Utrecht University

Faculty of Science

Department of Mathematics

Zeros of Modular Forms

Master Thesis

Author:
Berend Ringeling

Supervisor:
Prof. Dr. G.L.M. Cornelissen

Second reader:
Dr. D. Schindler

July 29, 2019

Abstract

For p a prime larger than 7, the Eisenstein series of weight $p-1$ has some remarkable congruence properties modulo p, implying for example that the j-invariants of its zeros (which are known to be real algebraic numbers in the interval $[0, 1728]$), are all modulo p at most quadratic over the field with p elements, are congruent modulo p to the zeros of certain truncated hypergeometric series. In my thesis, I introduce the "theta modular form" of weight k, defined as the unique modular form of that weight for which the first $\dim(M_k)$ Fourier coefficients are identical to those of the Jacobi theta series. Theta modular form modulo p relate to the average weight enumerators in coding theory. I show that theta modular forms of weight $(p+1)/2$ behave in many ways like Eisenstein series: the j-invariants of their zeros all belong to the interval $[0, 1728]$, are modulo p all in the ground field with p elements, and are congruent modulo p to the zeros of a truncated hypergeometric function (with parameters halved compared to the Eisenstein series).

Notation

B_k	The rational number defined by the relation $\frac{t}{\exp(t)-1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n$.
$\lfloor r \rfloor$	The largest integer n such that $n \leq r$.
$\mathbb{H}$	The complex upper half plane $\{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$.
$\mathbb{N}$	The set $\{1, 2, ...\}$ of natural numbers.
$\mathrm{ord}_z(f)$	The order of a meromorphic function f at the point z.
ρ	The complex number $e^{2\pi i/3}$.
$\mathrm{SL}_2(\mathbb{Z})$	The group of matrices $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$.

Contents

1 Introduction

1.1 Background

"Modular forms are everywhere"[1]. They are highly symmetrical functions $f : \mathbb{H} \to \mathbb{C}$ and play a central role in number theory, algebraic geometry, combinatorics, etc. This symmetry implies that any modular form $f(z)$ can be written as a Fourier series

$$f(z) = a_0 + a_1 q + a_2 q^2 + ..., \tag{1}$$

where $q = e^{2\pi i z}$. The Fourier coefficients a_i often contain a lot of number theoretical information. For example, modular forms can be used to find the number of representations of an integer as a sum of squares. Modular forms also turn up in physics, see [43]. They occur in topics like string theory, quantum mechanics, statistical physics and the theory of black holes.

One of the most important examples of modular forms are the *Eisenstein series of weight* k:

$$E_k(z) := \frac{1}{2} \sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1}} (cz+d)^{-k}, \tag{2}$$

for every even integer $k \geq 4$.

In this thesis, we will consider the *zeros* and *congruences* of modular forms.

The study of *zeros of modular forms* seems to be initiated by Hardy and Ramanujan in their paper [20] in 1919, in which they considered inverses of modular forms and needed to know the location of the poles of these functions.
The study of zeros of modular forms is separated into two classes: the *Eisenstein series* and the *cuspidal Hecke eigenforms*.

The study of the *zeros of Eisenstein series* was started by K. Wohlfahrt [44] in 1963. He computed the zeros of Eisenstein series of low weight k ($k \leq 24$) and showed that for these weights, all the zeros lie on the unit circle $\{e^{i\theta} \mid \theta \in [\pi/2, 2\pi/3]\}$ inside the fundamental domain. In [44], the author explicitly computes the corresponding modular polynomial and shows that the zeros of this polynomial all lie in a certain bounded interval. In 1969, R.A. Rankin [34] showed additionally that for $28 \leq k \leq 38$, except $k = 36$, the zeros of the Eisenstein series all lie on the unit circle, using a method very different from [44]. Rankin showed that for certain weights, $k \equiv 0 \pmod 4$, the v-th power sums of the j-invariants of the zeros of E_k equal:

$$(k/12) \cdot g_v + o(1),$$

as k increases, for a certain value g_v independent of k.

Rankin conjectured that for every even $k \geq 4$, the zeros of the Eisenstein series lie on the unit circle. Rankin tried to disprove the conjecture by showing that a certain Hankel determinant corresponding to the Eisenstein series is negative. However, in 2018 it was shown, by explicitly computing it, that this determinant is strictly positive, see [19].
In 1970, an elementary proof was given by H.P.F. Swinnerton-Dyer and F.K.C. Rankin[2][33] showing that for even $k \geq 4$, the zeros of the Eisenstein series lie on the unit circle. For the proof, Swinnerton-Dyer and Rankin considered the real valued function:

$$F_k(\theta) = e^{ik\theta/2} E_k(e^{i\theta}),$$

[1] This is the title of Don Zagier's 65th birthday conference [28].

[2] The daughter of R.A. Rankin. Swinnerton-Dyer had asked Rankin's daughter to help, apparrently in order to tease her father.

and showed that on $[\pi/2, 2\pi/3]$ the difference $R_k(\theta) := |F_k(\theta) - 2\cos(k\theta/2)|$ is strictly smaller than 2, and this gives a way of finding a lower bound for the number of zeros of E_k. Now the geometry of the fundamental region implies that the number of zeros of E_k on the unit circle has a certain upper bound, allowing them to conclude that all the zeros of E_k lie on the unit circle. The method of Swinnerton-Dyer and Rankin can be used to prove results on the zeros of different kinds of modular forms, even for congruence subgroups, see [16].

The method of Swinnerton-Dyer and Rankin applies for example to certain holomorphic weakly modular forms meromorphic at $i\infty$: Writing $k \in \mathbb{Z}$ as $k = 12\ell + k'$ for $k' = 0, 4, 6, 8, 10, 14$ and $\ell \in \mathbb{Z}$, it was shown by W. Duke and P. Jenkins [13] that the forms:

$$f_{k,m} = q^{-m} + \mathcal{O}(q^{\ell+1})$$

also have all their zeros in the fundamental domain on the unit circle if $m \geq |\ell| - \ell$. However, there seems to be no unifying method of proof.

For *cuspidal eigenforms*, the behaviour of the zeros is very different from the zeros of the Eisenstein series. The zeros of these forms are in fact equidistributed with respect to the hyperbolic measure in the fundamental domain, see [35].

Many number theoretical results can deduced using *congruences of modular forms*. For example, we have the surprising congruence as a power series in q established by Ramanujan [32]:

$$q\prod_{n=1}^{\infty}(1-q^n)^{24} \equiv \sum_{n=1}^{\infty}\sigma_{11}(n)q^n \pmod{691}.$$

It is a classical result by Deligne (for a proof see [22]) that the modular polynomial

$$\varphi_k(j) = \prod_{\substack{E_k(z)=0 \\ z\neq i,\rho}} (j - j(z)), \tag{3}$$

corresponding to the Eisenstein series of weight k, factors as a product of quadratic and linear factors modulo p, if $k = p - 1$. These factors are the j-invariants of supersingular elliptic curves over finite fields. In [22], it was shown that these polynomials are congruent to certain truncated hypergeometric functions.

1.2 New Results in This Thesis

In Chapter 3, we apply the methods of Rankin's original paper [34] to a different type of modular form Th_k, called the "Theta modular form" defined in [30]. These modular forms occur in coding theory as "average weight enumerators". In [30], it is conjectured that the zeros of all these forms lie on the unit circle. We show that power sums of the j-invariants of the zeros of these modular forms are:

$$(k/12) \cdot h_v + o(1),$$

as k increases for weights $k \equiv 0 \pmod 4$, for a certain constant value h_v.

We use the theory of orthogonal polynomials and hypergeometric functions to prove that the associated Hankel determinant:

$$\widetilde{\Delta}_n := \begin{vmatrix} h_0 & h_1 & h_2 & \dots & h_n \\ h_1 & h_2 & h_3 & \dots & h_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_n & h_{n+1} & h_{n+2} & \dots & h_{2n} \end{vmatrix}.$$

is strictly positive for all $n \in \mathbb{N}$ and has the factorization property:

Theorem A (Theorem 4.29)**.** *For all $n > 1$*

$$\widetilde{\Delta}_n = 2^{4n^2+5n} \cdot 3^{n^2} \cdot 11^n \cdot 23^n \cdot \prod_{r=2}^{n} \Big(\frac{(24r-29)(24r-17)(24r-1)(24r-13)}{(8r-5)^2(8r-9)(8r-1)} \Big)^{n-r+1}. \tag{4}$$

Further, we look at congruences of the modular polynomials R_k corresponding to these "Theta modular forms". As with the polynomials φ_k, we show that the polynomials R_k are congruent to certain truncated hypergeometric functions (lemma 4.37). Using this, we find the remarkable factorisation property:

Theorem B (Theorem 4.33)**.** *If $p \geq 7$ is a prime number with $p + 1 \equiv 0, 8 \pmod{24}$, then for $k = \frac{p+1}{2}$, R_k factors modulo p as a product of distinct linear factors.*

We conjecture that this also holds if $k \equiv 6, 10 \pmod{12}$. In Chapter 4, we apply the methods of Duke and Jenkins [13] to give a bound for the unique modular forms of the form:

$$f_{k,m} = q^{-m} + \mathcal{O}(q^{d_k}), \tag{5}$$

$m \leq 0$, where d_k is the dimension of the space of modular forms of weight k.

Lemma C (Lemma 5.3)**.** *For $m \leq 0$, let $f_{k,m}$ be the unique form defined by* (5)*. Then for $\theta \in [\pi/2, 2\pi/3]$ we have:*

$$|f_{k,m}(e^{i\theta})| \leq 3.985 \cdot e^{2\pi m 0.65}. \tag{6}$$

This lemma implies that for a certain class of modular forms, the zeros all lie on the unit circle.

Theorem D (Theorem 5.6)**.** *Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a formal power series with real coefficients and $a_0 = 1$. Let $\widetilde{f}$ be the unique modular of weight k such that*

$$\widetilde{f} = f + \mathcal{O}(q^{d_k}).$$

Let $R = 1.985$ and suppose that

$$\sum_{n=1}^{d_k - 1} |a_n| \cdot e^{-2\pi n 0.65} < \frac{2-R}{2+R}. \tag{7}$$

Then all the zeros of $\widetilde{f}$ in the fundamental domain lie on the arc $\{e^{i\theta} \mid \theta \in [\pi/2, 2\pi/3]\}$.

We use a stronger version of Theorem D, (see Theorem 5.14) to prove:

Corollary E (Corollary 5.15)**.** *Consider the theta series $\theta_0 = 1 + 2 \cdot \sum_{n=1}^{\infty} q^{n^2}$. Let Θ_k be the unique modular form such that $\Theta_k = \theta_0 + O(q^{d_k})$. Then all the zeros of Θ_k in the fundamental domain $\mathcal{F}$ lie on the circular arc $\{e^{i\alpha} \mid \alpha \in [\pi/2, 2\pi/3]\}$.*

2 Classical Theory of Modular Forms

In this section we recall the basic definitions and properties of modular forms needed for the following chapters. For proofs we refer to the literature, see for example [12] or [5].

There is a natural action of the group $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$.

Proposition 2.1. *The map*

$$\mathrm{SL}_2(\mathbb{Z}) \times \mathbb{H} \to \mathbb{H}$$
$$\left(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) \mapsto \gamma z := \frac{az+b}{cz+d}$$

defines an action of $\mathrm{SL}_2(\mathbb{Z})$ *on* $\mathbb{H}$.

We denote by $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ the set of all orbits under this action.

Remark 2.2. In fact, the quotient space of orbits $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ has the structure of a Riemann surface that can be compactified, for details see [12, §2].

We will start by defining modular forms for the group $\mathrm{SL}_2(\mathbb{Z})$:

Definition 2.3 (Classical Modular Form)**.** Let $f : \mathbb{H} \to \mathbb{C}$ and k a non-negative integer, f is called a *modular form of weight* k if f satisfies the following three properties:

1. f is holomorphic on $\mathbb{H}$
2. for all $z \in \mathbb{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, we have $f(\gamma z) = (cz+d)^k f(z)$. (*$f$ is weakly modular of weight k*)
3. f is holomorphic as $z \to i\infty$

Remark 2.4. The third part of the definition can be made more precise. For $z \in \mathbb{H}$, write $q = e^{2\pi i z}$. The first and the second part of the definition imply that f can be written in the form

$$f = \widetilde{f}(q), \tag{8}$$

where $\widetilde{f}$ is a holomorphic function on the punctured unit disk $\{q \in \mathbb{C} \mid 0 < |q| < 1\}$. We say that f *is holomorphic as* $z \to i\infty$ if $\widetilde{f}$ can be extended to be holomorphic on the whole unit disk $\{q \in \mathbb{C} \mid |q| < 1\}$, for details see [12, p. 4].

As the group $\mathrm{SL}_2(\mathbb{Z})$ is generated by

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

condition 2 of definition 2.3 can be reformulated as

$$f(z+1) = f(z) \qquad \text{and} \qquad f\left(-\frac{1}{z}\right) = z^k f(z) \quad \text{for all } z \in \mathbb{H}. \tag{9}$$

The $\mathbb{C}$-vector space of modular forms of weight $k \geq 0$ will be denoted by M_k. This vector space turns out to have finite dimension. As $f(-1/(-z)) = (-1)^k f(z)$ for any $f \in M_k$, it is clear that there are no non-zero modular forms of odd dimension. We have the following well known result for the dimension of M_k.

Proposition 2.5 (Dimension of M_k)**.** *If k is odd or $k = 0$, then $M_k = \{0\}$. If k is even, then*

$$\dim(M_k) = \begin{cases} \lfloor \frac{k}{12} \rfloor & \text{if } k \equiv 2 \pmod{12}, \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{if } k \not\equiv 2 \pmod{12}. \end{cases} \tag{10}$$

Proof. See [5, Theorem 2.11]. □

The following proposition gives us a way to count the number of zeros/poles of a meromorphic weakly modular form, meromorphic at $i\infty$.

Proposition 2.6 (Valence Formula)**.** *Let f be a non-zero meromorphic weakly modular form of weight k on $\mathbb{H}$. Then we have:*

$$\mathrm{ord}_{i\infty}(f) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \sum_{[w] \in SL_2(\mathbb{Z})\backslash\mathbb{H} - \{[i],[\rho]\}} \mathrm{ord}_w(f) = \frac{k}{12} \tag{11}$$

Remark 2.7. Here $\mathrm{ord}_{i\infty}(f) := \mathrm{ord}_{q=0}(\widetilde{f})$, where $\widetilde{f}$ is the Fourier-expansion of f as in (8). As the factor $(cz + d)^k$ in part 2 of definition 2.3 has no zeros/poles on $\mathbb{H}$, the order of a meromorphic weakly modular form at a point depends only on the $\mathrm{SL}_2(\mathbb{Z})$-orbit of that point.

Definition 2.8 (Fundamental Domain)**.** Let $\mathcal{F} \subset \mathbb{H} \cup \{i\infty\}$ be the set

$$\begin{aligned} \mathcal{F} :=& \{z \in \mathbb{H} \mid |z| > 1, -1/2 < \mathrm{Re}(z) < 1/2\} \\ & \cup \{z \in \mathbb{H} \mid |z| \geq 1, \mathrm{Re}(z) = -1/2\} \cup \{z \in \mathbb{H} \mid |z| = 1, -1/2 < \mathrm{Re}(z) \leq 0\} \cup \{i\infty\}. \end{aligned}$$

Then we call $\mathcal{F}$ the *fundamental domain.*

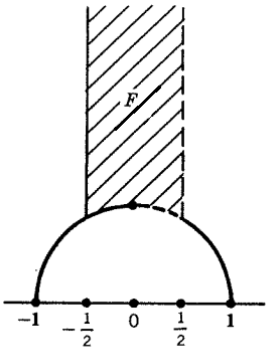

Figure 1: The striped region is the fundamental domain $\mathcal{F}$, the picture is taken from [3].

Proposition 2.9. *Every element $z \in \mathbb{H}$ is in the $\mathrm{SL}_2(\mathbb{Z})$-orbit of a unique element in $\mathcal{F}$.*

Proof. See [5, p. 11]. □

Remark 2.10. Using the previous remark 2.7, we see that it suffices to find zeros/poles of a modular form in the fundamental region $\mathcal{F}$.

2.1 Examples of Modular Forms

Let $k \geq 4$ be an even integer, then for $z \in \mathbb{H}$ we define the *Eisenstein series of weight* k as

$$G_k(z) = \sum_{\substack{c,d \in \mathbb{Z} \\ (c,d) \neq (0,0)}} \frac{1}{(cz+d)^k}. \tag{12}$$

This series is absolutely convergent (see for example [5, Proposition 2.1.]) and is a modular form of weight k. Now define

$$\sigma_t(n) = \sum_{\substack{d|n \\ d>0}} d^t,$$

and for $k \geq 0$, let B_k be the k-th Bernoulli number. The q-expansion of this modular form equals

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

for a proof, see [5, p. 19]. It is useful to normalize G_k such that the constant term in the q-expansion equals 1. So we define

$$E_k(z) = -\frac{k!}{(2\pi i)^k B_k} G_k, \tag{13}$$

$$= \frac{1}{2} \sum_{\substack{c,d \in \mathbb{Z} \\ \gcd(c,d)=1}} \frac{1}{(cz+d)^k}. \tag{14}$$

For the last equality see [12, §4.1]. The Fourier expansion of E_k is given by

$$E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n. \tag{15}$$

It will also be useful to the define the Eisenstein series of weight 2, E_2. Although the series in (12) fails to converge if $k = 2$, it still makes sense to define E_2 from the q-expansion in (15). E_2 is not a modular form, although it is a *quasimodular form*.

Example 2.11. By the valence formula 2.6 we have that E_4 only has a zero in (the $\mathrm{SL}_2(\mathbb{Z})$-orbit of) $z = \rho$. One can also explicitly see that

$$E_4(\rho) = E_4\left(-1 - \frac{1}{\rho}\right) = \rho^4 E_4(\rho),$$

so that $E_4(\rho) = 0$.

Now define $\Delta : \mathbb{H} \to \mathbb{C}$ as

$$\Delta = \frac{E_4^3 - E_6^2}{1728} \tag{16}$$

This is a modular form of weight 12, having the Fourier expansion

$$\Delta(z) = q - 24q^2 + 252q^3 + \mathcal{O}(q^4).$$

Modular forms with a q-expansion having constant term equal to zero are called *cusp forms* (equivalently, modular forms having a zero at $i\infty$).

We can also write down an explicit basis for the $\mathbb{C}$-vector space of modular forms M_k.

Lemma 2.12. *Let $k \geq 4$ be an even integer. Write k uniquely as $k = 12n_k + 6a_k + 4b_k$, where n_k is a non-negative integer, $a_k \in \{0, 1\}$ and $b_k \in \{0, 1, 2\}$. Then a basis of M_k is given by $\mathcal{B} = \{E_4^{b_k+3i} E_6^{a_k} \Delta^{n_k-i} \mid \text{ for } 0 \leq i \leq n_k\}$.*

Proof. Looking at the q-expansions of the elements in $\mathcal{B}$, we note that all the elements are linearly independent. As there are n_k+1 elements in $\mathcal{B}$, this must give a basis for M_k using the dimension formula, see proposition 2.5. □

One can check that the only modular forms of weight 0 are the constant functions, see [5, p. 30]. It is therefore useful to relax the notion of modular forms of weight 0. We call a *meromorphic* function $g : \mathbb{H} \to \mathbb{C}$ a *modular function* if it is weakly modular of weight 0 and *meromorphic* at $i\infty$, i.e. the q-expansion of g is a Laurent series. An example of such a function is the modular j-invariant:

$$j(z) = \frac{E_4^3}{\Delta}.$$

$$j(z) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \mathcal{O}(q^3).$$

Proposition 2.13. *The set of modular functions F form a field, and $F = \mathbb{C}(j)$, where j is the modular j-invariant.*

Proof. See [2, Theorem 2.8]. □

Proposition 2.14. *The modular j-invariant $j : SL_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$ defines a bijection.*

Proof sketch. For any $c \in \mathbb{C}$, the modular function $j(z) - c$ has a unique zero, by the valence formula (11). □

Define $\mathcal{R} \subset \mathcal{F}$ as

$$\mathcal{R} = \mathcal{F} \cap (\{z \in \mathbb{H} \mid \mathrm{Re}(z) = -1/2\} \cup \{z \in \mathbb{H} \mid \mathrm{Re}(z) = 0\} \cup \{e^{i\theta} \mid \theta \in (\pi/2, 2\pi/3)\}).$$

Proposition 2.15. *Let $z \in \mathcal{F}$, then $j(z) \in \mathbb{R}$ if and only if $z \in \mathcal{R}$.*

Proof. First of all, if $z \in \{z \in \mathbb{H} \mid \mathrm{Re}(z) = -1/2\} \cup \{z \in \mathbb{H} \mid \mathrm{Re}(z) = 0\}$, then $e^{2\pi i z} \in \mathbb{R}$. As the Fourier coefficients of the Eisenstein series E_k are all real, the Fourier coefficients of j are also real. We conclude that $j(z) \in \mathbb{R}$. Now assume that $z \in \{e^{i\theta} \mid \theta \in (\pi/2, 2\pi/3)\}$, again as the Fourier coefficients are all real, we have that $\overline{j(z)} = j(-\overline{z})$. As z lies on the unit circle, we have (using modularity)

$$j(-\overline{z}) = j(-1/z) = j(z).$$

Hence $j(z) \in \mathbb{R}$ if $z \in \mathcal{R}$.

For the converse we observe from the q-expansion of j that

$$\lim_{t\to\infty} j(-1/2 + it) = -\infty,$$
$$\lim_{t\to\infty} j(it) = \infty.$$

Now $j_{|\mathcal{R}} : \mathcal{R} \to \mathbb{R}$ defines a continuous map on a connected set $\mathcal{R} \subset \mathbb{C}$, so that $j(\mathcal{R}) \subset \mathbb{R}$ is connected. We see that $j(\mathcal{R})$ is an interval, and this interval must be $(-\infty, \infty) = \mathbb{R}$. □

2.2 Modular Forms for Congruence Subgroups

Modular forms can also be defined for certain subgroups of $\mathrm{SL}_2(\mathbb{Z})$, the congruence subgroups. Let $N \in \mathbb{N}$ and let

$$\Gamma(N) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod N\right\}.$$

$\Gamma(N)$ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and is called the *principal congruence subgroup* of level N.

Definition 2.16. A *congruence subgroup* is a subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{N}$. The minimal N is called the *level of the subgroup* Γ.

Example 2.17. In practice we will only need the following two types of congruence subgroups:

$$\Gamma_0(N) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N\right\},$$
$$\Gamma_1(N) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N\right\}.$$

Note that if $N = 1$ both these groups coincide with $\mathrm{SL}_2(\mathbb{Z})$.

Definition 2.18. A holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is a *modular form of weight k for a congruence subgroup* Γ if f is weakly modular of weight k for the subgroup Γ and holomorphic at the cusps of Γ, for more details see [5, Section 3.3].

2.3 The Theta and Eta Function

We will give some basic examples of modular forms on congruence subgroups.

Definition 2.19. For $\tau \in \mathbb{H}$ define

$$\theta_0(\tau) := 1 + 2\sum_{n=1}^{\infty} q^{n^2} \quad (q = e^{2\pi i \tau}),$$

θ_0 is called the *Jacobi theta function*. θ_0 satisfies the transformation

$$\theta_0\left(\frac{z}{4z+1}\right) = \sqrt{4z+1}\theta_0(z), \tag{17}$$

see [12, p. 12], where we take the principal branch of the square root. As the congruence subgroup $\Gamma_1(4)$ is generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}$, see [5, Example 3.9], θ_0^2 is a modular form of weight 1 for $\Gamma_1(4)$.

Definition 2.20. For $\tau \in \mathbb{H}$ define the *Dedekind eta function*

$$\eta(\tau) = e^{\pi i \tau/12} \prod_{n=1}^{\infty} (1 - q^n).$$

The function η is not a modular form in the sense of definition 2.3, but it is a modular form with a "multiplier system" as:

$$\eta(\tau + 1) = e^{\pi i/12}\eta(\tau) \tag{18}$$

and

$$\eta(-\tfrac{1}{\tau}) = \sqrt{-i\tau}\eta(\tau) \qquad \text{(see [39])}, \tag{19}$$

where the square root is taken to have a positive real part. Note that η^{24} *is* a modular form of weight 12 for the full modular group $\mathrm{SL}_2(\mathbb{Z})$. As the space of weight 12 cusp forms is 1-dimensional, we find the product expansion for Δ,

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}. \tag{20}$$

This product formula can be used to write the Eisenstein series E_2 as the logarithmic derivative of Δ. Comparing the coefficients in the q-expansion of E_2, we see that

$$E_2 = \frac{\Delta'}{\Delta}, \tag{21}$$

where the derivative is with respect to $1/(2\pi i)\tau$. Using the modularity of Δ, we find the transformation rule for E_2:

$$E_2\left(\frac{az+b}{cz+d}\right) = \frac{6c(cz+d)}{\pi i} + (cz+d)^2 E_2, \tag{22}$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

3 Eisenstein Series: Zeros and Congruences

In this section we will study properties of Eisenstein series. First we discuss the zeros of Eisenstein series. In [33] H.P.F. Swinnerton-Dyer and Rankin showed that the zeros of the Eisenstein series lie on the unit circle in the fundamental domain $\mathcal{F}$. Their proof was very elementary and short, only two pages long. We will present their proof. Further, we will discuss R.A. Rankin's original argument [34].

Next, we will discuss certain congruences related to the Eisenstein series. We will follow the argument of [22], showing that the modular polynomial corresponding to the Eisenstein series of weight $p-1$ for p prime, factors as a product of quadratic and linear factors modulo p.

3.1 Zeros of Classical Eisenstein Series: The Classical Proof

We will now show that the zeros of the classical Eisenstein series lie on the circular arc of the fundamental domain $\mathcal{F}$, following the argument of Swinnerton-Dyer and Rankin in [33]. Showing that the zeros lie on this arc will be equivalent to showing that the j-invariants of all the zeros are real and lie in the interval $[0, 1728]$.

We first start with an easy lemma.

Lemma 3.1. *Suppose f is a modular form of weight k with real Fourier coefficients. Then*

$$g(e^{i\theta}) := e^{ik\theta/2} f(e^{i\theta})$$

is real for $\theta \in [\pi/2, 2\pi/3]$.

