A GENERALIZATION OF A THEOREM OF RANKIN AND SWINNERTON-DYER ON ZEROS OF MODULAR FORMS

Jayce Getz

Abstract. Rankin and Swinnerton-Dyer [R, S-D] prove that all zeros of the Eisenstein series E_k in the standard fundamental domain for Γ lie on $A := \{e^{i\theta} : \frac{\pi}{2} \leq \theta \leq \frac{2\pi}{3}\}$. In this paper we generalize their theorem, providing conditions under which the zeros of other modular forms lie only on the arc A. Using this result we prove a speculation of Ono, namely that the zeros of the unique "gap function" in M_k, the modular form with the maximal number of consecutive zero coefficients in its q-expansion following the constant 1, has zeros only on A. In addition, we show that the j-invariant maps these zeros to totally real algebraic integers of degree bounded by a simple function of the weight k.

1. Introduction and Statement of Results.

Let $\mathbb{H}$ denote the complex upper half plane and $\Gamma := \mathrm{SL}_2(\mathbb{Z})$. The region

$$\mathbf{F} := \left\{ |z| \geq 1 \text{ and } -\frac{1}{2} \leq \mathrm{Re}(z) \leq 0 \right\} \bigcup \left\{ |z| > 1 \text{ and } 0 \leq \mathrm{Re}(z) < \frac{1}{2} \right\}$$

is the usual *fundamental domain* for $\mathbb{H}$ under the action of Γ. That is, $\mathbf{F}$ serves as a set of representatives for equivalence classes for $\mathbb{H}$ under the action of Γ by fractional linear transformations. We say that a meromorphic function f on $\mathbb{H}$ is a *modular function* of *weight* k for Γ if

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{-k} f(z) \tag{1.1}$$

for all $z \in \mathbb{H}$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$. Further, if f is holomorphic on $\mathbb{H}$ and at the cusps of $\mathbf{F}$, it is a *modular form*. Denote by M_k the finite-dimensional complex vector space of such modular forms under the action of Γ. The description of the zeros of a modular function $f \in M_k$ on $\mathbb{H}$ is clearly equivalent to the description of the zeros of f on $\mathbf{F}$. Thus, for the remainder of this paper, when we speak of a zero z_0 of $f \in M_k$, we assume $z_0 \in \mathbf{F}$.

For even integers $k \geq 2$, let $E_k(z)$ be the usual Eisenstein series

$$E_k(z) := 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n, \tag{1.2}$$

where $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$ and B_k is the kth Bernoulli number. Throughout this paper, $q = e^{2\pi i z}$ and we make the convention that $E_0(z) := 1$. Recall that if $k \geq 4$ is even, then

1991 *Mathematics Subject Classification.* Primary 11F.
Key words and phrases. Modular forms.

$E_k(z) \in M_k$. In [R, S-D], Rankin and Swinnerton-Dyer prove that if $E_k(z) = 0$ and $z \in \mathbf{F}$, then $z \in A$, where

$$A := \left\{ e^{i\theta} : \frac{\pi}{2} \leq \theta \leq \frac{2\pi}{3} \right\}. \tag{1.3}$$

In this paper we generalize their result, providing a method of determining that the zeros of a modular form f on $\mathbf{F}$ lie only on the arc A. Before we state this result, we recall the following definitions:

$$j(z) := q^{-1} + 744 + 196884q + \cdots \tag{1.4}$$

is the usual normalized weight zero modular function and

$$\Delta(z) = \frac{E_4(z)^3 - E_6(z)^2}{1728} = q - 24q^2 + 252q^3 - 1472q^4 + \cdots \tag{1.5}$$

is the unique normalized weight 12 cusp form on Γ. Further, we define

$$\epsilon := e^{-\pi\sqrt{3}} \left(\sum_{n=-\infty}^{\infty} e^{-\pi\sqrt{3}(3n^2-n)/2} \right)^{24} \sim 0.004809... \tag{1.6}$$

We note here, and will prove later in Proposition 2.2, that $|\Delta(z)| \leq \epsilon$ for $z \in A$. Finally, if $k = 12m + s$, where $s = 0, 4, 6, 8, 10, 12, 14$, let

$$m(k) := m. \tag{1.7}$$

Theorem 1. *Let $k \geq 4$ be even and $f(z) = E_k(z) + \sum_{i=1}^{m(k)} a_i E_{k-12i}\Delta^i \in M_k$, where $a_i \in \mathbb{R}$. Suppose*

$$\sum_{i=1}^{m(k)} |a_i|\epsilon^i < \frac{1-\delta}{3+\delta},$$

where $\delta := .03562$. If $f(z) = 0$ and $z \in \mathbf{F}$, then $z \in A$, and $j(z) \in [0, 1728]$. In particular, f has $m(k)$ simple zeros on $\{e^{i\theta} : \frac{\pi}{2} < \theta < \frac{2\pi}{3}\}$, and we have the following trivial zeros of f depending on k modulo 12:

