = (Y^2 - \lambda_n - \lambda_{n+1})P^*_n - \lambda_{n-1}\lambda_n P^*_{n-2} \tag{5.10}$$

for P^*_n of a given parity. On the other hand V can be identified with the even part of V^* by setting $X = Y^2$ and with compatible scalar products. This implies that $P^*_{2n}(Y) = P_n(Y^2) = P_n(X)$, which by (5.10) gives that

$$P_{n+1}(X) = (X - (\lambda_n + \lambda_{n+1}))P_n(X) - \lambda_n \lambda_{n-1} P_{n-1}(X),$$

thus $a_n = \lambda_n + \lambda_{n+1}$ and $b_n = \lambda_n \lambda_{n-1}$, which completes the proof of the proposition.

□

5.2. **The Atkin Polynomials.** Let V be the space of polynomials in j where j is the modular invariant $j(\tau) = q^{-1} + 744 + \cdots$, then V can be identified with the space of holomorphic Γ-invariant functions in the upper half plane $\mathcal{H}$ that grow at infinity by at most q^{-N}. These functions are meromorphic at infinity, i.e. for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, $f(\frac{a\tau+b}{c\tau+d}) = f(\tau)$ and f has a Laurent series expansion $f(\tau) = \sum_{n \gg -\infty} c_n q^n$. More precisely, the set of polynomials in j coincide with V, and either $q = e^{2\pi i \tau}$, $j = j(\tau) = q^{-1} + 744 + 19688q + \cdots$, or $\Delta = q - 24q^2 + 252q^3 + \cdots$ can be taken as a local parameter at infinity.

We will now give the proof of Proposition 1.5 before giving the proof of Theorem 1.4.

Proof of Proposition 1.5. Observe that by (2.12),

$$\frac{d\Delta(\tau)}{\Delta(\tau)} = 2\pi i E_2(\tau) d\tau,$$

and since $q = e^{2\pi i \tau}$

$$\frac{dq}{q} = 2\pi i e^{2\pi i} d\tau,$$

one gets

$$\frac{d\Delta(\tau)}{\Delta(\tau)} = 2\pi i E_2(\tau) d\tau = E_2(\tau) \frac{dq}{q}.$$

Now recall that the definition of j is given in (2.10), which gives that

$$dj(\tau) = \frac{3E_4(\tau)E_4'(\tau)\Delta(\tau) - E_4^3(\tau)\Delta'(\tau)}{\Delta^2(\tau)} 2\pi i d\tau.$$

Using (2.12), this becomes

$$\frac{-E_4^2(\tau)E_6(\tau)}{\Delta(\tau)} 2\pi i d\tau,$$

which gives that

$$\frac{dj(\tau)}{j(\tau)} = \frac{-E_6(\tau)}{E_4(\tau)} 2\pi i d\tau.$$

Multiplying by $-E_2E_4/E_6$ gives $E_2(\tau)2\pi i d\tau$, thus

$$\frac{d\Delta(\tau)}{\Delta(\tau)} = 2\pi i E_2(\tau)d\tau = E_2(\tau)\frac{dq}{q} = \frac{-E_2(\tau)E_4(\tau)}{E_6(\tau)}\frac{dj(\tau)}{j(\tau)}.$$

Therefore *i-iii* of the proposition are attained by writing the constant terms as $\frac{1}{2\pi i}$ times the corresponding residues and using the equations derived above.

For part *iv* of the proposition use the global residue theorem. Let $\mathcal{F}_a$ be the standard fundamental domain of Γ truncated at some height $a > 1$. Namely the domain given by $|x| \leq \pm\frac{1}{2}$, $x^2 + y^2 \geq 1$, $y \leq a$, where $\tau = x + iy$. Observe that the integral of $f(\tau)g(\tau)E_2(\tau) = (f, g)$ by *iii*. Due to the holomorphy of fgE_2, (f, g) must also be given by the sum of the integrals over the other three edges of the domain. Since fgE_2 is periodic of period 1, this gives that the integrals along the vertical edges, i.e. $|x| = \pm\frac{1}{2}$, cancel. Observe that f and g are invariant under the transformation obtained by replacing τ with $-1/\tau$. Therefore, replace τ with $-1/\tau$ along the left half of the bottom edge. This implies that (f, g) is equal to the integral along the arc from $e^{\pi i/3}$ to $e^{\pi i/2}$ of

$$[E_2(\tau) - \tau^{-2}E_2(-1/\tau)]f(\tau)g(\tau)d\tau.$$

By (2.8) the part of this equation in square brackets is equal to $\frac{-6i}{\pi\tau}$, which gives that (f, g) is equal to the following integral

$$\int_{e^{\pi i/3}}^{e^{\pi i/2}} \frac{-6i}{\pi\tau} f(\tau)g(\tau)d\tau.$$

When $\tau = e^{i\theta}$, this integral becomes

$$\frac{6}{\pi}\int_{\pi/3}^{\pi/2} f(e^{i\theta})g(e^{i\theta})d\theta,$$

with is *iv* of the proposition thus all four definitions of the scalar product coincide on V. □

Corollary 5.2. *The scalar product* $(\ ,\ )$ *is positive definite on* $V_{\mathbb{R}} = \mathbb{R}[j]$.

Proof. The proof of this corollary follows from definition iv of the scalar product since $j(e^{i\theta})$ is real for $\theta \in [\pi/3, \pi/2]$. Therefore $\int_{\pi/3}^{\pi/2} f(e^{i\theta})^2 d\theta$ is greater than 0 as long as $f(\tau)$ is a nonzero polynomial in $j(\tau)$ with real coefficients. □

The results of Proposition 5.1 applied to this scalar product imply that there is a unique sequence of monic orthogonal polynomials $A_n(j)$ of degree n. These are the Atkin orthogonal polynomials. Along with this the proposition gives that the scalar product of two monomials j^n and j^m equals g_{n+m} for g_n the coefficient of j^{-n-1} in

$$\Phi(\tau) = \frac{E_2(\tau)E_4(\tau)}{E_6(\tau)j(\tau)} = q - 24q^2 + 196812q^3 + ... = \frac{1}{j(\tau)} + \frac{720}{j(\tau)^2} + ...,$$

and that the denominators of the best rational approximations to Φ are given by the polynomials A_n. Lastly, the results of Proposition (5.1) give that the Atkin polynomials satisfy the following recursion

$$A_{n+1}(j) = (j - (\lambda_{2n} + \lambda_{2n+1}))A_n(j) - \lambda_{2n-1}\lambda_{2n}A_{n-1}$$

with the λ_n positive rational numbers given by the continued fraction expansion of Φ with respect to $1/j$. In [11], the authors numerically compute the first five values for $g_n = (j^n, 1)$ and λ_n, which are given below:

$$g_0 = 1, \quad g_1 = 720, \quad g_2 = 1301011200, \quad g_4 = 1958042030400$$

$$\lambda_1 = 720, \quad \lambda_2 = 546, \quad \lambda_3 = 374, \quad \lambda_4 = 475, \quad \lambda_5 = \frac{2001}{5}.$$

Proof of Theorem 1.4. Given $k \in \mathbb{Z}$, let V_k denote the space of holomorphic functions in $\mathcal{H}$ that transform like weight k modular forms and have at most exponential growth at infinity. Namely, V_k is the degree k part of the graded ring $\mathbb{C}[E_4, E_6, \Delta^{-1}]$. Observe that $V = V_0$ and that V_2 coincides with the set of derivatives of the functions in V. Recall the definitions given in (2.27) and (2.28) for the Hecke operator

and the Hecke operator at infinity. Using these it will then be shown that

$$\mathrm{Res}_\infty((f|_k T_n^\infty)\cdot h) = \mathrm{Res}_\infty(f\cdot(h|_{2-k}T_n^\infty)) \tag{5.11}$$

for $f, h \in \mathbb{C}[q^{-1}, q]$, and that

$$(gE_2)|_2 T_n^\infty = (g|_0 T_n)\cdot E_2 \pmod{V_2} \tag{5.12}$$

for $g \in V_0$. Note that $\mathrm{Res}_\infty(F)$ for F a 1-periodic holomorphic function on $\mathcal{H}$ denotes the residue at infinity of $2\pi i F(\tau)d\tau$. Namely, this is the constant term of F as a Laurent series in q. Now Theorem 2.27 will follow using *iii* of the Atkin scalar product definitions in (1.5) and the fact that $VV_2 \subseteq V_2$, since Res_∞ vanishes on V_2, thus

$$\begin{aligned}(f|_0 T_n, g) &= \mathrm{Res}_\infty((f|_0 T_n)\cdot g\cdot E_2)\\ &= \mathrm{Res}_\infty(f\cdot(gE_2)|_2 T_n^\infty)\\ &= \mathrm{Res}_\infty(f\cdot(g|_0 T_n)\cdot E_2)\\ &= (f, g|_0 T_n).\end{aligned} \tag{5.13}$$

To prove (5.11), it is sufficient to check that T_n^∞ acts on Foruier series by

$$\Big(\sum_r A_r q^r\Big)|_k T_n^\infty = n^{k/2}\sum_{ad=n} d^{1-k}\sum_r A_{rd}q^{ar},$$

since then one gets that

$$\begin{aligned}\mathrm{Res}_\infty((f|_k T_n^\infty)h) &= n^{k/2}\sum_{ad=n}\sum_r A_{dr}B_{-ar}\\ &= n^{1-k/2}\sum_{ad=n} a^{-1+k}\sum_s B_{as}A_{-ds}\\ &= \mathrm{Res}_\infty(f(h|_{2-k}T_n^\infty))\end{aligned}$$

for $f = \sum A_r q^r$ and $h = \sum B_s q^s$. To prove (5.12) use the following transformation property

$$E_2(\tau) = E_2^*(\tau) + \frac{3}{\pi y},$$

which is equivalent to (2.8), where $y = \Im(\tau)$ and the nonholomorphic E_2^* transforms like a weight 2 modular form. Let the space of functions with this last property be denoted by V_2^*. Since $VV_2^* \subseteq V_2^*$ and V_2^* is preserved by $|_2T_n$, one gets

$$(gE_2)|_2T_n^\infty - (g|_0T_n)E_2 \equiv \frac{3}{\pi}((gy^{-1})|_2T_n^\infty - (g|_0T_n)y^{-1}) \pmod{V_2^*}.$$

The right hand side of this vanishes by the following calculation

$$\begin{aligned}((gy^{-1})|_2T_n^\infty)(\tau) &= \sum_{\substack{ad=n \\ b \pmod d}} \frac{n}{d^2} g\Big(\frac{a\tau+b}{d}\Big)\Im\Big(\frac{a\tau+b}{d}\Big)^{-1} \\ &= y^{-1}(g|_0T_n)(\tau),\end{aligned}$$

therefore the holomorphic left hand side belongs to V_2 as desired. To prove uniqueness, look at the polynomials $h_n = j|T_n \cdot 1 - j \cdot 1|T_n$ for $n \geq 2$ and $h^* = j^2|T_2 \cdot j - j^2 \cdot j|T_2$, which are annihilated by any functional $\phi : V \to \mathbb{C}$ as in Theorem (2.27). On the other hand, these polynomials span a codimension 1 subspace of V. This is because $\deg H_n = n$ and h^* is not a linear combination of the h_n's, thus ϕ must be unique. □

5.3. **Hypergeometric Properties of the Atkin Polynomials.** The Atkin polynomials can be defined in terms of a recursion formula, closed formula, or differential equation as stated in Theorem 1.6. This theorem can be proved by showing the relation between the Atkin polynomials and hypergeometric series. Let ${}_2F_1$ be the classical Gauss hypergeometric series

$$(5.14) \qquad {}_2F_1(a,b;c;x) = \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n}x^n = \sum_{n=0}^{\infty} \frac{\binom{-a}{n}\binom{-b}{n}}{\binom{-c}{n}}(-x)^n, \quad |x| \leq 1.$$

Define U_n^ϵ and V_n^δ for $n \geq 0$ as the four monic polynomials

$$\begin{aligned} j^n F\Big(\frac{1}{12}, \frac{5}{12}; 1; \frac{1728}{j}\Big) &= U_n^0(j) + O(1/j) \\ j^{n-1}(j-1728) F\Big(\frac{7}{12}, \frac{11}{12}; 1; \frac{1728}{j}\Big) &= U_n^1 + O(1/j) \\ (j-1728)^n F\Big(\frac{1}{12}, \frac{7}{12}; 1; \frac{1728}{1728-j}\Big) &= V_n^0 + O(1/j) \\ j(j-1728)^{n-1} F\Big(\frac{5}{12}, \frac{11}{12}; 1; \frac{1728}{1728-j}\Big) &= V_n^1 + O(1/j) \end{aligned} \tag{5.15}$$

as $j \to \infty$. Using the above notations, the Atkin polynomials can be defined in terms of hypergeometric series as follows.