Proof. It suffices to show that $\overline{g(e^{i\theta})} = g(e^{i\theta})$. Write

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$$

and let $z := e^{i\theta}$. As all the a_n are real,

$$\begin{aligned}
\overline{g(z)} &= e^{-ik\theta/2} f(-\bar{z}) \\
&= e^{-ik\theta/2} f(-1/z) \\
&= e^{-ik\theta/2} z^k f(z) \qquad \text{(using the modularity of } f\text{)} \\
&= g(z).
\end{aligned}$$

□

Theorem 3.2 (Swinnerton-Dyer and Rankin [33])**.** *Let E_k be the Eisenstein series of weight $k \geq 4$. Write k in a unique way as $k = 12n_k + 6a_k + 4b_k$, $n_k \in \mathbb{Z}_{\geq 0}, a_k \in \{0, 1\}$ and $b_k \in \{0, 1, 2\}$. Then all the zeros $z \neq i, \rho$ in $\mathcal{F}$ of E_k are distinct and lie on the arc $\{e^{i\theta} |\ \theta \in (\pi/2, 2\pi/3)\}$. Furthermore,* $\mathrm{ord}_i(E_k(z)) = a_k$ *and* $\mathrm{ord}_\rho(E_k(z)) = b_k$.

Proof. We will follow the proof of [33]. We can assume $k > 10$, as the zeros of E_k for $k \leq 10$ are determined by the valence formula (11). Using the valence formula, we see that E_k has at most n_k zeros in $\mathcal{F} \setminus \{i, \rho\}$. Hence it will suffice to prove there are at least n_k zeros on the arc $\{e^{i\theta} | \theta \in (\pi/2, 2\pi/3)\}$. For this, we consider a scaled function

$$F_k(\theta) := e^{ik\theta/2} E_k(e^{i\theta})$$

on $(\pi/2, 2\pi/3)$ and compare the zeros of F_k with the zeros of $2\cos(k\theta/2)$. Note that the Fourier-coefficients of E_k are all real, so lemma 3.1 implies that $F_k(\theta)$ is real for $\theta \in (\pi/2, 2\pi/3)$. Using (14), we can write

$$F_k(\theta) = \frac{1}{2} \sum_{\substack{c,d\in\mathbb{Z} \\ \gcd(c,d)=1}} \frac{1}{(ce^{i\theta/2} + de^{-i\theta/2})^k}.$$

Now we can split this sum into two parts, a part where $c^2 + d^2 = 1$ and a part where $c^2 + d^2 > 1$, let $R_k(\theta)$ be the latter part. Hence we can write

$$F_k(\theta) = 2\cos(k\theta/2) + R_k(\theta).$$

The goal is to show that $|R_k(\theta)| < 2$ for all $\theta \in (\pi/2, 2\pi/3)$. Since $|R_k(\theta)| < 2$ implies that $F_k(4r\pi/k + 2\pi/k) < 0$ for all integers $r \in [\frac{k}{8} - \frac{1}{2}, \frac{k}{6} - \frac{1}{2}]$ and $F_k(4s\pi/k) > 0$ for all integers $s \in [\frac{k}{8}, \frac{k}{6}]$ it follows that $F_k(\theta)$ changes sign at least n_k times. Showing that F_k has at least n_k distinct zeros on $(\pi/2, 2\pi/3)$.
It remains to show that $|R_k(\theta)| < 2$. First of all we have that

$$|ce^{i\theta/2} + de^{-i\theta/2}|^2 = c^2 + d^2 + 2cd \cdot \cos(\theta),$$

and since $-\frac{1}{2} \leq \cos(\theta) \leq 0$, we have

$$c^2 + d^2 + 2cd \cdot \cos(\theta) \geq \frac{1}{2}(c^2 + d^2).$$

So that

$$|ce^{i\theta/2} + de^{-i\theta/2}|^{-k} \leq (\tfrac{1}{2}(c^2 + d^2))^{-k/2}. \tag{23}$$

We will give a upper bound for $R_k(\theta)$ by giving an upper bound for the sum with terms (c, d) with $c^2 + d^2 = N$ for $N > 1$. The number of terms with $c^2 + d^2 = N$ is bounded by $2(2\sqrt{N} + 1)$, as any c can be chosen in $\{-\lfloor\sqrt{N}\rfloor, ..., \lfloor\sqrt{N}\rfloor\}$ giving at most two choices for d. For $N \geq 5$ we have $2(2\sqrt{N} + 1) \leq 5\sqrt{N}$ so that

$$\frac{1}{2} \sum_{\substack{c,d\in\mathbb{Z} \\ c^2+d^2>5 \\ \gcd(c,d)=1}} \frac{1}{|ce^{i\theta/2} + de^{-i\theta/2}|^k} \leq \frac{1}{2} \sum_{N=10}^{\infty} 5\sqrt{N}(\tfrac{1}{2}N)^{-k/2}.$$

One can check that the terms in the right sum decrease monotonously as N increases, so that the sum can be bounded by an integral

$$\sum_{N=10}^{\infty} 5\sqrt{N}(\tfrac{1}{2}N)^{-k/2} \leq 5 \cdot \left(\tfrac{1}{2}\right)^{-k/2} \int_9^{\infty} x^{\frac{1}{2}(1-k)} dx = 270 \frac{1}{(k-3)(4.5)^{k/2}}.$$

Now the sum of terms with $c^2 + d^2 = 5$ is bounded by $2 \cdot (5/2)^{-k/2}$, using (23). For the terms where $c = d = \pm 1$ we have

$$|ce^{i\theta/2} + de^{-i\theta/2}|^2 = 2 + 2\cos(\theta) \geq 1.$$

Finally for the terms $c = \pm 1$ and $d = -c$ we have using (23)

$$|ce^{i\theta/2} + de^{-i\theta/2}|^2 = 2 - 2\cos(\theta) \geq 2.$$

We can now derive an upper bound for $R_k(\theta)$:

$$|R_k(\theta)| < 1 + \frac{1}{2^{k/2}} + 2 \cdot (2/5)^{k/2} + 135\frac{1}{(k-3)(4.5)^{k/2}}. \tag{24}$$

As this expression is decreasing in k, we can compute an upper bound taking $k = 12$ on the right of (24), which gives for $k \geq 12$:

$$|R_k(\theta)| < 1 + 0.015625 + 0.008192 + 0.00180641 < 2,$$

finishing the proof. □

Remark 3.3. From the proof of 3.2 it follows that if we divide the arc $A = \{e^{i\theta} |\ \theta \in (\pi/2, 2\pi/3)\}$ into n_k sub-arcs of equal length, any such sub-arc contains exactly one zero of E_k. Therefore, it follows that the set of zeros of E_k for $k = 4, 6, ...$ become *equidistributed* on A with respect to θ.

Example 3.4.

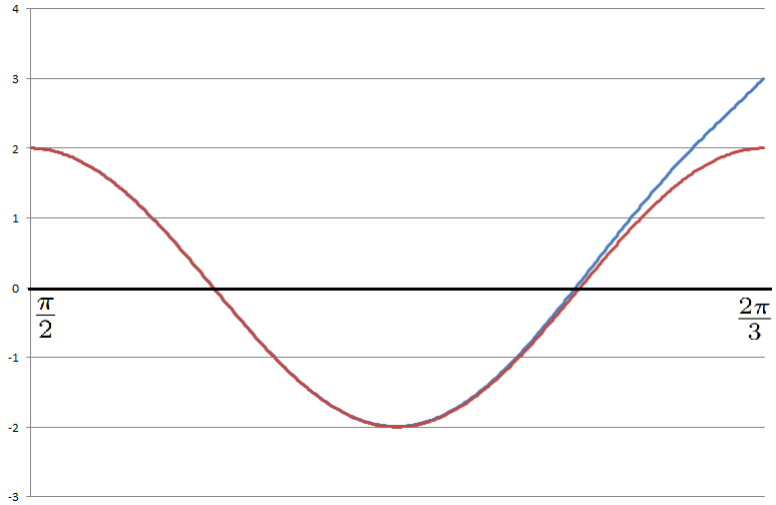

Figure 2: The graph of $e^{ik\theta/2}E_k(e^{i\theta})$ (blue) and $2\cos(k\theta/2)$ (red) for $k = 24$ on $(\pi/2, 2\pi/3)$.

Using proposition 2.15 we know that the j-invariant is real on the arc A. Since j is a bijection from the fundamental domain to $\mathbb{C}$, $S \subset \mathbb{C}$ is connected and we have $j(\rho) = 0$ and $j(i) = 1728$, we must have that $j(S) = [0, 1728]$. Hence we can rephrase the previous theorem.

Theorem 3.5. *For all zeros $z \in \mathcal{F}, z \neq i, \rho$ of E_k, we have that the $j(z)'s$ are real, distinct and $j(z) \in (0, 1728)$.*

Now consider the following polynomials, for $k \in \mathbb{Z}$ even and $k \geq 4$:

$$\varphi_k(X) = \prod_{\substack{z \in \mathbb{H}, E_k(z)=0 \\ j(z) \neq 0, 1728}} (X - j(z)).$$

A priori, this will be a *real* polynomial, but it will turn that it has rational coefficients. The degree of this polynomial is exactly n_k, with n_k as in the previous theorem.

Showing that the n_k zeros of E_k are on the arc $S = \{e^{i\theta} |\ \theta \in (\pi/2, 2\pi/3)\}$ is therefore equivalent to showing that the roots of the polynomials φ_k are all real and lie in the interval $(0, 1728)$.

Proposition 3.6. *Write k uniquely as $k = 12n_k + 6a_k + 4b_k$, where n_k is a non-negative integer, $a_k \in \{0, 1\}$ and $b_k \in \{0, 1, 2\}$. Then there exist a monic polynomial $P_k(X) \in \mathbb{Q}[X]$ of degree n_k such that*

$$E_k = P_k(j)\Delta^{n_k} E_4^{b_k} E_6^{a_k}.$$

Furthermore $P_k(X) = \varphi_k(X)$, so that $\varphi_k(X)$ has rational coefficients.

Proof. Using proposition 2.12, we can write E_k as a *rational* linear combination of elements $E_4^{b_k+3i} E_6^{a_k} \Delta^{n_k - i}$, where i is an integer $0 \leq i \leq n_k$. Dividing by $\Delta^{n_k} E_4^{b_k} E_6^{a_k}$ shows that

$$\frac{E_k}{\Delta^{n_k} E_4^{b_k} E_6^{a_k}}$$

is a polynomial with rational coefficients in the j-invariant of degree n_k. For any of the n_k zeros z of E_k with $j(z) \neq 0, 1728$, we must have that $P_k(j(z)) = 0$. As all these zeros are distinct and both polynomials P_k and φ_k are monic, we must have that $\varphi_k(X) = P_k(X)$. Hence $\varphi_k(X)$ has rational coefficients. □

Example 3.7 (Examples of polynomials φ_k)**.**

k	$\varphi_k(X)$
4	1
6	1
8	1
10	1
12	$X - \frac{432000}{691}$
14	1

k	$\varphi_k(X)$
16	$X - \frac{3456000}{3617}$
18	$X - \frac{9504000}{43867}$
20	$X - \frac{209520000}{174611}$
22	$X - \frac{35424000}{77683}$
24	$X^2 - \frac{340364160000}{236364091} X + \frac{30710845440000}{236364091}$
26	$X - \frac{457920000}{657931}$

Remark 3.8. From the Fourier expansion of E_k it is clear that the denominator of the coefficients of $\varphi_k(X)$ is given by the numerator of B_k/k.

We will use a recursion on the Eisenstein series to compute these polynomials. For this we define the well known *Weierstrass-$\wp$ function*. Define for a lattice $\Lambda \subset \mathbb{C}$ the *Weierstrass-$\wp$ function* as

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{w \in \Lambda - \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right), \tag{25}$$

defined for $z \in \mathbb{C} \backslash \Lambda$.

Proposition 3.9 ([12, Prop. 1.4.1.])**.** *For $\tau \in \mathbb{H}$, let $\Lambda_\tau = \mathbb{Z} \oplus \tau\mathbb{Z} \subset \mathbb{C}$ be a lattice.*

(i) $\wp_{\Lambda_\tau}$ satisfies the relation

$$(\wp'_{\Lambda_\tau}(z))^2 = 4(\wp_{\Lambda_\tau}(z))^3 - 60G_4(\tau)\wp_{\Lambda_\tau}(z) - 140G_6(\tau). \tag{26}$$

(ii) The Laurent series expansion of $\wp_{\Lambda_\tau}$ is given by

$$\wp_{\Lambda_\tau}(z) = \frac{1}{z^2} + \sum_{\substack{n=2 \\ n \text{ even}}} (n+1)G_{n+2}(\tau)z^n. \tag{27}$$

for all z such that $0 < |z| < \inf\{|w| : w \in \Lambda - \{0\}\}$.

Proof. See [12, Prop. 1.4.1.]. □

We see from 3.9.*i* that the Eisenstein series occur as the coefficients of the Weierstrass-p function. Taking the derivative with respect to z on both sides of (27) and dividing out $2\wp'_{\lambda_\tau}$ yields the following:

Corollary 3.10. *The function $\wp_{\lambda_\tau}$ satisfies*

$$\wp''_{\lambda_\tau} = 6\wp^2_{\lambda_\tau} - 30G_4(\tau). \tag{28}$$

For notational purposes let $F_k := -\frac{1}{(k-2)!}\frac{B_k}{2k}E_k$.

Proposition 3.11. *For $k \geq 4$ even, we have the following recursion:*

$$(k-2)(k+5)F_{k+4} = 12(F_4F_k + F_6F_{k-2} + ... + F_kF_4). \tag{29}$$

Proof. This follows from comparing the coefficients of z^k in (28). □

As $E_s = P_s(j)\Delta^{n_s}E_4^{b_s}E_6^{a_s}$ for any even integer $s \geq 4$, we can substitute this relation in (29) to give a recurrence relation between the polynomials φ_s.

Consider the following table of integer tuples:

(0,0)	(1,1)	(0,0)	(0,1)	(1,0)	(0,1)
(0,0)	(1,0)	(1,0)	(0,0)	(1,0)	(1,0)
(0,0)	(0,1)	(0,0)	(0,1)	(0,0)	(0,1)
(0,0)	(1,0)	(0,0)	(0,0)	(1,0)	(0,0)
(0,0)	(1,1)	(1,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)

Let $\alpha(i,j)$ denote the integer tuple corresponding to the the i-th row and j-th column in the table, counting from 0. Let $\alpha(i,j)(t)$ denote the t-th coordinate of the tuple $\alpha(i,j)$ for $t \in \{0,1\}$.

Proposition 3.12. *For $i \geq 4$ even, let $v_{i,k} = \alpha(k/2 \pmod 6, i/2 \pmod 6)$ and let $v_{i,k}(t)$ be the t-th coordinate of $v_{i,k}$ for $t \in \{0,1\}$. For even $k \geq 4$ we have the following recursion:*

$$\varphi_{k+4}(X) = \frac{\beta_{k+4}}{\beta_4^{b_{k+4}}\beta_6^{a_{k+4}}}\frac{12}{(k-2)(k+5)}\sum_{\substack{i=4 \\ i \text{ even}}}^{k}(\beta_4^{-3}X)^{v_{i,k}(0)}(\beta_6^{-2}(X-1728))^{v_{i,k}(1)}\varphi_i(X)\varphi_{k+4-i}(X). \tag{30}$$

Where $\beta_k = -\frac{(k-2)!2k}{B_k}$ and $\varphi_4 = \varphi_6 = 1$.

Proof. This follows from (29), keeping track of all the constants. □

This recursion, however, does not seem to give any (extra) information on the zeros of E_k. This is different in the function field analogue, where such a recursion can be used to prove the analogue of 3.5, see [9] and [10].

Using a similar argument as the one Swinnerton-Dyer and Rankin gave in [33], it has been shown that the zeros of the Eisenstein series have interlacing properties.

Theorem 3.13 (Interlacing Property [27]). *Let $k \geq 12$ be an even integer, and let E_k be the Eisenstein series of weight k for $SL_2(\mathbb{Z})$. Let $\{e^{ia_j} \mid a_1 < ... < a_{n_k}\}$ be the zeros of E_k on $\mathcal{F}-\{i,\rho\}$ and let $\{e^{ib_j} \mid b_1 < ... < b_{n_k+1}\}$ be the zeros of E_{k+12} on $\mathcal{F}-\{i,\rho\}$. Then $b_j < a_j < b_{j+1}$ for $j = 1, 2..., n$.*

As the j-invariant is increasing on the arc S as the argument is decreasing, we have that $\{\varphi_k, \varphi_{k+12}, ...\}$ also has the interlacing property ($k \geq 14$ and even). Furthermore, experiments in [17] suggest that all the polynomials φ_k are irreducible with the full symmetric group as Galois group. The interlacing property, simplicity and reality of the roots of φ_k suggests some relations with orthogonal polynomials, see propositions 3.50 and 3.51 below.

3.2 Congruence Properties of Eisenstein Series

It will turn out that the polynomials φ_k have remarkable congruence properties. We will discuss these properties and the relationship with supersingular elliptic curves defined over a finite field. The main reference of this section will be [17]. For general definitions and basic results on elliptic curves, we refer to [40].

We will first discuss congruences of Eisenstein series. We start with the following well-known lemma.

Lemma 3.14 (Von Staudt-Clausen). *The value*

$$B_n + \sum_{(p-1)|n} \frac{1}{p}$$

is an integer for every even n.

From this, we see that the denominator of B_n is exactly divisible by all primes p such that $(p-1)|k$. As a consequence from the Fourier-expansion of E_k, we see that

$$E_k \equiv 1 \pmod{p}, \tag{31}$$

if $(p-1)|k$, where the congruence means (mod p) as power series. Furthermore for the polynomials φ_k we find

Proposition 3.15. *If $k \equiv 0 \pmod{p-1}$, all the coefficients of φ_k are p-integral.*

Proof. The Fourier coefficients of E_k are p-integral, hence the polynomials φ_k are p-integral. □

We now explain the relation with elliptic curves. Let E be an elliptic curve defined over $\overline{\mathbb{F}}_p$, $p \geq 5$ a prime.

Proposition 3.16. *Let E, E' be two elliptic curves over $\overline{\mathbb{F}}_p$. Then E is isomorphic to E' over $\overline{\mathbb{F}}_p$ if and only if they have the same j-invariant.*

Proof. See [40, Proposition 1.4.]. □

We call E *supersingular* if the group $E(\overline{\mathbb{F}}_p)$ has no p-torsion.

Proposition 3.17. *Let E, E' be two elliptic curves over $\overline{\mathbb{F}}_p$ and E is isomorphic to E' over $\overline{\mathbb{F}}_p$. Assume that E is supersingular. Then E' is also supersingular.*

Hence we see that the j-invariants of elliptic curves fully determine whether an elliptic curve is supersingular. Now consider the following monic polynomial:

$$ss_p(X) := \prod_{\substack{E/\cong, \\ E \text{ is supersingular}}} (X - j(E)), \tag{32}$$

where $E/\cong$ is the set of elliptic curves up to $\overline{\mathbb{F}}_p$-isomorphism and $p \geq 5$ a prime number. This polynomial lies in $\mathbb{F}_p[X]$ as the set of supersingular j-invariants is invariant under the Frobenius endomorphism, see [40, Theorem 3.1.].
We have the following surprising result for the polynomials φ_k:

Theorem 3.18. $j^{b_{p-1}}(j - 1728)^{a_{p-1}}\varphi_{p-1} \equiv ss_p \pmod{p}$.

Proof. See [22]. □

Remark 3.19. It is a general fact (see [40, Theorem 3.1]) that the j-invariants of supersingular elliptic curves lie in $\mathbb{F}_{p^2}$, so this means that the polynomial φ_{p-1} factorises over $\mathbb{F}_p$ as products of only linear and quadratic terms.

In [22, §10] it was shown that the roots of $\varphi_{p-1} \pmod{p}$ lie in $\mathbb{F}_{p^2}$ using modular polynomials, without using knowledge of supersingular elliptic curves over finite fields. We will present this proof here.

For an integer $N > 1$, we can define the *Modular Polynomial* $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$. This polynomial will parametrize N-isogenous elliptic curves over $\mathbb{C}$. For the construction of this polynomial we follow [11, p. 229]. Let $\Gamma_0(N)\gamma_i$ be the right cosets of $C(N) := \Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z})$ for $i = 1, ..., |C(N)|$. Then for any $\tau \in \mathbb{H}$ we consider

$$\Phi_N(X, \tau) := \prod_{i=1}^{|C(N)|} (X - j(N\gamma_i\tau))$$

as a polynomial in the variable X. As $j(N\tau)$ is a modular function for $\Gamma_0(N)$, it is easy to see that this polynomial is well-defined. As the coefficients of this polynomial are symmetric polynomials in the $j(N\gamma_i\tau)$, we see that coefficients are invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. Clearly these coefficients are holomorphic in τ, showing that the coefficients are polynomials in the j-invariant, so this defines a polynomial $\Phi_N(X, Y) \in \mathbb{C}[X, Y]$. We have the following properties for the modular polynomial:

Theorem 3.20 ([11, Theorem 11.18])**.** *Let N be a positive integer.*

i $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$.

ii If N is a prime p, $\Phi_N(X, Y) \equiv (X^p - Y)(X - Y^p) \bmod p\mathbb{Z}[X, Y]$.

Proof. See [11, p. 231]. □

This last identity is also called *Kronecker's congruence*. Further we can relate the modular polynomials to elliptic curves over $\mathbb{C}$. For $E = E_\tau \cong \mathbb{C}/(\mathbb{Z} \oplus \tau\mathbb{Z})$, define the j-invariant of E_τ as $j(\tau)$, where j is the modular j-invariant. For elliptic curves E, E' over $\mathbb{C}$, if $\alpha : E \to E'$ is an isogeny, we say that α is *cyclic* if the kernel is cyclic.

Theorem 3.21 ([11, Theorem 14.11])**.** *let E and E' be elliptic curves over $\mathbb{C}$. Then there is a cyclic isogeny α from E to E' of degree $N > 1$ if and only if $\Phi_N(j(E), j(E')) = 0$.*

Proof. See [11, p. 315]. □

Theorem 3.22. *$\varphi_{p-1} \pmod p$ factors as a product of linear and quadratic factors.*

Proof. We will follow the proof of [22, §10]. Consider the holomorphic function

$$\psi_p(j(\tau)) := \frac{j(\tau)^p - j(p\tau)}{p}.$$

We will consider this function as a Laurent series in j^{-1}, so that $\psi(j) \in \mathbb{Z}((j^{-1}))$. Let $\Phi_p(X, Y) \in \mathbb{Z}[X, Y]$ be the modular function as defined before. Kronecker's identity (3.20) gives

$$\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) + pR_p(X, Y), \tag{33}$$

for $R \in \mathbb{Z}[X, Y]$. Clearly the elliptic curves E_τ and $E_{p\tau}$ are p-isogenous, so that

$$\Phi_p(j(\tau), j(p\tau)) = 0. \tag{34}$$

Using (33) and (34) we deduce that

$$\psi_p(j(\tau))(j(p\tau)^p - j(\tau)) = R_p(j(\tau), j(p\tau)). \tag{35}$$

As $j(p\tau) \equiv j(\tau)^p \pmod p$ (for any $F \in \mathbb{Z}((X))$ we have $F(X^p) \equiv F(X)^p \pmod p$), we find that

$$\psi_p(j) \equiv \frac{R_p(j, j^p)}{j^{p^2} - j} \pmod p. \tag{36}$$

From the last equation we see that the poles of the Laurent series $\psi_p(j)$ are all simple and lie in $\mathbb{F}_{p^2}$. The idea is to show that roots of the polynomial $\widetilde{\varphi}_{p-1} := \varphi_{p-1} \pmod p$ are the poles of $\psi_p(j)$, showing that the roots of $\tilde{\varphi}_{p-1}$ are all in $\mathbb{F}_{p^2}$.

We compute the derivative of $\psi_p(j(\tau))$ with respect to τ, (the derivative is defined to be $\frac{1}{2\pi i}\frac{d}{d\tau}$) to find

$$\frac{d\psi_p(j)}{dj} = j(\tau)^{p-1} - \frac{j'(p\tau)}{j'(\tau)} \equiv j(\tau)^{p-1} - j'(\tau)^{p-1} \pmod p. \tag{37}$$

as Laurent series in j^{-1}. As usual, write

$$E_{p-1} = \Delta^{n_{p-1}} E_4^{b_{p-1}} E_6^{a_{p-1}} \varphi_{p-1},$$

where $p - 1 = 12n_{p-1} + 4b_{p-1} + 6a_{p-1}$. Using (31), we have that $E_{p-1} \equiv 1 \pmod p$, so that

$$\tilde{\varphi}_{p-1} \equiv \Delta^{-n_{p-1}} E_4^{-b_{p-1}} E_6^{-a_{p-1}} \pmod p. \tag{38}$$

As

$$j'(\tau) = -\frac{E_6(\tau)}{E_4(\tau)} j(\tau),$$

we find using (38)

$$\begin{aligned} j'(\tau)^{p-1} &= E_6^{p-1} E_4^{2(p-1)} \Delta^{-(p-1)} \\ &\equiv (E_4^3)^{8n_{p-1}+4b_{p-1}+4a_{p-1}} (E_6^2)^{6n_{p-1}+2b_{p-1}+4a_{p-1}} \Delta^{-14n_{p-1}-6b_{p-1}-8a_{p-1}} \\ &\quad \cdot \tilde{\varphi}_{p-1}^{-2} E_4^{-6b_{p-1}} E_6^{-4a_{p-1}} \Delta^{2b_{p-1}+2a_{p-1}} \pmod p, \\ &\equiv \frac{j^{8n_{p-1}+4b_{p-1}+4a_{p-1}} (j - 1728)^{6n_{p-1}+2b_{p-1}+4a_{p-1}}}{(\tilde{\varphi}_{p-1} j^{b_{p-1}} (j - 1728)^{a_{p-1}})^2} \pmod p. \end{aligned}$$

Let $S_p(j) :\equiv \tilde{\varphi}_{p-1} j^{b_{p-1}} (j-1728)^{a_{p-1}} \pmod{p}$, we now find

$$\frac{d\psi_p}{dj} \equiv j^{p-1} - \frac{j^{8n_{p-1}+4b_{p-1}+4a_{p-1}} (j-1728)^{6n_{p-1}+2b_{p-1}+4a_{p-1}}}{S_p(j)^2} \pmod{p}. \tag{39}$$

As all the poles of $\frac{d\psi_p}{dj}$ are in $\mathbb{F}_{p^2}$, we conclude using (39) that the zeros of S_p and hence of $\tilde{\varphi}_{p-1}$ lie in $\mathbb{F}_{p^2}$. □

3.3 Power Sums of the zeros of Modular Forms

In this section we study power sums of Eisenstein series, based on the ideas of R.A. Rankin [34]. Given a modular form h, Rankin [34] estimates the j-invariants of the roots of h by computing a certain sum of residues in two different ways.
Let F be a meromorphic function on $\mathbb{H}$ and suppose $F(z+1) = F(z)$ for all $z \in \mathbb{H}$, i.e. F has a Fourier-expansion $G(q)$. Furthermore, suppose F is meromorphic at $i\infty$. This means that on $\{q \in \mathbb{C} \mid 0 < |q| < 1\}$, the function $G(q)$ can be extended to a meromorphic function on the whole open unit disk.
We define a sum of residues of F as follows:

$$R(F) := \frac{1}{2}\text{res}_i(F) + \frac{1}{3}\text{res}_\rho(F) + \text{res}_{q=0}(G/q) + \sum_{z \in \mathcal{F} - \{[\rho],[i],i\infty\}} \text{res}_z(F), \tag{40}$$

where the "res" is the residue defined as usual for a meromorphic function. From now on, let the derivative be with respect to $\frac{1}{2\pi i}\tau$.