$$\mathrm{ord}_i(f) = \begin{cases} 1 & \text{if } k \equiv 2 \pmod 4, \\ 0 & \text{if } k \equiv 0 \pmod 4, \end{cases}$$

and

$$\mathrm{ord}_\rho(f) = \begin{cases} 2 & \text{if } k \equiv 2 \pmod 6, \\ 1 & \text{if } k \equiv 4 \pmod 6, \\ 0 & \text{if } k \equiv 0 \pmod 6. \end{cases} \tag{1.8}$$

Here $\rho := e^{2\pi i/3}$.

A natural question to ask is whether or not Theorem 1 can be applied to any interesting families of modular forms. In Section 3 we provide such a family, the so-called "gap functions."

Definition. *If $k \geq 4$ is even, the gap function $F_k(z) \in M_k$ is the unique modular form with Fourier expansion*

$$F_k(z) = 1 + c(m(k)+1)q^{m(k)+1} + c(m(k)+2)q^{m(k)+2} + \cdots = 1 + \sum_{n \geq m(k)+1} c(n)q^n$$

where $c(n) \in \mathbb{C}$ is the nth Fourier coefficient.

For example, we have

$$F_{12}(z) = E_{12}(z) + \frac{24}{B_{12}}\Delta(z) = 1 + 196560q^2 + 16773120q^3 + \cdots .$$

These and similar functions are useful in coding theory. For example, [M, O, S] considered the parity of the real parts of the coefficients $c(m(k)+1)$, $c(m(k)+2)$, ... of F_k among other q-series. In this work we are interested in the zeros of F_k. Ono speculated that these zeros of F_k all lie on the arc A. Armed with Theorem 1, we prove this result:

Theorem 2. *Suppose $k \geq 4$ is even. If $F_k(z) = 0$ and $z \in \mathbf{F}$, then $z \in A$ and $j(z) \in [0, 1728]$, with $m(k)$ simple zeros on the interior of the arc. Moreover, F_k has trivial zeros at i and ρ depending on k modulo 12 as in (1.8).*

We can construct totally real extensions of $\mathbb{Q}$ by adjoining $j(z_0)$, where z_0 is a zero of any of the functions described in Theorems 1 and 2. It is a well-known fact from the theory of complex multiplication that if z is a CM point, $j(z)$ is an algebraic integer. We observe an analogous phenomenon in the case of the zeros of the gap functions; the j-invariant maps them to totally real algebraic integers. In addition, for certain weights, these algebraic integers reduce to supersingular j-invariants in in $\overline{\mathbb{F}}_p$.

Corollary 3. *Suppose $k \geq 4$ is even. If $F_k(z) = 0$ and $z \in \mathbf{F}$, then $j(z)$ is an algebraic integer. If $k = p - 1$, where $p \geq 5$ is prime, then there is a maximal ideal $\mathbf{m}$ of the ring of integers of $\mathbb{Q}(j(z))$ lying over p such that $j(z)$ modulo $\mathbf{m}$ is the j-invariant of a supersingular elliptic curve.*

2. Preliminaries and Proof of Theorem 1.

We begin with a general discussion of the zeros of a nonzero element $f \in M_k$. A classical result on this subject is the valence formula (see §[III.2][K]):

$$\frac{k}{12} = \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \mathrm{ord}_\infty(f) + \sum_{\tau \in \Gamma \backslash \mathbb{H} - \{i,\rho\}} \mathrm{ord}_\tau(f).$$

Writing $k = 12m(k) + s$ as in (1.7), note that s determines the residue class of k modulo 12. Bearing in mind the valence formula, an examination of the possible values of s implies that

$$\mathrm{ord}_i(f) \geq \begin{cases} 1 & \text{if } k \equiv 2 \pmod 4, \\ 0 & \text{if } k \equiv 0 \pmod 4, \end{cases}$$

and

$$\mathrm{ord}_\rho(f) \geq \begin{cases} 2 & \text{if } k \equiv 2 \pmod 6, \\ 1 & \text{if } k \equiv 4 \pmod 6, \\ 0 & \text{if } k \equiv 0 \pmod 6. \end{cases} \tag{2.1}$$

For example, let $k = 26$. We have

$$\frac{26}{12} = \frac{13}{6} = \frac{1}{2}\text{ord}_i(f) + \frac{1}{3}\text{ord}_\rho(f) + \text{ord}_\infty(f) + \sum_{\tau \in \Gamma\backslash\mathbb{H} - \{i,\rho\}} \text{ord}_\tau(f).$$

Clearly $\text{ord}_i(f)$ and ord_ρ are nonzero. If $\text{ord}_\rho(f) = 1$, then the left hand side of the above equation is of the form $\frac{1}{2}n + \frac{5}{6}$. There is no integer n such that $\frac{1}{2}n + \frac{5}{6} = \frac{13}{6}$, so we have $\text{ord}_\rho(f) \geq 2$. For further discussion of (2.1), see [A,O].

