ODD COEFFICIENTS OF WEAKLY HOLOMORPHIC MODULAR FORMS

Scott Ahlgren and Matthew Boylan

1. Introduction

Suppose that N is a positive integer, that w is an integer, and that

$$f(z) = \sum a(n)q^n, \qquad q := e^{2\pi iz} \tag{1.1}$$

is a weakly holomorphic modular form of integral or half-integral weight $\frac{w}{2}$ on the congruence subgroup $\Gamma_1(N)$. By a *weakly holomorphic modular form* we mean a function $f(z)$ which is holomorphic on the upper half-plane, meromorphic at the cusps, and which transforms in the usual way under the action of $\Gamma_1(N)$ on the upper half-plane (see, for example, [13] for generalities on modular forms of half-integral weight). We denote the space of such forms by $\mathcal{M}_{\frac{w}{2}}(\Gamma_1(N))$. Now, suppose that L is an algebraic number field, v is a place of L over 2, and $\mathcal{O}_v$ is the local ring at v. We assume that the coefficients $a(n)$ in (1.1) belong to $\mathcal{O}_v$, and if $\mathfrak{m}_v$ is the maximal ideal of $\mathcal{O}_v$, then we write $\pmod{v}$ to mean $\pmod{\mathfrak{m}_v}$. We will consider the question of estimating the number of integers n for which $a(n) \not\equiv 0 \pmod{v}$.

For a well-studied example, let $p(n)$ be the ordinary partition function. Many authors have considered the problem of estimating the number of odd values of $p(n)$. Among other references, one may see [1], [5], [15], [16], [17], [18], [19], [22], or [24]. To see the connection to the general situation above, we recall the definition of the Dedekind eta-function:

$$\eta(z) := q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n) = \sum_{m\in\mathbb{Z}} (-1)^m q^{\frac{(6m+1)^2}{24}}. \tag{1.2}$$

Then we have the identity

$$\sum_{n=0}^{\infty} p(n)q^{24n-1} = \frac{1}{\eta(24z)} \in \mathcal{M}_{\frac{-1}{2}}(\Gamma_1(576))$$

(this example will be discussed in more detail below).

We return to the general situation. To see the best that one might hope to prove, we recall the definition of the usual theta function

$$\theta(z) := 1 + 2\sum_{n=1}^{\infty} q^{n^2} \in \mathcal{M}_{\frac{1}{2}}(\Gamma_1(4)). \tag{1.3}$$

Received by the editors May 31, 2007.

The first author thanks the National Science Foundation for its support through grant DMS 01-34577. The second author thanks the National Science Foundation for its support through grant DMS 06-00400.

It is therefore possible for a form as in (1.1) to have only one non-vanishing coefficient modulo 2. For another example, we note that for all integers j the modular form

$$f(z) := \sum a(n)q^n = \frac{\eta(24z)}{\theta(z)^j} \equiv \sum_{m\in\mathbb{Z}} (-1)^m q^{(6m+1)^2} \pmod 2 \tag{1.4}$$

lies in $\mathcal{M}_{\frac{-j}{2}+\frac{1}{2}}(\Gamma_1(576))$. From (1.4), it follows that

$$\#\{n \le X \ : a(n) \not\equiv 0 \pmod 2\} \ll \sqrt{X}. \tag{1.5}$$

In this paper we will obtain a general lower bound which is quite close to the upper bound in (1.5). In particular we will prove the following.

Theorem 1.1. *Suppose that $\mathcal{O}$ is the ring of integers of an algebraic number field, that v is a place over the prime 2, that N is a positive integer, and that w is an integer. Let $f(z) = \sum a(n)q^n \in \mathcal{M}_{\frac{w}{2}}(\Gamma_1(N)) \cap \mathcal{O}_v((q))$ and suppose that $f(z)$ is not congruent to a constant modulo v. Then for any $K > 0$ we have*

$$\#\{n \le X \ : a(n) \not\equiv 0 \pmod v\} \gg \frac{\sqrt{X}}{\log X}(\log\log X)^K,$$

where the implied constant depends on f and K.

There is an analogous result in the case when ℓ is an odd prime (the proof, as we shall see, is easier in this case). For completeness we record the result here.