Proposition 5.3. *The Atkin polynomials A_n are given by the following*

$$\begin{aligned} A_n(j) &= \sum_{m=0}^{n} (-12)^{3m} \binom{n+\frac{1}{12}}{m} \binom{n-\frac{7}{12}}{m} \binom{2n-1}{m}^{-1} U_{n-m}^0(j), \\ A_n(j) &= \sum_{m=0}^{n} (-12)^{3m} \binom{n-\frac{5}{12}}{m} \binom{n-\frac{13}{12}}{m} \binom{2n-1}{m}^{-1} U_{n-m}^1(j) \\ A_n(j) &= \sum_{m=0}^{n} 12^{3m} \binom{n+\frac{1}{12}}{m} \binom{n-\frac{5}{12}}{m} \binom{2n-1}{m}^{-1} V_{n-m}^0(j), \\ A_n(j) &= \sum_{m=0}^{n} 12^{3m} \binom{n-\frac{7}{12}}{m} \binom{n-\frac{13}{12}}{m} \binom{2n-1}{m}^{-1} V_{n-m}^1 \end{aligned} \tag{5.16}$$

Proof. Since the proofs for all four equations are similar, only the first one will be shown here. Denote the right hand side of the equation by A_n^0. For $n \leq 2$, by direct computation, $A_n^0 = A_n$ for the A_n in (1.6). Therefore, it suffices to show the recursion $A_{n+1}^0 = (j - a_n)A_n^0 - b_n A_{n-1}^0$ where a_n and b_n are the rational functions of n from (1.3). Rewrite A_n^0 as $A_n^0 = c(n,k)U_k^0$ where

$$\begin{aligned} c(n,0) &= (-12)^{3n} \binom{\frac{-5}{12}}{n} \binom{\frac{-13}{12}}{n} \binom{2n-1}{n}^{-1}, \\ c(n,k) &= c(n,0) 12^{-3k} \binom{n}{k} \binom{-n}{k} \binom{\frac{-5}{12}}{k}^{-1} \binom{\frac{-13}{12}}{k}^{-1}. \end{aligned} \tag{5.17}$$

Since

$$jU_k^0 = U_{k+1}^0 - 12^{3k+3}\binom{\frac{-1}{12}}{k+1}\binom{\frac{-5}{12}}{k+1},$$

this gives that

$$\begin{aligned} &A_{n+1}^0(j) - (j-a_n)A_n^0(j) + b_nA_{n-1}^0(j) \\ &\qquad = \sum_{k=0}^{n}[c(n+1,k) - c(n,k-1) + a_nc(n,k) + b_nc(n-1,k)]U_k^0 \\ &\qquad + \sum_{k=0}^{n} 12^{3k+3}\binom{\frac{-1}{12}}{k+1}\binom{\frac{-5}{12}}{k+1}c(n,k) \end{aligned} \tag{5.18}$$

for $n \geq 2$ and with $c(n,-1) = 0$, $c(n,n) = 1$, and $c(n-1,n) = 0$. On the right hand side of this equation, the coefficient of U_k^0 is equal to 0 for $k \geq 1$ and is equal to $84c(n,0)/(n^2-1)$ for $k = 0$. By substituting in the values of $U_0^0 = 1$, a_n, b_n, and $c(n,k)$ and writing $k = n - m$ one gets that the right hand side of (5.18) equals

$$\frac{12c(n,0)}{n^2-1}\sum_{m=0}^{n+1}\binom{-n+1}{n+1-m}\left[7\binom{n+1}{m} - 12(n+1)\binom{n}{m}\right], \tag{5.19}$$

where the $m = n+1$ term comes from the multiple of U_0^0 in (5.18). This sum is the coefficient of x^{n+1} in

$$(1+x)^{1-n}[7(1+x)^{n+1} - 12(n+1)(1+x)^n],$$

and thus vanishes for $n \geq 2$. □

Proof of Theorem 1.6. i) By (2.12), $\Phi = -d(\log\Delta)/dj$, but Δ can be written in terms of j as

$$\Delta = \frac{1}{j}F(\frac{1}{12},\frac{5}{12};1;\frac{1728}{j})^12.$$

By Gauss's contiguous relations

$$\Phi = \frac{F(\frac{13}{12},\frac{5}{12};1;\frac{1728}{j})}{jF(\frac{1}{12},\frac{5}{12};1;\frac{1728}{j})},$$

and by Gauss's formula for the continued fraction expansion of a quotient of contiguous functions one gets that the λ_n from (5.5) are given by

$$\lambda_n = \begin{cases} 720 & \text{if } n = 1 \\ 12(6 + \frac{(-1)^n}{n-1})(6 + \frac{(-1)^n}{n}) & \text{if } n > 1, \end{cases}$$

thus we get (i) of (1.6). For more information on hypergeometric functions and contiguous relations see [1].

ii) Since the Atkin polynomials are the A_n of (5.3), the closed formula is obtained by a rewriting of the first formula of (5.3).

iii) The closed formula of (ii) gives that the $A_n(j)$ can be obtained from

$$F\Big(\frac{1}{12}, \frac{5}{12}; 1; x\Big) F\Big(-n - \frac{1}{12}, -n + \frac{7}{12}; 1 - 2n; x\Big) \tag{5.20}$$

by truncating at x^n then inverting it. Namely by setting $x = \frac{1728}{j}$ and multiplying by j^n. Since the second factor of (5.20) becomes infinite from degree $2n$ onward, some truncation is required.

One can truncate at any m between n and $2n-1$ since the coefficient of x^m in (5.20) vanishes for $n < m < 2n$. This can be seen by letting $\gamma \to 1$ in the following identity

$$\begin{aligned} &F(\alpha, \beta; \gamma; x) F(-n - \alpha, -n + 1 - \beta; -2n + 2 - \gamma; x) \\ &\quad + \delta_n x^{2n} (1 - x) F(1 - \alpha, 1 - \beta; 2 - \gamma; x) F(\alpha + n + 1, \beta + n; \gamma + 2n; x) \\ &\quad = \text{ polynomial of degree } n, \end{aligned}$$

where $n \geq 1$ and

$$\delta_n = \frac{\binom{-\alpha}{n+1}\binom{-\beta}{n}\binom{\alpha-\gamma}{n-1}\binom{\beta-\gamma}{n}}{\binom{-\gamma}{2n}\binom{1-\gamma}{2n}\binom{2n}{n}\binom{2n}{n-1}}.$$

This identity is a consequence of Gauss's contiguous relations and two formulas of Heine [8]. Since the product of two hypergeometric functions satisfies a fourth

order linear differential equation with explicitly calculated coefficients along with this truncation argument gives the differential equation for A_n.

If $A_n(j)$ is replaced by a polynomial beginning with j^d for $d \geq 0$ an integer, then the left hand side of (iii) has the leading term $n^2(n^2-d^2)^2$, thus $d=m$ is the only way the differential equation can be satisfied. This in turn gives uniqueness of the expression. □

We will now relate the U_n and V_n from (5.15) to the supersingular polynomial $ss_p(j)$.

Proposition 5.4. *Let $p \geq 5$ be prime and write $p = 12n - 8\delta - 6\epsilon + 1$ with $n \in \mathbb{N}$, δ, $\epsilon \in \{0,1\}$, then*

$$ss_p(j) \equiv U_n^{\epsilon}(j) \equiv V_n^{\delta}(j) \pmod{p}. \tag{5.21}$$

Proof. Here we will give only the proof for the case U_n^0 since the other cases are very similar. Begin by assuming that $p \equiv 1 \pmod 4$. Recall the trinomial theorem, which gives that

$$(x+y+z)^n = \sum_{r_1+r_2+r_3=n} \binom{n}{r_1, r_2, r_3} x^{r_1} y^{r_2} z^{r_3}.$$

Using this, expand H_{p-1} as follows

$$\begin{aligned} H_{p-1} &= \text{coefficient of } x^{p-1} \text{ in } (1 - 3E_4x^4 + 2E_6x^6)^{2\ell} \\ &= \sum_{\substack{r,s\geq 0 \\ 2r+3s=2\ell}} \frac{(2\ell)!}{r!s!(2\ell-r-s)!}(-3E_4)^r(2E_6)^s \\ &= (-3E_4)^{\ell} \sum_{k=0}^{\lfloor \ell/3 \rfloor} \frac{(2\ell)!}{(\ell-3k)!(2k)!(\ell+k)!}\Big(\frac{-4}{27}\frac{j-1728}{j}\Big)^k, \end{aligned} \tag{5.22}$$

for $k = s/2$ and where $\frac{j-1728}{j}$ comes from the fact that

$$\frac{E_6^2}{E_4^3} = \frac{j-1728}{j}.$$

Note that in the case U_n^1 one uses $p \equiv 3 \pmod 4$ and $s = 2k+1$; for V_n^δ set $r = 3k + \delta$ then expand in powers of $\frac{j}{j-1728}$.

Now, by induction on k one gets that

$$\frac{(2\ell)!}{(\ell-3k)!(2k)!(\ell+k)!}\Big(\frac{-4}{27}\Big)^k \equiv \binom{2\ell}{\ell}\frac{(\frac{1}{12})_k(\frac{5}{12})_k}{k!(\frac{1}{2})_k} \pmod p. \tag{5.23}$$

Therefore, by (4.4) and $\lfloor \ell/3 \rfloor = m = n - \delta$ and $(-1)^\delta = \left(\frac{-3}{p}\right) \equiv 3^{2\ell} \pmod p$, one gets, by writing $F_m(a,b;c;x)$ for the hypergeometric series truncated at degree m, that

$$ss_p(j) \equiv (-j)^\delta \widetilde{H}_{p-1} \equiv (-3)^{3\ell}\binom{2\ell}{\ell} j^n F_{\lfloor \ell/3 \rfloor}\Big(\frac{1}{12},\frac{5}{12};\frac{1}{2};1-\frac{1728}{j}\Big) \pmod p. \tag{5.24}$$

Since the coefficients of x^k and y^k in $F(\frac{1}{12},\frac{5}{12};1;x)$ and $F(\frac{1}{12},\frac{5}{12};\frac{1}{2};y)$ vanish modulo p for $k \in (\lfloor \ell/3 \rfloor, 2\ell]$, and $F(\frac{1}{12},\frac{5}{12};1;x)$ and $F(\frac{1}{12},\frac{5}{12};\frac{1}{2};1-x)$ satisfy the same second order linear differential equation with polynomial coefficients of degree no more than 2, one gets that the polynomial on the right hand side of the last equation is a multiple of $U_n^0(j)$. However, the supersingular polynomial is monic, thus the multiple must be 1. □

Using Proposition 5.4, a relation between the Atkin polynomials A_n and the supersingular polynomial $ss_p(j)$ for certain n can be proven. This relation between A_n and $ss_p(j)$ is given by Thereom 1.7.

Proof of Theorem 1.7. For $p = 2$ or 3, this is trivial. In the case $p \neq 2$ or 3, one gets that n_p is the same as n from Proposition 5.4. Apply Proposition 5.3 to U_n^ϵ or V_n^δ with this n. The result then follows since all of the coefficients vanish modulo p except the one for $m = 0$. □

6. Hypergeometric Properties of F_k

Recall that $F_k(\tau)$, $k \not\equiv 2 \pmod 3$, is a modular form and is the unique normalized solution of the second order differential equation

$$v_{k+2}v_k F_k - \frac{k(k+2)}{144}E_4 F_k = 0. \tag{6.1}$$

Define the following notations:

$$v_0 = \frac{1-2\delta}{3}, \quad v_1 = \frac{1-2\epsilon}{2}, \quad v_\infty = \frac{k+1}{6} \quad (v_0+v_1+v_\infty = 2m+1),$$
$$X_0 = J = \frac{j}{1728}, \quad X_1 = 1-J, \quad X_\infty = -1, \quad (X_0+X_1+X_\infty = 0),$$
$$Y_0 = E_4^3, \quad Y_1 = -E_6^2, \quad Y_\infty = -1728\Delta, \quad (Y_0+Y_1+Y_\infty = 0).$$

Note that m, δ, and ϵ are defined as in Section 4. Using these notations the following theorem gives explicit descriptions of the F_k and the associated polynomials $\widetilde{F}_k(j)$.