Again applying the valence formula for $k = 12m(k) + s$, by (2.1), there are at most $m(k)$ on $\mathbf{F} - \{\rho, i\}$. Thus if $f \in M_k$ satisfies the hypothesis of Theorem 1, then to prove Theorem 1 it suffices to demonstrate that f has $m(k)$ simple zeros in the interior of A.

We now require a proposition on normalization of modular functions on the arc A.

Proposition 2.1. *If f is a modular function of weight k with real coefficients, then $e^{ik\theta/2}f(e^{i\theta})$ is real on $\{\theta : \frac{\pi}{2} \leq \theta \leq \frac{2\pi}{3}\}$.*

Proof. From the functional equation (1.1) we have $f(-1/z) = z^k f(z)$. For $z = a + bi \in A$, we have $-\frac{1}{z} = \frac{-a+bi}{a^2+b^2} = -a + bi$. Write f in terms of its Fourier expansion as

$$f(z) = \sum_{n \geq n_f} a_n e^{2\pi i n(a+bi)} = \sum_{n \geq n_f} a_n e^{2\pi n(-b+ai)},$$

where n_f is an integer which depends on f. We have

$$f(-1/z) = \sum_{n \geq n_f} a_n e^{2\pi i n(-a+bi)} = \sum_{n \geq n_f} a_n e^{2\pi n(-b-ai)} = \overline{f(z)}.$$

Note that $-1/e^{i\theta} = e^{i(\pi-\theta)}$. The above facts imply that

$$e^{ik(\pi-\theta)/2}f(e^{i(\pi-\theta)}) = e^{ik(\pi-\theta)/2}e^{ik\theta}f(e^{i\theta})$$

$$e^{ik(\pi-\theta)/2}\overline{f(e^{i\theta})} = e^{ik(\pi+\theta)/2}f(e^{i\theta})$$

$$e^{-ik\theta/2}\overline{f(e^{i\theta})} = e^{ik\theta/2}f(e^{i\theta})$$

$$\overline{e^{ik\theta/2}f(e^{i\theta})} = e^{ik\theta/2}f(e^{i\theta}).$$

□

Notice that Proposition 2.1 shows us that $j(z)$ is real for $z \in A$. Furthermore, we have that $j(i) = 1728, j(\rho) = 0$, and that j is a bijection between $\mathbf{F}$ and $\mathbb{C}$. An application of the intermediate value theorem implies that $j(z) \in [0, 1728]$ for all $z \in A$. Similarly, in [R,S-D], Rankin and Swinnerton-Dyer use the intermediate value theorem to describe the zeros of $E_k(z)$ for $k \geq 12$ after proving that

$$e^{ik\theta/2}E_k(e^{i\theta}) = 2\cos(k\theta/2) + R_k, \tag{2.2}$$

where

$$|R_k| < 1 + \delta \tag{2.3}$$

where $\delta := .03562$ as above. A stronger bound will not be necessary for the purposes of this paper, though one could be easily calculated (again, see [R, S-D]). However, we will need a bound for $\Delta(z)$ when $z \in A$, which we now provide:

Proposition 2.2. *If $z \in A$, then $|\Delta(z)| \leq \epsilon$, where ϵ is defined as in (1.6).*

Proof. A standard identity (see §[III.2][K]) gives us

$$\Delta(z) = e^{2\pi iz}\prod_{n=1}^{\infty}(1-e^{2\pi inz})^{24} = \left(e^{2\pi iz/24}\prod_{n=1}^{\infty}(1-e^{2\pi inz})\right)^{24}.$$

By Euler's pentagonal number theorem §[14.5][A], we have

$$\prod_{n=1}^{\infty}(1-e^{2\pi inz}) = \sum_{n=-\infty}^{\infty}(-1)^n e^{2\pi iz(3n^2-n)/2}.$$

Writing $z = e^{i\theta} = a + bi$ for $a, b \in \mathbb{R}$, we have

$$\left|\prod_{n=1}^{\infty}(1-e^{2\pi inz})\right| \leq \sum_{n=-\infty}^{\infty}\left|(-1)^n e^{2\pi i(a+bi)}\right|^{(3n^2-n)/2} = \sum_{n=-\infty}^{\infty} e^{-\pi b(3n^2-n)}$$

Now, for $z = a + bi \in A$, $e^{-\pi b(3n^2-n)}$ is maximized at $z = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ so

$$|e^{2\pi iz}|\left|\prod_{n=1}^{\infty}(1-e^{2\pi inz})\right|^{24} \leq e^{-\pi\sqrt{3}}\left(\sum_{n=-\infty}^{\infty} e^{-\pi\sqrt{3}(3n^2-n)/2}\right)^{24} = \epsilon.$$

A Maple calculation shows that $\epsilon \sim 0.004809\ldots$. □

We are now ready to proceed with the proof of the main theorem.