Definition 3.23 (Generalized weakly modular form)**.** Suppose $f : \mathbb{H} \to \mathbb{C}$ is a meromorphic function and suppose

$$f\left(\frac{az+b}{cz+d}\right) = \epsilon(a,b,c,d)(cz+d)^k \cdot f(z), \tag{41}$$

where $\epsilon(a,b,c,d) \in \mathbb{C}$ with unit modulus and $k \in \mathbb{Z}$. Furthermore suppose f has a q-expansion

$$f(z) = \sum_{n \geq n_0} a_n q^{n/N},$$

for some $n_0 \in \mathbb{Z}$ and $N \in \mathbb{N}$. We call f a *weakly modular form with multiplier system* ϵ.

Lemma 3.24. *Suppose g is a modular function and f is a non-zero modular function with multiplier system ϵ* (i.e. $k = 0$)*. Then the meromorphic function*

$$g\frac{f'}{f}$$

is 1*-periodic and*

$$R\left(g\frac{f'}{f}\right) = 0. \tag{42}$$

Proof. The fact that $g\frac{f'}{f}$ is 1-periodic is easy to see and follows immediately from the definition of a generalized weakly modular form. We will prove (42) by integration over the boundary of the fundamental region $\mathcal{F}$ in two different ways. First we assume that $g\frac{f'}{f}$ has no poles on the boundary of $\mathcal{F}$. Let BB', CC' and DD' in figure 3 be arcs of small radius $\epsilon > 0$, let AE be high enough and ϵ small enough such that all the possible poles of $g\frac{f'}{f}$ in $\mathcal{F}$ lie in the region (which we will call W) with boundary $\mathcal{C}$, see figure 3. Now by the residue theorem we have

$$\oint_{\mathcal{C}} g\frac{f'}{f} = 2\pi i \sum_{p \in W} \text{res}_p\left(g\frac{f'}{f}\right). \tag{43}$$

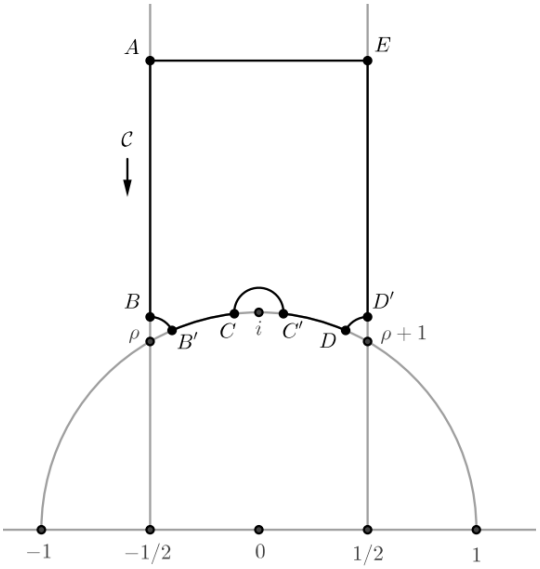

Figure 3: The contour integral $\mathcal{C}$, picture taken from [5]

On the other hand,

$$\oint_{\mathcal{C}} g\frac{f'}{f} = \left(\int_A^B + \int_B^{B'} + \int_{B'}^C + \int_C^{C'} + \int_{C'}^D + \int_D^{D'} + \int_{D'}^E + \int_E^A\right) g\frac{f'}{f}.$$

Clearly, using modularity we have

$$\left(\int_A^B + \int_{D'}^E\right) g\frac{f'}{f} = 0.$$

Furthermore if we write $\epsilon' = \epsilon(0, 1, -1, 0)$, we see that

$$\left(g\frac{f'}{f}\right)(-1/z) = g(z)\frac{z^2\epsilon' f'(z)}{\epsilon' f(z)} = z^2 g(z)\frac{f'(z)}{f(z)}.$$

So that

$$\left(\int_{B'}^C + \int_{C'}^D\right) g\frac{f'}{f} = 0.$$

Lastly, if $\epsilon \to 0$, we see that

$$\left(\int_B^{B'} + \int_D^{D'}\right) g\frac{f'}{f} \to -\frac{1}{3}\operatorname{ord}_{z=\rho}\left(g\frac{f'}{f}\right),$$
$$\int_C^{C'} g\frac{f'}{f} \to -\frac{1}{2}\operatorname{ord}_{z=i}\left(g\frac{f'}{f}\right).$$

Further, as there are no poles above the line AE in $\mathcal{F}$ we have using the residue theorem

$$\int_A^E g\frac{f'}{f} = 2\pi i \operatorname{res}_{z=i\infty} g\frac{f'}{f} = \operatorname{res}_{q=0}\left(g\frac{f'}{q\cdot f}\right).$$

If any pole lies on the boundary of $\mathcal{F}$, we will exclude it from the region W by drawing small half semicircles (of radius ϵ) around them. The result now follows. □

Proposition 3.25. *Let g be a modular function and h be a modular form of weight k, then*

$$R\left(g\frac{h'}{h}\right) = \frac{k}{12}R\left(gE_2\right).$$

Again the derivatives are with respect to q.

Proof. We will follow the proof of [34]. Let $f = h\cdot\eta^{-2k}$, where η is the eta function. Note that f is a modular function with respect to a certain multiplier ϵ. Now if we apply proposition 3.24 to f and g, and use that $\eta' = \frac{1}{24}\cdot E_2\eta$, we find

$$R\left(g\frac{h'\cdot\eta^{-2k} - \frac{1}{12}k\cdot h\cdot\eta^{-2k}E_2}{f}\right) = 0. \tag{44}$$

From this we deduce

$$R\left(g\frac{h'}{h}\right) = \frac{k}{12}R\left(gE_2\right). \tag{45}$$

□

Remark 3.26. Note that this result implies that the sum of residues of gh'/h on $\mathcal{F}$ only depends on the choice of modular function g.

Now, let v be a non-negative integer. Then proposition 3.25 can be applied to the modular function

$$g = j^v,$$

where j is the modular j-invariant. As the only possible pole of j^vE_2 is the pole at $i\infty$, $R(j^vE_2)$ is simply the constant coefficient in the q-expansion of j^vE_2. If we write $j^v = q^{-v}\sum_{n=0}^{\infty}a_{n,v}q^n$, then

$$g_v := R(j^vE_2) = a_{v,v} - 24\sum_{m=1}^{v}a_{v-m,v}\sigma_1(m). \tag{46}$$

As the $a_{n,v}$ are integers, so are the numbers (46).

Example 3.27 (Examples of values g_v)**.**

$$g_0 = 1,\ g_1 = 720,\ g_2 = 911520,\ g_3 = 130101120,\ g_4 = 1958042030400;$$

We have, using proposition 3.25,

$$R\left(j^v\frac{h'}{h}\right) = kg_v/12$$

for any modular form h of weight k. Now we can also compute $R(j^vh'/h)$ in a different way. Note that the possible poles of j^vh'/h consist of the pole at $i\infty$ (j has a simple pole at $i\infty$) and the zeros of h. Hence this residue should contain information about the zeros of h. Let

$r_\infty(j^v h'/h)$ be the residue of $j^v h'/h$ at $i\infty$, i.e. the constant term in the q-expansion of $j^v h'/h$. So we can write

$$R\left(j^v \frac{h'}{h}\right) = r_\infty\left(j^v \frac{h'}{h}\right) + S\left(j^v \frac{h'}{h}\right)$$

where $S(j^v h'/h)$ is the sum of the residues in the finite part of $\mathcal{F}$. As before, if we write $k = 12n_k + 6a_k + 4b_k$ for $a_k \in \{0,1\}$ and $b_k \in \{0,1,2\}$, then by the valence formula $\mathrm{ord}_i(h) - a_k$ and $\mathrm{ord}_\rho(h) - b_k$ are multiples of 2 respectively 3. By definition we have

$$\begin{aligned} S\left(j^v h'/h\right) &= \frac{1}{2}a_k j^v(i) + \frac{1}{3}b_k j^v(\rho) + S^*\left(j^v \frac{h'}{h}\right) \\ &= \frac{1}{2}a_k 1728^v + \frac{1}{3}b_k 0^v + S^*\left(j^v \frac{h'}{h}\right) \end{aligned}$$

where

$$S^*(j^v h'/h) = \sum_{\substack{x \in \mathcal{F} - \{i,\rho\} \\ h(x)=0}} j(x)^v + \frac{\mathrm{ord}_i(h) - a_k}{2} j(i)^v + \frac{\mathrm{ord}_i(h) - a_k}{3} j(\rho)^v,$$

counted with multiplicity. Hence S^* is the sum over n_k, not necessarily distinct, j-invariants of the zeros of h. So we conclude, using 3.25

$$kg_v/12 = r_\infty\left(j^v \frac{h'}{h}\right) + S\left(j^v \frac{h'}{h}\right). \tag{47}$$

This gives us a way of computing the j-invariants of the zeros of h in terms of the residue at $i\infty$ and the values g_v.

Remark 3.28. Suppose h is a modular form with only rational Fourier coefficients. In that case $r_\infty(j^v h'/h)$ is clearly rational for all non-negative integers v and therefore all the power sums of the j-invariants of the n_k roots (again where i and ρ are counted with weight 2 and 3 respectively) of h are rational. If one construct a monic polynomial P_h of degree n_k having exactly the j-invariants of the n_k roots of h as zeros, this will be a *rational polynomial*. As a consequence, the j-invariants of all the roots of h are algebraic over $\mathbb{Q}$. Furthermore, due to a result of Schneider (1973) [37] we know that if $j(z)$ is algebraic, then either z is transcendental over $\mathbb{Q}$ or z is imaginary quadratic.
In theorem 3.2 we showed that the n_k zeros of E_k all lie on the arc $\{e^{i\theta} \mid \theta \in (\frac{\pi}{2}, \frac{2\pi}{3})\}$. As there are no imaginary quadratic numbers on this arc, it follows that the n_k zeros of E_k are *transcendental* over $\mathbb{Q}$.

The idea is to apply (47) to Eisenstein series. Let $h = E_k$ be the Eisenstein series of weight k, so that for any non-negative v, the sum S^* gives precisely the sum of $j(x)^v$ over the n_k roots x of E_k (again, we count i and ρ with weight $1/2$ and $1/3$ respectively). This gives systems of equations:

$$\sum_{i=1}^{n_k} j(x_i)^v = \ kg_v/12 - r_\infty\left(j^v \frac{E_k'}{E_k}\right) - \frac{a_k}{2}1728^v, \text{ for } v = 1, ..., n \tag{48}$$

where $\{x_1, ..., x_{n_k}\}$ is the set of n_k roots of E_k and we hope to solve $j(x_i)$ for all i from this equation (if $j(x_j) = 1728$ or $j(x_j) = i$ turns out to be a solution, we have to count the root x_j with multiplicity 2 or 3 respectively).

Remark 3.29. In fact, if we compute (48) for $v = 1$ we find the result stated in [29]:

$$\frac{2}{\zeta(1-k)} = 60 \cdot k - \sum_{\tau \in \mathbb{H}/\operatorname{SL}_2(\mathbb{Z})} e_\tau \operatorname{ord}_\tau(E_k(\tau)) j(\tau), \tag{49}$$

where $e_\tau = 1/2$ if $\tau = [i]$, $e_\tau = 1/3$ if $\tau = [\rho]$ and $e_\tau = 1$ otherwise.

Example 3.30. Consider the Eisenstein series of weight 30, E_{30}. By the valence formula (11), E_{30} has a zero of order congruent to 1 (mod 2) at i and of order congruent to 0 (mod 3) at ρ. In this case we have $n_k = 2$,$a_k = 1$ and $b_k = 0$. To find the zeros of E_{30}, we need to solve the following system of equations:

$$S_1 := j(x_1) + j(x_2) = 30g_1/12 - \frac{1}{2}1728 - r_\infty\left(j\frac{E'_{30}}{E_{30}}\right),$$
$$S_2 := j(x_1)^2 + j(x_2)^2 = 30g_2/12 - \frac{1}{2}1728^2 - r_\infty\left(j^2\frac{E'_{30}}{E_{30}}\right).$$

As we have $E_{30} = 1 - \frac{2k}{B_k}q + \mathcal{O}(q^2)$, $E'_{30} = -\frac{2k}{B_k}q - \frac{4k}{B_k}\sigma_{29}(2)q^2 + \mathcal{O}(q^3)$, we conclude that $r_\infty\left(jE'_{30}/E_{30}\right) = -\frac{2k}{B_k}$. We find that

$$\begin{aligned} S_1 = j(x_1) + j(x_2) &= 30g_1/12 - \frac{1}{2}1728 - \frac{-60}{B_{30}}, \\ &= 936 + 9.97... \cdot 10^{-8} \end{aligned}$$

Also, we have that $j^2 = \frac{1}{q^2} + \frac{1488}{q} + \mathcal{O}(1)$ and one can compute that

$$\begin{aligned} r_\infty(j^2E'_{30}/E_{30})) &= -1488\frac{2k}{B_k} - \left(\frac{2k}{B_k}\right)^2 - \frac{2k}{B_k}2\sigma_{29}(2) \\ &= -107.092... \end{aligned}$$

So that

$$\begin{aligned} S_2 = j(x_1)^2 + j(x_2)^2 &= 30g_2/12 - \frac{1}{2}1728^2 - (-107.092) \\ &= 785915.092... \end{aligned}$$

In fact one can now check that $S_1^2 < 2S_2$ so that $j(x_1)$ and $j(x_2)$ are both real and distinct, furthermore

$$0 < \left(j(x_1) - \frac{1728}{2}\right)^2 + \left(j(x_2) - \frac{1728}{2}\right)^2 = S_2 - 1728 \cdot S_1 + \frac{1}{2}1728^2 < \left(\frac{1728}{2}\right)^2.$$

So that $0 < j(x_1), j(x_2) < 1728$. Hence the values $j(x_1)$ and $j(x_2)$ are real and lie in $(0, 1728)$, as expected.

Proposition 3.31 ([34] p. 141)**.** *If for a fixed non-negative integer v the weight k increases we get*

$$r_\infty\left(j^v\frac{E'_k}{E_k}\right) = o(1)$$

Proof. Note that it suffices to show that for a fixed integer $0 \leq w < v$ the q^w-coefficient of E_k'/E_k converges to 0. This q^w-coefficient is of the form

$$\sum_{i \in I_v} c_i \Big(\frac{2k}{B_k}\Big)^{\alpha_i} d_i^{k-1} \tag{50}$$

where I_v is a finite index set depending only on v, c_i a coefficient depending only on v, where α_i an integer $1 \leq \alpha_i \leq v$ and d_i an integer $1 \leq d_i \leq v^v$. Using Stirling's formula and the fact that $\zeta(k) \to 1$ as $k \to \infty$, we have

$$B_k \sim \sqrt{\pi k} \left(\frac{1}{2}\right)^k \Big(\frac{k}{\pi e}\Big)^k \text{ for } k \to \infty. \tag{51}$$

Now using (50) and (51), it follows that $r_\infty(j^v E_k'/E_k) = o(1)$ as $k \to \infty$. □

Using the previous proposition it follows that

$$S^*(j^v E_k'/E_k) = k g_v/12 - \frac{a_k}{2} 1728^v + o(1), \tag{52}$$

as $n_k \mapsto \infty$. This means that the v-th power sums of the roots of the polynomials $\varphi_k, \varphi_{k+12}, ...$ grow approximately linear. Furthermore, the power sums of the roots of the polynomials φ_k approximate an integer value. In the next paragraph we find polynomials having as Newton sums exactly these integer values. These turn out to be polynomials coming from extremal modular forms.

3.4 Power Sums and Hankel Matrices

In this section we explain how power sums of roots of polynomials give information about the reality of the roots. We show how this is related to the so called "Hankel determinant" of a polynomial.

3.4.1 Hankel Matrices

Suppose we are given a monic polynomial $P(X) \in \mathbb{R}[X]$ of degree $n > 0$, write $P(X) = \sum_{i=0}^{n} a_i X^i$ where $a_i \in \mathbb{R}$ for all $0 \leq i \leq n$ and $a_n = 1$. For convenience let $a_k := 0$ for $k > n$. Suppose $x_1, ..., x_n \in \mathbb{C}$ are the not necessarily distinct roots of $P(X)$, then for i a non-negative integer, we define the $i-$th power sum as

$$s_i := x_1^i + ... + x_n^i. \tag{53}$$

The well-known Newton-Girard formulae gives us a relation between the coefficients of the polynomial $P(X)$ and the power sums.

Proposition 3.32 (Newton-Girard formulae)**.** *We can express the power sums s_i, $(0 < i \leq n)$ in terms of the coefficients of $P(X)$.*

$$s_i = -(ia_{n-i} + \sum_{r=1}^{i-1} s_r a_{n-r}).$$

If $k > n$ we have:

$$s_k = -\sum_{i=k-n}^{k-1} a_{k-i} s_i.$$

Conversely,

$$a_{n-i} = -\frac{1}{i}(\sum_{r=1}^{i} a_{n-i+r} s_r).$$

Remark 3.33. First of all, by induction all the $s_i \in \mathbb{R}$. Furthermore, if $P(X) \in \mathbb{Q}[x]$, it follows from 3.32 that all the s_i are rational.

The question is whether these power sums give any information on the roots of $P(X)$. For this we define the $n \times n$-Hankel-matrix $H(P)$ of $P(X)$:

$$H(P) := \begin{pmatrix} s_0 & s_1 & \dots & s_{n-1} \\ s_1 & s_2 & \dots & s_n \\ \vdots & \vdots & \ddots & \vdots \\ s_{n-1} & s_n & \dots & s_{2n-2} \end{pmatrix}.$$

As a way to analyze the number of real roots of P, we can define for any real symmetric matrix A its signature. It is a basic fact from linear algebra that all the eigenvalues of A are real.

Definition 3.34 (signature and rank of a matrix)**.** Suppose A is a real symmetric $n \times n$-matrix. Let n_+, n_- be the number of positive, respectively negative eigenvalues of A. Then we define the *signature* of A

$$\mathrm{Sign}(A) = n_+ - n_-.$$

And we define the *rank* as

$$\mathrm{Rank}(A) = n_+ + n_-.$$

Lemma 3.35. *The signature of $H(P)$ equals the number of real roots of P and the rank of $H(P)$ is the number of distinct complex roots of P.*

Proof. See [31, Theorem 7.]. □

If the matrix $H(P)$ is positive definite, this lemma implies that the roots of P are real and distinct. A way of checking if a real symmetric $n \times n$-matrix A is positive definite is by means of Sylvester criterion. Let A_i be the upper-left $i \times i$ sub-matrix for $1 \leq i \leq n$.

Lemma 3.36 (Sylvester criterion)**.** *A matrix A is positive definite if and only if* $\det(A_i) > 0$ *for all* $1 \leq i \leq n$.

Proof. See for example [15, Theorem 16.4.3.]. □

This result gives a criterion for a polynomial to have real roots. We need to check that the determinants of the n upper left sub-matrices $H(P)_i$ are positive.

Example 3.37. Consider the polynomial $P(X) = X^3 - 4X - 1$. We compute

$$s_0 = 3;\ s_1 = 0;\ s_2 = 8;\ s_3 = 3;\ s_4 = 32.$$

We find that

$$H(P)_1 = 3 > 0;\ H(P)_2 = 24 > 0;\ H(P)_3 = 229 > 0.$$

Hence we can now conclude that the roots of P are all real and distinct.

3.4.2 Hankel Determinant of the g_i's

For $n \geq 0$ define the determinant:

$$\Delta_n = \begin{vmatrix} g_0 & g_1 & g_2 & \cdots & g_n \\ g_1 & g_2 & g_3 & \cdots & g_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_n & g_{n+1} & g_{n+2} & \cdots & g_{2n} \end{vmatrix}, \tag{54}$$

where the g_i are defined by (46). Now consider the matrix consisting of the power sums $s_{v,k} = S^*(j^v E_k'/E_k)$, for $0 \leq v \leq 2n_k$. Furthermore, let P_k be the monic real polynomial of degree n_k corresponding to these power sums. So that

$$H(P_k) = \begin{pmatrix} s_{0,k} & s_{1,k} & \cdots & s_{n_k-1,k} \\ s_{1,k} & s_{2,k} & \cdots & s_{n_k,k} \\ \vdots & \vdots & \ddots & \vdots \\ s_{n_k-1,k} & s_{n_k,k} & \cdots & s_{2n_k-2,k} \end{pmatrix}. \tag{55}$$

Let Δ_s^* be the determinant of the upper left $s \times s$ submatrix of $H(P_k)$, $1 \leq s \leq n_k - 1$. Using the theory in the previous section, we know that in order to show that the roots of P_k are all real and distinct, it suffices to show that all the Δ_s^* are strictly positive for $1 \leq s \leq n_k - 1$. We can relate Δ_s^* to Δ_{s-1} in the following way:

Proposition 3.38.

$$\Delta_s^* = 12^{-s}\Delta_{s-1}k^s + \mathcal{O}(k^{s-1}), \tag{56}$$

as $k \to \infty$.

Proof. This follows immediately from (52). □

Dividing both sides of (56) by k^s, we see that

$$\frac{\Delta_s^*}{k^s} = 12^{-s}\Delta_{s-1} + \mathcal{O}(k^{-1}),$$

as $k \to \infty$. In [34], R.A. Rankin tried to show that $\Delta_{s-1} < 0$ for some s, so that $\Delta_s^* < 0$ for big enough k_0, therefore concluding that P_k has non-real roots for $k > k_0$. However, R.A. Rankin [34] conjectured a remarkable explicit formula for Δ_{s-1}, showing that $\Delta_{s-1} > 0$ for all s. This conjecture was recently proven in a submitted paper by [19] using the theory from [22].

Proposition 3.39.

$$\Delta_s = 2^{s^2+4s}3^{s^2+2s}5^s7^s13^s\prod_{r=2}^{s}\left(\frac{(12r-3)(12r-7)(12r-5)(12r+1)}{(2r-1)^2(r-1)r}\right)^{s-r+1}.$$

Proof. See [19]. □

3.5 A Remark on Extremal Modular Forms

In this section we apply the methods of section 3.3 to extremal modular forms. We will give an explicit formula for certain power sums of the j-invariants of the zeros of these forms.

Lemma 3.40. *for every even $k \geq 4$, there exist a unique modular form $f_{k,0} \in M_k$ such that $f_{k,0}$ has as a q-expansion:*

$$f_{k,0}(z) = 1 + \mathcal{O}(q^{d_k}),$$

where $d_k := \dim(M_k)$. Furthermore the coefficients in the q-expansion of $f_{k,0}$ are all rational.

Proof. This follows from proposition 2.12. The rationality of the q-expansion of $f_{k,0}$ follows from the rationality of the basis elements in proposition 2.12. □

Using the theory in section 3, we have that for $v \geq 0$:

$$R\left(j^v \frac{f_k'}{f_k}\right) = r_\infty\left(j^v \frac{f_k'}{f_k}\right) + S_v\left(j^v \frac{f_k'}{f_k}\right).$$

Proposition 3.41. *Write $k = 12n_k + 6a_k + 4b_k$ for $a_k \in \{0,1\}$, $b_k \in \{0,1,2\}$ and n_k a non-negative integer. Then*

$$S^*\left(j^v \frac{f_{k,0}'}{f_{k,0}}\right) = kg_v/12 - \frac{a_k}{2} 1728^v,$$

for $v = 0, ..., n_k$ (with the convention $0^0 = 1$).

Proof. This follows from (47) and the observation that the meromorphic function $f_{k,0}'/f_{k,0}$ has a zero of order d_k at $q = 0$, so that

$$r_\infty\left(j^v \frac{f_{k,0}'}{f_{k,0}}\right) = 0 \quad \text{for } v = 0, ..., n_k,$$

the result now follows. □

Let

$$\chi_k(j) := \frac{f_{k,0}}{E_4^{b_k} E_6^{a_k} \Delta^{n_k}}$$

be the corresponding modular polynomial in the j-invariant of degree n_k. It follows from the explicit basis for M_k that these polynomials have integer coefficients.

Example 3.42.

$$\chi_{12}(X) = X - 720;$$
$$\chi_{24}(X) = X^2 - 1440X + 125280;$$
$$\chi_{36}(X) = X^3 - 2160X^2 + 965520X - 27302400;$$
$$\chi_{48}(X) = X^4 - 2880X^3 + 2324160X^2 - 465638400X + 5611550400.$$

Proposition 3.41 implies that the power sums of χ_k are exactly given by the values $kg_v/12 - \frac{a_k}{2}1728^v$. Further, let $H(\chi_k)$ be the Hankel matrix as in (55) with the $2n_k - 1$ power sums of χ_k as coefficients. We see that the corresponding determinants Δ_s' coincide (if $a_k = 0$) with Δ_{s-1}, up to a constant positive factor, if $0 \leq s \leq \frac{n_k}{2} + 1$. However, Δ_{s-1} and Δ_s' will not coincide for bigger $\frac{n_k}{2} + 1 < s < 2n_k - 2$. So, we cannot conclude that $H(\chi_k)$ is positive definite. Therefore, we cannot conclude that the roots of χ_k are real from the positivity of Δ_s.

