COEFFICIENTS OF HALF-INTEGRAL WEIGHT MODULAR FORMS MODULO ℓ^j

Scott Ahlgren and Matthew Boylan

Abstract. Suppose that $\ell \geq 5$ is prime, that $j \geq 0$ is an integer, and that $F(z)$ is a half-integral weight modular form with integral Fourier coefficients. We give some general conditions under which the coefficients of F are "well-distributed" modulo ℓ^j. As a consequence, we settle many cases of a classical conjecture of Newman by proving, for each prime power ℓ^j with $\ell \geq 5$, that the ordinary partition function $p(n)$ takes each value modulo ℓ^j infinitely often.

1. Introduction.

Suppose that $\lambda \geq 0$ and $N \geq 1$ are integers with $4 \mid N$, and that χ is a real Dirichlet character modulo N. In this paper we will study the Fourier coefficients of half-integral weight modular forms

$$F(z) := \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \cap \mathbb{Z}[[q]]. \tag{1.1}$$

If M is a positive integer, we say that the coefficients of F are *well-distributed* modulo M if, for every integer r, we have

$$\#\{1 \leq n \leq X \mid a(n) \equiv r \pmod{M}\} \gg_{r,M} \begin{cases} \frac{\sqrt{X}}{\log X} & \text{if } r \not\equiv 0 \pmod{M}, \\ X & \text{if } r \equiv 0 \pmod{M}. \end{cases}$$

In particular, this condition implies that every residue class modulo M contains infinitely many coefficients of F. (Of course, one might hope for a better lower bound than $\sqrt{X}/\log X$; we use the term "well-distributed" for convenience in stating our results.) In a recent paper [B-O 1], Bruinier and Ono prove that if ℓ is prime and the coefficients of F are not well-distributed modulo ℓ, then F must have a very special form modulo ℓ (see below for a precise description of these results).

After this work, there are some natural questions. First, it is natural to ask what can be said about the distribution of the coefficients of F modulo prime powers ℓ^j. One would also like to

1991 *Mathematics Subject Classification.* Primary: 11F33. Secondary: 11P83.

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 a VIGRE postdoctoral fellowship.

determine a simple set of conditions which guarantees the well-distribution of the coefficients of F modulo ℓ^j. Here we shed some light on both of these questions. We begin with an important result which follows from the arguments in [B-O 1].

Theorem 1. *Suppose that λ is a non-negative integer, that N is a positive integer with $4 \mid N$, that χ is a real Dirichlet character modulo N, and that*

$$F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \cap \mathbb{Z}[[q]].$$

Let ℓ be an odd prime and let j be a positive integer. Then at least one of the following is true:

(1) *The coefficients of $F(z)$ are well-distributed modulo ℓ^j.*
(2) *There are finitely many square-free integers n_1, $n_2, \dots, n_t$ for which*

$$F(z) \equiv \sum_{i=1}^{t} \sum_{m=1}^{\infty} a(n_i m^2) q^{n_i m^2} \pmod{\ell}.$$

Remark. Theorem 1 (and Theorem 2.3) of [B-O 1] are stated for an arbitrary odd modulus M. However, these results do not hold as stated except in the case when M is prime (i.e. the $j = 1$ case of Theorem 1 above; see [B-O 2]).

Given Theorem 1, it is natural to ask what can be said about modular forms $F(z)$ whose Fourier coefficients are supported on finitely many square classes modulo ℓ. For the analogous question in characteristic zero, we have the following result of Vignéras.

Theorem ([V, Théorème 3])**.** *Suppose that λ is a non-negative integer, that N is a positive integer with $4 \mid N$, and that $F(z) \in M_{\lambda+\frac{1}{2}}(\Gamma_1(N))$. If there are finitely many square-free integers $n_1, n_2, \dots, n_t$ for which*

$$F(z) = \sum_{i=1}^{t} \sum_{m=0}^{\infty} a(n_i m^2) q^{n_i m^2},$$

then $\lambda = 0$ or 1 and $F(z)$ is a linear combination of theta series.