Theorem 6.1. *Suppose $k \geq 0$, $k \not\equiv 2 \pmod 3$, then i) Differential equation: $\widetilde{F}_k(j)$ is the unique normalized polynomial solution of*

$$j(j-1728)\widetilde{F}_k'' + \{(1-v_1)j + (1-v_0)(j-1728)\}\widetilde{F}_k' + m(m-v_\infty)\widetilde{F}_k = 0.$$

ii) Closed formula: Let σ be any permutation of $\{0,1,\infty\}$, then

$$\widetilde{F}_k(j) = (sgn(\sigma)\cdot 1728)^m \binom{m-v_{\sigma(\infty)}}{m} X_{\sigma(0)}^m F(-m, -m+v_{\sigma(0)}; 1-v_{\sigma(\infty)}; -\frac{X_{\sigma(\infty)}}{X_{\sigma(\infty)}})$$

and

$$F_k(\tau) = sgn(\sigma)^m E_4^\delta E_6^\epsilon \sum_{l=0}^{m} (-1)^l \binom{m-v_{\sigma(0)}}{l}\binom{m-v_{\sigma(\infty)}}{m-1} Y_{\sigma(\infty)}^l Y_{\sigma(0)}^{m-1}.$$

iii) Recursion relation: The $\widetilde{F}_k(j)$ satisfy

$$\begin{aligned}(m+1)(m-v_\infty)(1-v_\infty)\widetilde{F}_{k+12}&\\ -v_\infty[(1+v_\infty)(1-v_\infty)(j-1728)((1-V_0)(V_0+v_1)+2m(m-v_\infty))]\widetilde{F}_k&\\ +1728^2(m-v_0)(m-v_1)(1-v_\infty)\widetilde{F}_{k-12}=0.&\end{aligned}$$

iv) Generating Function: For $k\in\mathbb{Z}_{\geq\not<}$ and any α denote by $G_{k,\alpha}(\tau)$ the coefficient of X^k in $(1-3E_4(\tau)X^4+2E_6(\tau)X^6)^\alpha$. Then

$$F_k(\tau)=(-1)^{m+\delta}2^{-2m+\epsilon}\binom{2m+\epsilon}{m}\binom{\frac{1}{6}(k-2)}{m+\epsilon}^{-1}G_{k,\frac{k-2}{6}}(\tau).$$

Proof. i)Begin with the equation given by (6.1), and recall by (4.2) that one can write $F(\tau)$ as $\Delta(\tau)^mE_4(\tau)^\delta E_6(\tau)^\epsilon\widetilde{F}(j(\tau))$, and that

$$\vartheta_k(f)=\frac{df}{d\tau}-\frac{E_2k}{12}f.$$

Therefore one gets that

(6.2)
$$\begin{aligned}\vartheta_{k+2}\vartheta_kF_k-\frac{k(k+2)}{144}E_4F_k=\frac{d}{d\tau}\Big(\frac{d}{d\tau}\Delta^mE_4^\delta E_6^\epsilon\widetilde{F}_k(j)-\frac{kE_2}{12}\Delta^mE_4^\delta E_6^\epsilon\widetilde{F}_k(j)\Big)&\\ -\frac{(k+2)E_2}{12}\Big(\frac{d}{d\tau}\Delta^mE_4^\delta E_6^\epsilon\widetilde{F}_k(j)-\frac{kE_2}{12}\Delta^mE_4^\delta E_6^\epsilon\widetilde{F}_k(j)\Big).&\end{aligned}$$

We begin computing this by taking the first derivative of $\Delta^mE_4^\delta E_6^\epsilon\widetilde{F}_k(j)$ as follows

(6.3)
$$\begin{aligned}\frac{d}{d\tau}(\Delta^mE_4^\delta E_6^\epsilon\widetilde{F}_k(j))=m\Delta^{m-1}E_4^\delta E_6^\epsilon\widetilde{F}_k(j)+\Delta^m\delta E_4^{\delta-1}E_4'E_6^\epsilon\widetilde{F}_k(j)&\\ +\Delta^mE_4^\delta\epsilon E_6^{\epsilon-1}\widetilde{F}_k(j)+\Delta^mE_4^\delta E_6^\epsilon\widetilde{F}_k'(j)j',&\end{aligned}$$

by substituting in the equations from (2.12) and equating terms this becomes

(6.4)
$$\begin{aligned}\Delta^mE_2E_4^\delta E_6^\epsilon\widetilde{F}_k(j)\Big(m+\frac{\delta}{3}+\frac{\epsilon}{2}\Big)-\frac{\delta}{3}\Delta^mE_4^{\delta-1}E_6^{\epsilon+1}\widetilde{F}_k(j)&\\ -\frac{\epsilon}{2}\Delta^mE_4^{\delta+2}E_6^{\epsilon-1}\widetilde{F}_k(j)-\Delta^mE_4^{\delta-1}E_6^{\epsilon+1}\widetilde{F}_k'(j)j.&\end{aligned}$$

This gives

(6.5)
$$\frac{d}{d\tau}\Big(\Delta^m E_4^\delta E_6^\epsilon \widetilde{F}_k(j)\Big) - \frac{kE_2}{12}(\Delta^m E_4^\delta E_6^\epsilon \widetilde{F}_k(j) = \Delta^m E_2 E_4^\delta E_6^\epsilon \widetilde{F}_k(j)\Big(m + \frac{\delta}{3} + \frac{\epsilon}{2} - \frac{k}{12}\Big)$$
$$- \frac{\delta}{3}\Delta^m E_4^{\delta-1} E_6^{\epsilon+1}\widetilde{F}_k(j) - \frac{\epsilon}{2}\Delta^m E_4^{\delta+2} E_6^{\epsilon-1}\widetilde{F}_k(j) - \Delta^m E_4^{\delta-1} E_6^{\epsilon+1}\widetilde{F}_k'(j)j,$$

but $(m + \delta/3 + \epsilon/2 - k/12) = 0$ so the full equation is equal to

$$-\frac{\delta}{3}\Delta^m E_4^{\delta-1} E_6^{\epsilon+1}\widetilde{F}_k(j) - \frac{\epsilon}{2}\Delta^m E_4^{\delta+2} E_6^{\epsilon-1}\widetilde{F}_k(j) - \Delta^m E_4^{\delta-1} E_6^{\epsilon+1}\widetilde{F}_k'(j)j.$$

Now take the derivative of this

(6.6) $$\frac{d}{d\tau}\Big(-\frac{\delta}{3}\Delta^m E_4^{\delta-1} E_6^{\epsilon+1}\widetilde{F}_k(j) - \frac{\epsilon}{2}\Delta^m E_4^{\delta+2} E_6^{\epsilon-1}\widetilde{F}_k(j) - \Delta^m E_4^{\delta-1} E_6^{\epsilon+1}\widetilde{F}_k'(j)j\Big),$$

substitute in the equations from (2.12) and equate terms as was done for the first derivative computes. Subtract

$$\frac{k(k+2)}{144}E_4(\Delta^m E_4^\delta E_6^\epsilon \widetilde{F}_k(j),$$

and simplify the coefficients of $\widetilde{F}_k(j)$, $\widetilde{F}_k'(j)$, and $\widetilde{F}_K''(j)$. Using the fact that

$$1728 = \frac{E_4^3 - E_6^2}{\Delta}$$

by the equation for Δ and that

$$j - 1728 = \frac{E_4^3}{\Delta} - \frac{E_4^3 - E_6^2}{\Delta} = \frac{E_6^2}{\Delta},$$

one gets the desired result.

ii) The equation from part (i) of the theorem is a hypergeometric differential equation, and thus has a polynomial solution of the form $F(-m, -m+v_\infty; 1-v_0; j/1728)$. More information on hypergeometric differential equations and their polynomial solutions can be found in [1]. By [1], there are 6 polymomial solutions from Kummer's 24 solutions to this equation. By making the expressions symmetric the formula i

obtained, and the formula for F_k follows.

iii) If one replaces k by k^+_-12 in the formula for $\widetilde{F}_k(j)$, the first three argument of the hypergeometric seris of $\widetilde{F}_k(j)$ change by 1. Therefore the recursion comes from Gauss's contiguous relations which can be found in [1].

iv) Let $Y_\alpha = (1 - 3E_4X^4 + 2E_6X^6)^\alpha$, and observe that

$$Y_\alpha = Y_{\alpha-1}(1 - 3E_4X^4 + 2E_6X^6),$$

$$\frac{\partial}{\partial X}Y_\alpha = \alpha Y_\alpha(-12E_4X^3 + 12E_6X^5)$$

$$\sum_{k=0}^{\infty} \vartheta_k G_{k,\alpha} X^k = \frac{1}{2\pi i}\frac{\partial}{\partial \tau}Y_\alpha - \frac{E_2}{12}X\frac{\partial}{\partial X}Y_\alpha = \alpha Y_{\alpha-1}(E_6X^4 - E_4^2X^6).$$

By these three relations one gets

$$G_{k,\alpha} = G_{k,\alpha-1} - 3E_4G_{k-4,\alpha-1} + 2E_6G_{k-6,\alpha-1}, \tag{6.7}$$

$$kG_{k,\alpha} = -12\alpha E_4G_{k-4,\alpha-1} + 12\alpha E_6G_{k-6,\alpha-1}, \tag{6.8}$$

$$\vartheta_k G_{k,\alpha} = \alpha E_6G_{k-4,\alpha-1} - \alpha E_4^2G_{k-6,\alpha-1}. \tag{6.9}$$

Solve (6.7) for $E_4G_{k-4,\alpha-1}$ to obtain

$$E_4G_{k-4,\alpha-1} = \frac{-1}{3}G_{k,\alpha} + \frac{1}{3}G_{k,\alpha-1} + \frac{2}{3}E_6G_{k-6,\alpha-1},$$

and solve (6.8) for $E_6G_{k-6,\alpha-1}$ to obtain

$$E_6G_{k-6,\alpha-1} = \frac{k}{12\alpha}G_{k,\alpha} + E_4G_{k-4,\alpha-1}.$$

Substituting these into (6.9) and simplifying, one gets

$$\vartheta_k G_{k,\alpha} = -\frac{1}{\alpha+1}\Big(\alpha - \frac{k}{6} + \frac{1}{3}\Big)\Big(\alpha - \frac{k}{6} + \frac{2}{3}\Big)G_{k+2,\alpha+1} + \Big(\alpha - \frac{k}{12} + \frac{1}{2}\Big)G_{k+2,\alpha}.$$

Repeating this process gives

$$\begin{aligned}
&\vartheta_{k+2}\vartheta_k G_{k,\alpha} - \frac{k(k+2)}{144}E_4 G_{k,\alpha} \\
&= \Big(\alpha - \frac{k}{6} + \frac{1}{3}\Big)\Big[\frac{1}{(\alpha+1)(\alpha+2)}\Big(\alpha - \frac{k}{6} + \frac{2}{3}\Big)\Big(\alpha - \frac{k}{6} + 1\Big)\Big(\alpha - \frac{k}{6} + \frac{4}{3}\Big)G_{k+4,\alpha+2} \\
&- \frac{1}{\alpha+1}\Big\{\Big(\alpha - \frac{k}{6} + \frac{2}{3}\Big)\Big(\alpha - \frac{k}{12} + \frac{4}{3}\Big) + \Big(\alpha - \frac{k}{6}\Big)\Big(\alpha - \frac{k}{12} + \frac{1}{2}\Big) - \frac{k(k+2)}{144}\Big\}G_{k+4,\alpha+1} \\
&+ \Big(\alpha + \frac{1}{2}\Big)G_{k+4,\alpha}\Big].
\end{aligned}$$

The right hand side of this expression vanishes if $\alpha = (k-2)/6$, thus $G_{k,(k-2)/6}(\tau)$ satisfies the same differential equation as $F_k(\tau)$. Along with this, the constant term of the Fourier expansion of $G_{k,(k-2)/6}$ is equal to the coefficient of X^k in the expression $(1-3X^4+2X^6)^{(k-2)/6} = (1-3X^2)^{(k-2)/3}(1+2X^2)^{(k-2)/6}$. This is equal to

$$\sum_{i=0}^{k/2}(-1)^i 2^{\frac{k}{2}-1}\binom{\frac{k-2}{3}}{i}\binom{\frac{k-2}{6}}{\frac{k}{2}-i} = (-1)^{\frac{k}{2}}\binom{\frac{k-2}{3}}{\frac{k}{2}}\sum_{i=0}^{k/2}2^i\binom{\frac{k}{2}}{i} = (-3)^{\frac{k}{2}}\binom{\frac{k-2}{3}}{\frac{k}{2}}.$$

This with (4.8) gives $F_k(\tau) = cG_{k,\frac{k-2}{6}}(\tau)$ where

$$c = (-1)^m\frac{\binom{\frac{k-5}{6}}{m}}{(-3)^{\frac{k}{2}}\binom{\frac{k-2}{3}}{\frac{k}{2}}} = (-1)^{m+\delta}2^{-2m-\epsilon}\binom{2m+\epsilon}{m}\binom{\frac{k-2}{6}}{m+\epsilon}^{-1}. \tag{6.10}$$

□

7. An Asymptotic Formula for $p(n)_{\mathbf{e}}$

Now we turn to the remaining results described in the introduction. Namely, we now discuss partition congruences and asymptotics in the context of the representation theory of finitary permutation groups. One of the tools needed to derive the asymptotic formula for the generalized partition function $p(n)_{\mathbf{e}}$ for any vector $\mathbf{e}$ is Ingham's Tauberian Theorem which is stated in [6, 10] as follows.