However, it was shown by [13] that the zeros of $f_{k,0}$ are all distinct and lie on the unit circle in $\mathcal{F}$ (see also chapter 5). As a consequence:

Theorem 3.43. *The roots of χ_k are all real, distinct and lie in the interval $(0, 1728)$.*

3.5.1 Congruences of Extremal Modular Forms

In this section we will prove some congruence properties of the polynomials χ_k. We will show that $\chi_{p-1} \equiv ss_p (\text{mod } p)$, where ss_p is the supersingular polynomial defined by (32). In order to prove this result we need to define *modular forms mod p*, for a general reference see [38].

Let $p \geq 5$ be a prime number and let $f = \sum_{n\geq 0} a_n q^n$ be a modular form of weight k with p-integral rational coefficients (meaning that the coefficients of the Fourier expansion of f have no denominator divisible by p). Define

$$\widetilde{f} = \sum_{n\geq 0} \widetilde{a_n} q^n \in \mathbb{F}_p[[q]],$$

where $\widetilde{a_n} \equiv a_n \pmod p$. Let $\widetilde{M_k}$ be the set of all such $\widetilde{f}$, then $\widetilde{M_k}$ is an $\mathbb{F}_p$-vector space. For $f, g \in \mathbb{F}_p[[q]]$ write $f \equiv g \pmod p$ if the corresponding Fourier coefficients are congruent (mod p).

Lemma 3.44. *Write $k = 12n_k + 6a_k + 4b_k$ with $n_k \in \mathbb{Z}_{\geq 0}$, $a_k \in \{0, 1\}$ and $b_k \in \{0, 1, 2\}$. Let $\widetilde{\mathcal{B}} = \{\widetilde{\Delta}^{n_k - i} \widetilde{E}_4^{b_k+3i} \widetilde{E}_6^{a_k} \mid 0 \leq i \leq n_k\}$ (this is well-defined as the Fourier coefficients of Δ,E_4 and E_6 are all integers). Then $\widetilde{\mathcal{B}}$ is a basis for $\widetilde{M_k}$.*

Proof. Let $\mathcal{B} = \{\Delta^{n_k - i} E_k^{b_k+3i} E_6^{a_k} \mid 0 \leq i \leq n_k\}$ be a basis of M_k. By induction one can show that any modular form with p-integral Fourier coefficients is a p-integral linear combination of elements in $\mathcal{B}$. Furthermore, by induction all the elements in $\widetilde{\mathcal{B}}$ are linearly independent. This shows $\widetilde{\mathcal{B}}$ is a basis of $\widetilde{M_k}$. □

As a consequence of (31), we have that $\widetilde{E}_{p-1} \in \widetilde{M_k}$ and $E_{p-1} \equiv 1 \pmod p$.
So that,

$$\widetilde{E}_{p-1} - \widetilde{f}_{0,p-1} \equiv \mathcal{O}(q^{n_k+1}) \pmod p \tag{57}$$

As $\widetilde{E}_{p-1} - \widetilde{f}_{p-1} \in \widetilde{M_k}$ if we write this form as a linear combination of elements in $\widetilde{\mathcal{B}}$ we conclude that $\widetilde{E}_{p-1} - \widetilde{f}_{p-1} \equiv 0 \pmod p$. This means that in M_k

$$E_{p-1} - f_{0,p-1} = c_0 E_4^{b_k+3n_k} E_6^{a_k} + c_1 E_4^{b_k+3(n_k-1)} E_6^{a_k} \Delta + ... + c_{n_k} E_4^{b_k} E_6^{a_k} \Delta^{n_k} \tag{58}$$

where all the $c_0, ..., c_{n_k}$ are p-integral rational numbers with $v_p(c_i) > 0$. Hence, $\chi_{p-1} \equiv \varphi_{p-1} \pmod p$. Using theorem 3.18, we deduce

Theorem 3.45. *For $p \geq 5$,*

$$\chi_{p-1} \equiv ss_p \pmod p.$$

3.6 Orthogonal Polynomials

In this section we will discuss some general properties of orthogonal polynomials. The main reference is [22]. The sequence of polynomials $\{\varphi_k, \varphi_{k+12}, ...\}$ for $k \geq 4$ even, although not orthogonal, shares these properties (see 3.13 and 3.2).

Consider the vector space of polynomials in one variable $V = K[X]$ over a field K. Suppose we are given a K-linear map $\psi : V \to K$. This induces a symmetric bilinear form $(f, g) := \psi(fg)$ on V. If we apply the Gram-Schmidt procedure to the basis $\{X^n \mid n \in \mathbb{Z}_{\geq 0}\}$ of V, we get a sequence of *orthogonal polynomials* P_n as follows: Let $P_0 = 1$ and for $n > 0$ define

$$P_n(X) = X^n - \sum_{m=0}^{n-1} \frac{(X^n, P_m)}{(P_m, P_m)} P_m(X) \tag{59}$$

provided that $(P_m, P_m) \neq 0$ for all m.

Remark 3.46. If $K = \mathbb{R}$ and $(\ ,\ )$ is positive definite, it will automatically follow that (59) is well-defined.

From now on we will assume that the $(P_m, P_m) \neq 0$.

Proposition 3.47. *The polynomials P_n satisfy the following recursion:*

$$P_{n+1}(X) = (X - a_n)P_n(X) - b_n P_{n-1}(X) \quad (n \geq 1), \tag{60}$$

with $P_0 = 1$, $P_1 = X - (X, 1)$, $a_n = \frac{(XP_n, P_n)}{(P_n, P_n)}$ and $b_n = \frac{(P_n, P_n)}{(P_{n-1}, P_{n-1})}$.

Proof. See [22, §4]. □

Let $r_i := (X^i, 1)$ and define the numbers $\lambda_n \in K$ for $n \geq 1$ by

$$\Psi(x) := r_0 + r_1 x + r_2 x^2 + ... = \cfrac{g_0}{1 - \cfrac{\lambda_1 x}{1 - \cfrac{\lambda_2 x}{1 - ...}}}. \tag{61}$$

Proposition 3.48. *All the 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. See [22, Prop. 2.iii]. □

Let $\widehat{\Delta}_n$ be the $(n+1) \times (n+1)$-Hankel determinant of the r_i. The following theorem gives a remarkable relation between the coefficients of the recursion (60) and this Hankel determinant.

Theorem 3.49 ([24, Theorem 29])**.** *Let V be the vector space of all polynomials in one variable over a field K. Let $\varphi : V \to K$ be a K-linear map and let $\mu_k = \varphi(X^k)$. Furthermore, let $P_n(X)_{n \geq 0}$ be the sequence of orthogonal polynomials with respect to φ, and let*

$$P_{n+1}(X) = (x - a_n)P_n(X) - b_n P_{n-1}(X)$$

be the corresponding three term recursion from (60)*. Then*

$$\det_{0 \leq i,j \leq n}(\mu_{i+j}) = \mu_0^{n+1} b_1^n b_2^{n-1} ... b_{n-1}^2 b_n. \tag{62}$$

As a consequence of 3.48, we see that

$$\widehat{\Delta}_n = \mu_0^{n+1} \prod_{r=1}^{n} (\lambda_{2r-1}\lambda_{2r})^{n-r+1}. \tag{63}$$

We will use this theorem to compute a certain Hankel determinant in section 3.

From now on let $K = \mathbb{R}$ and

$$\psi(f) = \int_a^b f(X)w(X)dx \tag{64}$$

for some real numbers $a < b$ and a positive integrable function $w(X)$ on (a, b). Then we have the following important property of orthogonal polynomials.

Proposition 3.50 (Real and Distinct Zeros)**.** *The zeros of orthogonal polynomials P_n over $\mathbb{R}$ are all real and distinct and lie in the interval (a, b).*

Proof. See [42, Thm. 3.3.1.] □

Proposition 3.51 (Interlacing Zeros)**.** *Suppose $\{x_1, ..., x_n\}$ are the (real) zeros of P_n over $\mathbb{R}$ and suppose $\{y_1, ..., y_{n+1}\}$ are the zeros of P_{n+1}, then we have*

$$y_1 < x_1 < y_2 < ... < x_n < y_{n+1}.$$

Proof. See [42, Thm. 3.3.2.]. □

3.7 Atkin Polynomials

In this section we define Atkin polynomials and we will briefly summarize some properties, including relations with the supersingular polynomial. The reference is a paper from Kaneko and Zagier [22].

Define the following inner product on $\mathbb{R}[X]$:

$$(f(X), g(X))_A := \text{constant term of } f(j)g(j)E_2 \text{ as a Laurent series in } q.$$

Then we see that

$$(X^v, 1) = g_v,$$

where the values g_v were defined by (46). This inner product can be written in the integral form of (64) as follows:

Proposition 3.52 ([22, §5, Corollary])**.**

$$(f, g)_A = \int_0^{1728} f(j)g(j)w(j)dj,$$

where $w(j) = \frac{6}{\pi}\alpha'(j)$ and $\alpha : [0, 1728] \to [\pi/3, \pi/2]$ is the inverse of the monotone increasing function $\alpha \mapsto j(e^{i\alpha})$.

Proof. See [22, §5, Corollary]. □

Now as $w(j) > 0$ on $[0, 1728]$, we see that $(\ ,\ )_A$ is positive definite.
Define the *Atkin Polynomials* as the orthogonal polynomials with respect to the inner product $(\ ,\ )_A$, defined via the Gram-Schmidt procedure (59) (as the inner product is positive definite, we see that the Gram-Schmidt procedure is well defined).

Example 3.53.

$$\begin{aligned}
A_0(X) &= 1;\\
A_1(X) &= X - 720;\\
A_2(X) &= X^2 - 1640X + 269280;\\
A_3(X) &= X^3 - \frac{12576}{5}X^2 + 1526958X - 107765856.
\end{aligned}$$

As a consequence of 3.50 and 3.52, we see that the roots of A_k are all real, distinct and lie in $(0, 1728)$. Using theory of hypergeometric functions, an explicit recursion formula for the A_k can be found:

Theorem 3.54 ([22, Theorem 4.])**.** *For $n \geq 2$:*

$$\begin{aligned}
A_{n+1}(X) = \left(X - 24\frac{144n^2 - 29}{(2n+1)(2n-1)}\right)A_n(X)\\
- 36\frac{(12n-13)(12n-7)(12n-5)(12n+1)}{n(n-1)(2n-1)^2}A_{n-2}(X).
\end{aligned}$$

These polynomials turn out to have very remarkable congruence properties. Let n_p be the degree of the supersingular polynomial ss_p, then $A_{n_p}(X)$ is p-integral, and we have:

Theorem 3.55 (Atkin)**.** *Let $p \geq 5$ be a prime number. Then $ss_p(X) \equiv A_{n_p}(X) \pmod{p}$.*

Proof. See [22, §6]. □

4 Eisenstein Polynomials and Modular Forms

In this section properties of the "Eisenstein polynomial" defined by M. Oura [30] are discussed. There is a natural way to associate a modular form of level 1 to this polynomial. These modular forms share some properties with Eisenstein series, such as (conjecturally) the location of the zeros and congruence properties. We prove a factorization property of the associated Hankel determinant, analogous to the Hankel determinant corresponding to the Eisenstein series.

4.1 Eisenstein Polynomials and Relations with Modular Forms

For $g \in \mathbb{N}$, we define the following matrix group:

$$H_g := \langle D_g, A_g \rangle \subset \mathrm{GL}_{2^g}(\mathbb{C}).$$

Where:

- D_g is the subgroup generated by all the diagonal matrices

  $$D_S = \mathrm{diag}(i^{a^t S a}; a \in \mathbb{F}_2^g),$$

  for all symmetric matrices $S \in \mathrm{Mat}_{g\times g}(\mathbb{Z})$.

- A_g is the $2^g \times 2^g$ matrix, whose (a,b)-coefficient is given by

  $$\left(\frac{1+i}{2}\right)^g (-1)^{\langle a,b\rangle}, \quad a,b \in \mathbb{F}_2^g, \tag{65}$$

  where we identify elements of $\mathbb{F}_2^g$ with $\{0,...,2^g-1\}$ via the binary number representation.

(Note that the definition of these diagonal matrices is independent of the choice of representative of $a \pmod 2$, so we might assume $a \in \mathbb{F}_2^g$)
For any $g \in \mathbb{N}$, H_g is a finite group of order

$$2^{g^2+2g+2}(4^g-1)(4^{g-1}-1)\cdots 3, \tag{66}$$

see [36, §2 p. 183].
The group H_g acts on the $\mathbb{C}$-vector space of complex polynomials in 2^g variables $\mathbb{C}[x_a : a \in \mathbb{F}_2^g]$, induced by the natural action on the indices of the variables: for $\gamma \in H_g$, define

$$\gamma x_a = \sum_{i=0}^{2^g-1} \gamma_{i,a} x_i,$$

where $\gamma_{i,a}$ means the coefficient of the a-th column and i-th row of γ, counting from 0. We are interested in the H_g-invariant subspace, which is clearly also a subring, of $\mathbb{C}[x_a : a \in \mathbb{F}_2^g]$, $\mathbb{C}[x_a : a \in \mathbb{F}_2^g]^{H_g}$. This invariant ring will have a close connection to Siegel modular forms, as we will explain in the next section.

An example of an element in this invariant ring is the *Eisenstein polynomial of weight* l, with $l \in \mathbb{N}$:

$$\varphi_l^{H_g}(x_a : a \in \mathbb{F}_2^g) := \frac{1}{|H_g|} \sum_{\sigma \in H_g} (\sigma x_0)^l. \tag{67}$$

4.1.1 Siegel Modular Forms and the Theta Map

For $g \in \mathbb{N}$, let

$$\mathbb{H}_g = \{z \in \mathrm{Mat}_{g\times g}(\mathbb{C}) \mid z^t = z \text{ and } \mathrm{Im}(z) > 0\},$$

here $\mathrm{Im}(z) > 0$ means that the imaginary part of the matrix z, $\mathrm{Im}(z)$ is positive definite.

Define the Siegel modular group (of degree g) as

$$\Gamma_g := \left\{M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \; A, B, C \text{ and } D \in \mathrm{Mat}_{g\times g}(\mathbb{Z}) \mid M^t J_g M = J_g\right\},$$

where $J_g = \begin{pmatrix} \mathbf{0} & I_g \\ -I_g & \mathbf{0} \end{pmatrix}$.

Remark 4.1. The condition $M^t J_g M = J_g$ is equivalent to $A^tC - C^tA = \mathbf{0}, B^tD - BD^t = \mathbf{0}$ and $A^tD - C^tB = I_g$, showing that $\Gamma_1 = \mathrm{SL}_2(\mathbb{Z})$.

The group Γ_g acts on $\mathbb{H}_g$; for $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathbb{H}_g$

$$M \cdot Z := (AZ + B)(CZ + D)^{-1}.$$

Lemma 4.2. *The group Γ_g is generated by*

$$J = \begin{pmatrix} \boldsymbol{0} & I_g \\ -I_g & \boldsymbol{0} \end{pmatrix} \text{ and } \sigma_S = \begin{pmatrix} I_g & S \\ \boldsymbol{0} & I_g \end{pmatrix},$$

for all symmetric matrices $S \in GL_g(\mathbb{C})$.

Proof. See [14, Lemma 1.3.]. □

Definition 4.3 (Siegel Modular Form)**.** Let $f : \mathbb{H}_g \to \mathbb{C}$ be a holomorphic function, f is called a *(Classical) Siegel Modular Form for Γ_g of weight k* if

$$f(M \cdot Z) = \det(CZ + D)^k f(Z), \tag{68}$$

and if $g = 1$, we additionally demand that f is holomorphic at the cusp at $i\infty$.

The space of all Siegel modular forms for Γ_g is a $\mathbb{C}$-vector space and is denoted by $M(\Gamma_g)$.

Remark 4.4. Note that Siegel modular forms for Γ_1 coincide with classical modular forms for the full modular group.

We will now show that to every element in the invariant ring $\mathbb{C}[x_a : a \in \mathbb{F}_2^g]^{H_g}$ we can associate a Siegel modular form for Γ_g via the *Theta map*.

For $a \in \mathbb{Z}^g$, define the *Theta Functions:*

$$\theta_a(\tau) = \sum_{x\in\mathbb{Z}^g} e^{2\pi i(x+\frac{1}{2}a)^t \tau (x+\frac{1}{2}a)}. \tag{69}$$

The functions f_a are independent of the choice of $a \pmod 2$, hence we can consider $a \in \mathbb{F}_2^g$.

Proposition 4.5. *The $\mathbb{C}$-linear map*

$$Th_g : \mathbb{C}[x_a : a \in \mathbb{F}_2^g]^{H_g} \to M(\Gamma_g),$$

induced by $x_a \mapsto f_a(\tau)$ is well-defined.

Proof. See [36, p. 179] □

Remark 4.6. As the $f_a(\tau)$ are Siegel modular forms of weight $1/2$, it follows from proposition 4.5 that Th_g sends $\varphi_l^{H_g}$ to a Siegel modular form of weight $l/2$.

4.2 Relations with (Binary) Coding Theory

We will now discuss the relation of the Eisenstein polynomials with coding theory. These Eisenstein polynomials will occur, up to a constant, as "average weight enumerators" in the space of all weight enumerators of doubly even binary codes. We will first start by recalling some basic concepts from coding theory.

Definition 4.7. A *code* is a binary linear code, i.e. a k-dimensional linear subspace of $\mathbb{F}_2^n$, denoted by $[n, k, d]$, where $d = \min\{\mathrm{wt}(c) \mid c \in C\}$ is the minimal weight of the code. Here, the weight $wt(c)$ is defined to be the number of non-zero components in $c \in \mathbb{F}_2^n$. Furthermore, we define the *dual code* $C^\perp = \{x \in \mathbb{F}_2^n \mid \langle x, y\rangle = 0 \text{ for all } y \in C\}$. A code is called *doubly even* if the weights of all the codes are divisible by 4.

To a code C of length N we can associate a weight polynomial:

$$W_C(x, y) := \sum_{c \in C} x^{N-wt(c)} y^{wt(c)}. \tag{70}$$

The coefficient of $x^{N-i}y^i$ gives the number of codewords of weight i. We can extend this definition to a g-weight polynomial in 2^g variables. For $a \in \mathbb{F}_2^g$ we define a *generalized weight function* w_a on $C \times C \times ... \times C \subset (\mathbb{F}_2^N)^g$ as

$$w_a(\alpha_1, ..., \alpha_g) = |\{i \ : \ a = (\alpha_1(i), ..., \alpha_g(i)\}|,$$

where $\alpha_j(i)$ denotes the i-th component of α_j. Then we define the *g-weight polynomial* as

$$P_g(C)(x_a; a \in \mathbb{F}_2^g) := \sum_{\alpha_1,...,\alpha_g \in C} \prod_{a \in \mathbb{F}_2^g} x_a^{w_a(\alpha_1,...,\alpha_g)},$$

where the x_a are formal variables, so we consider $P_g(C)$ as a polynomial in $\mathbb{C}[x_a \ : \ a \in \mathbb{F}_2^g]$. Note that the 1-weight polynomial coincides with (70). Let $\epsilon = (1+i)/\sqrt{2} \cdot I_{2^g} \in GL_{2^g}(\mathbb{C})$ and define

$$G_g := \langle H_g, \epsilon \rangle,$$

to be the group generated by H_g and ϵ.

Theorem 4.8 ([36, Theorem 3.6.])**.** *The ring $\mathbb{C}[x_a : a \in \mathbb{F}_2^g]^{G_g}$ is the ring of g-weight polynomials corresponding to self dual doubly even codes.*

If $l \equiv 0 \pmod 8$, the Eisenstein polynomial $\varphi_l^{H_g}$ lies in $\mathbb{C}[x_a \ : \ a \in \mathbb{F}_2^g]^{G_g}$, as $\varphi_l^{H_g}$ is invariant under ϵ in that case.

Lemma 4.9 (Runge, Nebe and Rains, [26, Theorem 6.3.])**.** *For any doubly even binary code C of length $N \equiv 0 \pmod 8$ containing $\mathbf{1}_N$ and of dimension $N/2 - r$,*

$$\frac{1}{|G_g|} \sum_{\sigma \in G_g} \sigma \cdot P_g(C) = \prod_{0 \le i < r} (2^m + 2^i)^{-1} \sum_{C'} P_g(C'), \tag{71}$$

where the sum is over all doubly even self dual codes C' containing C.

The idea is to apply this theorem to $C = \langle \mathbf{1}_N \rangle$, the $\mathbb{F}_2$-vector space generated by $\mathbf{1}_N$, where $\mathbf{1}_N$ is the all-one vector of length N.

Lemma 4.10. *Any self dual code C contains the all-one vector.*

Proof. As $\langle c, c\rangle \equiv 0 \pmod 2$, wee see that c has even weight. As $\langle x, \mathbf{1}_N\rangle \equiv \mathrm{wt}(c) \equiv 0 \pmod 2$, it follows that C contains the all-one vector. □

Theorem 4.11. *Suppose $N \equiv 0 \pmod 8$,*

$$\varphi_N^{H^g} = \frac{N!}{2^g \prod_{0\le i<N/2-1}(2^m + 2^i)} \sum_{[C]} \frac{1}{|\mathrm{Aut}(C)|} P_g(C),$$

where the sum is over all doubly even self dual codes C of length N up to isomorphism.

Proof. Let C be the code generated by the all one vector of length N, $\mathbf{1}_N$. We have

$$P_g(C) = \sum_{a\in\mathbb{F}_2^g} x_a^N.$$

As the g-weight enumerator of any code containing $\mathbf{1}_N$ is invariant under permutation, it follows from theorem 4.9 and 4.10, that the group G_g contains all permutations of the variables, we therefore see that

$$\sum_{\sigma\in G_g} \sigma P_g(C) = 2^g \varphi_N^{H^g}.$$

Using 4.9 we have

$$\sum_{\sigma\in G_g} \sigma P_g(C) = \prod_{0\le i<N/2-1} (2^g + 2^i) \sum_{C'} P_g(C'),$$

where the sum is over all self dual doubly even codes, see lemma 4.10. We find

$$\begin{aligned}
\frac{1}{|G_g|} \sum_{\sigma\in G_g} \sigma P_g(C) &= \prod_{0\le i<N/2-1} (2^g + 2^i)^{-1} \sum_{C'} P_g(C'), \\
&= \prod_{0\le i<N/2-1} (2^g + 2^i)^{-1} \sum_{[C']} \frac{N!}{|\mathrm{Aut}(C')|} P_g(C'), \\
&= N! \prod_{0\le i<N/2-1} (2^g + 2^i)^{-1} \sum_{[C']} \frac{1}{|\mathrm{Aut}(C')|} P_g(C').
\end{aligned}$$

□

The previous result shows that Eisenstein polynomials are, up to a constant, equal to the "average weight enumerator" of the doubly even self dual codes if $l \equiv 0 \pmod 8$.

Example 4.12. Suppose $N = 8$ and $g = 1$. The only doubly even self dual codes of length 8 is the $[8, 4, 4]$ Hamming code C. As $|\mathrm{Aut}(C)| = 1344$ and $P_1(C) = x_0^8 + x_0^4 x_1^4 + x_1^8$, see [8, p. 80]). We compute using corollary 4.11:

$$\varphi_8^{H_1} = \frac{5}{24}(x_0^8 + 14 x_0^4 x_1^4 + x_1^8).$$

4.3 Eisenstein polynomials for $g = 1$

From now on, we will be only considering the case $g = 1$. In this case the group H_1 is:

$$H_1 = \left\langle \frac{1}{2}\begin{pmatrix} 1+i & 1+i \\ 1+i & -1-i \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\rangle,$$

This is a group of order 96, using (66). Note that in this case the theta functions as in 69 are

$$\theta_0(\tau) = \sum_{n\in\mathbb{Z}} q^{n^2},$$
$$\theta_1(\tau) = q^{1/4}\sum_{n\geq 0} q^{n(n+1)},$$

where $q = e^{2\pi i\tau}$. We have the following structural theorem for the ring of invariant polynomials (note the similarity with the ring of modular forms):

Theorem 4.13 ([25, p. 3.])**.** $\mathbb{C}[x_0,x_1]^{H_1} = \mathbb{C}[\varphi_8^{H_1}(x_0,x_1), \varphi_{12}^{H_1}(x_0,x_1)]$*, and* $\varphi_8^{H_1}(x_0,x_1), \varphi_{12}^{H_1}(x_0,x_1)$ *are algebraically independent.*

Explicitly, we have

$$\varphi_8^{H_1} = \frac{5}{24}(x_0^8 + 14x_0^4x_1^4 + x_1^8), \tag{72}$$
$$\varphi_{12}^{H_1} = \frac{5}{32}(x_0^{12} - 33x_0^4x_1^8 - 33x_0^4x_1^8 + x_1^{12}). \tag{73}$$

Remark 4.14. From 4.13 and the formulas (72), (73) it follows that $\varphi_l^{H_1} \equiv 0$ if $l = 4$ or $l \not\equiv 0 \pmod 4$. Further, it follows from 4.13 and 4.5 that the map Th_g is an isomorphism if $g = 1$.

We find the following explicit formula for the polynomials $\varphi_l^{H_1}$.