In [B], Bruinier obtains mod ℓ analogues of the theorem of Vignéras. Bruinier shows, for example, that if $F(z)$ is a common eigenform of the half-integral weight Hecke operators $T(p^2)$, then $F(z)$ can have the form displayed in part (2) of Theorem 1 only for primes ℓ in a certain finite set (which is defined explicitly in terms of the Hecke eigenvalues λ_p.)

As an indication of the most one might hope for in positive characteristic, we recall the following conjecture of Balog, Darmon, and Ono.

Conjecture A ([B-D-O, §2])**.** *Suppose that λ is a non-negative integer, that N is a positive integer with $4 \mid N$, and that ℓ is an odd prime. If $F(z) \in M_{\lambda+\frac{1}{2}}(\Gamma_1(N)) \cap \mathbb{Z}[[q]]$ is a modular form whose coefficients are almost all (but not all) divisible by ℓ, then either $\lambda \equiv 0 \pmod{\frac{\ell-1}{2}}$ or $\lambda \equiv 1 \pmod{\frac{\ell-1}{2}}$.*

In our main result, we prove that if $F(z)$ is a modular form whose coefficients are supported on finitely many square classes modulo ℓ, then, as predicted by this conjecture, the possible values of λ are restricted. To state the result requires some notation. If n is a non-negative integer, then we define the integer $\overline{n} \in \{0, \dots, \ell - 2\}$ by

$$\overline{n} := n \pmod{\ell - 1}. \tag{1.2}$$

Then for each non-negative integer λ, we define the integer i_λ by

$$\lambda = \overline{\lambda} + i_\lambda(\ell - 1). \tag{1.3}$$

Using this notation, we have the following result.

Theorem 2. *Suppose that $\lambda \geq 2$ is an integer, that N is a positive integer with $4 \mid N$, and that χ is a real Dirichlet character modulo N. Suppose that*

$$F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \cap \mathbb{Z}[[q]].$$

Suppose further that $\ell \geq 5$ is a prime such that $\ell \nmid N$ and such that $F(z) \not\equiv 0 \pmod{\ell}$, and that there are finitely many square-free integers $n_1, n_2, \dots, n_t$ such that

$$F(z) \equiv \sum_{i=1}^{t} \sum_{m=1}^{\infty} a(n_i m^2) q^{n_i m^2} \pmod{\ell}. \tag{1.4}$$

Then the following are true:

(1) *If $\ell \nmid n_i$ for some i, then*

$$\overline{\lambda} \leq 2i_\lambda + 1.$$

(2) *If $\ell \mid n_i$ for all i and $\overline{\lambda} \leq \frac{\ell-3}{2}$, then*

$$\overline{\lambda} \leq 2i_\lambda - \frac{\ell - 1}{2}.$$

(3) *If $\ell \mid n_i$ for all i and $\overline{\lambda} \geq \frac{\ell-1}{2}$, then*

$$\overline{\lambda} \leq 2i_\lambda + \frac{\ell + 3}{2}.$$

For convenience, we record the following easy corollary of Theorem 2.

Corollary 3. *Suppose that $\lambda \geq 2$ is an integer, that N is a positive integer with $4 \mid N$, and that χ is a real Dirichlet character modulo N. Suppose that*

$$F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \cap \mathbb{Z}[[q]].$$

Suppose further that $\ell \geq 5$ is a prime such that $\ell \nmid N$ and such that $F(z) \not\equiv 0 \pmod{\ell}$, and that $F(z)$ has the form (1.4). Then the following are true:

(1) *If $\overline{\lambda} \leq \frac{\ell-3}{2}$, then $\overline{\lambda} \leq 2i_\lambda + 1$.*
(2) *If $\overline{\lambda} \geq \frac{\ell-1}{2}$, then $\overline{\lambda} \leq 2i_\lambda + \frac{\ell+3}{2}$.*

As another corollary, we obtain a result in the direction of a mod ℓ analogue of the result of Vignéras for forms $F(z)$ whose weight is small compared with ℓ. In particular, the following is immediate after Corollary 3.