Theorem 7.1. *Let $f(q) = \sum_{n=0}^{\infty} a(n)q^n$ be a power series with weakly increasing coefficients and radius of convergence equal to 1. If there are constants $A > 0$, $\lambda, \alpha \in \mathbb{R}$ such that*

$$f(e^{-\epsilon}) \sim \lambda \epsilon^{\alpha} e^{A/\epsilon}$$

as $\epsilon \to 0^+$, then as $n \to \infty$, we have

$$a(n) \sim \frac{\lambda}{2\sqrt{\pi}} \frac{A^{\frac{\alpha}{2}+\frac{1}{4}}}{n^{\frac{\alpha}{2}+\frac{3}{4}}} e^{2\sqrt{An}}.$$

Now, given $\mathbf{e} := (e_1, e_2, \ldots, e_k)$, let $d = \gcd\{m : e_m \neq 0\}$, and define quantities β, γ, and δ by

$$\beta := \beta(\mathbf{e}) = \sum_{n=1}^{\frac{k}{d}} n e_{dn}, \tag{7.1}$$

$$\gamma := \gamma(\mathbf{e}) = \sum_{n=1}^{\frac{k}{d}} e_{dn}, \tag{7.2}$$

and

$$\delta := \delta(\mathbf{e}) = \sum_{n=1}^{\frac{k}{d}} \frac{e_{dn}}{n}. \tag{7.3}$$

Also, define $\mathbf{e}' := (e'_1, e'_2, \ldots, e'_k)$ by $e'_m = e_{dm}$. Given these notations one gets Theorem 1.9.

Lemma 7.2. *Assume the notation above. Then $p(dn)_{\boldsymbol{e}} = p(n)_{\boldsymbol{e}'}$ for all $n \geq 0$.*

Proof. This follows from a simple change of variables $q \to q^d$. □

Proof of Theorem 1.9. By Lemma 7.2, since $p(dn)_{\mathbf{e}} = p(n)_{\mathbf{e}'}$ for all $n \geq 0$, it suffices to find an asymptotic for $p(n)_{\mathbf{e}'}$. First note that $\gcd\{m : e'_m \neq 0\} = 1$ by definition of $\mathbf{e}'$. Now let

$$f(q) = \sum_{n=0}^{\infty} p(n)_{\mathbf{e}'} q^n = q^{\frac{\beta}{24}} \prod_{m=1}^{k} \frac{1}{\eta(mz)^{e'_m}}.$$

Then we have

$$f(e^{-\epsilon}) = e^{-\frac{\beta\epsilon}{24}} \prod_{m=1}^{k} \frac{1}{\eta\left(\frac{-m\epsilon}{2\pi i}\right)^{e'_m}}.$$

By (2.25), it follows that

$$\begin{aligned}\prod_{m=1}^{k} \eta\left(\frac{-m\epsilon}{2\pi i}\right)^{e'_m} &= \prod_{m=1}^{k} \left(\frac{2\pi}{m\epsilon}\right)^{\frac{e'_m}{2}} \eta\left(\frac{2\pi i}{m\epsilon}\right)^{e'_m} \\ &= \epsilon^{-\frac{\gamma}{2}} \prod_{m=1}^{k} \left(\frac{2\pi}{m}\right)^{\frac{e'_m}{2}} \eta\left(\frac{2\pi i}{m\epsilon}\right)^{e'_m}.\end{aligned}$$

Therefore, one gets

$$f(e^{-\epsilon}) = e^{-\frac{\beta\epsilon}{24}} \epsilon^{\frac{\gamma}{2}} \prod_{m=1}^{k} \left(\frac{m}{2\pi}\right)^{\frac{e'_m}{2}} \eta\left(\frac{2\pi i}{m\epsilon}\right)^{-e'_m}.$$

As $\epsilon \to 0^+$, it follows that

$$\prod_{m=1}^{k} \eta\left(\frac{2\pi i}{m\epsilon}\right)^{-e'_m} \sim \prod_{m=1}^{k} e^{\frac{\pi^2 e'_m}{6m\epsilon}} \sim e^{\frac{\pi^2\delta}{6\epsilon}},$$

so as $\epsilon \to 0^+$, we obtain

$$f(e^{-\epsilon}) \sim \epsilon^{\frac{\gamma}{2}} e^{\frac{\pi^2\delta}{6\epsilon}} \prod_{m=1}^{k} \left(\frac{m}{2\pi}\right)^{\frac{e'_m}{2}} \sim \lambda\epsilon^{\frac{\gamma}{2}} e^{\frac{A}{\epsilon}},$$

where λ and A are defined in the statement of Theorem 1.9. Note that $p(n)_{\mathbf{e}'}$ is supported for all $n \geq \max\{m : e'_m \neq 0\}$ since $\gcd\{m : e'_m \neq 0\} = 1$, thus for all $n \geq \operatorname{lcm}\{m : e'_m \neq 0\}$, $p(n)_{\mathbf{e}'}$ is weakly increasing. Furthermore, $f(q)$ has radius of convergence 1. Every modular form maps the upper half plane $\mathbb{H}$ to the unit disk and thus has radius of convergence at least 1. Since $f(q)$ has a pole at $q = 1$, the radius of convergence of $f(q)$ must equal 1. By Theorem 7.1, it then follows that

$$p(n)_{\mathbf{e}'} \sim \frac{\lambda A^{\frac{1+\gamma}{4}}}{2\sqrt{\pi} n^{\frac{3+\gamma}{4}}} e^{2\sqrt{An}}.$$

By Lemma 7.2, we have that

$$p(dn)_{\mathbf{e}} \sim \frac{\lambda A^{\frac{1+\gamma}{4}}}{2\sqrt{\pi} n^{\frac{3+\gamma}{4}}} e^{2\sqrt{An}}.$$

□

Example 7.3. Let $\mathbf{e} := (1, 0, 1)$. Then $d = 1$, $\gamma = 2$, and $\delta = \frac{4}{3}$, so $A = \frac{2\pi^2}{9}$ and $\lambda = \frac{\sqrt{3}}{2\pi}$. Then by Theorem 1.9, we have that

$$p(n)_{\mathbf{e}} \sim P(n)_{\mathbf{e}},$$

where

$$P(n)_{\mathbf{e}} := \frac{1}{6 \cdot 2^{\frac{1}{4}} n^{\frac{5}{4}}} e^{\frac{2\pi\sqrt{2n}}{3}}.$$

Below we display the first 10000 values of $p(n)_{\mathbf{e}}$ and $P(n)_{\mathbf{e}}$ (computed in Mathematica).

TABLE 1. Ratio of $p(n)_{\mathbf{e}}$ and $P(n)_{\mathbf{e}}$

n	$p(n)_{\mathbf{e}}$	$P(n)_{\mathbf{e}}$	$p(n)_{\mathbf{e}}/P(n)_{\mathbf{e}}$
1000	$1.155 \cdot 10^{36}$	$1.187 \cdot 10^{36}$	0.97266
2000	$3.459 \cdot 10^{52}$	$3.527 \cdot 10^{52}$	0.98057
3000	$1.775 \cdot 10^{65}$	$1.804 \cdot 10^{65}$	0.98410
4000	$9.855 \cdot 10^{75}$	$9,993 \cdot 10^{75}$	0.98621
5000	$2.992 \cdot 10^{85}$	$3.029 \cdot 10^{85}$	0.98765
6000	$1.145 \cdot 10^{94}$	$1.158 \cdot 10^{94}$	0.98872
7000	$9.106 \cdot 10^{101}$	$9.198 \cdot 10^{101}$	0.98955
8000	$2.079 \cdot 10^{109}$	$2.099 \cdot 10^{109}$	0.99022
9000	$1.711 \cdot 10^{116}$	$1.727 \cdot 10^{116}$	0.99078
10000	$5.990 \cdot 10^{122}$	$6.042 \cdot 10^{122}$	0.99125

As $n \to \infty$, we observe that the ratio $p(n)_{\mathbf{e}}/P(n)_{\mathbf{e}}$ approaches 1.

8. Generalized Ramanujan Congruences

8.1. **Sturm's Theorem.** We will now introduce the tools used to determine the number of coefficients needed to guarantee a generalized Ramanujan congruence.

Assume that

$$f = \sum_{n \geq n_0} a(n) q^n$$

is a formal power series with coefficients in $\mathcal{O}_K$, the ring of integers of a number field K. If $\mathfrak{m} \subset \mathcal{O}_K$ is an ideal, then define $\mathrm{ord}_{\mathfrak{m}}(f)$, the *order of f modulo $\mathfrak{m}$*, by

$$\mathrm{ord}_{\mathfrak{m}}(f) := \min\{n : a(n) \notin \mathfrak{m}\}. \tag{8.1}$$

If $a(n) \in \mathfrak{m}$ for all n, then let $\mathrm{ord}_{\mathfrak{m}}(f) := +\infty$.

Using this notation, we recall a theorem of Sturm's from [13, p. 40]:

Theorem 8.1. *Let $f(z) = \sum_{n=0}^{\infty} a(n) q^n \in M_{\frac{k}{2}}(\Gamma_0(N), \chi)$ be a modular form where k is a positive integer. Furthermore, suppose that its coefficients are in $\mathcal{O}_K$, the ring of integers of a number field K. If $\mathfrak{m} \subset \mathcal{O}_K$ is an ideal for which*

$$\mathrm{ord}_{\mathfrak{m}}(f) > \frac{k}{24}[\Gamma_0(1) : \Gamma_0(N)],$$

then $\mathrm{ord}_{\mathfrak{m}}(f) = +\infty$.

If $\mathcal{O}_K = \mathbb{Z}$ and $\mathfrak{m} = \langle \ell \rangle$, then $\mathrm{ord}_{\ell}(f) = \min\{n : \ell \nmid a(n)\}$ and if $\ell \mid a(n)$ for all n, then $\mathrm{ord}_{\ell}(f) := +\infty$. Therefore Theorem 8.1 can be reformulated as seen in the next corollary.

Corollary 8.2. *Let $f(z) = \sum_{n=0}^{\infty} a(n) q^n \in M_{\frac{k}{2}}(\Gamma_0(N), \chi) \cap \mathbb{Z}[[q]]$ be a modular form where k is a positive integer. If $a(n) \equiv 0 \pmod{\ell}$ for all $0 \leq n \leq \frac{k}{24}[\Gamma_0(1) : \Gamma_0(N)]$, then $a(n) \equiv 0 \pmod{\ell}$ for all $n \geq 0$.*

8.2. **An Algorithm for the Vector $\mathbf{c}_e$.** Now we give an algorithm used to confirm or refute alleged generalized Ramanujan congruences. Define α by (1.21). Given a prime $\ell \geq 2$ where if $\ell = 2$ or 3, $\alpha \equiv 0 \pmod{\ell}$, and a vector $\mathbf{e} := (e_1, e_2, \ldots, e_k) \in \mathbb{Z}^k$ with $0 \leq e_m \leq \ell - 1$, we must construct a vector $\mathbf{c}_e$ so that $\mathbf{e}' = \mathbf{e} - \ell \mathbf{c}_e$ satisfies the following conditions:

(i) $e'_m \leq 0$ for all m,

(ii) $\sum_{m=1}^{k} me'_m \equiv 0 \pmod{24}$,

(iii) $w \in \mathbb{Z}$, and

(iv) $\sum_{m=1}^{k} \frac{N}{m} e'_m \equiv 0 \pmod{24}$

where w and N are defined by (1.18) and (1.19).