Proposition 4.15. *If* $l \equiv 0 \pmod 4$ *and* $l \neq 4$*, we have*

$$\varphi_l^{H_1} = \frac{2^{\frac{4-l}{2}}(-1)^{l/4}+1}{6}x_0^l + \frac{2^{\frac{4-l}{2}}(-1)^{l/4}+1}{6}x_1^l + \frac{2^{\frac{2-l}{2}}}{3}(-1)^{l/4}\sum_{\substack{j\equiv 0 \pmod 4,\\ 0<j<l}} \binom{l}{n} x_0^j x_1^{l-j}.$$

Proof. We prove this formula by explicitly computing σx_0 for all $\sigma \in H_1$. Recall that if $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we have $\sigma x_0 = ax_0 + cx_1$. As H_1 is a finite group, one can compute all the possible pairs (a,c). As $l \equiv 0 \pmod 4$, we find:

$$\varphi_l^{H_g} = \frac{1}{96}\Big(16x_0^l + 16\big((\tfrac{1}{2}i+\tfrac{1}{2})x_0 + (\tfrac{1}{2}i+\tfrac{1}{2})x_1\big)^l + 16\big((\tfrac{1}{2}i+\tfrac{1}{2})x_0 + (\tfrac{1}{2}i-\tfrac{1}{2})x_1\big)^l$$
$$+ 16\big((\tfrac{1}{2}i+\tfrac{1}{2})x_0 + (-\tfrac{1}{2}i+\tfrac{1}{2})x_1\big)^l + 16\big((\tfrac{1}{2}i+\tfrac{1}{2})x_0 + (-\tfrac{1}{2}i-\tfrac{1}{2})x_1\big)^l + 16x_1^l\Big).$$

Using the binomial theorem, we derive

$$\varphi_l^{H_1} = \frac{2^{\frac{4-l}{2}}(-1)^{l/4}+1}{6}x_0^l + \frac{2^{\frac{4-l}{2}}(-1)^{l/4}+1}{6}x_1^l + \frac{2^{\frac{2-l}{2}}}{3}(-1)^{l/4}\sum_{\substack{j\equiv 0 \pmod 4,\\ 0<i<l}} \binom{l}{n} x_0^j x_1^{l-j}. \tag{74}$$

□

For notational purposes, normalize $\varphi_l^{H_1}$ such that the coefficient of x_0^l is 1, write

$$\widetilde{\varphi}_l^{H_1} := \frac{6}{2^{\frac{4-l}{2}}(-1)^{l/4}+1}\varphi_l^{H_1}. \tag{75}$$

We can consider the modular form $Th_1(\tilde{\varphi}_l^{H_1})$. As the forms θ_0^2, θ_1^2 have weight a 1 for the congruence subgroup $\Gamma(2)$, it is clear that $Th_k := Th_1(\tilde{\varphi}_l^{H_1})$ is a modular form of weight $k = \frac{l}{2}$ for the full modular group.

Example 4.16. It is easy to see that $Th_4 = E_4$ and $Th_6 = E_6$.

$$Th_{12} = E_4^3 - 518784/1025\Delta;$$
$$Th_{16} = E_4^4 - 97280/113\Delta E_4;$$
$$Th_{20} = E_4^5 - 121472/109\Delta E_4^2;$$
$$Th_{24} = E_4^6 - 1126806528/838861 E_4^3\Delta + 358849019904/4194305\Delta^2.$$

The modular forms Th_k and the Eisenstein series are conjectured to have some analogous properties.

Conjecture 4.17 ([25, Conjecture 1.1.])**.** All the zeros of $Th(\varphi_l)$ in the fundamental domain lie on the unit circle $\{e^{i\theta} \mid \theta \in [\pi/2, 2\pi/3]\}$.

4.4 Power Sums of Th_k

Using the method of R.A. Rankin, we will try to compute the power sums of the j-invariants of the zeros of Th_k. Using formula (47), we have that

$$kg_v/12 = r_\infty\left(j^v\frac{Th_k'}{Th_k}\right) + S\left(j^v\frac{Th_k'}{Th_k}\right), \tag{76}$$

where the derivative is taken with respect to $\frac{1}{2\pi i}\tau$. We now compute the value of $r_\infty\left(j^v\frac{Th_k'}{Th_k}\right)$ and we will show this value is $O(1)$ as k increases.

Proposition 4.18. *For a fixed $v \geq 0$,*

$$r_\infty\left(j^v\frac{Th_k'}{Th_k}\right) = 2k\cdot r_\infty\left(j^v\frac{\theta_0'}{\theta_0}\right) + o(1),$$

as k increases.

Proof. For $n \in \mathbb{N}$ fixed let $a_{n,k}$, b_n be the n-th Fourier coefficients of Th_k and θ_0 respectively. Since θ_1^4 is a cusp form, we have

$$Th_k = \theta_0^{2k} + \frac{(-1)^{k/2}}{(-1)^{k/2}+2^{k-2}}\sum_{0<j<n, j\equiv 0 \pmod 4}\binom{2k}{n}\theta_1^j\theta_0^{2k-j} + O(q^n). \tag{77}$$

As

$$\lim_{k\to\infty}\frac{(-1)^{k/2}}{(-1)^{k/2}+2^{k-2}}\binom{2k}{n} = 0,$$

it is clear that $\lim_{k\to\infty} a_{n,k} = b_n$. Hence we see that

$$2k\cdot r_\infty\left(j^v\frac{\theta_0'}{\theta_0}\right) = r_\infty\left(j^v\frac{(\theta_0^{2k})'}{\theta_0^{2k}}\right) = r_\infty\left(j^v\frac{Th_k'}{Th_k}\right) + o(1).$$

□

As in the case of Eisenstein series, the values of $r_\infty\left(j^v\theta_0'/\theta_0\right)$ are strongly related to hypergeometric functions, as we will we see in the next paragraph. Using 4.18 we have

$$\sum_{i=1}^{n_k} j(x_i)^v = kg_v/12 - r_\infty\left(j^v\frac{Th_k'}{Th_k}\right) - \frac{a_k}{2}1728^v, \tag{78}$$

$$= kg_v/12 - 2k\cdot r_\infty\left(j^v\frac{\theta_0'}{\theta_0}\right) - \frac{a_k}{2}1728^v + o(1), \tag{79}$$

as n_k increases. Write

$$Th_k = \Delta^{n_k} E_4^{b_k} E_6^{a_k} Q_k(j),$$

where $k = 12n_k + 6a_k + 4b_k$, $n_k \in \mathbb{Z}_{\geq 0}, a_k \in \{0,1\}$ and $b_k \in \{0,1,2\}$. Then Q_k is a monic polynomial of degree n_k with rational coefficients in the j-invariant. We have that (78) implies that the power sums of the n_k roots of $Q_k(j)$ increases linearly as n_k increases.

Example 4.19.

$$\begin{aligned}
Q_{12}(X) &= X - \frac{518784}{1025};\\
Q_{24}(X) &= X^2 - \frac{1126806528}{838861}X + \frac{358849019904}{4194305};\\
Q_{36}(X) &= X^3 - \frac{6926919963264}{3435973837}X^2 + \frac{2652630646063104}{3435973837}X - \frac{248220139256807424}{17179869185}.
\end{aligned}$$

The result (78) implies, for example, that the X^{n-1} coefficient of $Q_{12n}(X)$ is approximately $-672 \cdot n$.

4.5 Hankel Determinants of the Forms Th_k

As with the Eisenstein series we can consider the Hankel determinant corresponding to the power sums of Q_k. If this Hankel determinant $\widetilde{\Delta}_n$ were negative for some $n \in \mathbb{N}$, we would conclude that Q_k has non-real roots. However, we will show that this determinant $\widetilde{\Delta}_n$ is always positive. As $n_k \to \infty$ we have that for $k \equiv 0 \pmod 4$,

$$S\left(j^v \frac{Th_k'}{Th_k}\right) = kg_v/12 - 2k \cdot r_\infty\left(j^v \frac{\theta_0'}{\theta_0}\right) + o(1), \tag{80}$$

see (78). Now let

$$h_v := g_v - 24 \cdot r_\infty\left(j^v \frac{\theta_0'}{\theta_0}\right),$$

we are interested in the sign of the Hankel determinant:

$$\widetilde{\Delta}_n = \begin{vmatrix} h_0 & h_1 & h_2 & \dots & h_n \\ h_1 & h_2 & h_3 & \dots & h_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_n & h_{n+1} & h_{n+2} & \dots & h_{2n} \end{vmatrix}. \tag{81}$$

We will show that for $n > 1$:

$$\widetilde{\Delta}_n = 2^{4n^2+5n} \cdot 3^{n^2} \cdot 11^n \cdot 23^n \cdot \prod_{r=2}^{n} \left(\frac{(24r-29)(24r-17)(24r-1)(24r-13)}{(8r-5)^2(8r-9)(8r-1)}\right)^{n-r+1}, \tag{82}$$

so that $\widetilde{\Delta}_n > 0$. Note the resemblance with the Hankel determinant in proposition 3.50.

As with the values g_v in section 3.9, the values h_v induce a symmetric bilinear form on the space of real polynomials. Let

$$(f(X), g(X))_T := \text{constant term in the } q\text{-expansion of } f(j)g(j)\left(E_2 - 24\frac{\theta_0'}{\theta_0}\right),$$

where j is the modular j-invariant. Clearly, $h_v = (X^v, 1)_T$.

Example 4.20.

$$h_0 = 1;\ h_1 = 672;\ h_2 = 840192;\ h_3 = 1193164800;\ h_4 = 1790864130048;$$

We will prove (82) as follows:

- We will show that $(\ ,\ )_T$ defines an inner product on $\mathbb{R}[X]$, using some numerical analysis.
- We will compute the continued fraction expansion of the moment generating function

  $$\psi(X) = h_0 + h_1 X + h_2 X^2 + ...,$$

  using hypergeometric functions.
- Using 3.49, we will compute the determinant $\widetilde{\Delta}_n$ using this continued fraction expansion.

4.5.1 $(\ ,\ )_T$ is an Inner Product

From now on let

$$H(\tau) := E_2 - 24\frac{\theta_0'}{\theta_0},$$

we can rewrite H in the following way:

Lemma 4.21. *For all $\tau \in \mathbb{H}$,*

$$H(\tau) = E_2(\tau) + 2E_2(2\tau) - 2E_2(\tau + \tfrac{1}{2}). \tag{83}$$

Proof. This follows from the Jacobi triple product identity [21]: For $q, y \in \mathbb{C}$, $|q| < 1$ and $y \neq 0$, we have the identity

$$\prod_{m=1}^{\infty}(1-q^{2m})(1+q^{2m-1}y^2)\left(1+\frac{q^{2m-1}}{y^2}\right) = \sum_{n=-\infty}^{\infty} q^{n^2}y^{2n}. \tag{84}$$

For $y = 1$, this gives

$$\theta_0 = \prod_{m=1}^{\infty}(1-q^{2m})(1+q^{2m-1})^2. \tag{85}$$

Now taking the logarithmic derivative with respect to $\frac{1}{2\pi i}\tau$, gives

$$\frac{\theta_0'}{\theta_0} = -\sum_{m=1}^{\infty}\frac{2mq^{2m}}{1-q^{2m}} + 2\sum_{m=1}^{\infty}\frac{(2m-1)q^{2m-1}}{1+q^{2m-1}} \tag{86}$$

$$= -2\sum_{m=1}^{\infty}\frac{mq^{2m}}{1-q^{2m}} - 2\left(\sum_{k=1}^{\infty}\frac{k(-q)^k}{1-(-q)^k} - \sum_{n=1}^{\infty}\frac{2n(-q)^{2n}}{1-(-q)^{2n}}\right) \tag{87}$$

$$= -\tfrac{1}{12}(E_2(2\tau)-1) + \tfrac{1}{12}(E_2(\tau+\tfrac{1}{2})-1), \tag{88}$$

using the identity

$$E_k = 1 + \frac{2}{\zeta(1-k)}\sum_{n=1}^{\infty}\frac{n^{k-1}q^n}{1-q^n},$$

we conclude that $H(\tau) = E_2(\tau) + 2E_2(2\tau) - 2E_2(\tau + \frac{1}{2})$.

□

Lemma 4.22. *The following linear functionals on $\mathbb{R}[x]$ coincide:*

1. $(f(X), g(X))_T$;
2. $(f(X), g(X)) :=$ constant term as Laurent series in j^{-1} of $f(j)g(j)\frac{E_4(\tau)}{E_6(\tau)}H(\tau)$;
3. $(f(X), g(X)) := \int_{\pi/3}^{\pi/2} f(j(e^{i\alpha}))g(j(e^{i\alpha}))W(\alpha)d\alpha$;

where $W(\alpha) = i(H(-e^{-i\alpha})e^{-i\alpha} - e^{i\alpha}H(e^{\alpha}))d\alpha$.

Proof. We first start proving 1 implies 2. Write a_0 for the constant term in the q-expansion of $f(j)g(j)H(\tau)$. By the residue formula

$$a_0 = \frac{1}{2\pi i}\oint_C f(j)g(j)H(\tau)\frac{dq}{q},$$

for some small enough circle around $q = 0$. Further as

$$q\frac{d}{dq}j = -j\frac{E_6}{E_4}$$

we see that

$$a_0 = \frac{1}{2\pi i}\oint_C f(j)g(j)H(\tau)\frac{E_4}{E_6}\frac{d(1/j)}{1/j},$$

hence the result follows using the residue theorem.

For 1 implies 3, note that we have

$$\oint_C f(j)g(j)H(\tau)\frac{dq}{q} = \int_{-0.5+a\cdot i}^{0.5+a\cdot i} f(j)g(j)H(\tau)d\tau$$

for some $a > 1$. Now using the residue formula, the sum of integrals over the horizontal part $\{0.5 + a\cdot i \mid |a| \leq 1/2\}$, the vertical parts $\mathrm{Re}(\tau) = \pm 1/2$ and the circular part of the fundamental domain equals zero. As $f(j)g(j)H(\tau)$ is 1-periodic, the sum of integrals over the vertical parts vanishes. Hence we find

$$\int_{-0.5+a\cdot i}^{0.5+a\cdot i} f(j)g(j)Hd\tau = \int_{2\pi/3}^{\pi/3} f(j(e^{i\alpha}))g(j(e^{i\alpha}))H(e^{i\alpha})d\tau,$$

where $\tau = e^{i\theta}$. As $f(j(\tau))g(j(\tau))$ is invariant under the action $\tau \mapsto -\frac{1}{\tau}$, we find

$$\begin{aligned}\int_{2\pi/3}^{\pi/3} f(j(\tau))g(j(\tau))H(\tau)d\tau &= \int_{2\pi/3}^{\pi/2} f(j(\tau))g(j(\tau))H(\tau)d\tau - \int_{\pi/3}^{\pi/2} f(j(\tau))g(j(\tau))H(\tau)d\tau \\ &= \int_{\pi/3}^{\pi/2} f(j(\tau))g(j(\tau))\left(H\left(\frac{-1}{\tau}\right)\frac{1}{\tau^2} - H(\tau)\right)d\tau.\end{aligned}$$

As $d\tau = i\tau d\alpha$, we derive the desired result. □

We would like to show that this linear functional is positive definite and therefore defines an inner product on $\mathbb{R}[X]$. As $(f(X), f(X)) = \int_{\pi/3}^{\pi/2} f(j(e^{i\alpha}))^2 i\left(H(-e^{-i\alpha})e^{-i\alpha} - H(e^{i\alpha})e^{i\alpha}\right)d\alpha$, it suffices to show that

$$i\left(H(-e^{-i})e^{-i\alpha} - H(e^{i\alpha})e^{i\alpha}\right) > 0$$

on $(\pi/3, \pi/2)$. We will prove this using the following two lemma's:

Lemma 4.23. *For $\tau = e^{i\theta}$ with $\theta \in (\pi/3, \pi/2)$, we have*

$$i\left(E_2\left(2\frac{-1}{\tau}\right)\frac{1}{\tau} - E_2(2\tau)\tau\right) > \frac{3}{\pi} + 0.77.$$

Proof. We use the transformation law for E_2:

$$E_2\left(\frac{-1}{\tau}\right) = \frac{6}{\pi i}\tau + \tau^2 E_2(\tau),$$

to find

$$E_2\left(2\frac{-1}{\tau}\right) = E_2\left(\frac{-1}{\tau/2}\right) = \frac{3}{\pi i}\tau + \frac{\tau^2}{4}E_2(\tau/2). \tag{89}$$

So that

$$i\left(E_2\left(2\frac{-1}{\tau}\right)\frac{1}{\tau} - E_2(\tau)\tau\right) = \frac{3}{\pi} + \frac{i}{4}\tau\left(E_2(\tau/2) - 4E_2(2\tau)\right). \tag{90}$$

We will show that $G(\tau) := \frac{i}{4}\tau\left(E_2(\tau/2) - 4E_2(2\tau)\right) > 0.77$ for $\theta \in (\pi/3, \pi/2)$. Write $E_2(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i \tau n}$. Using *Mathematica* one can show that

$$\mathrm{Re}\left(G_N(\tau)\right) > .776, \tag{91}$$

where $G_N(\tau) := \frac{i}{4}\tau\sum_{n=1}^{N} a_n(e^{\pi i\tau n} - 4e^{4\pi i\tau n})$ and $N = 100$. Further we find that

$$|\mathrm{Re}(G(\tau)) - \mathrm{Re}(G_N(\tau))| \le \frac{1}{4}\sum_{n=N+1}^{\infty}|a_n|e^{-\pi\frac{1}{2}\sqrt{3}n} + \sum_{n=N+1}^{\infty}|a_n|e^{-2\pi\sqrt{3}n} \tag{92}$$

As $|a_n| = 24\sigma_0(n) \le 24n$, we have

$$|\mathrm{Re}(G(\tau)) - \mathrm{Re}(G_N(\tau))| \le \frac{1}{4}\int_N^{\infty} 24ne^{-\pi\frac{1}{2}\sqrt{3}n}dn + \int_N^{\infty} 24ne^{-2\pi\sqrt{3}n}dn. \tag{93}$$

$$< 10^{-115}. \tag{94}$$

Hence $G(\tau) = \mathrm{Re}(G(\tau)) > 0.77$. □

Lemma 4.24. *For $\tau = e^{i\theta}$ with $\theta \in (\pi/3, \pi/2)$, we have*

$$F(\tau) := i\left(E_2\left(\frac{-1}{\tau} + \frac{1}{2}\right)\frac{1}{\tau} - E_2(\tau + \frac{1}{2})\tau\right) < 2.1$$

Proof. Using a computer algebra system one can show that

$$\mathrm{Re}(F_N(\tau)) < 2.09, \tag{95}$$

where

$$F_N(\tau) = i\left(\frac{1}{\tau}\sum_{n=0}^{N} a_n e^{2\pi i(\frac{-1}{\tau}+\frac{1}{2})n} - \tau\sum_{n=0}^{N} a_n e^{2\pi i(\tau+\frac{1}{2})n}\right)$$

and $N = 100$, using the same notation as in the proof of the previous lemma. Further we see that

$$\begin{aligned}|\mathrm{Re}(F(\tau)) - \mathrm{Re}(F_N(\tau))| &\le 2\sum_{n=N+1}|a_n|e^{-\pi\sqrt{3}} \\ &< 2\int_N^{\infty} 24ne^{-\pi\sqrt{3}n}dn \\ &< 10^{-233}.\end{aligned}$$

We conclude that $F(\tau) = \mathrm{Re}(F(\tau)) < 2.1$. □

Corollary 4.25. *The linear functional* $(\ ,\ )_T$ *is positive definite, hence defines an inner product on* $\mathbb{R}[X]$.

Proof. Using lemmas 4.23, 4.24 and the fact that $i(E_2(\frac{-1}{\tau})\frac{1}{\tau} - E_2(\tau)\tau) = \frac{6}{\pi}$, we deduce that

$$i\left(H\left(\frac{-1}{\tau}\right)\frac{1}{\tau} - H(\tau)\tau\right) > \frac{12}{\pi} - 2.66 > 0. \tag{96}$$

Hence it defines an inner product. □

4.5.2 The Moment Generating Function

We want to compute the continued fraction of the moment generating function with respect to $(\ ,\ )_T$, i.e. we want to compute the λ_i such that

$$\Psi(z) := h_0 + h_1 z + h_2 z^2 + ... = \cfrac{\lambda_0}{1 - \cfrac{\lambda_1 z}{1 - \cfrac{\lambda_2 z}{1 - \cfrac{\lambda_3 z}{1 - ...}}}}. \tag{97}$$

Write $H(\tau)\frac{E_4(\tau)}{E_6(\tau)}$ locally as a power series in $1/j$. Using characterization 2 in lemma 4.22 of $(\ ,\ )_T$, we see that

$$\Psi\left(\frac{1}{j}\right) = H(\tau)\frac{E_4(\tau)}{E_6(\tau)}, \tag{98}$$

as a power series in $1/j$. We will relate $H(\tau)E_4(\tau)/E_6(\tau)$ to a fraction of hypergeometric functions. We start with the following lemma.

Lemma 4.26. *We have*

$$\theta_0^{24} = \Delta \cdot j \cdot {}_2F_1\Big(\frac{-1}{24}, \frac{7}{24}, \frac{3}{4}; \frac{1728}{j}\Big)^{24}, \tag{99}$$

as a power series in $1/j$.

Proof. The function $F(z) = {}_2F_1\left(\frac{-1}{24}, \frac{7}{24}, \frac{3}{4}; z\right)$ is the unique holomorphic solution around $z = 0$ having $F(0) = 1$ of the differential equation:

$$z(z-1)\frac{d^2F}{dz^2} + (\tfrac{5}{4}z - \tfrac{3}{4})\frac{dF}{dz} - \frac{7}{576}F = 0. \tag{100}$$

We will show that $G(\tau) := \frac{\theta}{\eta} \cdot j^{-\frac{1}{24}}$ satisfies this differential equation as a function in $z = \frac{1728}{j}$, where

$$\eta = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1 - q^n)$$

and $\eta^{24} = \Delta$. As $\frac{dz}{d\tau} = z\frac{E_6}{E_4}$ we get

$$\frac{dF}{dz} = \frac{1}{z}\frac{E_4}{E_6}\frac{dF}{d\tau}, \tag{101}$$

$$\frac{d^2F}{dz^2} = \frac{E_4}{E_6}\frac{1}{z^2}\Big(-\frac{4}{3} - \frac{1}{6}\frac{E_2E_4}{E_6} + \frac{1}{2}\frac{E_4^3}{E_6^2}\Big)\frac{dF}{d\tau} + \frac{1}{z^2}\frac{E_4^2}{E_6^2}\frac{d^2F}{d\tau^2}. \tag{102}$$

By substituting the above equations and dividing out

$$\frac{1}{z}\frac{E_4}{E_6},$$

the differential equation (100) becomes

$$(z-1)\frac{E_4}{E_6}\frac{d^2F}{d\tau^2}+\left(\frac{5}{4}z-\frac{3}{4}+S\cdot(z-1)\right)\frac{dF}{d\tau}-z\frac{E_6}{E_4}\frac{7}{576}F=0,$$

where $S=-\frac{4}{3}-\frac{1}{6}\frac{E_2E_4}{E_6}+\frac{1}{2}\frac{E_4^3}{E_6^2}$. As we have

$$\theta_0=\frac{\eta^5(2\tau)}{\eta^2(\tau)\eta^2(4\tau)},$$

an easy computation (using that $\eta'=\frac{1}{24}E_2\eta$) shows that

$$\frac{dG}{d\tau}=G\cdot T,$$
$$\frac{d^2G}{d\tau^2}=G\cdot(T^2+T'),$$

where

$$T(\tau)=\frac{5}{12}E_2(2\tau)-\frac{1}{8}E_2(\tau)-\frac{1}{3}E_2(4\tau)+\frac{1}{24}\frac{E_6}{E_4}.$$

If we substitute G in the left side of (100), we find

$$\begin{aligned}(z-1)\frac{E_4}{E_6}\frac{d^2G}{d\tau^2}+(\tfrac{5}{4}z-\tfrac{3}{4}+S\cdot(z-1))\frac{dG}{d\tau}-z\frac{E_6}{E_4}\frac{7}{576}G=\frac{1}{FE_4^4E_6^2}[(1728\Delta E_4^2-E_4^5)E_6(T^2+T')\\+\left(\tfrac{5}{4}\cdot 1728\cdot E_4\Delta E_6^2-\tfrac{3}{4}E_4^4E_6^2+1728\Delta E_4(-\tfrac{4}{3}E_6^2-\tfrac{1}{6}E_2E_4E_6+\tfrac{1}{2}E_4^3)\right.\\\left.+E_4^4\left(\tfrac{4}{3}E_6^2-\tfrac{1}{6}E_2E_4E_6+\tfrac{1}{2}E_4^3\right)\right)T-1728\frac{7}{576}\Delta E_6^3].\end{aligned}$$

The expression inside the brackets "[ ]" is a quasimodular form (i.e. an "almost holomorphic modular form", see [6, §5.3.] for definitions) of weight $k=30$ for the congruence subgroup $\Gamma=\Gamma_0(4)$, as any term is the (second order) derivative of a modular form for $\Gamma_0(4)$. An easy computation shows that the term in brackets is $\mathcal{O}(q^{100})$, and an explicit computation of the space of quasimodular forms of weight k for Γ gives that the term in brackets must be identically equal to zero, showing that G satisfies the correct differential equation. Hence we see that as a power series in $1/j$,

$$\frac{\theta_0}{\eta}j^{-\frac{1}{24}}={}_2F_1\left(\frac{-1}{24},\frac{7}{24},\frac{3}{4};\frac{1728}{j}\right). \tag{103}$$

We deduce that

$$\theta_0^{24}=\Delta\cdot j\cdot {}_2F_1\left(\frac{-1}{24},\frac{7}{24},\frac{3}{4};\frac{1728}{j}\right)^{24}, \tag{104}$$

as a power series in $1/j$. □

Lemma 4.27. *Let ${}_2F_1(a,b,c;z)$ be a hypergeometric function, then*

$$\frac{{}_2F_1(a+1,b,c;z)}{{}_2F_1(a,b,c;z)} = \cfrac{1}{1-\cfrac{\lambda_1 z}{1-\cfrac{\lambda_2 z}{1-\cfrac{\lambda_3 z}{1-...}}}},$$

where $\lambda_1 = \frac{b}{c}$ and for $n>0$, $\lambda_{2n} = \frac{(a+n)(c-b+n-1)}{(c+2n-2)(c+2n-1)}$ and $\lambda_{2n+1} = \frac{(c-a+n-1)(b+n)}{(c+2n)(c+2n-1)}$.