Proof of Theorem 1. Write $k = 12m(k) + s$ as in (1.7). The theorem is easily proven for the lower weights by noting that E_4, E_6 are supported by zeros at ρ and i respectively, and that for $k < 12$ and $k = 14$, we have $E_k = E_4^a E_6^b$, where $a, b \in \mathbb{Z}_{\geq 0}$ are chosen so that $4a + 6b = k$ §[III.2][K]. Write

$$H(\theta) := e^{ik\theta/2}f(e^{i\theta}) = H_0(\theta) + \sum_{j=1}^{m(k)} a_j e^{12ji\theta/2}\Delta^j H_j(\theta), \tag{2.4}$$

where $H_j(\theta) = e^{(k-12j)i\theta/2}E_{k-12j}(e^{i\theta})$. By (2.2) and (2.3), we have $H_j(\theta) = 2\cos((k-12j)\theta/2) + R_{k-12j}$, where $|R_{k-12j}| < 1 + \delta$. Thus

$$H(\theta) := 2\cos(k\theta/2) + R_k + \sum_{j=1}^{m(k)} a_j e^{12ji\theta/2}\Delta^j(2\cos((k-12j)\theta/2) + R_{k-12j}) \tag{2.5}$$

The bound on $\Delta(z)$ from Proposition 2.1, (2.2) and (2.3) imply that

$$\left|R_k + \sum_{j=1}^{m(k)} a_j e^{12ji\theta/2}\Delta^j(2\cos((k-12j)\theta/2) + R_{k-12j})\right| \leq 1 + \delta + \sum_{j=1}^{m(k)}|a_j|\epsilon^j(3+\delta).$$

Now, assuming

$$\sum_{i=1}^{m(k)}|a_i|\epsilon^i < \frac{1-\delta}{3+\delta},$$

we have

$$1+\delta+\sum_{i=1}^{m(k)}|a_i|\epsilon^i(3+\delta)<2. \tag{2.6}$$

Let n be an integer such that $\frac{k}{4}\leq n\leq\frac{k}{3}$. Note that $H(\theta)$ is a real-valued function dominated by the trigonometric function $2\cos(k\theta/2)$. Considering the bound (2.6), (2.5) implies that $H(2n\pi/k)$ is strictly positive or negative depending on the parity of n. Thus, by the intermediate value theorem, $H(\theta)$ has at least as many zeros in the open interval $(\pi/2,2\pi/3)$ as there are integers in the the interval $[\frac{k}{4},\frac{k}{3}]$ minus one, and this number is $m(k)$. Recalling (2.1) and the following discussion, this fact is sufficient to finish the proof. □

3. Gap Functions and the j-invariant

We begin by providing the following bound on the coefficients of the q-expansion of arbitrary powers of $\Delta(z)$.

Theorem 3.1. *If s is a positive integer, then define integers $\tau_s(n)$ by*

$$\Delta(z)^s=\sum_{n=0}^{\infty}\tau_s(n)q^n:=q^s\prod_{n=1}^{\infty}(1-q^n)^{24s}.$$

If $n\geq 1$, then

$$|\tau_s(n)|\leq\frac{n^{7s-1}}{s^{6s}}.$$

Proof. We have

$$\tau_s(n)=\sum_{\substack{k_1+\ldots+k_s=n\\1\leq k_i\leq n}}\prod_{i=1}^{s}\tau(k_i).$$

A well-known result of Deligne (see, for example, §[III.2][K]) gives the following strong bound on the q-expansion coefficients of $\Delta(z)$:

$$|\tau(n)|\leq n^{11/2}\sigma_0(n).$$

For $n\geq 40$, $n^{11/2}\sigma_0(n)\leq n^{11/2}(\frac{\log n}{\log 2}+1)\leq n^{11/2}n^{1/2}=n^6$, and a simple Maple calculation shows that $|\tau(n)|\leq n^6$ for $1\leq n\leq 40$. Thus

$$|\tau_s(n)|\leq\sum_{\substack{k_1+\cdots+k_s=n\\1\leq k_i\leq n}}\prod_{i=1}^{s}|\tau(k_i)|\leq\sum_{\substack{k_1+\cdots+k_s=n\\1\leq k_i\leq n}}\prod_{i=1}^{s}k_i^6$$

which implies

$$|\tau_s(n)|\leq\sum_{\substack{k_1+\cdots+k_s=n\\1\leq k_i\leq n}}\left(\frac{n}{s}\right)^{6s}\leq n^{s-1}\left(\frac{n}{s}\right)^{6s}.$$