Proposition 8.3. *Assume the notation above. Given a prime $\ell \geq 2$ where if $\ell = 2$ or 3, $\alpha \equiv 0 \pmod{\ell}$, and a vector $\boldsymbol{e} := (e_1, e_2, \ldots, e_k) \in \mathbb{Z}^k$ with $0 \leq e_m \leq \ell - 1$, it is possible to construct a vector $\mathbf{c}_e$ such that the above conditions are satisfied.*

Proof. First define

$$\chi(m) := \begin{cases} 1 & e_m \neq 0 \text{ or } m = 1 \\ 0 & \text{otherwise} \end{cases} \tag{8.2}$$

and α by (1.21). Then define

$$\beta_{\mathbf{e}} := \begin{cases} \min\{n \in \mathbb{N} : n \equiv \ell^{-1}\alpha \pmod{24} \text{ and } n > \sum_{m=1}^{k} m\chi(m)\} & \ell \nmid 24 \\ \min\{n \in \mathbb{N} : n \equiv \ell^{-1}\alpha \pmod{\frac{24}{\ell}} \text{ and } n > \sum_{m=1}^{k} m\chi(m)\} & \ell \mid 24 \end{cases} \tag{8.3}$$

where in the first case, ℓ^{-1} is taken as the multiplicative inverse of $\ell \pmod{24}$, and in the second case, since $\ell \mid \alpha$, $\ell^{-1} = \frac{1}{\ell}$.

Define $c'_m = 0$ if $e_m = 0$. We now define the vector $\mathbf{c}'_e$ recursively beginning with c'_k as follows:

$$c'_m = \left\lfloor \frac{1}{m} \left(\beta_{\mathbf{e}} - \sum_{n=1}^{m-1} n\chi(n) - \sum_{n=m+1}^{k} nc'_n \right) \right\rfloor. \tag{8.4}$$

Note that $c_1' = \beta_{\mathbf{e}} - \sum_{n=2}^{k} nc_n'$, so $\sum_{m=1}^{k} mc_m' = \beta_{\mathbf{e}}$ and

$$\begin{aligned}\sum_{m=1}^{k} me_m' &= \sum_{m=1}^{k} me_m - \ell \sum_{m=1}^{k} mc_m \\ &= \alpha - \ell\beta_{\mathbf{e}} \\ &\equiv 0 \pmod{24}\end{aligned}$$

so condition (ii) is satisfied. If $\frac{1}{2}\sum_{m=1}^{k}(e_m - \ell c_m') \in \mathbb{Z}$, then define $\mathbf{c}_e = \mathbf{c}_e'$.

Suppose $\frac{1}{2}\sum_{m=1}^{k}(e_m - \ell c_m') \notin \mathbb{Z}$. Then choose the smallest j such that j is even and $c_j' > 1$. Define $c_j := c_j' - 1$ and $c_1 := c_1' + j$. For all other m, let $c_m := c_m'$. Let $\mathbf{c}_e = (c_1, c_2, \ldots, c_k)$ and define $\mathbf{e}' = \mathbf{e} - \ell\mathbf{c}_e$. Then $\sum_{m=1}^{k} mc_m = \sum_{m=1}^{k} mc_m'$ and $e_m' \leq 0$ for all m, so conditions (i)-(ii) hold. Since $\sum_{m=1}^{k} c_m = \sum_{m=1}^{k} c_m' - 1 + j$ and $-1 + j$ is odd, the parity of the sum $\sum_{m=1}^{k} e_m' = \sum_{m=1}^{k} e_m - \ell\sum_{m=1}^{k} c_m$ changes and $w = -\frac{1}{2}\sum_{m=1}^{k}(e_m - \ell c_m') \in \mathbb{Z}$.

Suppose $c_j' \leq 1$ for all j even. Then choose the smallest $j \neq 1$ such that j is odd and $c_j > 1$. Define $c_j = c_j' - 1$, $c_{j-1} = c_{j-1}' + 1$, and $c_1 = c_1' + 1$. For all other m, let $c_m = c_m'$. Let $\mathbf{c}_e = (c_1, c_2, \ldots, c_k)$ and define $\mathbf{e}' = \mathbf{e} - \ell\mathbf{c}_e$. Then, as before, $\sum_{m=1}^{k} mc_m = \sum_{m=1}^{k} mc_m'$ and $e_m' \leq 0$ for all m, so conditions (i)-(ii) hold. Since $\sum_{m=1}^{k} c_m = \sum_{m=1}^{k} c_m' + 1$, the parity of the sum $\sum_{m=1}^{k} e_m'$ changes and $w \in \mathbb{Z}$.

If there exists no j such that $c_j' > 1$, replace $\beta_{\mathbf{e}}$ by

$$\beta_{\mathbf{e}}' = \begin{cases} \beta_{\mathbf{e}} + 24 & \ell \nmid 24 \\ \beta_{\mathbf{e}} + \frac{24}{\ell} & \ell \mid 24 \end{cases} \tag{8.5}$$

and repeat the algorithm. By construction there must exist at least one $c_j' > 1$, so if $w \notin \mathbb{Z}$, it will be possible to run through the replacements described above and to define a vector $\mathbf{c}_e$ that satisfies conditions (i)-(iii).

Note that by the definition of N in (1.19), $\sum_{m=1}^{k} \frac{N}{m} e_m' \equiv 0 \pmod{24}$, so condition (iv) holds. Thus the vector $\mathbf{e}'$ satisfies conditions (i)-(iv) as desired. $\square$

We now use the algorithm in Proposition 8.3 to prove Theorems 1.14 and 1.15 and establish a method of confirming or refuting alleged generalized Ramanujan congruences that fall into two different types. First note the following fact from [3]:

Proposition 8.4. *Consider a sequence* $\boldsymbol{e} := (e_1, e_2, \ldots, e_k) \in \mathbb{Z}^k$*, an arithmetic progression* $(An + B)_{n\geq 0}$ *with* $A \geq 2$ *and* $1 \leq B \leq A - 1$*, a prime* ℓ*, and another sequence* $\boldsymbol{e}' = (e'_1, e'_2, \ldots, e'_k) \in \mathbb{Z}^k$*. Assume that* $e'_m \equiv e_m \pmod{\ell}$ *for all* $m \geq 0$*. Then* $p(An + B)_{\boldsymbol{e}} \equiv 0 \pmod{\ell}$ *for all* $n \geq 0$ *if and only if* $p(An + B)_{e'} \equiv 0 \pmod{\ell}$ *for all* $n \geq 0$*.*

8.3. **Proof of Theorem 1.14.** By Proposition 8.4, it suffices to consider vectors $\mathbf{e} = (e_1, e_2, \ldots, e_k)$ with $0 \leq e_m \leq \ell - 1$ for all m. Define $\mathbf{e}' = \mathbf{e} - \ell\mathbf{c}_e$ by Proposition 8.3. Then since $e'_m \equiv e_m \pmod{\ell}$ for all $m \geq 0$, by Proposition 8.4, it is enough to show that $p(\ell n + \delta_\ell)_{\mathbf{e}'} \equiv 0 \pmod{\ell}$ for all $n \geq 0$. Note that

$$\begin{aligned}\sum_{n=0}^{\infty} p(n)_{\mathbf{e}'} q^n &= \prod_{m=1}^{k} \prod_{n=1}^{\infty} \frac{1}{(1-q^{mn})^{e'_m}} \\ &= q^{\omega} \prod_{m|N} \eta(mz)^{-e'_m} \\ &=: q^{\omega} g(z)\end{aligned}$$

where $\omega = \frac{1}{24} \sum_{m=1}^{k} m e'_m$. Note that $\omega \equiv \delta_\ell \pmod{\ell}$.

Since $g(z)$ is an eta-product, we can write its Fourier expansion

$$g(z) := \sum_{n=0}^{\infty} b(n) q^n.$$

Then $p(\ell n + \delta_\ell)_{\mathbf{e}'} \equiv 0 \pmod{\ell}$ for all $n \geq 0$ if and only if $b(\ell n + \delta_\ell - \omega) \equiv 0 \pmod{\ell}$ for all $n \geq 0$. Since $\delta_\ell - \omega \equiv 0 \pmod{\ell}$, $p(\ell n + \delta_\ell)_{\mathbf{e}'} \equiv 0 \pmod{\ell}$ for all $n \geq 0$ if and only if $b(\ell n) \equiv 0 \pmod{\ell}$ for all $n \geq 0$.

Now, note that $g(z)$ has weight $w = -\frac{1}{2} \sum_{m=1}^{k} e'_m$. By condition (iii), w must be an integer. Furthermore, based on our choices of $\mathbf{c}_e$ and N, $\mathbf{e}'$ satisfies conditions

(ii) and (iv), which are the necessary conditions of Theorem 2.9. Since $g(z)$ is additionally holomorphic at all the cusps of $\Gamma_0(N)$, $g(z) \in M_w(\Gamma_0(N), \chi)$. We can therefore act on $g(z)$ with the Hecke operator $T_{\ell,w,\chi}$ and define

$$\begin{aligned} f(z) &:= g(z) \mid T_{\ell,w,\chi} \\ &= \sum_{n=0}^{\infty} (b(\ell n) + \chi(\ell)\ell^{w-1} b(n/\ell)) q^n. \end{aligned}$$

By Proposition 2.27, $f(z) \in M_w(\Gamma_0(N), \chi)$ and we can write its Fourier series expansion as

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

Then $a(n) = b(\ell n) + \chi(\ell)\ell^{w-1} b(n/\ell)$, so $a(n) \equiv b(\ell n) \pmod{\ell}$ for all n. Thus $b(\ell n) \equiv 0 \pmod{\ell}$ for all $n \geq 0$ if and only if $a(n) \equiv 0 \pmod{\ell}$ for all $n \geq 0$.

Since $f(z)$ has weight w and is a level N modular form, by Theorem 8.1, $a(n) \equiv 0 \pmod{\ell}$ for all $n \geq 0$ if and only if $a(n) \equiv 0 \pmod{\ell}$ for all $0 \leq n \leq \frac{w}{12}[\Gamma_0(1) : \Gamma_0(N)]$. By Proposition 2.3,

$$[\Gamma_0(1) : \Gamma_0(N)] = N \prod_{p \mid N} \left(1 + \frac{1}{p}\right),$$

so by our definition of $K_{\mathbf{e}}$ in (1.20), $a(n) \equiv 0 \pmod{\ell}$ for all $n \geq 0$ if and only if $a(n) \equiv 0 \pmod{\ell}$ for all $0 \leq n \leq K_{\mathbf{e}}$. Since this is true if and only if $p(\ell n + \delta_\ell)_{\mathbf{e}} \equiv 0 \pmod{\ell}$ for $0 \leq n \leq K_{\mathbf{e}}$, we have $p(\ell n + \delta_\ell)_{\mathbf{e}} \equiv 0 \pmod{\ell}$ for all n if and only if $p(\ell n + \delta_\ell)_{\mathbf{e}} \equiv 0 (\mathrm{mod}\ \ell)$ for $0 \leq n \leq K_{\mathbf{e}}$. □

8.4. **Proof of Theorem 1.15.** As in the proof of Theorem 1.14, by Proposition 8.4, it suffices to consider vectors $\mathbf{e} = (e_1, e_2, \ldots, e_k)$ with $0 \leq e_m \leq \ell - 1$ for all m. Define $\mathbf{e}'$ using Proposition 8.3. Again, let $g(z) = \prod_{m \mid N} \eta(mz)^{-e'_m} = \sum_{n=0}^{\infty} b(n) q^n$. As in the previous proof, $p(\ell n + \gamma_\ell) \equiv 0 \pmod{\ell}$ for all $n \geq 0$ if and only if $b(\ell n + \gamma_\ell - \delta_\ell) \equiv 0 \pmod{\ell}$ for all $n \geq 0$.