Proof. We will use $F(a,b,c)$ as shorthand for ${}_2F_1(a,b,c;z)$. Using the contiguous relations (152) and (153) we have

$$F(a+1,b,c) - F(a,b,c) = z\frac{b}{c}F(a+1,b+1,c+1). \tag{105}$$

So that

$$\frac{F(a+1)}{F} = \frac{1}{1-\frac{b}{c}zF(a+1,b+1,c+1)},$$

hence $\lambda_1 = \frac{b}{c}$. Further, using the relations (152), (157) and (158) we have

$$F(a+1) - F(a+1,b+1,c+1) = \frac{(a+1)(b-c)}{c(c+1)}zF(a+2,b+1,c+2). \tag{106}$$

Using the relations (152), (153) and (155), we find

$$F(a+1,b+1,c+1) - F(a+2,b+1,c+2) = \frac{(a-c)(b+1)}{(c+2)(c+1)}zF(a+2,b+2,c+3). \tag{107}$$

In general we have

$$F(a+n,b+n-1,c+2n-2) - F(a+n,b+n,c+2n-1) = \frac{(a+n)(b-c-n+1)}{(c+2n-2)(c+2n-1)}zF(a+n+1,b+n,c+2n)$$

and

$$F(a+n,b+n,c+2n-1) - F(a+n+1,b+n,c+2n) = \frac{(a-c-n+1)(b+n)}{(c+2n)(c+2n-1)}zF(a+n+1,b+n+1,c+2n+1).$$

Hence we see that

$$\lambda_{2n} = -\frac{(a+n)(b-c-n+1)}{(c+2n-2)(c+2n-1)} = \frac{(a+n)(c-b+n-1)}{(c+2n-2)(c+2n-1)} \tag{108}$$

and

$$\lambda_{2n+1} = -\frac{(a-c-n+1)(b+n)}{(c+2n)(c+2n-1)} = \frac{(c-a+n-1)(b+n)}{(c+2n)(c+2n-1)}. \tag{109}$$

□

Proposition 4.28. $\lambda_0 = 1$, $\lambda_1 = 672$ *and for* $n > 0$ *we have*

$$\lambda_{2n} = \frac{48(24n-1)(24n-13)}{(8n-5)(8n-1)}$$

and

$$\lambda_{2n+1} = \frac{48(24n-5)(24n+7)}{(8n-1)(8n+3)}.$$

Proof. We are interested in the coefficients of

$$H(\tau)\frac{E_4}{E_6}$$

expressed as a power series in $z = 1/j$. First of all note that

$$\begin{aligned} H(\tau)\frac{E_4}{E_6} = \left(E_2 - 24\frac{\theta_0'}{\theta_0}\right)\frac{E_4}{E_6} &= \left(\frac{1}{2\pi i}\frac{d}{d\tau}\log\left(\frac{\Delta}{\theta_0^{24}}\right)\right)\frac{E_4}{E_6} \\ &= z\frac{d}{dz}\log\left(\frac{\Delta}{\theta_0^{24}}\right), \end{aligned}$$

here we use that $j' = -jE_6/E_4$. Using 4.26 we have

$$z\frac{d}{dz}\log\left(\frac{\Delta}{\theta_0^{24}}\right) = -z\left(-\frac{1}{z} + 24\frac{\frac{d}{dz}{}_2F_1(\frac{-1}{24},\frac{7}{24},\frac{3}{4};1728z)}{{}_2F_1(\frac{-1}{24},\frac{7}{24},\frac{3}{4};1728z)}\right).$$

Using (153), we find

$$\frac{d}{dz}{}_2F_1\left(\frac{-1}{24},\frac{7}{24},\frac{3}{4};1728z\right) = -\frac{1728}{24}\left({}_2F_1\left(\frac{23}{24},\frac{7}{24},\frac{3}{4};1728z\right) - {}_2F_1\left(-\frac{1}{24},\frac{7}{24},\frac{3}{4};1728z\right)\right).$$

We conclude that

$$H(\tau)\frac{E_4}{E_6} = \frac{{}_2F_1(\frac{23}{24},\frac{7}{24},\frac{3}{4};1728z)}{{}_2F_1(-\frac{1}{24},\frac{7}{24},\frac{3}{4};1728z)},$$

as a power series in $z = 1/j$. The values for λ_i now follow from lemma 4.27. □

Using (63) and proposition 4.28, we find

Theorem 4.29. *For* $n > 1$*:*

$$\widetilde{\Delta}_n = 2^{4n^2+5n}\cdot 3^{n^2}\cdot 11^n\cdot 23^n\cdot\prod_{r=2}^{n}\Big(\frac{(24r-29)(24r-17)(24r-1)(24r-13)}{(8r-5)^2(8r-9)(8r-1)}\Big)^{n-r+1}. \quad (110)$$

Note that this determinant is positive for all $n > 0$, hence this theorem does not give any information on the location of the roots of Th_k.

Remark 4.30. As the h_i are all integers, it is clear that $\widetilde{\Delta}_n$ is integral. However, from (110) this is not immediately obvious.

Corollary 4.31. $v_p(\widetilde{\Delta}_n) = 0$ *if* $p > 24n - 1$.

4.6 Congruence Properties of Th_k

Consider the modular form Th_k and assume that $p = 2k - 1$ is a prime number (as $k \geq 4$, we have $p \geq 7$). In this section we discuss congruence properties of Th_k. We will show that the modular polynomial corresponding to Th_k factors as a product of distinct linear factors if $k \equiv 0, 4 \pmod{12}$ and conjecture it for $k \equiv 6, 10 \pmod{12}$.

We start with an easy lemma.

Lemma 4.32. *The modular form Th_k is p-integral, i.e. none of the denominators in the q-expansion are divisible by p, and $Th_k \equiv \theta_0 + O(q^{d_k}) \pmod{p}$ (by "mod p" we mean that we reduce all the coefficients in the Fourier expansion mod p) , where $d_k := \dim(M_k)$.*

Proof. Consider the denominator in (75), an easy computation shows that this denominator is given by $2^{k-2}(-1)^{k/2} + 1 = 2^{-1}2^{\frac{p-1}{2}}(-1)^{k/2} + 1$. We have $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$, and this implies

$$2^{-1}2^{\frac{p-1}{2}}(-1)^{k/2} + 1 \not\equiv 0,$$

as $2^{-1} \not\equiv \pm 1 \pmod{p}$. Furthermore if $n < p + 1$ we have $\binom{p+1}{n} \equiv 0 \pmod{p}$, showing that

$$\begin{aligned} Th_k &\equiv \theta_0^{2k} + \theta_1^{2k} \pmod{p} \\ &\equiv \theta_0\theta_0^p + \theta_1^{p+1} \pmod{p} \\ &\equiv \theta_0 + O(q^{d_k}) \pmod{p}, \end{aligned}$$

for the last line we use that $(p + 1)/4 \geq d_k$. □

Next, we write Θ_k for the unique modular form of weight k such that $\Theta_k = \theta_0 + \mathcal{O}(q^{d_k})$, and we let R_k be the monic polynomial in the j-invariant such that $\Theta_k = \Delta^{n_k}E_4^{b_k}E_6^{a_k}R_k(j)$. Using lemma 4.32, we see that $R_k(X) \equiv Q_k(X) \pmod{p}$ as polynomials in X.

Theorem 4.33. *For any $k \equiv 0, 4 \pmod{12}$, $R_k(X) \pmod{p}$ factors as a product of distinct linear factors in the j-invariant.*

Conjecture 4.34. Theorem 4.33 also holds if $k \equiv 6, 10 \pmod{12}$.

Example 4.35.

k	R_k	$R_k \pmod{p}$
12	$j - 18$	$j + 18$
16	$j - 958$	$j + 3$
22	$j - 454$	$j + 19$
24	$j^2 - 1438j + 123888$	$(j + 9)(j + 10)$
30	$j^2 - 934j + 44760$	$(j + 25)(j + 44)$
34	$j^2 - 1174j + 145800$	$(j + 44)(j + 55)$

Remark 4.36. Note that theorem 4.33 is the analogy of theorem 3.18.

In order to prove theorem 4.33, we will rewrite the polynomial $R_k(j)$ in terms of the modular λ-function and show, using hypergeometric properties, that this polynomial (as a polynomial in λ) will factor as a product of distinct linear factors.

We can express these polynomials in terms of hypergeometric functions in the following way: Let W_n^0 and W_n^1 be the unique polynomials of degree $n \geq 0$ such that:

$$j^n \cdot {}_2F_1\left(\frac{-1}{24}, \frac{7}{24}, \frac{3}{4}; \frac{1728}{j}\right) = W_n^0(j) + \mathcal{O}(1/j), \tag{111}$$

$$j^n \cdot {}_2F_1\left(\frac{11}{24}, \frac{19}{24}, \frac{3}{4}; \frac{1728}{j}\right) = W_n^1(j) + \mathcal{O}(1/j). \tag{112}$$

We can interpret the polynomials W_n^0 and W_n^1 as "the polynomial in j-part" of the left hand side of (111) and (112) respectively.

Lemma 4.37. *Let $k = \frac{p+1}{2}$ for a prime $p \geq 7$, then*

$$R_k(j) \equiv W_{n_k}^{a_k}(j) \pmod{p}. \tag{113}$$

Proof. Assume that $k \equiv 0 \pmod{12}$, we need to show that $\theta_0 \equiv \Delta^{n_k} W_{n_k}^0 \pmod{p, q^{n_k+1}}$ (this notation means that the Fourier coefficients should coincide modulo p, up to the coefficient of q^{n_k}). Using lemma 4.26 we have that

$${}_2F_1\left(\frac{-1}{24}, \frac{7}{24}, \frac{3}{4}, \frac{1728}{j}\right) = \theta_0 \cdot \Delta^{-1/24} \cdot j^{-1/24}.$$

First of all note that

$$\Delta^{n_k} \cdot W_{n_k}^0(j) \equiv \theta_0 \cdot \Delta^{n_k} \cdot j^{n_k - \frac{1}{24}} \Delta^{-\frac{1}{24}} \pmod{q^{n_k+1}}.$$

i.e. their q-expansions coincide up to q^{n_k+1}. Hence in order to show (113), it suffices to show

$$\theta_0 \equiv \theta_0 \Delta^{n_k - \frac{1}{24}} j^{n_k - \frac{1}{24}} \pmod{p, q^{n_k+1}}. \tag{114}$$

As

$$\Delta^{n_k - \frac{1}{24}} j^{n_k - \frac{1}{24}} = E_4^{\frac{p}{8}}$$

and

$$\left(E_4^{\frac{1}{8}}\right)^p \equiv 1 \pmod{p, q^p} \tag{115}$$

, we deduce that (114) holds (note that $p \geq n_k + 1$). For $k \equiv 4 \pmod{12}$ the proof is similar.

Now suppose $k \equiv 6 \pmod{12}$. Using proposition A.1, we have

$${}_2F_1\left(\frac{-1}{24}, \frac{7}{24}, \frac{3}{4}; z\right) = (1-z)^{\frac{1}{2}} \cdot {}_2F_1\left(\frac{11}{24}, \frac{19}{24}, \frac{3}{4}; z\right). \tag{116}$$

So that we have

$$\begin{aligned} E_6 \Delta^{n_k} \cdot W_{n_k}^1(j) &\equiv E_6 \Delta^{n_k} j^{n_k} {}_2F_1\left(\frac{11}{24}, \frac{19}{24}, \frac{3}{4}, \frac{1728}{j}\right) \pmod{q^{n_k+1}}, \\ &\equiv E_6 \Delta^{n_k - \frac{1}{24}} j^{n_k - \frac{1}{24}} \left(1 - \frac{1728}{j}\right)^{-\frac{1}{2}} \cdot \theta_0 \pmod{q^{n_k+1}}. \\ &\equiv E_4^{\frac{p}{8}} \theta_0 \pmod{q^{n_k+1}}. \end{aligned}$$

Using (115), we see that (113) holds. Again, if $k \equiv 10 \pmod{12}$ we can give a similar argument. □

Now we will rewrite our polynomial R_k in terms of the *modular λ-function*. We will define this form using the Weierstrass relation. Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be a lattice such that $\tau := \frac{\omega_2}{\omega_1} \in \mathbb{H}$, then we have the following elliptic curve over $\mathbb{C}$ coming from the Weierstrass's differential equation (see 26)

$$Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda), \tag{117}$$

where

$$g_2(\Lambda) = 60 \cdot \sum_{z \in \Lambda - \{0\}} \frac{1}{z^4} \qquad \text{and} \qquad g_3(\Lambda) = 140 \cdot \sum_{z \in \Lambda - \{0\}} \frac{1}{z^6}.$$

Further, let

$$e_1 = \wp_\Lambda\left(\frac{\omega_1}{2}\right), \qquad e_2 = \wp_\Lambda\left(\frac{\omega_2}{2}\right) \quad \text{and} \quad e_3 = \wp_\Lambda\left(\frac{\omega_3}{2}\right).$$

The $e_i's$ are the (distinct) roots of the right hand side of (117) (see [11, Proposition 10.7.]). Now let $j(\Lambda)$ be the j-invariant of (117) and let $\Delta(\Lambda)$ be the discriminant of the right hand side of (117).

Lemma 4.38. *We have the following equalities*

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{\Delta(\Lambda)} = 1728\frac{g_2(\Lambda)^3}{16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^3} = j(\tau), \tag{118}$$

where $j(\tau)$ is the modular j-invariant.

Proof. See for example [11, §10.B.]. □

Note that (118) is independent of the choice of basis for Λ. From now on fix

$$\omega_1 = \pi \sum_{n \in \mathbb{Z}} 2(q')^{n^2} \qquad \text{where } q' := e^{\pi i \tau},$$

and $\omega_2 := \tau\omega_1$. Now we define the λ-function as

$$\lambda(\tau) = \frac{e_3 - e_2}{e_1 - e_2}.$$

$\lambda(\tau)$ is a modular function for the congruence group $\Gamma(2)$ (See [7, §7 Theorem 2], in fact λ is a hauptmodul, for $\Gamma(2)$ of genus 0). We will now give a relation between the j-invariant and the λ-function:

Proposition 4.39.

$$j(\tau) = \frac{256(1 + \lambda(\lambda - 1))^3}{(\lambda(\lambda - 1))^2}. \tag{119}$$

Proof. We can write the right hand side of (119) in terms of e_1, e_2, e_3

$$\begin{aligned}\frac{256(1 + (\lambda(\lambda - 1)))^3}{(\lambda(\lambda - 1))^2} &= \frac{256((e_1 - e_2)^2 - (e_3 - e_2)(e_1 - e_3))^3}{(e_1 - e_2)^2(e_1 - e_3)^2(e_1 - e_3)^2}, \\ &= \frac{4096((e_1 + e_2 + e_3)^2 - 3(e_1e_2 + e_2e_3 + e_1e_3))}{\Delta(\Lambda)}.\end{aligned}$$

As the e_i are the roots of $4X^3 - g_2(\Lambda)X + g_3(\Lambda)$, we see that

$$\begin{aligned}e_1 + e_2 + e_3 &= 0, \\ e_1e_2 + e_2e_3 + e_1e_3 &= \frac{-g_2(\Lambda)}{4}.\end{aligned}$$

So that

$$\frac{256(1+\lambda(\lambda-1))^3}{(\lambda(\lambda-1))^2} = \frac{4096(\frac{3}{4}g_2(\Lambda))^3}{\Delta(\Lambda)} = j(\tau).$$

□

Now define the polynomials

$$F_k(\lambda) := \frac{(\lambda(\lambda-1))^{2n_k}}{256^{n_k}} \cdot W_{n_k}^{a_k}\left(\frac{256(1+\lambda(\lambda-1))^3}{(\lambda(\lambda-1))^2}\right).$$

These are monic polynomials of degree $6n_k$ in the variable λ. As the relation (119) is six to one, i.e. any value of $j \in \overline{\mathbb{F}}_p$ corresponds to at most 6 values of $\lambda \in \overline{\mathbb{F}}_p$, it suffices to show that all the polynomials $\widetilde{F_k} :\equiv F_k \pmod p$ have $6n_k$ distinct roots $t \in \mathbb{F}_p$ with $t \neq 0, 1 \pmod p$. Define the following truncated hypergeometric function of degree $\frac{p+1}{4}$:

$$G(\lambda)_p := {}_2F_1\left(-\frac{1}{4}, \frac{1}{4}, \frac{1}{2}; \lambda\right)_{\left(\frac{p+1}{4}\right)} \pmod p. \tag{120}$$

This is well-defined as:

Lemma 4.40. *The hypergeometric function ${}_2F_1\left(-\frac{1}{4}, \frac{1}{4}, \frac{1}{2}; \lambda\right)$ is p-integral, for all $p > 2$.*

Proof. This follows from the expression in A.3, since the Taylor expansion of both $\sqrt{1+x}$ and $\sqrt{1-x}$ is p-integral for $p > 2$. □

If $k \equiv 0, 4 \pmod{12}$, we have the following hypergeometric expression for $\widetilde{F_k}$

Proposition 4.41.

$$\widetilde{F_k}(\lambda) \equiv \begin{cases} G(\lambda)_p, & \text{if } k \equiv 0 \pmod{12} \\ \dfrac{G(\lambda)_p}{1+\lambda(\lambda-1)}, & \text{if } k \equiv 4 \pmod{12} \end{cases}$$

Proof. Let $k \equiv 0 \pmod{12}$. We will first write $\tilde{F_k}$ as a hypergeometric series in $\lambda(\lambda-1)$. Write

$${}_2F_1\left(\frac{-1}{24}, \frac{7}{24}, \frac{3}{4}; \frac{1728}{j}\right) = \sum_{m \geq 0} a_m j^{-m}.$$

Using the binomial theorem, we find that

$$\begin{aligned} F_k(\lambda) &= a_0(1+\lambda(\lambda-1))^{3n_k} + \frac{a_1}{256}(1+\lambda(\lambda-1))^{3(n_k-1)}(\lambda(\lambda-1))^2 + \ldots + \frac{a_{n_k}}{256^{n_k}}(\lambda(\lambda-1))^{2n_k} \\ &= \sum_{i=0}^{3n_k} b_i(\lambda(\lambda-1))^i, \end{aligned}$$

where

$$b_i = \sum_{r=0}^{\lfloor \frac{i}{2} \rfloor} \binom{3n_k - 3j}{i-2j} \frac{a_j}{256^j}.$$

As $n_k = (p+1)/24$, we see that

$$\binom{3n_k - 3j}{i-2j} \equiv (-1)^i \frac{1}{(i-2j)!}\left(\frac{1}{8} + 3j\right)_{i-2j} \pmod p,$$

where $(\ .\ )_n$ is the Pochhammer symbol. Using *Mathematica*, we find the identity

$$b_i \equiv (-4)^i \cdot \frac{(-\frac{1}{8})_i(\frac{1}{8})_i}{(\frac{1}{2})_i i!} \pmod{p},$$

so that

$$\widetilde{F_k}(\lambda) \equiv {}_2F_1\left(-\frac{1}{8}, \frac{1}{8}, \frac{1}{2}, -4\lambda(\lambda-1)\right)_{\left(\frac{p+1}{8}\right)} \pmod{p}.$$

As the coefficients z^n of ${}_2F_1\left(-\frac{1}{8}, \frac{1}{8}, \frac{1}{2}, z\right)$ vanish modulo p if $\frac{p+1}{8} \leq n \leq \frac{p+1}{4}$, it suffices to show that

$${}_2F_1\left(-\frac{1}{8}, \frac{1}{8}, \frac{1}{2}, -4\lambda(\lambda-1)\right) = {}_2F_1\left(-\frac{1}{4}, \frac{1}{4}, \frac{1}{2}, \lambda\right).$$

Now using (161), we see that

$${}_2F_1\left(-\frac{1}{8}, \frac{1}{8}, \frac{1}{2}, -4\lambda(\lambda-1)\right) = \cos\left(\frac{1}{8}\arccos(1+8\lambda(\lambda-1))\right).$$

As ${}_2F_1\left(-\frac{1}{4}, \frac{1}{4}, \frac{1}{2}, \lambda\right) = \frac{1}{2}\left((1-\lambda^{\frac{1}{2}})^{\frac{1}{2}} + (1+\lambda^{\frac{1}{2}})^{\frac{1}{2}}\right)$, (see corollary A.3) it suffices to show that

$$T_8\left(\frac{1}{2}\left((1-\lambda^{\frac{1}{2}})^{\frac{1}{2}} + (1+\lambda^{\frac{1}{2}})^{\frac{1}{2}}\right)\right) = 1 + 8\lambda(\lambda-1),$$

where T_8 is the eigth Chebyshev polynomial of the first kind (see the Appendix), the latter identity can be easily checked. The proof for the case $k \equiv 4 \pmod{12}$ proceeds similarly. □

For weights $k \equiv 6, 10 \pmod{12}$, we conjecture the following:

Conjecture 4.42.

$$\widetilde{F_k}(\lambda) \equiv \begin{cases} \dfrac{G(\lambda)_p}{(\lambda+1)(\lambda-2)(\lambda-\frac{1}{2})}, & \text{if } k \equiv 6 \pmod{12} \\ \dfrac{G(\lambda)_p}{(\lambda+1)(\lambda-2)(\lambda-\frac{1}{2})(\lambda^2+1)}, & \text{if } k \equiv 10 \pmod{12} \end{cases}$$

In order to prove theorem 4.33, we will show that the truncated hypergeometric function $G(\lambda)_p$ factors as a product of distinct linear factors over $\mathbb{F}_p$. We need the following easy lemma.

Lemma 4.43. *Let $n \in \mathbb{Z}_{\geq 0}$ and $p > 2$ a prime, then*

$$\sum_{a \in \mathbb{F}_p} a^n = \begin{cases} -1, & \text{if } n | p-1. \\ 0, & \text{otherwise.} \end{cases} \tag{121}$$

Proof. Assume $n \nmid p-1$ and let $S = \sum_{a \in \mathbb{F}_p} a^n$. As $\mathbb{F}_p^*$ is cyclic, there is a $g \in \mathbb{F}_p^*$ such that $g^n \neq 1$. Clearly $a \to g \cdot a$ permutes $\mathbb{F}_p$ so that $g^n S = S$ and hence $S = 0$, as $g^n \neq 1$. □

Proposition 4.44. *Let p be a prime $p \equiv 3 \pmod{4}$. The polynomial $\widetilde{G}_p(\lambda)$ splits over $\mathbb{F}_p$ as a product of distinct linear factors. More specifically:*

$$\widetilde{G}_p(\lambda) \equiv \prod_{\substack{t \text{ is not a square } (\mathrm{mod}\ p) \\ t-1 \text{ is a square } (\mathrm{mod}\ p)}} (\lambda - t) \pmod{p}.$$

Proof. Let $\widetilde{H}_p(\lambda)$ be the polynomial on the right hand side. We will compute the power sums of the roots of $\widetilde{H}_p(\lambda)$ and show, using symmetric polynomials, that the coefficients of $\widetilde{H}_p(\lambda)$ and $\widetilde{G}_p(\lambda)$ are congruent. First we show that the degrees of $\widetilde{G}_p(\lambda)$ and $\widetilde{H}_p(\lambda)$ coincide. The degree of $\widetilde{H}_p(\lambda)$ is exactly

$$N_p := \#\{t \in \mathbb{F}_p | -t \text{ and } t-1 \text{ are squares } (\mathrm{mod}\ p)\},$$

as -1 is not a square (mod p). In terms of Legendre symbols, this is

$$\begin{aligned} N_p &= \sum_{a=0}^{p-1} \frac{1}{4}\left(\left(\frac{-a}{p}\right)+1\right)\left(\left(\frac{a-1}{p}\right)+1\right), \\ &= \frac{p+1}{4} + \frac{1}{4}\left(\sum_{a=0}^{p-1}\left(\frac{-a}{p}\right) + \sum_{a=0}^{p-1}\left(\frac{a-1}{p}\right) + \sum_{a=0}^{p-1}\left(\frac{-a(a-1))}{p}\right)\right), \\ &= \frac{p+1}{4} + \frac{1}{4}\sum_{a=0}^{p-1}\left(\frac{-a(a-1)}{p}\right) + \frac{1}{2}\sum_{b=0}^{p-1}\left(\frac{b}{p}\right), \end{aligned}$$

where we use that the Legendre symbol is multiplicative. As $a \mapsto (\frac{a}{p})$ defines a non-trivial multiplicative character on $\mathbb{F}_p$, we have

$$\sum_{a=0}^{p-1}\left(\frac{a}{p}\right) = 0.$$

Further as $\left(\frac{x}{p}\right) = \left(\frac{x^{-1}}{p}\right)$ for $x \in \mathbb{F}_p^*$, we find

$$\begin{aligned} \sum_{a=0}^{p-1}\left(\frac{-a(a-1)}{p}\right) &= \sum_{a=0}^{p-1}\left(\frac{-a^{-1}(a-1)}{p}\right) \\ &= \sum_{a=1}^{p-1}\left(\frac{-1+a^{-1}}{p}\right) \\ &= \sum_{c=2}^{p-2}\left(\frac{c}{p}\right) = \sum_{c=0}^{p-1}\left(\frac{c}{p}\right) - 1 + 1 = 0. \end{aligned}$$

Hence $\deg(\widetilde{H}_p(\lambda)) = N_p = \frac{p+1}{4}$ and this coincides with the degree of $\widetilde{G}_p(\lambda)$.