Theorem 1.2. *Suppose that $\mathcal{O}$ is the ring of integers of an algebraic number field, that v is a place over an odd prime ℓ, that N is a positive integer, and that λ is an integer. Suppose that $f(z) = \sum a(n)q^n \in \mathcal{M}_{\lambda+\frac{1}{2}}(\Gamma_1(N)) \cap \mathcal{O}_v((q))$ and that $f(z) \not\equiv 0$ $\pmod v$. Then for any $K > 0$ we have*

$$\#\{n \le X \ : a(n) \not\equiv 0 \pmod v\} \gg \frac{\sqrt{X}}{\log X}(\log\log X)^K,$$

where the implied constant depends on f, ℓ, and K.

Remark. Let v and $f(z)$ be as in the hypotheses of Theorem 1.2. Then the theorem shows that $f(z)$ cannot be congruent to a non-zero constant modulo v (when $f(z)$ is holomorphic, this is a special case of a result of Koblitz [12]). As stated, the theorem is not true for forms of integral weight, since in this case there are forms which are congruent to 1 modulo ℓ. In the case of holomorphic integral weight forms, more precise asymptotics for the number of non-vanishing coefficients modulo ℓ are available (see, for example, Theorem 1 of [25] or Theorem 4.7 of [26]).

We give some examples of these results.

Example 1. Let $p(n)$ be the ordinary partition function. As mentioned above,

$$\frac{1}{\eta(24z)} = \sum_{n=0}^{\infty} p(n)q^{24n-1} = q^{-1} + \dots$$

is a weakly holomorphic modular form of weight $-1/2$ on $\Gamma_1(576)$. It follows that the number of $n \le X$ for which $p(n)$ is odd is $\gg \frac{\sqrt{X}}{\log X}(\log\log X)^K$ for any integer K. This recovers a recent result of Nicolas [17] which improved previous results of Mirsky [15], Nicolas, Ruzsa, and Sárközy [18], Ahlgren [2], and Nicolas [16]. Our method of proof, in fact, is similar in spirit to that of Nicolas. Ono has informed us that he can dramatically improve the lower bound for this particular modular form, although a written paper is not yet available.

Example 2. If $f(z) = \sum a(n)q^n \in \mathcal{M}_{\frac{w}{2}}(\Gamma_1(N))$, t is a positive integer, and r is an integer, then standard arguments show that

$$\sum_{n \equiv r \pmod{t}} a(n)q^n \in \mathcal{M}_{\frac{w}{2}}(\Gamma_1(N'))$$

for some N'. Therefore the estimates above apply equally well to coefficients in any arithmetic progression. We note that Theorem 1.1 quantifies a result of Ono and Wilson [23] in the odd case.

Applying this principle to the modular form in Example 1, we deduce the following corollary from the theorems above.

Corollary 1.3. *Suppose that ℓ is prime and that $r \pmod{t}$ is an arithmetic progression. Suppose that there exists $n \equiv r \pmod{t}$ such that $p(n) \not\equiv 0 \pmod{\ell}$. Then for any $K > 0$ we have*

$$\#\{n \leq X \ : \ n \equiv r \pmod{t}, \ \ p(n) \not\equiv 0 \pmod{\ell}\} \gg \frac{\sqrt{X}}{\log X}(\log\log X)^K,$$

where the implied constant depends on t, ℓ, and K.

Corollary 1.3 is related to a conjecture of Subbarao [27] which asserts that in any progression $r \pmod{t}$ there are infinitely many odd values and infinitely many even values of $p(n)$ (see Chapter 5.3 of the book of Ono [22] or the survey [21] for a good description of work on this problem). In particular, Corollary 1.3 improves results of Ahlgren [1], [2] and Ono [19] in the "odd case" of this conjecture (and also answers Problem 5.47 of the book of Ono [22]).

Of course, the problem of proving the existence of the first non-vanishing coefficient remains. In this direction, Boylan and Ono [7] (in the case when $\ell = 2$) and Boylan [6] (in the case when $\ell = 3$) have verified the hypothesis of the corollary for all r when t is a power of ℓ. A result of Ono [20] implies that the hypothesis is "usually" satisfied. A result of the present authors [3] implies that $\sum p(\ell n + r)q^n \not\equiv 0 \pmod{\ell}$ when $\ell \geq 13$ is prime.

Example 3. One could take for an example any half-integral weight weakly holomorphic modular form $f(z)$ on $\Gamma_1(N)$ which is an "eta-quotient" (i.e. $f(z) = \prod_{\delta|N} \eta^{r_\delta}(\delta z)$ where $\sum_{\delta|N} \delta r_\delta \equiv 0 \pmod{24}$).