Here we use that the maximum product of s positive integers whose sum is n is bounded by $\left(\frac{n}{s}\right)^s$. We also use that the first $s-1$ choices $k_1,\ldots,k_{s-1}$ determine the choice of k_s. Thus

$$|\tau_s(n)|\leq n^{s-1}\left(\frac{n}{s}\right)^{6s}=\frac{n^{7s-1}}{s^{6s}}.$$

□

Proof of Theorem 2. We proceed by induction on the weight k. Three facts are needed to establish the basis of our induction. For $k \leq 300$, Maple calculations, using the method of this proof, establish first that the zeros of F_k lie on the arc A as in the statement of the theorem, and second that $|e^{ik\theta/2}F_k(e^{i\theta})| < 4$ for $\frac{\pi}{2} < \theta < \frac{2\pi}{3}$. Write

$$e^{ik\theta/2}F_k(e^{i\theta}) = e^{ik\theta/2}E_k(e^{i\theta}) + \sum_{j=1}^{m(k)} a_j e^{12ij\theta/2}\Delta(e^{i\theta})^j e^{(k-12j)i\theta/2}F_{k-12j}(e^{i\theta}) \tag{3.1}$$

with the convention that $F_0 := 1$. We note here that the q-expansion coefficients of Δ are integers and so $a_j \in \mathbb{R}$. The third fact which we require, and will prove later, is that if $k \geq 300$, then

$$\sum_{j=1}^{m(k)} |a_j|\epsilon^j < \frac{1-\delta}{4}. \tag{3.2}$$

These three facts complete the basis step of our induction. Assuming (3.2), we have

$$1 - \delta > 4\sum_{j=1}^{m(k)} |a_j|\epsilon^j \geq \sum_{j=1}^{m(k)} |a_j||e^{12ij\theta/2}\Delta^j||e^{(k-12j)i\theta/2}F_{k-12j}|$$

which implies

$$1 - \delta > \left|\sum_{j=1}^{m(k)} a_j e^{12ij\theta/2}\Delta^j e^{(k-12j)i\theta/2}F_{k-12j}\right|. \tag{3.3}$$

From (3.1),(3.3),(2.2), and (2.3), we have

$$e^{ik\theta/2}F_k(e^{i\theta}) = 2\cos(k\theta/2) + R_k + T_k, \tag{3.4}$$

where $|R_k| < 1 + \delta$ and $|T_k| < 1 - \delta$. Noting that $|R_k| + |T_k| < 2$ and arguing in a manner analogous to the proof of Theorem 1, again assuming (3.2), (3.4) proves that F_k has zeros on the arc A as described in the statement of Theorem 2. Assuming (3.2) for $k \geq 300$, we must show that $|F_k(z)| < 4$ for $z \in A$ to complete the induction. By (2.2),(2.3), and (3.2) we have

$$|e^{ik\theta/2}F_k(e^{i\theta})| < 2 + R_k + \sum_{j=1}^{m(k)} |a_j||e^{12ij\theta/2}\Delta^j||e^{(k-12j)i\theta/2}F_{k-12j}| < 4.$$

Thus we have proven that F_k has zeros on A as desired, and its normalization is bounded in such a way that we can move on to prove the same result for F_{k+12} This completes the induction, though we must now establish (3.2).

As a modular form in M_k, $F_k = 1 + c(m(k)+1)q^{m(k)+1} + c(m(k)+2)q^{m(k)+2} + \dots$ is completely determined by its first $m(k)+1$ coefficients. Thus the problem of calculating the a_i can be reduced to a linear algebra problem; given the first few q-expansion coefficients, we wish to compute the coefficients a_i of the modular form with respect to the alternate basis $E_k, \Delta F_{k-12}, ..., \Delta^{m(k)}F_{k-12m(k)}$. Note that

$$\Delta^s F_{k-12s} = q^s + \tau_s(s+1)q^{s+1} + \tau_s(s+2)q^{s+2} + \cdots + \tau_s(m(k))q^{m(k)} + \dots.$$