Now we compute the n-th power sums S_n of $\widetilde{H}_p(\lambda)$ for $0 < n \leq \frac{p+1}{4}$, so

$$S_n \equiv \sum_{\substack{t \text{ is not a square } (\mathrm{mod}\ p) \\ t-1 \text{ is a square } (\mathrm{mod}\ p)}} t^n \pmod{p}.$$

Again we can compute S_n in terms of Legendre symbols, so that

$$\begin{aligned} S_n &= \sum_{a=0}^{p-1} \frac{1}{4}\left(\left(\frac{-a}{p}\right)+1\right)\left(\left(\frac{a-1}{p}\right)+1\right)a^n \\ &= \frac{1}{4}\left(\sum_{a=0}^{p-1} a^n + \sum_{a=0}^{p-1}\left(\frac{-a}{p}\right)a^n + \sum_{a=0}^{p-1}\left(\frac{a-1}{p}\right)a^n + \sum_{a=0}^{p-1}\left(\frac{-a(a-1)}{p}\right)a^n\right). \end{aligned}$$

By Euler's criterion we have $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$ for all $a \in \mathbb{Z}$. Hence

$$\begin{aligned} S_n &\equiv \frac{1}{4}\left(\sum_{a=0}^{p-1} a^n - \sum_{a=0}^{p-1} a^{n+\frac{p-1}{2}} + \sum_{a=0}^{p-1}(a-1)^{\frac{p-1}{2}}a^n + \sum_{a=0}^{p-1}(1-a)^{\frac{p-1}{2}}a^{n+\frac{p-1}{2}}\right) \\ &\equiv \frac{1}{4}\left(\sum_{a=0}^{p-1} a^n - \sum_{a=0}^{p-1} a^{n+\frac{p-1}{2}} + \sum_{k=0}^{\frac{p-1}{2}}(-1)^k\binom{\frac{p-1}{2}}{k}\sum_{a=0}^{p-1}a^{k+n} + \sum_{k=0}^{\frac{p-1}{2}}(-1)^k\binom{\frac{p-1}{2}}{k}\sum_{a=0}^{p-1}a^{k+n+\frac{p-1}{2}}\right). \end{aligned}$$

Using (121) and the fact that $0 < n \leq \frac{p+1}{4} < \frac{p-1}{2}$ if $p > 3$, we find that for primes $p > 3$

$$S_n \equiv -\frac{1}{4}\sum_{k=0}^{\frac{p-1}{2}}(-1)^k\binom{\frac{p-1}{2}}{k}\sum_{a=0}^{p-1}a^{k+n+\frac{p-1}{2}}.$$

Note that a non-zero contribution only occurs if $k+n+\frac{p-1}{2} = p-1$ i.e., if $k = \frac{p-1}{2} - n$. Therefore we find

$$S_n \equiv \frac{(-1)^n}{4}\binom{\frac{p-1}{2}}{n} \equiv \frac{1}{4}\frac{(\frac{1}{2})_n}{n!}.$$

Using the power sums, we can compute the coefficients of $\tilde{G}_p(\lambda)$ using Newton's identities: Let c_n be the λ^n coefficient of $\widetilde{H}_p(\lambda)$, then

$$c_n \equiv -\frac{1}{n}(c_{n-1}S_1 + c_{n-2}S_2 + ... + c_1S_{n-1} + S_n). \tag{122}$$

We need to show

$$c_n \equiv \frac{(-\frac{1}{4})_n(\frac{1}{4})_n}{(\frac{1}{2})_n n!}.$$

Using mathematical induction, it suffices to prove that

$$c_n \equiv -\frac{1}{4n}\sum_{r=0}^{n-1}\frac{(\frac{-1}{4})_r(\frac{1}{4})_r}{(\frac{1}{2})_r r!}\frac{(\frac{1}{2})_{n-r}}{(n-r)!}.$$

Using *Mathematica* we find the following identity:

$$\sum_{r=0}^{n}\frac{(\frac{-1}{4})_r(\frac{1}{4})_r}{(\frac{1}{2})_r r!}\frac{(\frac{1}{2})_{n-r}}{(n-r)!} = \frac{\left(\frac{4n-1}{2}\right)!}{(2n)!\left(-\frac{1}{2}\right)!}. \tag{123}$$

Therefore, using this identity, it suffices to show

$$\frac{(\frac{-1}{4})_n(\frac{1}{4})_n}{(\frac{1}{2})_n n!}\left(1 - \frac{1}{4n}\right) = -\frac{\left(\frac{4n-1}{2}\right)!}{4n(2n)!\left(-\frac{1}{2}\right)!},$$

and this can easily be verified by induction. □

Remark 4.45. As $p \equiv 3 \pmod 4$, we see that $\widetilde{G}_p(\lambda)$ is non-zero if $\lambda = 0, 1$.

Remark 4.46. Note that the polynomial $G(\lambda)_p$ is the analogon of the Hasse-polynomial ${}_2F_1\left(\frac{1}{2}, \frac{1}{2}, 1, \lambda\right)_{\left(\frac{p+1}{2}\right)}$, factoring modulo p as a product of linear and quadratic factors, with as roots mod p the supersingular λ-invariants.

Now we can prove:

Theorem 4.47. *If $k \equiv 0, 4 \pmod{12}$ and suppose $p = 2k-1$ is prime $p > 7$, then $\widetilde{R_k}$ splits over $\mathbb{F}_p$ as a product of distinct linear factors.*

Proof. This follows directly from 4.45, 4.41 and 4.44. □

4.7 Properties of The Orthogonal Polynomials

We have shown that the functional $(\ ,\ )_T$ defines an inner product on the space of real polynomials. This inner product is analogous to the inner product defined in [22]. As in [22], we will compute the orthogonal polynomials with respect to $(\ ,\ )_T$, using the Gram-Schmidt procedure, see (59). These polynomials B_i will therefore be the analogue of the Atkin polynomials.
We find:

$$\begin{aligned}
B_0 &= 1\\
B_1 &= X - 672\\
B_2 &= X^2 - \frac{17792}{11}X + \frac{2714112}{11}\\
B_3 &= X^3 - \frac{47392}{19}X^2 + \frac{28296960}{19}X - 98279424\\
B_4 &= X^4 - \frac{30272}{9}X^3 + \frac{719159296}{207}X^2 - \frac{75652628480}{69}X + \frac{924787539968}{23}.
\end{aligned}$$

Using proposition 3.48 and the values λ_i we computed in (4.28), we get for $n \geq 2$ an explicit recursion formula for the B_i:

$$B_{n+1} = \Big(X - \frac{96(576n^2 - 144n - 107)}{(8n-5)(8n+3)}\Big)B_n - \frac{2304(24n-1)(24n-13)(24n-29)(24n-17)}{(8n-9)(8n-1)(8n-5)^2}B_{n-1}. \tag{124}$$

Proposition 4.48. *All the n zeros of B_n are real, distinct and lie in the interval $(0, 1728)$.*

Proof. We can rewrite the inner product $(f(X), g(X))_T = \int_{\pi/3}^{\pi/2} f(j(e^{i\alpha}))g(j(e^{i\alpha}))W(\alpha)d\alpha$ as

$$(f(X), g(X))_T = \int_0^{1728} f(j)g(j)W(\alpha)\alpha'(j)dj,$$

where $\alpha(j)$ is the inverse of $j(e^{i\alpha})$ on $(\pi/3, \pi/2)$. Clearly $W(\alpha)\alpha'(j) > 0$ on $(\pi/3, \pi/2)$. Using proposition 3.50, we derive our result. □

4.7.1 Congruence Observations

From the recursion (124), it is clear that the polynomials B_n are p-integral if $p > 8(n-1)+3 = 8n-5$. So that $\widetilde{B_n} := B_n \pmod p$ is well-defined. Similar to the Atkin polynomials, we observed some factorization properties modulo p:

Conjecture 4.49. Let $n \geq 2$, then $R_{\frac{p+1}{2}} \pmod p$ divides $\widetilde{B_n}$ for all primes $24n > p > 8n-5$, $p \equiv 3 \pmod 4$.

Example 4.50. We consider the factorization of $\widetilde{B_4}$ for primes $31 \leq p \leq 83$, $p \equiv 3 \pmod 4$.

p	$\widetilde{B_4}(X)$
31	$X(X+3)(X^2+9X+1)$
43	$X(X+19)(X+32)(X+35)$
47	$(X+9)(X+10)(X^2+38X+38)$
59	$(X+13)(X+25)(X+42)(X+44)$
67	$X(X+14)(X+44)(X+55)$
71	$(X+29)(X+33)(X+39)(X+46)$
79	$X(X+16)(X+45)(X+69)$
83	$(X+15)(X+17)(X+33)(X+39)$

5 Modular Forms With All Zeros on The Unit Circle

In this section, we will give an explicit sufficient condition for a modular form to have all its zeros on the unit circle, see theorem 5.6. This sufficient condition will depend on the bound we can give for a certain cuspidal modular form on the unit circle. For the bounds on these modular forms, we will use the theory of W. Duke and P. Jenkins [13].

5.1 Results for Certain Weakly Modular Forms

In this section we review the results of [13]. In [13], the authors studied the location of the zeros of certain weakly modular forms.
For $k \in 2\mathbb{Z}$, write $k = 12\ell + k'$, where $k' \in \{0, 4, 6, 8, 10, 14\}$ and $\ell \in \mathbb{Z}$. As in [13] fix the notation $f_{k,m}$ for the unique holomorphic weakly modular form of weight k such that:

$$f_{k,m} = q^{-m} + O(q^{\ell+1}), \tag{125}$$

with $m \geq -\ell$. Note that if $k \geq 4$, the value $\ell + 1$ coincides with $d_k := \dim(M_k)$. In [13], the authors showed that:

Theorem 5.1 ([13, Theorem 1.]). *If $m \geq |\ell| - \ell$, then all the zeros of $f_{k,m}$ in the finite part of $\mathcal{F}$ lie on the unit circle $\{e^{i\theta} | \theta \in [\pi/2, 2\pi/3]\}$.*

The authors used a similar argument as in [33]. More specifically they proved the following:

Lemma 5.2 ([13, Lemma 2.]). *For all $\theta \in (\pi/2, 2\pi/3)$ and $m \geq 0$:*

$$|e^{ik\theta/2} e^{-2\pi m \sin(\theta)} f_{k,m}(e^{i\theta}) - 2\cos\left(k\theta/2 - 2\pi m \cos(\theta)\right)| < 1.985. \tag{126}$$

If $m \geq 0$, the function

$$\theta \mapsto 2\cos\left(k\theta/2 - 2\pi m \cos(\theta)\right)$$

has exactly $\ell + 1 + m$ values on $[\pi/2, 2\pi/3]$ where it takes on absolute value 2, alternating between 2 and -2 as θ increases, see [13] for more details. By the intermediate value theorem, it follows that the real valued function

$$\theta \mapsto e^{ik\theta/2} f_{k,m}(e^{i\theta}) e^{-2\pi m \sin(\theta)}$$

has *at least* $\ell + m$ zeros on $(\pi/2, 2\pi/3)$. Using the valence formula (11), we see that $f_{k,m}$ has *exactly* $\ell + m$ zeros on $(\pi/2, 2\pi/3)$, as $f_{k,m}$ has a pole of order m at $i\infty$.

As an application of lemma 5.2, we find that

$$|e^{ik\theta/2} f_{k,0}(e^{i\theta}) - 2\cos(k\theta/2)| < 1.985, \tag{127}$$

so that the zeros of the extremal modular forms $f_{k,0}$ in the fundamental domain $\mathcal{F}$ lie on the unit circle.

5.2 Bounds for Cusp Forms on the Unit Circle

In this section we will present Theorem 5.6. In order to prove this result, we will show the following result for the value of cusp forms on the unit circle:

Lemma 5.3. *For $m \leq 0$, let $f_{k,m}$ be the unique form defined by* (125)*. Then for $\theta \in [\pi/2, 2\pi/3]$ we have:*

$$|f_{k,m}(e^{i\theta})| \leq 3.985 \cdot e^{2\pi m 0.65}. \tag{128}$$

This result gives an explicit way of bounding the values of the cusp forms $f_{k,m}$ on the unit circle. We will prove this result in the next section. Lemma 5.3 allows us to prove the main lemma:

Lemma 5.4. *Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a formal power series in q with real coefficients, such that $a_0 = 1$. Let $\widetilde{f}$ be the unique modular form of weight k such that $\widetilde{f} = f + O(q^{d_k})$. Let $R = 1.985$ and assume that*

$$M = \sum_{n=1}^{d_k - 1} |a_n| \cdot e^{-2\pi n 0.65} < \frac{2-R}{2+R}. \tag{129}$$

Then

$$|e^{ik\theta/2}\widetilde{f}(e^{i\theta}) - 2\cos(k\theta/2)| < 2,$$

for $\theta \in [\pi/2, 2\pi/3]$.

Proof. We can write

$$\widetilde{f} = f_{k,0} + \sum_{n=1}^{d_k - 1} a_n f_{k,-n},$$

as the difference is a modular form of the form $\mathcal{O}(q^{d_k})$, and such a form must be identically equal to 0 (using the valence formula (11) for example). Now

$$\begin{aligned} |e^{ik\theta/2}\widetilde{f}(e^{i\theta}) - 2\cos(k\theta/2)| &\leq |e^{ik\theta/2} f_{k,0}(e^{i\theta}) - 2\cos(k\theta/2)| + \sum_{n=1}^{d_k-1} |e^{ik\theta/2}||a_n||f_{k,-n}(e^{i\theta})| \\ &< R + \sum_{n=1}^{d_k-1} |a_n| \cdot (2+R) \cdot e^{-2\pi n 0.65} \\ &< R + (2-R) = 2, \end{aligned}$$

using (127), for all $\theta \in [\pi/2, 2\pi/3]$. □

Remark 5.5. An analogous result can be found in [41] for certain modular functions.

Theorem 5.6. *Suppose $\widetilde{f}$ is a modular form as in lemma 5.4 satisfying* (129)*, then all the zeros of $\widetilde{f}$ in the fundamental domain $\mathcal{F}$ lie on the arc $\{e^{i\theta} \mid \theta \in [\pi/2, 2\pi/3]\}$.*

Proof. Using lemma 5.4, we have that $|e^{ik\theta/2}\tilde{f}(e^{i\theta}) - 2\cos(k\theta/2)| < 2$. Using lemma 3.1, we see that $e^{ik\theta/2}\widetilde{f}(e^{i\theta})$ is real for $\theta \in [\pi/2, 2\pi/3]$. Write $k = 12n_k + 6a_k + 4b_k$, $n_k \in \mathbb{Z}_{\geq 0}$, $a_k \in \{0, 1\}$ and $b_k \in \{0, 1, 2\}$. As in the proof of theorem 3.2, we conclude that $\widetilde{f}$ has *at least* n_k zeros on the arc $\{e^{i\theta} \mid \theta \in (\pi/2, 2\pi/3)\}$ and by the valence formula (11) it has *exactly* n_k zeros on this arc, finishing the proof. □

5.3 Proof of Lemma 5.3

The proof of lemma 5.3 will proceed as follows; we will extend lemma 5.2 for $m \leq 0$ using the methods from [13]. We will show that for $m \leq 0$ and $d_k > 12$:

Lemma 5.7. *For $\theta \in [\pi/2, 2\pi/3]$ we have the following inequality:*

$$|e^{ik\theta/2}e^{-2\pi m\sin(\theta)}f_{k,m}(e^{i\theta})-2\cos(k\theta/2-2\pi m\cos(\theta))| \leq \begin{cases} 1.985e^{-2\pi m(\sin(\theta)-0.75)}; & \theta \in [\pi/2, 1.9) \\ 1+0.985e^{-2\pi m(\sin(\theta)-0.65)}; & \theta \in [1.9, 2\pi/3] \end{cases}.$$

Assuming this lemma, we can prove lemma 5.3: For $\theta \in [1.9, 2\pi/3]$ we find, using the triangle inequality

$$\begin{aligned} |e^{ik\theta/2}e^{-2\pi m\sin(\theta)}f_{k,m}(e^{i\theta})| &\leq 1+0.985e^{-2\pi m(\sin(\theta)-0.65)}+|2\cos\left(k\theta/2-2\pi m\cos(\theta)\right)| \\ &\leq 3+0.985e^{-2\pi m(\sin(\theta)-0.65)}, \end{aligned}$$

dividing by $e^{-2\pi m\sin(\theta)}$ gives

$$|f_{k,m}(e^{i\theta})| \leq 3e^{2\pi m\sin(\theta)}+0.985e^{2\pi m0.65} \leq 3.985e^{2\pi m0.65},$$

as $\sin(\theta) > 0.65$.
Similarly, for $\theta \in [\pi/2, 1.9)$ we find, using the triangle inequality

$$\begin{aligned} |e^{ik\theta/2}e^{-2\pi m\sin(\theta)}f_{k,m}(e^{i\theta})| &\leq 1.985e^{-2\pi m(\sin(\theta)-0.75)}+|2\cos\left(k\theta/2-2\pi m\cos(\theta)\right)| \\ &\leq 2+1.985e^{-2\pi m(\sin(\theta)-0.75)}, \end{aligned}$$

dividing by $e^{-2\pi m\sin(\theta)}$ gives

$$|f_{k,m}(e^{i\theta})| \leq 2e^{2\pi m\sin(\theta)}+0.985e^{2\pi m0.75} \leq 2.985e^{2\pi m0.75} \leq 3.985e^{2\pi m0.65},$$

as $\sin(\theta) > 0.75$.

We shall treat the cases of low weight separately: If $d_k \leq 12$, we can write the form $f_{k,m}$, $-d_k+1 \leq m \leq 0$ as the linear combination

$$f_{k,m} = \sum_{i=-m}^{d_k-1} c_i f_{k-12i,0}\Delta^i,$$

for some $c_i \in \mathbb{R}$. Using lemma B.4 we see that

$$|f_{k,m}(e^{i\theta})| \leq \sum_{i=-m}^{d_k-1} |c_i||f_{k-12i,0}(e^{i\theta})| \cdot 0.00481^i.$$

As $|e^{ik\theta/2}f_{k-2i,0}(e^{i\theta})-2\cos(k\theta/2)| < 1.985$, we find that $|f_{k-12i,0}(e^{i\theta})| \leq 3.985$. An easy computation for all k with $d_k \leq 12$, shows that

$$|f_{k,m}(e^{i\theta})| \leq \sum_{i=-m}^{d_k-1} |c_i| \cdot 3.985 \cdot 0.00481^i \leq 3.985 \cdot e^{2\pi m0.65}.$$

This proves lemma 5.3. In the remainder of this section we will prove lemma 5.7.

Let k be a positive even integer and write k uniquely as $k = 12(d_k - 1) + k'$, where $k' \in \{0, 4, 6, 8, 10, 14\}$. For the proof of lemma 5.7, we use the following the following remarkable formula:

Lemma 5.8 ([13, lemma 2])**.** *Let m be an integer such that $m \geq -d_k + 1$, then we have*

$$f_{k,m}(z) = \frac{1}{2\pi i} \oint_C \frac{\Delta(z)^{d_k-1} E_{k'}(z) E_{14-k'}(\tau)}{\Delta(\tau)^{d_k}(j(\tau) - j(z))} q^{-m-1} dq, \tag{130}$$

for C a (counterclockwise) circle centered at $q = 0$ with a sufficiently small radius.

Remark 5.9. We use the convention $E_0 \equiv 1$.

Proof. We follow the proof of [13]. We can write:

$$f_{k,m}(\tau) = \Delta^{d_k-1} E_{k'} F_{k,D}(j),$$

where $F_{k,D}(j)$ is a monic polynomial of degree $D = m + d_k - 1 \geq 0$ in the j-invariant. Using Cauchy's integral theorem twice, we have

$$\begin{aligned} F_{k,D}(x) = \frac{1}{2\pi i} \oint_{C'} \frac{F_{k,D}(j)}{j - x} dj &= \frac{1}{2\pi i} \oint_{C'} \frac{q^{-m}}{\Delta(\tau)^{d_k-1} E_{k'}(\tau)(j - x)} dj + \oint_{C'} \frac{\mathcal{O}(q^{d_k})}{\Delta(\tau)^{d_k-1} E_{k'}(\tau)(j - x)} dj, \\ &= \frac{1}{2\pi i} \oint_{C'} \frac{q^{-m}}{\Delta(\tau)^{d_k-1} E_{k'}(\tau)(j - x)} dj, \end{aligned}$$

for a sufficient large counterclockwise oriented circle C' around $j = 0$. Now using the identity

$$q \frac{dj}{dq} = \frac{-E_{14}}{\Delta},$$

we find

$$f_{k,m}(z) = \Delta(z)^{d_k-1} E_{k'}(z) F_{k,D}(j(z)) = \frac{1}{2\pi i} \oint_C \frac{\Delta(z)^{d_k-1} E_{k'}(z) E_{14-k'}(\tau)}{\Delta(\tau)^{d_k}(j(\tau) - j(z))} q^{-m-1} dq,$$

for C a (counterclockwise) circle centered at $q = 0$ with a sufficiently small radius. □

For $A > 1$ big enough, lemma 5.8 implies that, after changing variables $q = e^{2\pi i \tau}$ with τ, we find:

$$f_{k,m}(z) = \int_{-\frac{1}{2}+iA}^{\frac{1}{2}+iA} \frac{\Delta(z)^{d_k-1} E_{k'}(z) E_{14-k'}(\tau)}{\Delta(\tau)^{d_k}(j(\tau) - j(z))} e^{-2\pi i m \tau} \, \mathrm{d}\tau, \tag{131}$$

using Cauchy's integral theorem. As in [13], we will write

$$G(\tau, z) := \frac{\Delta(z)^{d_k-1} E_{k'}(z) E_{14-k'}(\tau)}{\Delta(\tau)^{d_k}(j(\tau) - j(z))} e^{-2\pi i m \tau}.$$

From now on let $z = e^{i\theta}$ for $\theta \in (\pi/2, 2\pi/3)$. For $0 < A' < A$, define the box

$$B_{A'} := \{\tau \in \mathbb{H} \mid -\frac{1}{2} \leq \mathrm{Re}(\tau) \leq \frac{1}{2} \text{ and } A' \leq \mathrm{Im}(\tau) \leq A\}.$$

Then by the residue theorem, assuming there are no poles on the boundary of $B_{A'}$,

$$\int_{-\frac{1}{2}+iA'}^{\frac{1}{2}+iA'} G(\tau,z)\,\mathrm{d}\tau = \int_{-\frac{1}{2}+iA}^{\frac{1}{2}+iA} G(\tau,z)\,\mathrm{d}\tau + 2\pi i \sum_{\tau_0\in B_{A'}} \mathrm{Res}_{\tau=\tau_0} G(\tau,z), \tag{132}$$

$$= f_{k,m}(z) + 2\pi i \sum_{\tau_0\in B_{A'}} \mathrm{Res}_{\tau=\tau_0} G(\tau,z). \tag{133}$$

Note that the only possible poles of $G(\tau,z)$ in $B_{A'}$, seen as a function in the variable τ, are at $\tau=\gamma z$, for $\gamma\in \mathrm{SL}_2(\mathbb{Z})$. As we have the identity

$$q\frac{dj}{dq} = \frac{-E_{14}}{\Delta}$$

and $\frac{dq}{d\tau} = 2\pi i q$, we can rewrite $G(\tau,z)$ as:

$$G(\tau,z) = \frac{e^{-2\pi i m\tau}}{-2\pi i}\frac{\Delta(z)^{d_k-1}E_{k'}(z)}{\Delta(\tau)^{d_k-1}E_{k'}(\tau)}\cdot\frac{\frac{d}{d\tau}(j(\tau)-j(z))}{(j(\tau)-j(z))}.$$

Hence, the residue at the points $\tau_0=\gamma z$ for $\gamma=\begin{pmatrix} a & b\\ c & d\end{pmatrix}$, is given by:

$$\mathrm{Res}_{\tau=\gamma z} G(\tau,z) = -\frac{e^{-2\pi i m\cdot(\gamma z)}}{2\pi i}(cz+d)^{-k}. \tag{134}$$

As we have

$$\mathrm{Im}(\gamma z) = \frac{\sin(\theta)}{c^2+d^2+2cd\,\cos(\theta)}, \tag{135}$$

we see that if $\sqrt{3}/2 < \widetilde{A} < \sin(\theta)$, the region $B_{\widetilde{A}}$ contains exactly two poles of $G(\tau,z)$:

$$\tau_0 = z \quad \text{and} \quad \tau_0 = -\frac{1}{z}.$$

Hence, for these $\widetilde{A}$ we have:

$$\int_{-\frac{1}{2}+\widetilde{A}i}^{\frac{1}{2}+\widetilde{A}i} G(\tau,z)\mathrm{d}\tau = f_{k,m}(z) - e^{-2\pi i m z} - z^{-k}e^{-2\pi i m(-1/z)}.$$

If we multiply both sides of the equation by $e^{ik\theta/2}e^{-2\pi m\sin(\theta)}$, we find:

$$e^{ik\theta/2}e^{-2\pi m\sin(\theta)}\int_{-\frac{1}{2}+\widetilde{A}i}^{\frac{1}{2}+\widetilde{A}i} G(\tau,z)\mathrm{d}\tau = e^{ik\theta/2}e^{-2\pi m\sin(\theta)} f_{k,m}(e^{i\theta}) - 2\cos(\tfrac{k\theta}{2} - 2\pi m\cos(\theta)). \tag{136}$$

The goal is to bound the left side of the equation.

If $1.9 \le \theta < 2\pi/3$, one can check using (135) that if we choose $A' = 0.65$, we have that the only poles in $B_{A'}$ are given by

$$\tau_0 = z, \qquad \tau_0 = -\frac{1}{z}, \qquad \tau_0 = -\frac{1}{z+1} \qquad \text{and} \qquad \tau_0 = \frac{z}{z+1}.$$

As $-\frac{1}{z+1}$ and $\frac{z}{z+1}$ have real part $-\frac{1}{2}$ and $\frac{1}{2}$ respectively, these poles lie on the vertical boundary of $B_{A'}$. Adding a small circular arc of the same size around each of these points, we get using (134) and Cauchy's residue theorem:

$$e^{ik\theta/2}e^{-2\pi m\sin(\theta)}\int_{-\frac{1}{2}+\widetilde{A}i}^{\frac{1}{2}+\widetilde{A}i} G(\tau,z)d\tau \tag{137}$$

$$= e^{ik\theta/2}e^{-2\pi m\sin(\theta)}\left(-2\pi i\cdot \mathrm{Res}_{\tau=-\frac{1}{z+1}}G(\tau,z)+\int_{-\frac{1}{2}}^{\frac{1}{2}} G(x+0.65i,z)dx\right)$$

$$= \frac{e^{-\pi im}}{(2\cos(\theta/2))^k}e^{-\pi m(2\sin(\theta)-\tan(\theta/2))}+$$

$$e^{ik\theta/2}e^{-2\pi m\sin(\theta)}\int_{-\frac{1}{2}}^{\frac{1}{2}} G(x+0.65i,z)dx. \tag{138}$$

If $\pi/2 \le \theta < 1.9$, one can similarly show that if $A' = 0.75$, the poles of $G(\tau,z)$ in $B_{A'}$ are given by

$$\tau_0 = z \qquad \text{and} \qquad \tau_0 = -\frac{1}{z},$$

hence we need to give a bound for

$$e^{ik\theta/2}e^{-2\pi m\sin(\theta)}\int_{-\frac{1}{2}}^{\frac{1}{2}} G(x+0.75i,z)dx \tag{139}$$

in this case. The next sections will be devoted to bounding (138) and (139).