Example 4. Many other examples of such weakly holomorphic modular forms have been recently studied; we mention here the crank generating functions studied by Mahlburg [14], various rank generating functions (and, more generally, holomorphic parts of certain weakly holomorphic Maass forms of weight 1/2) studied by Bringmann and Ono [8], and Bringmann, Ono, and Rhoades [9], and generating functions for traces of singular moduli (see, e.g., Zagier [28] or Bruinier and Funke [10]).

2. Proof of Theorem 1.1

Let N be a positive integer, w be an integer, and

$$f(z) = \sum a(n)q^n \in \mathcal{M}_{\frac{w}{2}}(\Gamma_1(N)) \tag{2.1}$$

be as in (1.1). To begin, we recall the notion of the twist of a modular form. Suppose that T is a positive integer and suppose that χ is a Dirichlet character modulo T. If $f(z)$ is as in (2.1) then the twist of f by χ is

$$f(z) \otimes \chi := \sum \chi(n)a(n)q^n \in \mathcal{M}_{\frac{w}{2}}(\Gamma_1(NT^2)). \tag{2.2}$$

Suppose that v is a place over 2 and that $f(z) = \sum a(n)q^n \in \mathcal{O}_v((q))$ is a modular form satisfying the hypotheses of Theorem 1.1. Let n_0 be the least integer n with $a(n) \not\equiv 0 \pmod{v}$. We claim that there is no loss of generality in assuming that $n_0 \neq 0$. For, if $n_0 = 0$, then since by hypothesis $f(z)$ is non-constant modulo v, there is a least positive integer n_1 with $a(n_1) \not\equiv 0 \pmod{v}$. Let s be a positive integer with $\gcd(s, n_1) = 1$ and let χ_s^{triv} be the trivial character modulo s. Then we have $f(z) \otimes \chi_s^{\text{triv}} \in \mathcal{M}_{\frac{w}{2}}(\Gamma_1(Ns^2))$ and

$$f(z) \otimes \chi_s^{\text{triv}} = \sum_{\gcd(n,s)=1} a(n)q^n \equiv a(n_1)q^{n_1} + \cdots \not\equiv 0 \pmod{v}.$$

The claim follows, since a lower bound for the coefficients of $f(z) \otimes \chi_s^{\text{triv}}$ clearly implies the same lower bound for the coefficients of $f(z)$.

Before proceeding we require two further operators. Let N and m be positive integers, let w be an integer, and let $F(z) = \sum a(n)q^n \in \mathcal{M}_{\frac{w}{2}}(\Gamma_1(N))$. Then define U_m and V_m via the formulas

$$F(z) \mid U_m := \sum a(mn)q^n, \tag{2.3}$$

$$F(z) \mid V_m := \sum a(n)q^{mn}. \tag{2.4}$$

We have

$$U_m, V_m \ : \mathcal{M}_{\frac{w}{2}}(\Gamma_1(N)) \mapsto \mathcal{M}_{\frac{w}{2}}(\Gamma_1(Nm)).$$

Let $\operatorname{sgn}(n_0)$ denote the sign of n_0. We have the following lemma.

Lemma 2.1. *Let $\mathcal{O}$ be the ring of integers of an algebraic number field and let v be a place over 2. Suppose that N is a positive integer, that w is an integer, and that $f(z) = \sum a(n)q^n \in \mathcal{M}_{\frac{w}{2}}(\Gamma_1(N)) \cap \mathcal{O}_v((q))$ satisfies the hypothesis of Theorem 1.1. Suppose further that n_0 is the least integer n with $a(n) \not\equiv 0 \pmod{v}$ and that $n_0 \neq 0$. Then there are positive integers $M = M(f)$ and $j_0 = j_0(f)$ with the following property: For all $j \geq j_0(f)$, there is a positive integer $k = k(f, j)$ and a cusp form*

$$f_j(z) = \sum_{n=1}^{\infty} a_j(n)q^n \in S_{k(f,j)}(\Gamma_1(M)) \cap \mathcal{O}_v[[q]]$$

which satisfies the congruence

$$0 \not\equiv f_j(z) \equiv \left(f(z) \mid U_{|n_0|}\right) \cdot \sum_{n=0}^{\infty} q^{2^j(2n+1)^2} \equiv a(n_0)q^{2^j + \operatorname{sgn}(n_0)} + \cdots \pmod{v}. \tag{2.5}$$