Letting

$$A := \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ -\frac{2k}{B_k} & 1 & 0 & \cdots & 0 & 0 \\ -\frac{2k}{B_k}\sigma_{k-1}(2) & \tau(2) & 1 & \cdots & 0 & 0 \\ -\frac{2k}{B_k}\sigma_{k-1}(3) & \tau(3) & \tau_2(3) & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ -\frac{2k}{B_k}\sigma_{k-1}(m(k)-1) & \tau(m(k)-1) & \tau_2(m(k)-1) & \cdots & 1 & 0 \\ -\frac{2k}{B_k}\sigma_{k-1}(m(k)) & \tau(m(k)) & \tau_2(m(k)) & \cdots & \tau_{m(k)-1}(m(k)) & 1 \end{pmatrix},$$

we apply Cramer's rule to the equation

$$A(a_0, \cdots, a_{m(k)}) = (1, 0, \cdots, 0)$$

to arrive at the equality

$$a_i = \begin{vmatrix} 1 & 0 & 0 & \cdot & 0 & 1 & 0 & \cdot & 0 \\ -\frac{2k}{B_k} & 1 & 0 & \cdot & 0 & 0 & 0 & \cdot & 0 \\ -\frac{2k}{B_k}\sigma_{k-1}(2) & \tau(2) & 1 & \cdot & 0 & 0 & 0 & \cdot & 0 \\ -\frac{2k}{B_k}\sigma_{k-1}(3) & \tau(3) & \tau_2(3) & \cdot & 0 & 0 & 0 & \cdot & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ -\frac{2k}{B_k}\sigma_{k-1}(i-1) & \tau(i-1) & \tau_2(i-1) & \cdot & 1 & 0 & 0 & \cdot & 0 \\ -\frac{2k}{B_k}\sigma_{k-1}(i) & \tau(i) & \tau_2(i) & \cdot & \tau_{i-1}(i) & 0 & 0 & \cdot & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ -\frac{2k}{B_k}\sigma_{k-1}(m(k)-1) & \tau(m(k)-1) & \tau_2(m(k)-1) & \cdot & \tau_{i-1}(m(k)-1) & 0 & \tau_{i+1}(m(k-1)) & \cdot & 0 \\ -\frac{2k}{B_k}\sigma_{k-1}(m(k)) & \tau(m(k)) & \tau_2(m(k)) & \cdot & \tau_{i-1}(m(k) & 0 & \tau_{i+1}(m(k)) & \cdot & 1 \end{vmatrix}.$$

Clearly $a_0 = 1$ and $a_1 = \frac{2k}{B_k}$. Fix an $i > 1$. To simplify the corresponding matrix, we expand by minors on the on the $(i+1)$st column, and then "move up the diagonal," expanding by minors on the $(m(k)+1)$st column, the $m(k)$th column, the $(m(k)-1)$st column etc., reducing our problem to the calculation of the i by i matrix formed by taking the upper left $(i+1)$ by $(i+1)$ matrix and eliminating the 1st row and the $(i+1)$st column. This reduces the calculation of a_i to the calculation of the determinant of the matrix

$$\begin{pmatrix} -\frac{2k}{B_k} & 1 & 0 & \cdot & 0 \\ -\frac{2k}{B_k}\sigma_{k-1}(2) & \tau(2) & 1 & \cdot & 0 \\ -\frac{2k}{B_k}\sigma_{k-1}(3) & \tau(3) & \tau_2(3) & \cdot & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -\frac{2k}{B_k}\sigma_{k-1}(i-1) & \tau(i-1) & \tau_2(i-1) & \cdot & 1 \\ -\frac{2k}{B_k}\sigma_{k-1}(i) & \tau(i) & \tau_2(i) & \cdot & \tau_{i-1}(i) \end{pmatrix} \tag{3.5}$$

Denote the matrix in (3.5) by $D_{ki} = (d_{\alpha\beta})$ and note that

$$\det D_{ki} = \sum_{\sigma \in S_i} \operatorname{sgn}(\sigma) d_{1\sigma(1)} \cdots d_{i\sigma(i)}.$$

Consider a permutation σ of columns of $(d_{\alpha\beta})$ which induces a nonzero product $d_{1\sigma(1)}\cdots d_{i\sigma(i)}$. We have two nonzero choices for $d_{1\sigma(1)}$. There are three nonzero entries in the 2nd row and we cannot choose $d_{2\sigma(1)}$, so there are two nonzero choices. Continuing in this manner and noting that $d_{i\sigma(i)}$ is determined by $d_{1\sigma(1)},...,d_{i-1\sigma(i-1)}$, we have 2^{i-1} possible nonzero products. With this in mind we define a new function B on the matrices D_{ki} by

$$B(D_{ki}) = 2^{i-1}\max\{|d_{1\sigma(1)}|\cdots|d_{i\sigma(i)}| : \sigma \in S_i\}$$

and note that $|a_i| = |\det D_{ki}| \leq B(D_{ki})$.