Define the following Dirichlet characters:

$$\psi_0(n) := \begin{cases} 1 & \gcd(n,\ell) = 1 \\ 0 & \text{otherwise} \end{cases}$$

and

$$\psi_1(n) := \left(\frac{n}{\ell}\right).$$

Note that $\psi_0^2(n)$ and $\psi_1^2(n)$ both yield the trivial character. Now define

$$G(z) := g_{\psi_0}(z) = \sum_{\ell \nmid n} b(n) q^n$$

and

$$G_{\psi_1}(z) = \sum_{\ell \nmid n} \left(\frac{n}{\ell}\right) b(n) q^n.$$

By Proposition 2.13, $G(z) \in M_w(\Gamma_0(N\ell^2), \chi\psi_0^2) = M_w(\Gamma_0(N\ell^2), \chi)$ and $G_{\psi_1}(z) \in M_w(\Gamma_0(N\ell^2), \chi\psi_1^2) = M_w(\Gamma_0(N\ell^2), \chi)$. Now define

$$H_+(z) := \frac{G(z) + G_{\psi_1}(z)}{2} = \sum_{\left(\frac{n}{\ell}\right)=1} b(n) q^n$$

and

$$H_-(z) := \frac{G(z) - G_{\psi_1}(z)}{2} = \sum_{\left(\frac{n}{\ell}\right)=-1} b(n) q^n.$$

Then $H_\pm(z) \in M_w(\Gamma_0(N\ell^2), \chi)$. Recalling our definitions of the sets $S_\pm$ in (1.23) and (1.24), note that

$$H_\pm(z) = \sum_{\substack{n \equiv \gamma_\ell + \delta_\ell \\ (\text{mod } \ell) \\ \gamma_\ell \in S_\pm}} b(n) q^n.$$

Now, write $H_\pm(z) := \sum_{n=0}^{\infty} a_\pm(n) q^n$. Since $a_+(n)$ is only supported where $n \equiv \gamma_\ell + \delta_\ell \pmod{\ell}$ where $\gamma_\ell \in S_+$, $b(\ell n + \gamma_\ell - \delta_\ell) \equiv 0 \pmod{\ell}$ for all $n \geq 0$ and for all $\gamma_\ell \in S_+$ if and only if $a_+(n) \equiv 0 \pmod{\ell}$ for all $n \geq 0$. By Theorem 8.1, $a_+(n) \equiv 0 \pmod{\ell}$ for all $n \geq 0$ if and only if $a_+(n) \equiv 0 \pmod{\ell}$ for all $0 \leq n \leq \frac{w}{12}[\Gamma_0(1) : \Gamma_0(N\ell^2)]$.

By our definition of $K'_{\mathbf{e}}$ in (1.25), $a_+(n) \equiv 0 \pmod{\ell}$ for all $n \geq 0$ if and only if $a_+(n) \equiv 0 \pmod{\ell}$ for all $0 \leq n \leq K'_{\mathbf{e}}$. As $a_+(n) \equiv 0 \pmod{\ell}$ for all $0 \leq n \leq K'_{\mathbf{e}}$ if and only if $p(\ell n + \gamma_\ell)_{\mathbf{e}} \equiv 0$ for all $0 \leq n \leq K'_{\mathbf{e}}$ and for all $\gamma_\ell \in S_+$, the theorem holds for $\gamma_\ell \in S_+$. Replacing S_+ by S_-, $a_+(n)$ by $a_-(n)$, and $H_+(z)$ by $H_-(z)$, the same argument works for $\gamma_\ell \in S_-$. □

8.5. **Examples of Congruences.** Given an alleged congruence of the form $p(\ell n + B)_{\mathbf{e}} \equiv 0 \pmod{\ell}$ that falls into either the Theorem 1.14 or Theorem 1.15 case, we can use the finite algorithm from Section 3 and Theorems 1.14 and 1.15 to confirm or refute it. First use the algorithm to determine $K_{\mathbf{e}}$ and $K'_{\mathbf{e}}$. By Theorems 1.14 and 1.15, it suffices to check numerically that the conjectured congruences hold for all $0 \leq n \leq K_{\mathbf{e}}$ or $K'_{\mathbf{e}}$ respectively.

Example 8.5. We have that $p(5n+2)_{(2,0,0,4)} \equiv 0 \pmod{5}$ for all $n \geq 0$, as conjectured by [3].

Proof. Note that $\alpha = 18$, so $\delta_\ell = 2$; this is an example of the Theorem 1.14 case. Using our algorithm, we have $\mathbf{c}_e = (2, 0, 0, 4)$, so $\mathbf{e}' = (-8, 0, 0, -16)$. Then $w = 12$ and $N = 4$, so $K_{\mathbf{e}} = 6$. Computing the first 6 values of $p(5n+2)_{(2,0,0,4)}$, we find that they are equivalent to 0 (mod 5). Thus the congruence holds. □

Example 8.6. We have that $p(5n+2)_{(2,0,0,2)} \equiv p(5n+3)_{(2,0,0,2)} \equiv 0 \pmod{5}$ for all $n \geq 0$, as conjectured by [3].

Proof. Note that $\alpha = 10$, so $\delta_\ell = 0$. In this case $S_{-1} = \{2, 3\}$, so this is an example of the Theorem 1.15 case. Using our algorithm, we have $\mathbf{c}_e = (2, 0, 0, 6)$ so $\mathbf{e}' = (-8, 0, 0, -28)$. Then $w = 18$ and $N = 8$, so $K'_e = 540$. Computing the first 540 values of $p(5n+2)_{(2,0,0,2)}$ and $p(5n+3)_{(2,0,0,2)}$, we find that they are equivalent to 0 (mod 5). Thus the congruence holds. □

9. Proof of Theorem 1.19

Ramanujan conjectured the following congruences for the partition function modulo powers of the primes 5 and 7, which Watson proved in [18].

Theorem 9.1 (Ramanujan). *Let $\ell = 5$, 7, or 11 and let $j \geq 1$. Then if $24n \equiv 1 \pmod{\ell^j}$, we have that*

$$\begin{cases} p(n) \equiv 0 \pmod{\ell^j} & \ell = 5, 11 \\ p(n) \equiv 0 \pmod{\ell^{\lfloor j/2 \rfloor + 1}} & \ell = 7. \end{cases}$$

In [2], Atkin generalized the Ramanujan congruences modulo powers of 5, 7, and 11 to the function $p_k(n)$, which counts the number of k-colored partitions of n.

Theorem 9.2 (Atkin). *Let $k > 0$, $\ell = 2, 3, 5, 7$ or 13, and $j \geq 1$. Then if $24n \equiv k \pmod{\ell^j}$, we have that*

$$p_k(n) \equiv 0 \pmod{\ell^{\lfloor \alpha j/2 + \epsilon \rfloor}},$$

where $\epsilon := \epsilon(k) = O(\log k)$ and $\alpha = \alpha(k, \ell)$ depending on ℓ and the residue of k modulo 24.

Atkin computes the value of $\alpha(k, \ell)$ in a table in [2]. We note the following values of α:

$$\alpha(2, 5) = \alpha(2, 7) = 1. \tag{9.1}$$

In addition, following Atkin's method to calculate ϵ exactly, we observe

$$\epsilon = \begin{cases} 1 - \lfloor \log(48)/\log(\ell) \rfloor = -1 & \ell = 5 \\ -\lfloor \log(48)/\log(\ell) \rfloor = -1 & \ell = 7. \end{cases} \tag{9.2}$$

Therefore, for the case where $k = 2$ and $\ell = 5$ or 7, we have that for all $24n \equiv k \pmod{\ell^j}$,

$$p_2(n) \equiv 0 \pmod{\ell^{\lfloor j/2-1 \rfloor}}. \tag{9.3}$$

We make use of the following theorem of Serre's regarding congruences for certain types of modular forms, stated in [17]:

Theorem 9.3 (Serre)**.** *Suppose that $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_k(\Gamma_0(N), \chi)$ has coefficients in the ring of integers $\mathcal{O}_K$ of a number field K and M is a positive integer. Furthermore, suppose that $k \geq 1$. Then a positive proportion of the primes $p \equiv -1 \pmod{MN}$ have the property that*

$$f(z) \mid T_{p,k,\chi} \equiv 0 \pmod{M}.$$

Serre's theorem guarantees the existence of congruences for cusp forms with coefficients in the ring of integers of a number field, which we will use to prove properties of the coefficients of the conjugacy growth series for $(\mathrm{Alt}(\mathbb{N}), S')$ and $(\mathrm{Sym}(\mathbb{N}), S)$.

Proof of Theorem 1.19. We first prove congruences for arbitrary powers of $\ell = 5$ or 7. Let $j \geq 1$ and suppose that $24n \equiv 1 \pmod{\ell^j}$. Then by Theorem 9.1, we have that

$$\gamma_{\mathrm{Sym}(\mathbb{N}),S}(n) = p(n) \equiv 0 \pmod{\ell^{\lfloor j/2 \rfloor + 1}}. \tag{9.4}$$

Additionally, we have that $24(2n) \equiv 2 \pmod{\ell^j}$. Using the case of Theorem 9.2 where $k = 2$ and $\ell = 5$ or 7, as in (9.3), we have that

$$p_2(2n) \equiv 0 \pmod{\ell^{\lfloor j/2-1 \rfloor}}. \tag{9.5}$$

Therefore, for all $24n \equiv 1 \pmod{\ell^j}$, we obtain from (1.17), (9.4), and (9.5) that

$$\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2n) \equiv \gamma_{\mathrm{Sym}(\mathbb{N}),S}(n) \equiv 0 \pmod{\ell^{\lfloor j/2-1 \rfloor}}, \tag{9.6}$$

as desired. □

10. Congruences for $p_2(n)$

Because of the relationship between the conjugacy growth series for $(\mathrm{Alt}(\mathbb{N}), S')$ and the function $p_2(n)$, here, we focus on congruences for $p_2(n)$. By the definition of the 2-colored partition function $p_2(n)$, we have that

$$\sum_{n=0}^{\infty} p_2(n)q^n = \prod_{n=1}^{\infty} \frac{1}{(1-q^n)^2} = \frac{q^{\frac{1}{12}}}{\eta^2(z)}. \tag{10.1}$$

Throughout, we let

$$f(z) := \frac{1}{\eta(12z)^2} = \sum_{n=-1}^{\infty} a(n)q^n. \tag{10.2}$$

Then we have that $p_2\left(\frac{n+1}{12}\right) = a(n)$. In order to prove congruences between the coefficients of the conjugacy growth series for $(\mathrm{Alt}(\mathbb{N}), S')$ and $(\mathrm{Sym}(\mathbb{N}), S)$, we first prove a theorem concerning the coefficients of $f(z)$. This makes effective the following result of Treneer [17] by determining the exact value of m that is sufficiently large.

Proposition 10.1 (Treneer)**.** *Suppose that ℓ is an odd prime and that k and m are integers. Let N be a positive integer with $(N, p) = 1$, and let χ be a Dirichlet character modulo N. Let K be an algebraic number field with ring of integers $\mathcal{O}_K$, and suppose $f(z) = a(n)q^n \in M_k^!(\Gamma_0(N), \chi) \cap \mathcal{O}_K((q))$. If m is sufficiently large, then for each positive integer j, a positive proportion of the primes $Q \equiv -1 \pmod{N\ell^j}$ have the property that*

$$a(Q\ell^m n) \equiv 0 \pmod{\ell^j}$$

for all n coprime to $Q\ell$.

This section closely follows Section 3 in [17]. Throughout this section, let $f(z)$ be defined by (10.2).

Theorem 10.2. *Let $\ell \geq 5$ be prime and $j \in \mathbb{N}$. Then for a positive proportion of primes $Q \equiv -1 \pmod{144\ell^j}$, we have that*

$$a(Q\ell^{m_\ell} n) \equiv 0 \pmod{\ell^j}$$

for all n coprime to $Q\ell$.

The proof of Theorem 10.2 requires the construction of a cusp form that preserves congruence properties of the function $f(z)$.

Proposition 10.3. *For every positive integer j, there exists an integer $\beta \geq j-1$ and a cusp form*

$$g_{\ell,j}(z) \in S_\kappa(\Gamma_0(144\ell^2), \chi) \cap \mathbb{Z}((q)),$$

where $\kappa := -1 + \frac{\ell^\beta(\ell^2-1)}{2}$, with the property that

$$g_{\ell,j}(z) \equiv \sum_{\substack{n \geq 1 \\ \ell \nmid n}} a(\ell^{m_\ell} n) q^n \pmod{\ell^j}.$$

We first require the following proposition concerning the Fourier expansion of $f(z)$ at a given cusp after being acted on by the $U(\ell^m)$ operator for $m \geq 1$.

Proposition 10.4. *Let $\gamma := \begin{pmatrix} a & b \\ c\ell^2 & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ where $c \in \mathbb{Z}$ and $ac > 0$. Then there exists an integer $n_0 \geq -24$ and a sequence $\{a_0(n)\}_{n \geq n_0}$ such that for each $m \geq 1$, we have that*

$$(f(z) \mid U_{\ell^m}) \mid_{-1} \gamma = \sum_{\substack{n=n_0 \\ n \equiv 0 \pmod{\ell^m}}}^{\infty} a_0(n) q_{24\ell^m}^n,$$

where $q_{24\ell^m} := e^{\frac{2\pi i z}{24\ell^m}}$.