Proof. Multiplying $f(z)$ by $\theta(z)$ if necessary, we may assume that $w/2 \in \mathbb{Z}$. From (2.3) we see that $f(z) \mid U_{|n_0|} \in \mathcal{M}_{\frac{w}{2}}(\Gamma_1(N \cdot |n_0|))$ and that

$$f(z) \mid U_{|n_0|} \equiv \sum_{n=\operatorname{sgn}(n_0)}^{\infty} a(|n_0|n)q^n \equiv a(n_0)q^{\operatorname{sgn}(n_0)} + \cdots \not\equiv 0 \pmod{v}. \tag{2.6}$$

Next, recall that

$$\Delta(z) = q + \cdots \in S_{12}(\Gamma_1(1))$$

satisfies

$$\Delta(z) \equiv \sum_{n=0}^{\infty} q^{(2n+1)^2} \pmod{2}.$$

For all non-negative integers j, it follows that $\Delta^{2^j}(z) \in S_{12\cdot 2^j}(\Gamma_1(1))$ and that

$$\Delta^{2^j}(z) \equiv \Delta(2^j z) \equiv \sum_{n=0}^{\infty} q^{2^j(2n+1)^2} \equiv q^{2^j} + \cdots \pmod{2}. \tag{2.7}$$

Since the poles of $f(z) \mid U_{|n_0|}$ (if it has any) are supported at the cusps and since $\Delta(z)$ is a cusp form, there is a positive integer j_0 such that for each integer $j \geq j_0$, the product $(f(z) \mid U_{|n_0|}) \cdot \Delta^{2^j}(z)$ vanishes at all cusps. Setting $M = N \cdot |n_0|$, we define $f_j(z)$ by

$$f_j(z) := \big(f(z) \mid U_{|n_0|}\big) \cdot \Delta^{2^j}(z) \in S_{\frac{w}{2}+12\cdot 2^j}(\Gamma_1(M)).$$

Using (2.6) and (2.7), we see that the modular forms $f_j(z)$ satisfy all of the requirements of the lemma. □

Theorem 1.1 will be an easy consequence of the next result.

Theorem 2.2. *Suppose that v is a place over 2 and that K is a positive integer. Let $f(z)$ be as in the hypotheses of Theorem 1.1 and let $j_0(f)$ be the integer given by Lemma 2.1. Then there exists an integer $j \geq j_0(f)$ with the property that, with the cusp form $f_j(z) = \sum_{n=1}^{\infty} a_j(n)q^n$ as given by Lemma 2.1, we have*

$$\#\{n \leq X \ : \ a_j(n) \not\equiv 0 \pmod{v}\} \gg \frac{X}{\log X}(\log\log X)^K, \tag{2.8}$$

where the implied constant depends on f and K.

To deduce Theorem 1.1 from Theorem 2.2, we use an elementary lemma (c.f. [16], Lemme 1). Suppose that ℓ is prime and that v is a place over ℓ. Suppose also that

$$G = \sum_{m=m_0}^{\infty} a_G(m)q^m \in \mathcal{O}_v((q)), \tag{2.9}$$

and define, for $X > 0$, the quantity

$$P(G,X) := \#\{n \leq X \ : \ a_G(m) \not\equiv 0 \pmod{v}\}.$$

Lemma 2.3. *If $X > 0$ then the following are true.*

(1) *If $F = GH$ with $H \in \mathcal{O}[[q]]$ then*

$$P(F,X) \leq P(G,X)P(H,X-m_0).$$

(2) *If G is as in (2.9) and t is a positive integer, then*

$$P(G \mid U_t, X) \leq P(G, tX).$$

Proof. Write $F = \sum a_F(m)q^m$ and $H = \sum_{m=0}^{\infty} a_H(m)q^m$. Then $F = GH$ implies that

$$a_F(n) = \sum_{i+j=n} a_G(i)a_H(j).$$

Hence, if $a_F(n) \not\equiv 0 \pmod{v}$, then for some i, j with $i+j = n$ we have $a_G(i)a_H(j) \not\equiv 0 \pmod{v}$. The first assertion follows from the estimates

$$\begin{aligned} P(F, X) &\leq \sum_{\substack{i+j\leq X \\ a_G(i)a_H(j)\not\equiv 0 \pmod{v}}} 1 \\ &\leq \sum_{\substack{m_0\leq i\leq X \\ a_G(i)\not\equiv 0 \pmod{v}}} 1 \cdot \sum_{\substack{0\leq j\leq X-m_0 \\ a_H(j)\not\equiv 0 \pmod{v}}} 1 = P(G, X)P(H, X - m_0). \end{aligned} \tag{2.10}$$