Corollary 4. *Suppose that $F(z)$ is a form satisfying the hypotheses of Theorem 2 (so that in particular $F(z)$ has the form (1.4)). Suppose further that $\lambda \leq \ell-2$. Then $\lambda \in \{0, 1, \frac{\ell-1}{2}, \frac{\ell+1}{2}, \frac{\ell+3}{2}\}$.*

One might hope for a mod ℓ analogue of the result of Vignéras in the following form.

Conjecture B. *Suppose that $F(z)$ is a form satisfying the hypotheses of Theorem 2. Then either $\lambda \equiv 0 \pmod{\frac{\ell-1}{2}}$ or $\lambda \equiv 1 \pmod{\frac{\ell-1}{2}}$.*

The truth of Conjecture B (together with Theorem 1) would imply a weak version of the conjecture of Balog, Darmon, and Ono mentioned above (see also Conjecture B of [B-D-O]).

Remarks.

(1) The hypothesis that $\ell \nmid N$ is necessary in Theorem 2 (notice that this hypothesis is not present in Conjecture A). To see this, let $\eta(z)$ denote Dedekind's eta-function, and consider the modular form $f_1(z) := \eta(24z)\eta^\ell(z)/\eta(\ell z)$, which is a cusp form of weight $\ell/2$ on $\Gamma_0(576\ell)$ with quadratic Nebentypus. Since $\eta(24z) = \sum_{n\in\mathbb{Z}}(-1)^n q^{(6n+1)^2}$ and $\eta^\ell(z)/\eta(\ell z) \equiv 1 \pmod{\ell}$, we see that f_1 has the form (1.4); however we have $\overline{\lambda} = \frac{\ell-1}{2}$ and $i_\lambda = 0$, which is against the assertion in part (1).
(2) To illustrate the quality of the bounds in parts (1) and (3) of Theorem 2, we consider two examples. First let $f_2(z) := \eta^3(8z)E_{\ell-1}(z)$, where $E_{\ell-1}(z) \equiv 1 \mod \ell$ is the normalized Eisenstein series of weight $\ell-1$ on $\mathrm{SL}_2(\mathbb{Z})$. Since $\eta^3(8z) = \sum_{n=0}^{\infty}(-1)^n(2n+1)q^{(2n+1)^2}$, we see that the hypotheses of part (1) are satisfied. We have $\overline{\lambda} = 1$ and $i_\lambda = 1$, so that the inequality in part (1) reads $1 \leq 3$.

For an example in part (3), we define $f_3(z) := \eta^\ell(24z)$. We have $\overline{\lambda} = \frac{\ell-1}{2}$ and $i_\lambda = 0$, so the hypotheses of part (3) are satisfied. In this case the asserted inequality reads $\frac{\ell-1}{2} \leq \frac{\ell+3}{2}$.

These examples illustrate that the inequalities in the first and third parts are fairly sharp. For an example in the second case we may take $f_4(z) := \eta^{\ell^2}(24z)$; here we have $\overline{\lambda} = 0$ and $i_\lambda = \frac{\ell+1}{2}$.

(3) When applying Theorems 1 and 2 in tandem to the question of well-distribution modulo ℓ^j, one would start with a modular form $F \pmod{\ell^j}$. If F is not well-distributed modulo ℓ^j, then after Theorem 1 one is reduced to the study of $F \pmod{\ell}$. When passing from $F \pmod{\ell^j}$ to $F \pmod{\ell}$ one may be able to reduce the value of λ used in Theorem 2. This is certainly the case in our application of these results below.

As an application of (and a motivation for) these results, we consider a classical conjecture of M. Newman [N] on the distribution of the values of the ordinary partition function $p(n)$ modulo positive integers M. We recall that $p(n)$ is the number of ways to write the positive integer n as the sum of a non-increasing sequence of positive integers.