The proof of this proposition makes use of the following lemma, which relies on the proof of Theorem 1 in [9].

Lemma 10.5. *Given any matrix $A \in \mathrm{SL}_2(\mathbb{Z})$, we have that*

$$f(z) \mid_{-1} A = \sum_{n=n_0}^{\infty} a_0(n) q_{24}^n$$

where $a_0(n) \in \mathbb{Z}$ and $n_0 \geq -24$.

Proof. Let $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Then, as in the proof of Theorem 1 in [9], we can write

$$\begin{pmatrix} 12 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \tag{10.3}$$

where $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, $\alpha, \beta, \delta \in \mathbb{Z}$, and $\alpha, \delta > 0$. Then we have that $12a = a'\alpha$ and $c = c'\alpha$, so $\alpha = (a'\alpha, c'\alpha) = (12a, c) = (12, c) \leq 12$. Again, by Theorem 1 in [9], we obtain

$$f(z) \mid_{-1} A = \sum_{n=n_0}^{\infty} a_0(n) q_{24}^n \tag{10.4}$$

where $n_0 := \frac{-2\alpha}{\delta} > -2\alpha \geq -24$. □

Proof of Proposition 10.4. Let $N = 144$, the level of f. As in [17], for each $0 \leq v \leq \ell^m - 1$, choose an integer s_v such that

$$s_v N \equiv (a + vc\ell^2)^{-1}(b + vd) \pmod{\ell^m} \tag{10.5}$$

and define $w_v := s_v N = 144 s_v$. We let

$$\alpha_0 := \begin{pmatrix} a & \frac{b - aw_0}{\ell^m} \\ c\ell^{m+2} & d - w_0 c\ell^2 \end{pmatrix}. \tag{10.6}$$

By (2.10), we have that

$$(f(z) \mid U_{\ell^m}) \mid_{-1} \gamma = (\ell^m)^{-\frac{3}{2}} \sum_{v=0}^{\ell^m-1} f(z) \mid_{-1} \sigma_{v,\ell^m}\gamma. \tag{10.7}$$

We observe that $\sigma_{v,\ell^m}\gamma = \beta\alpha_0\sigma_{w_v,\ell^m}$ for some $\beta \in \Gamma_0(144\ell^m)$, so we have that

$$(f(z) \mid U_{\ell^m}) \mid_{-1} \gamma = (\ell^m)^{-\frac{3}{2}} \sum_{v=0}^{\ell^m-1} f(z) \mid_{-1} \alpha_0\sigma_{w_v,\ell^m}. \tag{10.8}$$

By Lemma 10.5, we have that

$$f(z) \mid_{-1} \alpha_0 = \sum_{n=n_0}^{\infty} a_0(n) q_{24}^n,$$

so we obtain

$$\begin{aligned} \sum_{v=0}^{\ell^m-1} f(z) \mid_{-1} \alpha_0\sigma_{w_v,\ell^m} &= \sum_{v=0}^{\ell^m-1} \ell^{\frac{m}{2}} \sum_{n=n_0}^{\infty} a_0(n) e^{\frac{2\pi i n(z+w_v)}{24\ell^m}} \\ &= \ell^{\frac{m}{2}} \sum_{n=n_0}^{\infty} a_0(n) q_{24\ell^m}^n \sum_{v=0}^{\ell^m-1} e^{\frac{2\pi i n w_v}{24\ell^m}}. \end{aligned} \tag{10.9}$$

By Lemma 3.3 in [17], the numbers $\frac{w_v}{24}$ run through the residue classes modulo ℓ^m as v does. Therefore, we have that

$$\sum_{v=0}^{\ell^m-1} e^{\frac{2\pi i n w_v}{24\ell^m}} = \sum_{v=0}^{\ell^m-1} e^{\frac{2\pi i n v}{\ell^m}} = \begin{cases} \ell^m & n \equiv 0 \pmod{\ell^m} \\ 0 & \text{else.} \end{cases} \tag{10.10}$$

Combining (10.9) and (10.10), we have that

$$\sum_{v=0}^{\ell^m-1} f(z) \mid_{-1} \alpha_0\sigma_{w_v,\ell^m} = \ell^{\frac{3}{2}} \sum_{\substack{n=n_0 \\ n\equiv 0 \pmod{\ell^m}}}^{\infty} a_0(n) q_{24\ell^m}^n. \tag{10.11}$$

Using (10.7) and (10.11), we obtain

$$(f(z) \mid U_{\ell^m}) \mid_{-1} \gamma = \sum_{\substack{n=n_0 \\ n\equiv 0 \pmod{\ell^m}}}^{\infty} a_0(n) q_{24\ell^m}^n, \tag{10.12}$$

the Fourier expansion of $f(z) \mid U_{\ell^m}$ at the cusp $\frac{a}{c\ell^2}$. $\square$

We now construct a weakly holomorphic modular form which vanishes at certain cusps of $\Gamma_0(144\ell^2)$.

Proposition 10.6. *For each nonnegative integer m, define*

$$f_m(z) := f(z) \mid U_{\ell^m} - f(z) \mid U_{\ell^{m+1}} \mid V_\ell \in M^!_{-1}(\Gamma_0(144\ell^2), \chi).$$

Then, for m_ℓ as in 1.26, f_{m_ℓ} vanishes at each cusp $\frac{a}{c\ell^2}$ of $\Gamma_0(144\ell^2)$ with $ac > 0$.

Proof. By Proposition 10.4, we have that

$$(f(z) \mid U_{\ell^{m_\ell}}) \mid \gamma = \sum_{\substack{n=n_0 \\ n\equiv 0 \pmod{\ell^{m_\ell}}}}^{\infty} a_0(n) q_{24\ell^{m_\ell}}^n \tag{10.13}$$

where $n_0 \geq -24$. We now consider two cases. If $5 \leq \ell \leq 23$, we have that

$$-\ell^{m_\ell} \leq -25 < -24 \leq n_0,$$

and if $\ell \geq 29$, we have that

$$-\ell^{m_\ell} \leq -29 < -24 \leq n_0.$$

Suppose $a_0(n) \neq 0$. Then $n \geq n_0 > -\ell^{m_\ell}$, but $n \equiv 0 \pmod{\ell^{m_\ell}}$, so $n \geq 0$. Therefore, we obtain

$$(f(z) \mid U_{\ell^{m_\ell}}) \mid \gamma = \sum_{\substack{n=0 \\ n\equiv 0 \pmod{\ell^{m_\ell}}}}^{\infty} a_0(n) q_{24\ell^{m_\ell}}^n \tag{10.14}$$

so $f(z) \mid U_{\ell^{m_\ell}}$ is holomorphic at the cusp $\frac{a}{c\ell^2}$.

Now, by the proof of Proposition 3.5 in [17], we have that

$$f_m(z) \mid_{-1} \gamma = \sum_{\substack{n=0 \\ n\equiv 0 \pmod{\ell^m}}}^{\infty} a_0(n) q_{24\ell^m}^n - \sum_{\substack{n=0 \\ n\equiv 0 \pmod{\ell^{m+1}}}}^{\infty} a_0(n) q_{24\ell^m}^n, \tag{10.15}$$

so the constant term in each expansion is $a_0(0)$, and they cancel. Therefore, f_{m_ℓ} vanishes at the cusp $\frac{a}{c\ell^2}$. $\square$

We are now ready to prove Proposition 10.3.

Proof of Proposition 10.3. As in [17], we define the eta-quotient

$$F_\ell(z) := \frac{\eta^{\ell^2}(z)}{\eta(\ell^2 z)} \in M_{\frac{\ell^2-1}{2}}(\Gamma_0(\ell^2)). \tag{10.16}$$

By Theorem 1.65 in [13], we see that F_ℓ vanishes at every cusp $\frac{a}{c}$ of $\Gamma_0(144\ell^2)$ with $\ell^2 \nmid c$. We also have that $F_\ell(z)^{\ell^{s-1}} \equiv 1 \pmod{\ell^s}$ for any integer $s \geq 1$.

Now, define

$$g_{\ell,j}(z) := f_{m_\ell}(z) \cdot F_\ell(z)^{\ell^\beta} \tag{10.17}$$

where $\beta \geq j-1$ is sufficiently large such that $g_{\ell,j}(z)$ vanishes at all cusps $\frac{a}{c}$ of $\Gamma_0(144\ell^2)$ where $\ell^2 \nmid c$. By Theorem 1.65 in [13], it is possible to choose such a β such that the order of vanishing of $g_{\ell,j}(z)$ is at least one at all such cusps. Then $g_{\ell,j} \in \mathbb{Z}((q))$ and

$$g_{\ell,j}(z) \equiv f_{m_\ell}(z) \pmod{\ell^j}. \tag{10.18}$$

Furthermore, by Proposition 10.6, $g_{\ell,j}(z)$ vanishes at all cusps $\frac{a}{c}$ where $\ell^2 \mid c$. Define $\kappa := -1 + \frac{\ell^\beta(\ell^2-1)}{2}$. Then we have that

$$g_{\ell,j}(z) \in S_\kappa(\Gamma_0(144\ell^2), \chi). \tag{10.19}$$

By definition of f_{m_ℓ}, we obtain

$$g_{\ell,j}(z) \equiv \sum_{n=1}^{\infty} a(\ell^{m_\ell} n) q^n - \sum_{n=1}^{\infty} a(\ell^{m_\ell+1} n) q^{\ell n} \equiv \sum_{\substack{n=1 \\ \ell \nmid n}}^{\infty} a(\ell^{m_\ell} n) q^n \pmod{\ell^j}. \tag{10.20}$$

Thus $g_{\ell,j}$ satisfies the conditions of Proposition 10.3. $\square$

Now that we have constructed the necessary cusp form, we arrive at the proof of Theorem 10.2.

Proof of Theorem 10.2. By Proposition 10.3, we can construct a cusp form $g_{\ell,j} \in S_\kappa(\Gamma_0(144\ell^2), \chi) \in \mathbb{Z}((q))$ such that

$$g_{\ell,j}(z) \equiv \sum_{\substack{n=1 \\ \ell \nmid n}}^{\infty} a(\ell^{m_\ell} n) q^n \pmod{\ell^j}. \tag{10.21}$$

By Theorem 9.3, for a positive proportion of the primes $Q \equiv -1 \pmod{144\ell^{j+2}}$, we have that

$$g_{\ell,j}(z) \mid T_{Q,\kappa,\chi} \equiv 0 \pmod{\ell^j}. \tag{10.22}$$

We can then write $g_{\ell,j}(z) = \sum_{n=1}^{\infty} b(n) q^n$ to obtain

$$g_{\ell,j}(z) \mid T_{Q,\kappa,\chi} = \sum_{n=1}^{\infty} \left(b(Qn) + \chi(Q) Q^{\kappa-1} b(n/Q) \right) q^n \equiv 0 \pmod{\ell^j}. \tag{10.23}$$

If $(Q, n) = 1$, then the coefficient of q^n in (10.23) is $b(Qn)$, so

$$a(Q\ell^{m_\ell} n) \equiv b(Qn) \equiv 0 \pmod{\ell^j} \tag{10.24}$$

for all n coprime to $Q\ell$. □

10.1. **Proof of Theorem 1.21.** We now make use of Theorem 10.2 to prove congruences between the coefficients of the conjugacy growth series for $(\mathrm{Alt}(\mathbb{N}), S')$ and $(\mathrm{Sym}(\mathbb{N}), S)$.

Proof of Theorem 1.21. By (1.17), it is enough to show that $p_2(2Q\ell^{m_\ell} n + 2\delta_\ell) \equiv 0 \pmod{\ell^j}$. By (10.1) and (10.2), we observe $p_2\left(\frac{n+1}{12}\right) = a(n)$, so it suffices to prove the existence of congruences for $a(n)$.