For the second assertion, we compute

$$P(G \mid U_t, X) = \sum_{\substack{m\leq X \\ a_G(tm)\not\equiv 0 \pmod{v}}} 1 = \sum_{\substack{tm\leq tX \\ a_G(tm)\not\equiv 0 \pmod{v}}} 1 \leq \sum_{\substack{j\leq tX \\ a_G(j)\not\equiv 0 \pmod{v}}} 1 = P(G, tx).$$

□

Suppose that v and $f(z)$ are as in the hypothesis of Theorem 1.1 (as mentioned at the start of this section, we may assume that $f \pmod{v}$ does not begin with the constant term). Let $j_0(f)$ be the integer given by Lemma 2.1 and let $j \geq j_0(f)$ be the integer produced by Theorem 2.2. Using Lemma 2.3 and (2.7) we see that for this j we have

$$\begin{aligned} P\left(f_j, X\right) &\leq P\left(f \mid U_{|n_0|}, X\right) \cdot P\left(\Delta^{2^j}, X + 1\right) \\ &\ll P(f, |n_0|X) \cdot \sqrt{X}. \end{aligned}$$

It follows from Theorem 2.2 that

$$P(f, |n_0|X) \gg \frac{\sqrt{X}}{\log X} (\log\log X)^K,$$

where the implied constant depends on f and K. Theorem 1.1 therefore follows from Theorem 2.2.

3. Proof of Theorem 2.2

It remains to prove Theorem 2.2. We begin with a lemma which is slightly more general than required for our particular application. When $a = 1$ (the case we require here), M. Filaseta has pointed out that the result follows in a more elementary way from a theorem of Bang [4] which implies that if $n > 6$, then $2^n - 1$ has a primitive prime divisor (i.e. a prime divisor which does not divide $2^d - 1$ for any positive integer $d < n$).

Lemma 3.1. *Suppose that $\epsilon \in \{\pm 1\}$ and that K is a positive integer. Suppose that $M \equiv 0 \pmod{4}$ is an integer, and that $a \equiv 1 \pmod{4}$ is coprime to M. Then there exist distinct primes p_0, $p_1, \ldots, p_K$ and a positive integer j such that*

(1) $p_i \equiv a \pmod{M}$ *for all* i.
(2) $p_i \mid (2^j + \epsilon)$ *for all* i.

Proof. If $\epsilon = -1$, then let $p_0, \ldots, p_K$ be odd primes congruent to a modulo M. The requirements are satisfied whenever j is a positive integer with

$$j \equiv 0 \pmod{\operatorname{lcm}(p_0 - 1, \ldots, p_K - 1)}.$$

Suppose then that $\epsilon = 1$. If n is a positive integer, then let ζ_n denote a primitive nth root of unity. Let L be the degree 8 number field defined by

$$L := \mathbb{Q}(i, \sqrt[4]{2}) = \mathbb{Q}(\zeta_8, \sqrt[4]{2}).$$

Then L is the ring class field of the order $\mathbb{Z}[\sqrt{-64}]$ in the field $\mathbb{Q}(i)$. It is known that a prime p may be written in the form $p = x^2 + 64y^2$ if and only if p splits completely in L, which occurs if and only if the conjugacy class given by the Artin symbol $\left(\frac{L/\mathbb{Q}}{p}\right)$ in $\mathrm{Gal}(L/\mathbb{Q})$ contains only the identity element. A complete discussion of this topic can be found in the book of Cox [11]; see in particular Theorems 9.4 and 9.5.