Now, substituting the trivial bound $\sigma_{k-1}(n) \leq n^k$ and the bound of Theorem 3.1, we have

$$|a_i| \leq B\begin{pmatrix} |\frac{2k}{B_k}| & 1 & 0 & \cdot & 0 \\ |\frac{2k}{B_k}|2^k & 2^6 & 1 & \cdot & 0 \\ |\frac{2k}{B_k}|3^k & 3^6 & \frac{3^{13}}{3^{12}} & \cdot & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ |\frac{2k}{B_k}|(i-1)^k & (i-1)^6 & \frac{(i-1)^{13}}{3^{12}} & \cdot & 1 \\ |\frac{2k}{B_k}|i^k & i^6 & \frac{i^{13}}{3^{12}} & \cdot & \frac{i^{7(i-1)-1}}{(i-1)^{6(i-1)}} \end{pmatrix}. \tag{3.6}$$

If we write D_{ik} as a set of i column vectors $(v_1,\cdots,v_j,\cdots,v_i)$, it follows from the definition of B that $B(v_1,\cdots,cv_j,\cdots,v_i) = cB(v_1,\cdots,v_j,\cdots,v_i)$ for any complex number c. This is because factoring out c is equivalent to multiplying every element in the set $\{d_{1\sigma(1)}\cdots d_{i\sigma(i)} : \sigma \in S_i\}$ by c^{-1}, which doesn't change which element of that set has maximal absolute value. Thus factoring $|\frac{2k}{B_k}|$ from the first column and $\frac{1}{(j-1)^{6(j-1)}}$ from the jth for $j > 1$, we have that (3.6) is equal to $\left(\left|\frac{B_k}{2k}\right| 2^{12}\cdots(i-1)^{6(i-1)}\right)^{-1}$ times

$$B\begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 2^k & 2^6 & 2^{12} & \cdots & 0 & 0 \\ 3^k & 3^6 & 3^{13} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ (i-1)^k & (i-1)^6 & (i-1)^{13} & \cdots & (i-1)^{7(i-2)-1} & (i-1)^{6(i-1)} \\ i^k & i^6 & i^{13} & \cdots & i^{7(i-2)-1} & i^{7(i-1)-1} \end{pmatrix} \tag{3.7}$$

Denote the matrix in (3.7) by $U_{ki} = (u_{\alpha\beta})$. We now claim that

$$\max\{|u_{1\sigma(1)}|\cdots|u_{i\sigma(i)}| : \sigma \in S_i\} = u_{12}u_{23}\cdots u_{(i-1)i}u_{i1} = i^k(1)(2^{12})\cdots(i-1)^{6(i-1)}. \tag{3.8}$$

To see this, first note that we must choose one entry from the first column. Say this entry is u_{r1}. In addition, we must choose one nonzero entry from every row besides the rth, and none of these entries can be in the first column. In order to maximize the product, we want to choose the entry in each row that is not in the first column of maximum absolute value. Thus we choose the entries $u_{12}, u_{23}, ..., u_{(r-1)r}, u_{(r+1)(r+2)}, ..., u_{(i-1)i}$. Note that the structure of the matrix, which is "almost diagonal," allows this as a possible element of the set $\{u_{1\sigma(1)}\cdots u_{i\sigma(i)} : \sigma \in S_i\}$. In particular, it gives us the product $u_{12}u_{23}\cdots u_{(r-1)r}u_{r1}u_{(r+1)(r+2)}\cdots u_{(i-1)i}$. Examining the matrix $(u_{\alpha\beta})$, it is clear that the maximum product is induced when $r = i, u_{r1} = i^k$.

From (3.7) and (3.8), we have

$$|a_i| \leq \left(\left|\frac{B_k}{2k}\right| 2^{12}\cdots(i-1)^{6(i-1)}\right)^{-1} B(U_{ki})$$

which implies

$$|a_i| \leq \left|\frac{B_k}{2k}\right|^{-1} \left((2^{12})\cdots(i-1)^{6(i-1)}\right)^{-1} 2^{i-1} i^k (1) \left((2^{12})\cdots(i-1)^{6(i-1)}\right) = \left|\frac{2k}{B_k}\right| 2^{i-1} i^k.$$

Thus

$$\sum_{j=1}^{m(k)} |a_j| \epsilon^j \leq \left|\frac{2k}{B_k}\right| \sum_{j=1}^{m(k)} 2^{j-1} j^k \epsilon^j \tag{3.9}$$

A standard bound on the Bernoulli numbers (see §[15][I, R], pp. 232) gives us $|\frac{2k}{B_k}| < \frac{k(\pi e)^k}{(k/2)^k}$, which implies

$$\left|\frac{2k}{B_k}\right| \sum_{j=1}^{m(k)} 2^{j-1} j^k \epsilon^j < \frac{k(\pi e)^k}{(k/2)^k} \sum_{j=1}^{m(k)} 2^{j-1} j^k \epsilon^j$$