By Theorem 10.2, for a positive proportion of primes $Q \equiv -1 \pmod{144\ell^j}$, we have that

$$p_2\left(\frac{Q\ell^{m_\ell}n+1}{12}\right) = a(Q\ell^{m_\ell}n) \equiv 0 \pmod{\ell^j} \tag{10.25}$$

for all n coprime to $Q\ell$. Defining δ_ℓ and β_ℓ by (1.27) and (1.28), respectively, we can rewrite the left-hand side of equation (10.25) as

$$p_2\left(2Q\ell^{m_\ell}n + 2\delta_\ell\right) \tag{10.26}$$

for all $24n+\beta_\ell$ coprime to $Q\ell$. Therefore, for a positive proportion of primes $Q \equiv -1 \pmod{144\ell^j}$, we have that

$$p_2\left(2Q\ell^{m_\ell}n + 2\delta_\ell\right) \equiv 0 \pmod{\ell^j}, \tag{10.27}$$

so we obtain

$$2\gamma_{\mathrm{Alt}(\mathbb{N}),S'}(2Q\ell^{m_\ell}n + 2\delta_\ell) \equiv \gamma_{\mathrm{Sym}(\mathbb{N}),S}(Q\ell^{m_\ell}n + \delta_\ell) \pmod{\ell^j},$$

as desired. □

11. Appendix

We include here a list of the conjectures from [3]. They are all true.

11.1. Some examples of the form $p(3n+B)_{\mathbf{e}} \equiv 0 \pmod 3$.

$p(3n+2)_{(1,1),(2,1,0,2),(2,1,0,1,2,1_{10},1_{20}),(1,1,0,2,1,1_{10},2_{20})}$.

11.2. Some examples of the form $p(5n+B)_{\mathbf{e}} \equiv 0 \pmod 5$.

$p(5n+1)_{(0,2,2),(0,4,2),(0,2,3,0,0,1)}$,

$p(5n+2)_{(2),(3,1),(1,3),(1,3,2),(2,0,0,2),(3,1,0,2),(3,1,0,3),(2,0,0,4),(4,1,0,4),(1,3,4,0,0,1)}$,

$p(5n+2)_{(4,1,1,0,0,3),(4,1,3,0,0,3),(3,1,1,0,0,4),(3,1,3,0,0,4),(2,2_8),(1,3,2_8),(3,1,0,3,2_8),(4,1,0,4,2_8)}$,

$p(5n+3)_{(2),(4),(3,1),(1,2,0,1),(2,0,0,2),(4,0,0,2),(3,1,0,3),(1,2,0,3),(3,1,0,1,1_8),(2,0,0,3,1_8),(1,1,1,0,0,1)}$,

$p(5n+3)_{(1,4,3,0,0,1),(1,3,4,0,0,1),(3,3,4,0,0,1),(3,1,0,0,0,2),(2,3,4,0,0,2),(4,2,2,0,0,3),(3,2,2,0,0,4)}$,

$p(5n+4)_{(1),(2),(4),(2,2),(1,3),(0,2,2),(0,2,4),(1,2,0,1),(3,2,0,1),(2,1,0,3),(3,1,0,3),(3,3,0,3)}$,

$p(5n+4)_{(4,1,0,4),(4,3,0,4),(1,4,3,0,0,1),(3,4,3,0,0,1),(2,4,3,0,0,2),(4,1,1,0,0,3),(4,3,1,0,0,3),(1,4,3,0,0,3)}$,

$p(5n+4)_{(3,1,1,0,0,4),(3,3,1,0,0,4),(4,4,3_8),(1,1,0,1,3_8),(2,3,0,1,3_8),(3,4,0,4,3_8),(2,4,0,1,4_8),(3,0,0,4,4_8)}$.

11.3. **Some examples of the form** $p(7n+B)_{\mathbf{e}} \equiv 0 \pmod 7$**.**

$p(7n+2)_{(4),(2,2),(1,5),(3,5),(6,1,0,3),(3,5,0,3),(4,0,0,4),(1,5,0,4),(5,1,0,5),(6,1,0,6)}$,

$p(7n+3)_{(6),(5,1),(2,2),(1,4,0,1),(2,2,0,2),(5,1,0,4),(5,1,0,5),(2,2,0,6)}$,

$p(7n+4)_{(4),(6),(1,2),(2,2),(4,4),(1,5),(1,4,0,1),(3,6,0,1),(3,2,0,3),(3,5,0,3)}$,

$p(7n+4)_{(4,1,0,5),(5,1,0,5),(6,1,0,6),(6,5,0,6)}$,

$p(7n+5)_{(1),(4),(5,1),(1,5),(5,5),(2,2,0,2),(2,6,0,2),(4,3,0,3),(3,5,0,3),(3,1,0,6),(6,1,0,6),(6,3,0,6)}$,

$p(7n+6)_{(4),(6),(2,1),(5,1),(2,2),(5,3),(1,4,0,1),(4,5,0,1),(2,2,0,2),(6,2,0,2),(2,4,0,2)}$,

$p(7n+6)_{(3,5,0,3),(1,6,0,3),(3,3,0,4),(5,0,0,5),(5,1,0,5)}$.

11.4. **Some examples of the form** $p(11n+B)_{\mathbf{e}} \equiv 0 \pmod{11}$**.**

$p(11n+2)_{(8),(9,1),(2,6),(1,9),(3,2,0,2),(2,6,0,2),(6,6,0,2),(3,2,0,3),(5,2,0,7),(9,1,0,9),(8,0,0,10),(10,1,0,10)}$,

$p(11n+3)_{(10),(4,1),(6,2),(2,6),(1,8,0,1),(5,9,0,4),(5,9,0,5),(7,2,0,7),(9,1,0,9),(6,2,0,10)}$,

$p(11n+4)_{(8),(2,3),(2,6),(8,9,0,1),(3,2,0,3),(3,0,0,4),(9,2,0,7),(9,1,0,9),(2,7,0,9),(9,9,0,9)}$,

$p(11n+5)_{(8),(6,2),(7,7),(1,9),(6,0,0,1),(3,2,0,3),(10,5,0,3),(1,2,0,4),(4,6,0,4),(5,9,0,5),(5,7,0,6),(10,1,0,10)}$,

$p(11n+6)_{(1),(10),(9,1),(6,2),(2,5),(2,6),(9,7),(4,2,0,1),(1,8,0,1),(2,1,0,2),(2,6,0,2),(8,7,0,3)}$,

$p(11n+6)_{(5,9,0,5),(3,9,0,6),(7,3,0,8),(9,0,0,9),(9,1,0,9),(10,3,0,10)}$,

$p(11n+7)_{(3),(8),(9,1),(2,6),(1,9),(7,9),(4,1,0,2),(2,6,0,2),(3,2,0,3),(6,9,0,3),(4,8,0,4),(10,3,0,5),(1,0,0,6)}$,

$p(11n+7)_{(8,2,0,6),(5,5,0,8),(8,9,0,8),(9,1,0,9),(7,2,0,9),(3,4,0,9),(10,1,0,10)}$,

$p(11n+8)_{(5),(8),(10),(9,1),(6,2),(8,4),(1,9),(9,9),(1,8,0,1),(2,3,0,2),(2,6,0,2),(4,0,0,3)}$,

$p(11n+8)_{(3,2,0,3),(3,6,0,3),(9,1,0,4),(8,5,0,5),(5,9,0,5),(10,2,0,6)}$,

$p(11n+8)_{(6,4,0,6),(2,6,0,6),(1,10,0,7),(3,7,0,8),(7,1,0,10),(10,1,0,10)}$,

$p(11n+9)_{(7),(8),(10),(3,2),(6,2),(2,6),(6,6),(1,9),(1,8,0,1),(9,8,0,1),(2,2,0,3),(3,2,0,3),(9,4,0,3),(4,10,0,4)}$,

$p(11n+9)_{(5,2,0,5),(6,7,0,5),(2,9,0,5),(5,9,0,5),(10,1,0,7),(8,0,0,8),(1,9,0,8),(9,1,0,9),(10,1,0,10),(5,3,0,10)}$,

$p(11n+10)_{(10),(9,1),(5,2),(6,2),(1,4),(4,8),(1,8,0,1),(7,10,0,1),(2,6,0,2),(9,7,0,2)}$,

$p(11n+10)_{(5,9,0,2),(2,1,0,4),(7,2,0,5),(4,9,0,5),(5,9,0,5),(6,6,0,6),(8,3,0,7)}$

$p(11n+10)_{(7,9,0,7),(10,0,0,8),(6,2,0,8),(4,1,0,9),(1,8,0,9),(3,5,0,10),(10,7,0,10)}$.

11.5. **Some examples of the form $p(13n+B)_{\mathbf{e}} \equiv 0 \pmod{13}$.**

$p(13n+2)_{(11,1),(2,8),(2,8,0,2),(8,8,0,6),(11,1,0,11),(5,6,0,11)}$,

$p(13n+3)_{(12),(8,2),(1,10,0,1),(5,0,0,5),(10,6,0,6),(3,10,0,9)}$,

$p(13n+4)_{(10),(12),(8,2),(2,8),(1,11),(2,6,0,1),(1,10,0,1),(3,4,0,3),\ldots}$,

$p(13n+5)_{(10),(11,1),(1,11),(6,1,0,2),(2,8,0,2),(3,4,0,3),\ldots}$,

$p(13n+6)_{(12),(11,1),(8,2),(2,8),(1,10,0,1),(2,8,0,2),(8,12,0,2),\ldots}$,

$p(13n+7)_{(10),(11,1),(8,2),(6,3),(1,11),(2,8,0,2),(10,10,0,2),(3,4,0,3),\ldots}$,

$p(13n+8)_{(10),(12),(8,1),(11,1),(8,2),(1,10,0,1),(2,8,0,2),(12,8,0,2),(8,10,0,2),\ldots}$,

$p(13n+9)_{(10),(2,8),(1,11),(10,12),(12,9,0,1),(1,6,0,2),(10,8,0,2),\ldots}$,

$p(13n+10)_{(12),(8,2),(2,8),(12,10),(8,12),(1,7,0,1),(1,10,0,1),(5,1,0,3),\ldots}$,

$p(13n+11)_{(10),(12),(11,1),(8,2),(1,8),(10,10),(1,11),(3,5,0,1),(2,8,0,2),\ldots}$,

$p(13n+12)_{(10),(3,6),(2,8),(12,8),(1,11),(5,3,0,1),(1,5,0,1),(7,0,0,2),\ldots}$.

References

[1] G. Andrews, R. Askey, and R. Roy, *Special functions*, Cambridge University Press (1999).

[2] A.O.L. Atkin, *Ramanujan congruences for $p_{-k}(n)$*, Canad. J. Math **21** (1968), no. 256, 67–78.

[3] R. Bacher and P. de la Harpe, *Conjugacy growth series of some infinitely generated groups*, arxiv:1603.07943 [math.GR] (2016).

[4] B. Berndt, *Number theory in the spirit of Ramanujan*, AMS Student Mathematical Library **34** (2000).

[5] A. Bjorner and F. Brenti, *Combinatorics of coxeter groups*, Springer (2005).

[6] K. Bringmann and K. Mahlburg, *Asymptotic formulas for stacks and unimodal sequences*, Journal of Combinatorial Theory **A** (2014), no. 126, 194–215.

[7] J.P. Buhler, *Elliptic curves, modular forms, and applications*, IAS/Park City Mathematics Series **9** (2001), 7–81.

[8] E. Heine, *"Uber die z"ahler und nenner der n"aherungswerthe von kettenbr"uchen*, J. Reine Angew. Math **57** (1860), 231–247.

[9] T. Honda and I. Miyawaki, *Zeta-functions of elliptic curves of 2-power conductor*, Journal of the Mathematical Society of Japan **26** (1974), no. 2, 362–373.

[10] A.E. Ingham, *A Tauberian theorem for partitions*, Annals of Mathematics **42** (1941), no. 5, 1075–1090.

[11] M. Kaneko and D. Zagier, *Supersingular j-invariants, hypergeometric series, and atkin's orthogonal polynomials*, Proceedings of the Conference on Computational Aspects of Number Theory" (1997), 97–126.

[12] N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag (1984).

[13] K. Ono, *The web of modularity: Arithmetic of the coefficients of modular forms and q-series*, AMS and CBMS, Providence, RI **102** (2004).

[14] A. Silverberg, *Introduction to elliptic curves*, IAS/Park City Mathematics Series **XX** (2009), no. XXXX.

[15] J.H. Silverman, *The arithmetic of elliptic curves*, Springer (2009).

[16] J.H. Silverman and J.T. Tate, *Rational points on elliptic curves*, Springer (2009).

[17] S. Treneer, *Congruences for the coefficients of weakly holomorphic modular forms*, Proc. London Math. Soc. **93** (2006), no. 2, 304–324.

[18] G.N. Watson, *Ramanujan's Vermutung über Zerfallungsanzahlen*, J. Reine Angew. Math. **179** (1938), 97–128.