We may assume without loss of generality that $8 \mid M$. Note that $\sqrt[4]{2}$ is quadratic over $\mathbb{Q}(\zeta_M)$ (if $\sqrt[4]{2} \in \mathbb{Q}(\zeta_M)$ then L would be a non-abelian subfield of $\mathbb{Q}(\zeta_M)$). Letting $K := \mathbb{Q}(\zeta_M, \sqrt[4]{2})$, it follows that there exists an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ which takes ζ_M to ζ_M^a and interchanges $\sqrt[4]{2}$ and $-\sqrt[4]{2}$. By the Chebotarev Density Theorem, a positive proportion of primes p have the property that the conjugacy classes $\left(\frac{K/\mathbb{Q}}{p}\right)$ and $\langle \sigma \rangle$ in $\mathrm{Gal}(K/\mathbb{Q})$ are equal. Such primes have $p \equiv a \pmod{M}$ and $\left(\frac{L/\mathbb{Q}}{p}\right) \neq \{1\}$, so that $p \neq x^2 + 64y^2$ by the discussion above. To summarize, let S be the set of primes

$$S := \{p \ : \ p \equiv a \pmod{M} \ \text{ and } p \text{ not of the form } x^2 + 64y^2\}.$$

We have shown that

$$\#\{p \in S \ : \ p \leq X\} \gg \frac{X}{\log X}. \tag{3.1}$$

For each $p \in S$, let e_p be the order of 2 modulo p, and write

$$e_p = 2^{f_p} e_p', \quad \text{with } e_p' \text{ odd}.$$

Since $p \neq x^2 + 64y^2$ it follows by a theorem of Gauss that 2 is not a biquadratic residue modulo p . Therefore $f_p \geq 1$ for all $p \in S$. (To see this, write $2 \equiv g^j \pmod{p}$ where g is a primitive root. Then $4 \mid (p-1)$, but $4 \nmid j$, so we must have $2 \mid e_p$.) Now let B be a large positive integer. If $p \in S$ and $p \leq 2^B$, then $1 \leq f_p \leq B$. By (3.1) we see that the number of such p is easily $\gg 2^{B/2}$. If B is sufficiently large, it follows that there exist distinct primes $p_0, \ldots, p_K \in S$, each $\leq 2^B$, such that $f_{p_0} = \cdots = f_{p_K}$. Denote this common value by f, write $e_{p_i} = 2^f e_{p_i'}$ for each i, and set

$$j := 2^{f-1} e_{p_0}' \ldots e_{p_K}'.$$

Then $2^j \equiv -1 \pmod{p_i}$ for each i. □

We proceed with the proof of Theorem 2.2. Let v, $f(z)$, and n_0 be as in the hypotheses of Theorem 1.1 and Lemma 2.1, and let K be given. Let $M = M(f)$ and $j_0(f)$ be the integers given by Lemma 2.1. Using (2.5) and Lemma 3.1 we may fix distinct odd primes $p_0, \ldots, p_K \equiv 1 \pmod{M}$ and an integer $j \geq j_0(f)$ with the property that if $a := a(n_0) \not\equiv 0 \pmod{v}$, we have

$$f_j(z) \equiv aq^{m_0} + \cdots \in S_k(\Gamma_1(M)) \tag{3.2}$$

where

$$m_0 = 2^j + \operatorname{sgn}(n_0) = sp_0 \ldots p_K \quad \text{for some } s. \tag{3.3}$$

(Note that if j satisfies the requirements of Lemma 3.1 then there are arbitrarily large values of j which satisfy these requirements.)

For each prime $p \nmid M$ there is a Hecke operator $T_p \ : \ S_k(\Gamma_1(M)) \mapsto S_k(\Gamma_1(M))$ whose action is described by

$$F(z) \mid T_p := F \mid U_p + p^{k-1}(\langle p \rangle F) \mid V_p, \tag{3.4}$$

where $\langle p \rangle$ is the usual diamond operator. Recall the decomposition $S_k(\Gamma_1(M)) = \oplus_\chi S_k(\Gamma_0(M), \chi)$. If $p \equiv 1 \pmod{M}$ is prime, then the operator $\langle p \rangle$ is the identity on each component of this direct sum. On $S_k(\Gamma_1(M))$, we therefore have

$$F \mid T_p = F \mid U_p + p^{k-1} F \mid V_p \quad \text{if } p \equiv 1 \pmod{M}. \tag{3.5}$$

Let $f_j(z)$ be as in (3.2). Using the factorization (3.3) together with (3.5), we see that

$$f_j(z)|T_{p_0}| \ldots |T_{p_K} \equiv aq^s + \cdots \not\equiv 0 \pmod{v}. \tag{3.6}$$

We require a general fact about the action of Hecke operators modulo v.