5.3.1 The Case $1.9 \le \theta < 2\pi/3$

We assume $1.9 \le \theta < 2\pi/3$ and $A' = 0.65$. We need to give an upper bound for:

$$\left|\frac{e^{-\pi im}}{(2\cos(\theta/2))^k}e^{-\pi m(2\sin(\theta)-\tan(\theta/2))}+e^{ik\theta/2}e^{-2\pi m\sin(\theta)}\int_{-\frac{1}{2}}^{\frac{1}{2}} G(x+0.65i,z)dx\right|. \tag{140}$$

Clearly this is bounded above by

$$\frac{1}{(2\cos(\theta/2))^k}e^{-\pi m(2\sin(\theta)-\tan(\theta/2))}+e^{-2\pi m\sin(\theta)}\int_{-\frac{1}{2}}^{\frac{1}{2}} |G(x+0.65i,z)|dx. \tag{141}$$

We claim that $g(\theta) := \frac{1}{(2\cos(\theta/2))^k}e^{-\pi m(2\sin(\theta)-\tan(\theta/2))}$ is bounded above by 1 on $[1.9, 2\pi/3)$. The derivative of $g(\theta)$ is given by

$$g'(\theta) = \frac{e^{-\pi m(2\sin(\theta)-\tan(\theta/2))}\cdot\left(-\pi m\left(2\cos(\theta)-\frac{1}{2\cos(\theta/2)^2}\right)+k(2\cos(\theta/2)^{k-1}\sin(\theta/2))\right)}{(2\cos(\theta/2))^{2k}}.$$

An easy computation shows that

$$-3 < 2\cos(\theta)-\frac{1}{2\cos(\theta/2)^2} \le -1,$$

and for all even positive k

$$\frac{\sqrt{3}}{2} < (2\cos(\theta/2))^{k-1}\sin(\theta/2).$$

As $-\frac{k}{12} \leq m \leq 0$ and $-3\frac{\pi k}{12} + k\frac{\sqrt{3}}{12} > 0$, we deduce that $g'(\theta) > 0$ and hence $g(\theta)$ is strictly increasing on $[1.9, 2\pi/3)$. Therefore

$$g(\theta) < g(2\pi/3) = 1$$

and it suffices to bound the value

$$e^{-2\pi m\sin(\theta)} \int_{-\frac{1}{2}}^{\frac{1}{2}} |G(x + 0.65i, z)|\mathrm{d}x. \tag{142}$$

Proposition 5.10.

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} \left| \frac{\Delta(z)^{d_k-1}E_{k'}(z)E_{14-k'}(x + 0.65i)}{\Delta(x + 0.65i)^{d_k}(j(x + 0.65i) - j(z))} \right| dx < 516 \cdot 0.481^{d_k-1}. \tag{143}$$

So that for $d_k > 8$, the right side of (146) *is bounded by* 0.985.

Proof. We prove this by giving lower bounds for terms in the denominator and upper bounds for the terms in the numerator. First of all we fix some notation, given a Laurent series $F = \sum_{n=-s}^{\infty} a_n q^n$, for some $s \in \mathbb{Z}_{\geq 0}, a_n \in \mathbb{C}$, we define F_N to be the truncated series $\sum_{n=-s}^{N} a_n q^n$.

Using *Mathematica*, one can show that for all $k' \in \{0, 4, 6, 8, 10, 14\}$

$$\max_{|x|\leq\frac{1}{2}} |E_{14-k'}(x + 0.65i)_{13}| \leq 416.$$

This implies that

$$\begin{aligned}
|E_{14-k'}(x + 0.65i)| &= |E_{14-k'}(x + 0.65i)_{13} + E_{14-k'}(x + 0.65i) - E_{14-k'}(x + 0.65i)_{13}| \\
&\leq |E_{14-k'}(x + 0.65i)_{13}| + |E_{14-k'}(x + 0.65i) - E_{14-k'}(x + 0.65i)_{13}| \\
&\leq 416 + \sum_{n=14}^{\infty} |a_n| e^{-2\pi 0.65n} \\
&\leq 416 + \int_{13}^{\infty} 504x^{14-k'} e^{-2\pi 0.65x} dx \\
&\qquad \text{(Using lemma B.1 and the fact that the integrand is decreasing)} \\
&\leq 416 + 1.14 \cdot 10^{-8} \\
&< 417.
\end{aligned}$$

Similar arguments (using lemmas B.2 and B.3) show that $|\Delta(x+0.65i)| > 0.01$, $|E_{k'}(z)| < 4$ and $|j(x + 0.65i) - j(z)| > 323$ for all $-\frac{1}{2} \leq x \leq \frac{1}{2}$ and $1.9 \leq \theta \leq 2\pi/3$. This shows that

$$\left| \frac{E_{k'}(z)E_{14-k'}(x + 0.65i)}{\Delta(x + 0.65i)(j(x + 0.65i) - j(z))} \right| < \frac{4 \cdot 416}{0.01 \cdot 323} < 516. \tag{144}$$

Furthermore, we have that $|\Delta(z)| < 0.00481$ (see lemma B.4) for all $\theta \in (\pi/2, 2\pi/3)$, hence

$$\frac{|\Delta(z)|}{|\Delta(x + 0.65i)|} < \frac{0.00481}{0.01} = .481. \tag{145}$$

So we conclude that the bound (146) holds. □

For $m \leq 0$ and $d_k > 8$ this implies that,

$$e^{-2\pi m \sin(\theta)} \int_{-\frac{1}{2}}^{\frac{1}{2}} |G(x+0.65i, z)| \mathrm{d}x$$

$$= e^{-2\pi m \sin(\theta)} \cdot \int_{-\frac{1}{2}}^{\frac{1}{2}} \Big| e^{-2\pi i m(x+0.65i)} \frac{\Delta(z)^{d_k-1} E_{k'}(z) E_{14-k'}(\tau)}{\Delta(x+0.65i)^{d_k}(j(x+0.65i)-j(z))} \Big| \mathrm{d}x$$

$$\leq 0.985 e^{-2\pi m(\sin(\theta)-0.65)}.$$

From this we conclude that for $\theta \in [1.9, 2\pi/3]$ and $d_k > 8$:

$$|e^{ik\theta/2} e^{-2\pi m \sin(\theta)} f_{k,m}(e^{i\theta}) - 2\cos\big(k\theta/2 - 2\pi m \cos(\theta)\big)| \leq 1 + 0.985 e^{-2\pi m(\sin(\theta)-0.65)}.$$

5.3.2 The Case $\pi/2 < \theta < 1.9$

We assume $\pi/2 < \theta < 1.9$ and $A' = 0.75$.

Proposition 5.11.

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} \left| \frac{\Delta(z)^{d_k-1} E_{k'}(z) E_{14-k'}(x+0.75i)}{\Delta(x+0.75i)^{d_k}(j(x+0.75i)-j(z))} \right| dx < 167 \cdot 0.67^{d_k-1}. \tag{146}$$

So that for $d_k > 12$, the right side of (146) is bounded by 1.985.

Proof. Using a similar argument as in proposition 5.11 we have:

$$\left| \frac{E_{k'}(z) E_{14-k'}(x+0.75i)}{\Delta(x+0.75i)(j(x+0.75i)-j(z))} \right| < 167, \tag{147}$$

and

$$\left| \frac{\Delta(z)}{\Delta(x+0.75i)} \right| < 0.67 \tag{148}$$

for all $-1/2 \leq x \leq 1/2$ and $\theta \in (\pi/2, 1.9)$. So that

$$\left| \frac{\Delta(z)^{d_k-1} E_{k'}(z) E_{14-k'}(x+0.75i)}{\Delta(x+0.75i)^{d_k}(j(x+0.75i)-j(z))} \right| < 167 \cdot 0.67^{d_k-1}.$$

□

Using a similar reasoning as before, we conclude that for $d_k > 12$ and $\theta \in [\pi/2, 1.9)$:

$$|e^{ik\theta/2} e^{-2\pi m \sin(\theta)} f_{k,m}(e^{i\theta}) - 2\cos\big(k\theta/2 - 2\pi m \cos(\theta)\big)| \leq 1.985 e^{-2\pi m(\sin(\theta)-0.75)}.$$

This finishes the last case.

5.4 Stronger variant of Theorem 5.6

We can make the value R in the theorem 5.6 dependent on k, finding an even stronger result.

If $1.9 \leq \theta \leq 2\pi/3$, using (145), (141) and (144) we get that for $m \leq 0$

$$\begin{aligned}|e^{ik\theta/2}e^{-2\pi m\sin(\theta)}f_{k,m}(e^{i\theta}) - 2\cos(k\theta/2 - 2\pi m\cos(\theta))| &\leq 1 + \int_{-1/2}^{1/2} |G(x+0.65i, z)|\mathrm{d}x \\ &\leq 1 + 0.481^{d_k-1} \cdot 516 \cdot e^{-2\pi m(\sin(\theta)-0.65)}.\end{aligned}$$

So that

$$|f_{k,m}(e^{i\theta})| \leq 3e^{2\pi m\sin(\theta)} + 0.481^{d_k-1} \cdot 516 \cdot e^{2\pi m 0.65} \leq (3 + 0.481^{d_k-1} \cdot 516) \cdot e^{2\pi m 0.65}.$$

Further, if $\pi/2 < \theta < 1.9$, using the estimates (147) and (148), we find

$$\begin{aligned}|e^{ik\theta/2}e^{-2\pi m\sin(\theta)}f_{k,m}(e^{i\theta}) - 2\cos(k\theta/2 - 2\pi m\cos(\theta))| &\leq \int_{-1/2}^{1/2} |G(x+0.75i, z)|\mathrm{d}x \\ &\leq 0.67^{d_k-1} \cdot 167 \cdot e^{-2\pi m(\sin(\theta)-0.75)}.\end{aligned}$$

Similarly, we find

$$|f_{k,m}(e^{i\theta})| \leq (2 + 0.67^{d_k-1} \cdot 167) \cdot e^{2\pi m 0.75}.$$

An easy computation shows that if $d_k > 14$,

$$0.67^{d_k-1} \cdot 167 \leq 1 + 0.481^{d_k-1} \cdot 516.$$

So that:

Lemma 5.12. *For $d_k > 14$ and $\theta \in [\pi/2, 2\pi/3]$, we have*

$$\left|e^{ik\theta/2}f_{k,0}(e^{i\theta}) - 2\cos(k\theta/2)\right| \leq 1 + 0.481^{d_k-1} \cdot 516.$$

Lemma 5.13. *For $d_k > 14$, $m \leq 0$ and $\theta \in [\pi/2, 2\pi/3]$, we have*

$$|f_{k,m}(e^{i\theta})| \leq (3 + 0.481^{d_k-1} \cdot 516) \cdot e^{2\pi m 0.65}. \tag{149}$$

This allows us to replace R in theorem 5.4 with the value $1 + 0.481^{d_k-1} \cdot 516$.

Theorem 5.14. *Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a formal power series in q with real coefficients, such that $a_0 = 1$. Let $\widetilde{f}$ be the unique modular form of weight k with $d_k > 14$ such that $\widetilde{f} = f + O(q^{d_k})$. Let $R = 1 + 0.481^{d_k-1} \cdot 516$, assume that*

$$M := \sum_{n=1}^{d_k-1} |a_n| \cdot e^{-2\pi n 0.65} < \frac{2-R}{2+R}. \tag{150}$$

Then all the zeros of $\widetilde{f}$ in $\mathcal{F}$ lie on the unit circle $\{e^{i\alpha} \mid \alpha \in [\pi/2, 2\pi/3]\}$.

Corollary 5.15. *Consider the theta series $\theta_0 = 1 + 2 \cdot \sum_{n=1}^{\infty} q^{n^2}$. Let Θ_k be the unique modular form such that $\Theta_k = \theta_0 + O(q^{d_k})$. Then all the zeros of Θ_k in the fundamental domain $\mathcal{F}$ lie on the circular arc $\{e^{i\alpha} \mid \alpha \in [\pi/2, 2\pi/3]\}$.*

Proof. Let a_n be the n-th Fourier coefficient of Θ_k. Then

$$M := \sum_{n=1}^{d_k-1} |a_n| \cdot e^{-2\pi n 0.65} \leq 2 \sum_{n=1}^{\infty} e^{-2\pi n 0.65} = 2 \frac{e^{-2\pi 0.65}}{1 - e^{-2\pi 0.65}} < 0.0343.$$

Note that

$$M < \frac{2-R}{2+R},$$

where R is as in theorem 5.14. Hence if $d_k > 14$, we conclude that all the zeros of Θ_k in the fundamental domain $\mathcal{F}$ lie on the circular arc.
For $d_k \leq 14$, one can explicitly compute the polynomial

$$Q_k(j) = \frac{\Theta_k}{\Delta^{n_k} E_4^{b_k} E_6^{a_k}}$$

in the j-invariant of degree n_k $(= d_k - 1)$, and show that the zeros of this polynomial lie in the interval $[0, 1728]$. □

A Hypergeometric Functions

In this appendix we recall some basic notations and properties of hypergeometric functions. For a general reference see [1]. We will only be considering the classical *Gauss' hypergeometric function*. Let $a, b, c \in \mathbb{R}$ and $c \notin \mathbb{Z}_{\leq 0}$. Define the ordinary hypergeometric function

$$ {}_2F_1(a,b,c;z) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n} \frac{z^n}{n!}, \tag{151} $$

where

$$ (q)_n = \begin{cases} 1 & n = 0, \\ q(q+1)\cdots(q+n-1) & n > 0. \end{cases} $$

If $a, b \notin \mathbb{Z}_{\geq 0}$ this defines an infinite series with radius of convergence 1 (if a and b are positive integers, (151) is just a polynomial).

A.1 Contiguous Relations

Let $F = {}_2F_1(a,b,c;z)$, then we have the following relations:

$$ \begin{aligned} z\frac{dF}{dz} &= z\frac{ab}{c}F(a+,b+,c+) && (152)\\ &= a(F(a+) - F) && (153)\\ &= b(F(b+) - F) && (154)\\ &= (c-1)(F(c-) - F) && (155)\\ &= \frac{(c-a)F(a-) + (a-c+bz)F}{1-z} && (156)\\ &= \frac{(c-b)F(b-) + (b-c+az)F}{1-z} && (157)\\ &= z\frac{(c-a)(c-b)F(c+) + c(a+b-c)F}{c(1-z)} && (158) \end{aligned} $$

where $F(a+)$ means ${}_2F_1(a+1,b,c;z)$ etc.

A.2 Hypergeometric Differential Equation

The hypergeometric function ${}_2F_1(a,b,c;z)$ is a solution to the differential equation:

$$ z(1-z)\frac{d^2w}{dz^2} + [c - (a+b+1)z]\frac{dw}{dz} - ab\,w = 0. \tag{159} $$

A.3 Hypergeometric Relations

We recall a few well-known relations between hypergeometric functions.

Proposition A.1 (Euler's transformation formula)**.**

$$ {}_2F_1(a,b,c;z) = (1-z)^{c-a-b}\,{}_2F_1(c-a,c-b,c;z). \tag{160} $$

Another relation is given by

Proposition A.2. *For $a \in \mathbb{Z}_{>0}$ we have*

$$ {}_2F_1\left(a, -a, \frac{1}{2}; \frac{1}{2}(1-\cos(z))\right) = \cos(az), \tag{161}$$

$$ = T_a(\cos(z)), \tag{162}$$

where T_a is the a-th Chebyshev polynomial of the first kind.

From the previous statement we immediately deduce the following:

Corollary A.3.

$$ {}_2F_1\left(\frac{-1}{4}, \frac{1}{4}, \frac{1}{2}; z\right) = \frac{1}{2}\left((1-z^{\frac{1}{2}})^{\frac{1}{2}} + (1+z^{\frac{1}{2}})^{\frac{1}{2}}\right). \tag{163}$$

B Bounds for Modular Forms

In this appendix we discuss some bounds for the coefficients of modular forms we need for section 5.

Lemma B.1. *Let $E_k = \sum_{n=0}^{\infty} a_n q^n$ be the Eisenstein series of weight $k \in \{4, 6, 8, 10, 12, 14\}$ (normalized such that $a_0 = 1$), then $|a_n| \leq 504 n^k$ for $n \geq 1$.*

Proof. Clearly $|a_1| \leq 504$ for all $k \in \{4, 6, 8, 10, 12, 14\}$, furthermore $|a_n| \leq 504\sigma_{k-1}(n)$ is trivially bounded by $504n^k$. □

Lemma B.2. *Write $\Delta = \sum_{n=0}^{\infty} \tau(n) q^n$, then $|\tau(n)| \leq 2n^6$.*

Proof. Using a bound by Deligne, see for example [23, p. 164], we have

$$|\tau(n)| \leq \sigma_0(n) n^{11/2}.$$

Trivially we have $\sigma_0(n) \leq 2\sqrt{n}$, so that $|\tau(n)| \leq 2n^6$. □

Lemma B.3. *Let $j = \sum_{n=-1}^{\infty} c_n q^n$ be the modular j-invariant. Then for $n \geq 1$:*

$$|c_n| \leq e^{4\pi n}.$$

Proof. Using [4], we have that for $n \geq 1$,

$$c_n \leq \frac{e^{4\pi\sqrt{n}}}{\sqrt{2} n^{3/4}}.$$

As

$$\frac{e^{4\pi\sqrt{n}}}{\sqrt{2} n^{3/4}} \leq e^{4\pi n}$$

and the coefficients of the j-invariant are all positive, the result follows. □

We finish this appendix with a bound for Δ on the unit circle:

Lemma B.4. *Let $\theta \in [\pi/2, 2\pi/3]$. Then we have $|\Delta(e^{i\theta})| \leq 0.00481$.*

Proof. See [18, Prop. 2.2.]. □

References

[1] Kazuhiko Aomoto and Michitake Kita, *Theory of hypergeometric functions*, Springer Monographs in Mathematics, Springer-Verlag, Tokyo, 2011, With an appendix by Toshitake Kohno, Translated from the Japanese by Kenji Iohara. MR 2799182

[2] Tom M. Apostol, *Modular functions and Dirichlet series in number theory*, second ed., Graduate Texts in Mathematics, vol. 41, Springer-Verlag, New York, 1990. MR 1027834

[3] Jonathan M. Borwein and Peter B. Borwein, *Pi and the AGM*, Canadian Mathematical Society Series of Monographs and Advanced Texts, vol. 4, John Wiley & Sons, Inc., New York, 1998, A study in analytic number theory and computational complexity, Reprint of the 1987 original, A Wiley-Interscience Publication. MR 1641658

[4] Nicolas Brisebarre and Georges Philibert, *Effective lower and upper bounds for the Fourier coefficients of powers of the modular invariant j*, J. Ramanujan Math. Soc. **20** (2005), no. 4, 255–282. MR 2193216

[5] Peter Bruin and Sander Dahmnen, *Modular forms*, 2016, URL: `https://www.few.vu.nl/~sdn249/modularforms16/Notes.pdf`. Accessed 2019-07-28.

[6] Jan H. Bruinier, Gerard van der Geer, Günter Harder, and Don Zagier, *The 1-2-3 of modular forms*, Universitext, Springer-Verlag, Berlin, 2008, Lectures from the Summer School on Modular Forms and their Applications held in Nordfjordeid, June 2004, Edited by Kristian Ranestad. MR 2385372

[7] Komaravolu Chandrasekharan, *Elliptic functions*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 281, Springer-Verlag, Berlin, 1985. MR 808396

[8] John H. Conway and Neil J. A. Sloane, *Sphere packings, lattices and groups*, third ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1999, With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. MR 1662447

[9] Gunther Cornelissen, *Sur les zéros des séries d'Eisenstein de poids $q^k - 1$ pour* $\mathrm{GL}_2(\mathbf{F}_q[T])$, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 7, 817–820. MR 1355834

[10] ———, *Zeros of Eisenstein series, quadratic class numbers and supersingularity for rational function fields*, Math. Ann. **314** (1999), no. 1, 175–196. MR 1689268

[11] David A. Cox, *Primes of the form $x^2 + ny^2$*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication. MR 3236783

[12] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005. MR 2112196

[13] William Duke and Paul Jenkins, *On the zeros and coefficients of certain weakly holomorphic modular forms*, Pure Appl. Math. Q. **4** (2008), no. 4, Special Issue: In honor of Jean-Pierre Serre. Part 1, 1327–1340. MR 2441704

[14] Eberhard Freitag, *Siegelsche Modulfunktionen*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 254, Springer-Verlag, Berlin, 1983. MR 871067

[15] Stephan R. Garcia and Roger A. Horn, *A second course in linear algebra*, Cambridge Mathematical Textbooks, Cambridge University Press, 2017.

[16] Sharon A. Garthwaite, Ling Long, Holly Swisher, and Stephanie Treneer, *Zeros of classical Eisenstein series and recent developments*, WIN—women in numbers, Fields Inst. Commun., vol. 60, Amer. Math. Soc., Providence, RI, 2011, pp. 251–263. MR 2777810

[17] Ernst-Ulrich Gekeler, *Some observations on the arithmetic of Eisenstein series for the modular group* $\mathrm{SL}(2,\mathbb{Z})$, Arch. Math. (Basel) **77** (2001), no. 1, 5–21, Festschrift: Erich Lamprecht. MR 1845671

[18] Jayce Getz, *A generalization of a theorem of Rankin and Swinnerton-Dyer on zeros of modular forms*, Proc. Amer. Math. Soc. **132** (2004), no. 8, 2221–2231. MR 2052397

[19] Oscar González, *An observation of rankin on hankel determinants*, `https://faculty.math.illinois.edu/~oscareg2/resources/publications/rankinDeterminantsV11.pdf`, Accessed: 2019-07-28.

[20] Godfrey H. Hardy and Srinivasa Ramanujan, *On the coefficients in the expansions of certain modular functions [Proc. Roy. Soc. A* **95** *(1919), 144–155]*, Collected papers of Srinivasa Ramanujan, AMS Chelsea Publ., Providence, RI, 2000, pp. 310–321. MR 2280880

[21] Carl G. J. Jacobi, *De functionibus elliptiques commentatio*, J. Reine Angew. Math. **4** (1829), 371–390. MR 1577743

[22] Masanobu Kaneko and Don Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials*, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 97–126. MR 1486833

[23] Neal Koblitz, *Introduction to elliptic curves and modular forms*, second ed., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993. MR 1216136

[24] Christian Krattenthaler, *Advanced determinant calculus: a complement*, Linear Algebra Appl. **411** (2005), 68–166. MR 2178686

[25] Tsuyoshi Miezaki and Manabu Oura, *On eisenstein polynomials and zeta polynomials ii*, arXiv preprint arXiv:1903.03281 (2019).

[26] Gabriele Nebe, Eric M. Rains, and Neil J. A. Sloane, *Codes and invariant theory*, Math. Nachr. **274/275** (2004), 104–116. MR 2092326

[27] Hiroshi Nozaki, *A separation property of the zeros of Eisenstein series for* $\mathrm{SL}(2,\mathbb{Z})$, Bull. Lond. Math. Soc. **40** (2008), no. 1, 26–36. MR 2409175

[28] Ken Ono, *Modular forms are everywhere: celebration of Don Zagier's 65th birthday*, Res. Math. Sci. **6** (2019), no. 1, Paper No. 15, 2. MR 3895432

[29] Ken Ono and Matthew A. Papanikolas, *p-adic properties of values of the modular j-function*, Galois theory and modular forms, Dev. Math., vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, pp. 357–365. MR 2059773

[30] Manabu Oura, *Eisenstein polynomials associated to binary codes*, Int. J. Number Theory **5** (2009), no. 4, 635–640. MR 2532271

[31] Pablo A. Parrilo, *MIT 6.256 algebraic techniques and semidefinite optimization*, `https://homepages.cwi.nl/~monique/eidma-seminar-parrilo/Parrilo-LectureNotes-EIDMA.pdf`. Last visited on 29-7-2019.

[32] Srinivasa Ramanujan, *On certain arithmetical functions [Trans. Cambridge Philos. Soc.* **22** *(1916), no. 9, 159–184]*, Collected papers of Srinivasa Ramanujan, AMS Chelsea Publ., Providence, RI, 2000, pp. 136–162. MR 2280861

[33] Fenny K. C. Rankin and Henry P. F. Swinnerton-Dyer, *On the zeros of Eisenstein series*, Bull. London Math. Soc. **2** (1970), 169–170. MR 0260674

[34] Robert A. Rankin, *The zeros of Eisenstein series*, Publ. Ramanujan Inst. No. **1** (1968/1969), 137–144. MR 0269598

[35] Zeév Rudnick, *On the asymptotic distribution of zeros of modular forms*, Int. Math. Res. Not. (2005), no. 34, 2059–2074. MR 2181743

[36] Bernhard Runge, *Codes and Siegel modular forms*, Discrete Math. **148** (1996), no. 1-3, 175–204. MR 1368288

[37] Theodor Schneider, *Arithmetische Untersuchungen elliptischer Integrale*, Math. Ann. **113** (1937), no. 1, 1–13. MR 1513075

[38] Jean P. Serre, *Congruences and modular forms*, Uspehi Mat. Nauk **28** (1973), no. 2(170), 183–196, Translated from the French (Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416, pp. 319–338, Lecture Notes in Math., Vol. 317, Springer, Berlin, 1973) by Ju. I. Manin. MR 0466021

[39] Carl L. Siegel, *A simple proof of* $\eta(-1/\tau) = \eta(\tau)\sqrt{\tau/i}$, Mathematika **1** (1954), 4. MR 0062774

[40] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR 817210

[41] Naomi Sweeting and Katharine Woo, *On the zeros of a class of modular functions*, Ann. Comb. **23** (2019), no. 2, 417–422. MR 3962865

[42] Gábor Szegő, *Orthogonal polynomials*, fourth ed., American Mathematical Society, Providence, R.I., 1975, American Mathematical Society, Colloquium Publications, Vol. XXIII. MR 0372517

[43] Edward Witten, *Three-Dimensional Gravity Revisited*, arXiv e-prints (2007), arXiv:0706.3359.

[44] Klaus Wohlfahrt, *Über die Nullstellen einiger Eisensteinreihen*, Math. Nachr. **26** (1963/64), 381–383. MR 167470