Noting that $m(k) \leq k/12$ and $2^{j-1} j^k \epsilon^j$ is monotonically increasing for $1 \leq j \leq m(k)$, we have

$$\frac{k(\pi e)^k}{(k/2)^k} \sum_{j=1}^{m(k)} 2^{j-1} j^k \epsilon^j < \frac{k(\pi e)^k}{(k/2)^k} m(k)^{k+1} \epsilon^{m(k)} 2^{m(k)-1} \leq \frac{k^2 (\pi e \epsilon^{1/12} 2^{1/12})^k}{24(6)^k}$$

which decreases monotonically as $k \geq 59$ approaches infinity. Further, for $k \geq 300$, $\frac{k^2(\pi e \epsilon^{1/12} 2^{1/12})^k}{24(6)^k} < \frac{1-\delta}{4}$. This implies (3.2) and completes the proof. □

As stated before, if a zero of a modular function lies on A, then the j-invariant of that zero is a real number in the interval $[0, 1728]$. In order to prove Corollary 3, however, we need more information. Following [A, O], we define the following polynomials h_k and modular forms $\widetilde{E}_k(z)$ for even $k \geq 4$:

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

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

In [A, O], Ahlgren and Ono prove the following lemma using these definitions:

Lemma 3.2. *Suppose that $f \in M_k$ has leading coefficient 1. Let $\widetilde{F}(f, x)$ be the unique rational function in x for which*

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

Then $\widetilde{F}(f,x)$ is a polynomial.

For $f(z) \in M_k$, we then define the polynomial $F(f,x)$ by

$$F(f,x) := h_k(x)\widetilde{F}(f,x). \tag{3.10}$$

Note that F is constructed so that $F(f,x) = 0$ if and only if $x = j(z)$, where $z \in \mathbf{F}$ is a zero of f.

Proof of Corollary 3. Fix a weight k, and write

$$F_k' = \sum_{j=0}^{m(k)} a_j' \Delta^j E_4^{r_j} E_6^{s_j} = 1 + c'(m(k)+1)q^{m(k)+1} + c'(m(k)+2)q^{m(k)+2} + \cdots$$

where $r_i, s_i \in \mathbb{Z}_{\geq 0}$ are chosen so that $4r_i + 6s_i = k - 12j$. Because $F_k' \in M_k$, it is determined by its first $m(k)+1$ coefficients. Thus $F_k' = F_k$, our familiar gap function. Observe that the coefficients of the q-expansions of Δ, E_4, E_6 are integers. Therefore $a_j', c_j' \in \mathbb{Z}$; the coefficients of F_k are integers. Noting that $\widetilde{E}_k(z)$ is a product of E_4, E_6 for each k, we have that $F(F_k,x)$ is a monic polynomial in $\mathbb{Z}[x]$. Thus the zeros of $F(F_k,x)$ are algebraic integers, and these zeros are precisely the $j(z)$ where $F_k(z) = 0$.

Consider the polynomial

$$S_p(x) := \prod_{\substack{E/\overline{\mathbb{F}}_p \\ \text{supersingular}}} (x - j(E)) \in \mathbb{F}_p[x]$$

A well-known result of Deligne (see [S]) implies that if $p \geq 5$ is prime, then

$$S_p(x) \equiv F(E_{p-1}, x) \pmod{p}.$$

Note that the Von-Staudt congruences imply that $\frac{2(p-1)}{B_{p-1}} \equiv 0 \pmod{p}$. In addition, F_k, as a modular form in M_k, is determined by its first $m(k)+1$ coefficients. Thus, considering these q-expansion coefficients,

$$F_{p-1} \equiv E_{p-1} \equiv 1 \pmod{p}.$$

which implies

$$F(F_{p-1}, x) \equiv F(E_{p-1}, x) \equiv S_p(x) \pmod{p}.$$

□

References

[A, O] S. Ahlgren and K. Ono, *Weierstrass points on $X_0(p)$ and supersingular j-invariants*, Math. Ann. accepted for publication.

[A] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

[I, R] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1990.

[K] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, 1993.

[M, O, S] C. L. Mallows, A.M. Odlyzko and N.J.A. Sloane, *Upper Bounds for Modular Forms, Lattices, and Codes*, Journal of Algebra **36** (1975), 68-76.

[R, S-D] F.K.C. Rankin and H.P.F. Swinnerton-Dyer, *On the zeros of Eisenstein series*, Bull. London Math. Soc. **2** (1970), 169-170.

[S] J-P. Serre, *Congruences et formes modulaires (d'après H. P. F. Swinnerton-Dyer)*, Sem. Bourbaki **416** (1971-1972), 74-88.

4404 South Avenue West, Missoula, MT 59804

E-mail address: getz@fas.harvard.edu