Theorem 3.2. *Suppose that $\mathcal{O}$ is the ring of integers of an algebraic number field, that v is a place over the prime ℓ, that M and k are positive integers, and that $F(z) \in S_k(\Gamma_1(M)) \cap \mathcal{O}_v[[q]]$. Suppose that $p' \equiv 1 \pmod{M}$ is prime. Then we have*

$$\#\{p \leq X \ : \ p \equiv 1 \pmod{M}, \quad F|T_p \equiv F|T_{p'} \pmod{v}\} \gg \frac{X}{\log X},$$

where the implied constant depends on F and ℓ.

Proof. This can be proved using a slight modification of an argument of Serre (see §6.4 of [26]) to treat forms on $\Gamma_1(M)$. □

Applying Theorem 3.2 repeatedly and using (3.6), we obtain sets $S_0, \ldots, S_K$ of primes, each of positive density and containing only primes congruent to 1 modulo M, such that whenever $q_i \in S_i$ for $i = 0, \ldots, K$ we have

$$f_j(z)|T_{q_0}| \ldots |T_{q_K} \equiv aq^s + \cdots \not\equiv 0 \pmod{v}. \tag{3.7}$$

Suppose in addition that the q_i are distinct and coprime to s. Using the definition (3.5), we conclude from (3.7) that the coefficient on $q^{sq_0 \cdots q_K}$ in $f_j(z)$ is congruent to a modulo v.

It follows that $P(f_j, X)$ is at least as large as the number of integers $n \leq X$ which can be written in the form

$$n = sq_0 \ldots q_K \quad \text{with distinct } q_i \in S_i, \text{ each coprime to } s. \tag{3.8}$$

An argument of Landau (see Section 2.5 of [17] for a complete discussion) shows that the number of $n \leq X$ of the form (3.8) is

$$\gg \frac{X}{\log X} (\log\log X)^K,$$

where the implied constant depends on K. Theorem 2.2 follows.

4. Proof of Theorem 1.2

Let ℓ be an odd prime, let $\mathcal{O}$ be the ring of integers of a number field, let v be a place over ℓ, and let $f(z) = \sum a(n)q^n \in \mathcal{M}_{\lambda+\frac{1}{2}}(\Gamma_1(N)) \cap \mathcal{O}_v((q))$ be as in the hypotheses of Theorem 1.2. For all non-negative integers j we have $\eta^{\ell^j}(24z) \in S_{\frac{\ell^j}{2}}(\Gamma_1(576))$ and

$$\eta^{\ell^j}(24z) \equiv \eta(24 \cdot \ell^j z) \equiv \sum_{m\in\mathbb{Z}} (-1)^m q^{\ell^j(6m+1)^2} \pmod{\ell}. \tag{4.1}$$

Since the poles of $f(z)$ (if it has any) are supported at the cusps and since $\eta(24z)$ is a cusp form, it follows that that if j is sufficiently large, then with $k := \lambda + \frac{\ell^j+1}{2} \in \mathbb{Z}$ we have

$$f_j(z) := f(z) \cdot \eta^{\ell^j}(24z) \in S_k(\Gamma_1(576N)) \cap \mathcal{O}_v[[q]]. \tag{4.2}$$

In this setting we have the following.

Theorem 4.1. *Suppose that $\mathcal{O}$ is the ring of integers of a number field, that v is a place over an odd prime ℓ, that M is a positive integer, and that $F(z) = \sum_{n=1}^{\infty} b(n)q^n \in S_k(\Gamma_1(M)) \cap \mathcal{O}_v[[q]]$ has $F(z) \not\equiv 0 \pmod{v}$. Then for all K we have*

$$\#\{n \leq X \ : \ b(n) \not\equiv 0 \pmod{v}\} \gg \frac{X}{\log X}(\log\log X)^K,$$

where the implied constant depends on F, ℓ, and K.

Proof. Serre states this result for cusp forms on $\Gamma_0(N)$ in §6.5 of [26]; the argument can be adapted to treat cusp forms on $\Gamma_1(N)$. □

Theorem 1.2 now follows by applying Theorem 4.1 to the form $f_j(z)$ in (4.2) and using (4.1) together with Lemma 2.3.

References

[1] S. Ahlgren, *Distribution of the parity of the partition function in arithmetic progressions*, Indag. Math. (N. S.) **10** (1999), no. 2, 173-181.

[2] S. Ahlgren, *Non-vanishing of the partition function modulo odd primes ℓ*, Mathematika **46** (1999), no. 1, 185-192.

[3] S. Ahlgren and M. Boylan, *Arithmetic properties of the partition function*, Invent. Math. **153** (2003), 487-502.

[4] A. S. Bang, *Taltheoretiske Undersgelser*, Tidsskrift for Mat. 4 (1886), 70-80, 130-137.

[5] B. C. Berndt, A. J. Yee and A. Zaharescu, *On the parity of partition functions*, Internat. J. Math. **14** (2003), no. 4, 437-459.

[6] M. Boylan, *Nonvanishing of the partition function modulo small primes*, Int. Math. Res. Not. **2006**, Art. ID 46120, 17 pp. MR2264719.

[7] M. Boylan and K. Ono, *Parity of the partition function in arithmetic progressions, II*, Bull. London Math. Soc. **33** (2001), no. 5, 558-564.

[8] K. Bringmann and K. Ono, *Dyson's ranks and Maass forms*, Ann. of Math., to appear.

[9] K. Bringmann, K. Ono, and R. Rhoades, *Eulerian series as modular forms*, preprint.

[10] J. H. Bruinier and J. Funke, *Traces of CM values of modular functions*, J. Reine Angew. Math. **594** (2006), 1-33.

[11] David A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication*, John Wiley & Sons, Inc., New York, 1989. xiv+351 pp.

[12] N. Koblitz, *p-adic congruences and modular forms of half-integral weight*, Math. Ann. **274** (1986), 199-220.

[13] N. Koblitz, *Introduction to elliptic curves and modular forms*, Second edition, Springer, New York, 1993. MR1216136 (94a:11078)

[14] K. Mahlburg, *Partition congruences and the Andrews-Garvan-Dyson crank*, Proc. Natl. Acad. Sci. USA **102** (2005), no. 43, 15373-15376.

[15] L. Mirsky, *The distribution of the partition function in residue classes*, J. Math. Anal. Appl. **93** (1983), no. 2, 593-598.

[16] J.-L. Nicolas, *Valeurs impaires de la fonction partition $p(n)$*, Int. J. of Number Theory, to appear.

[17] J.-L. Nicolas, *Parité des valuers de la fonction de partition $p(n)$ et anatomie des entiers*, preprint.

[18] J.-L. Nicolas, I. Z. Ruzsa, and A. Sárközy (with an appendix by J.-P. Serre), *On the parity of additive representation functions*, J. Number Theory **73** (1998), no. 2, 292-317.

[19] K. Ono, *Parity of the partition function in arithmetic progressions*, J. Reine Angew. Math. **472** (1996), 1-15.

[20] K. Ono, *The partition function in arithmetic progressions*, Math. Ann. **312** (1998), 251-260.

[21] K. Ono, *Arithmetic of the partition function*, in *Special functions 2000: current perspective and future directions (Tempe, AZ)*, 243–253, Kluwer Acad. Publ., Dordrecht. MR2006291 (2004f:11113)

[22] K. Ono, *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004. MR2020489 (2005c:11053)

[23] K. Ono and B. Wilson, *Parity of Fourier coefficients of modular forms*, Illinois J. Math. **41** (1997), no. 1, 142–150. MR1433192 (98j:11033)

[24] A. Sárközy, *Jean-Louis Nicolas and the partitions*, Ramanujan J. **9** (2005), no. 1-2, 7–17. MR2166373 (2006d:11122)

[25] J.-P. Serre, *Divisibilité des coefficients des formes modulaires de poids entier*, C. R. Acad. Sci. Paris Sér. A **279** (1974), 679–682. MR0382172 (52 #3060)

[26] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Enseignement Math. 2 **22** (1976), no. 3-4, 227-260.

[27] M. V. Subbarao, *Some remarks on the partition function*, Amer. Math. Monthly **73** (1966), 851–854. MR0201409 (34 #1293)

[28] D. Zagier, *Traces of singular moduli*, Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998) (2002) Int. Press Lect. Ser., 3, I, Int. Press, Somerville, MA, 211-244.

Department of Mathematics, University of Illinois, Urbana, IL 61801
E-mail address: `ahlgren@math.uiuc.edu`

Department of Mathematics, University of South Carolina, Columbia, SC 29208
E-mail address: `boylan@math.sc.edu`