Newman's Conjecture. *If M is a positive integer, then for every integer r there are infinitely many non-negative integers n such that $p(n) \equiv r \pmod{M}$.*

Atkin, Kolberg, Newman, and Kløve [At, Kol, N, Kl] proved the conjecture for $M = 2$, 5, 7, 13, 17, 19, 29, and 31 (the $M = 11$ case follows in a similar manner). Some conditional results were obtained in work of Ono, the first author, and Bruinier and Ono [O], [A], [B-O 1]. In particular, in [B-O 1] it is shown, for primes $\ell \geq 13$, that if Newman's conjecture is false for ℓ, then $p\left(\frac{\ell n+1}{24}\right) \equiv 0 \pmod{\ell}$ for all n. Recently [A-B] the present authors have shown that for each prime $\ell \geq 13$ we have

$$\sum p\left(\frac{\ell n+1}{24}\right) q^n \not\equiv 0 \pmod{\ell}; \tag{1.5}$$

it follows that Newman's conjecture is true for all primes $\ell \geq 5$.

Here we show that Newman's Conjecture is in fact true for all prime powers. In particular, we have

Theorem 5. *If $\ell \geq 5$ is prime and $j \geq 1$ is an integer, then Newman's Conjecture is true for the modulus ℓ^j. Moreover, we have*

$$\#\{0 \leq n \leq X \ : \ p(n) \equiv r \pmod{\ell^j}\} \gg_{r,\ell^j} \begin{cases} \frac{\sqrt{X}}{\log X} & \text{if } r \not\equiv 0 \pmod{\ell^j}, \\ X & \text{if } r \equiv 0 \pmod{\ell^j}. \end{cases}$$

In Section 2 we give some preliminaries. In Section 3 we sketch the proof of Theorem 1, using arguments of [B-O 1]. In Section 4 we prove Theorem 2. Here we employ a result of Bruinier and Ono which restricts the possible image of a modular form satisfying (1.4) under the half-integral weight Hecke algebra. We also require properties of the Shimura correspondence, the theory of modular Galois representations, and the theory of modular forms in positive characteristic. In the final section, we prove Theorem 5. Here the main tools are Theorem 2, together with the non-vanishing result (1.5) described above.

2. Preliminaries.

Suppose that λ is a non-negative integer, that N is a positive integer with $4 \mid N$, and that χ is a Dirichlet character defined modulo N. Then we denote by $S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi)$ the usual complex vector space of cusp forms of weight $\lambda+\frac{1}{2}$ on $\Gamma_0(N)$ with character χ. If k is an integer

and N is a positive integer, then we denote by $M_k(\Gamma_1(N))$ the space of weight k modular forms on $\Gamma_1(N)$ and by $S_k(\Gamma_1(N))$ the subspace of cusp forms; we have the decomposition

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi} M_k(\Gamma_0(N), \chi),$$

where the sum runs over all Dirichlet characters modulo N. For background, one may consult, for example, [Kob].

For each prime $p \nmid N$, there is a Hecke operator

$$T(p^2, \lambda, \chi) \ : \ S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \to S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi);$$

the action of this operator on Fourier expansions is given by

$$\left(\sum_{n=1}^{\infty} a(n)q^n\right) \Big| T(p^2, \lambda, \chi)$$
$$= \sum_{n=1}^{\infty} \left(a(p^2n) + \left(\frac{n}{p}\right)\chi^*(p)p^{\lambda-1}a(n) + \chi^*(p^2)p^{2\lambda-1}a(n/p^2)\right)q^n, \quad (2.1)$$

where χ^* is the Dirichlet character defined by

$$\chi^*(n) := \left(\frac{(-1)^{\lambda}}{n}\right)\chi(n). \quad (2.2)$$

We shall also require the Shimura correspondence [Sh]. If $\lambda \geq 2$, then for each positive square-free integer t, we have the Shimura lift

$$\mathrm{Sh}_t \ : \ S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \to S_{2\lambda}(\Gamma_0(N), \chi^2) \quad (2.3)$$

defined in the following way: if $F(z) := \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi)$, then $\mathrm{Sh}_t(f)(z) := \sum_{n=1}^{\infty} A_t(n)q^n$, where the coefficients $A_t(n)$ are given by

$$\sum_{n=1}^{\infty} A_t(n)n^{-s} = L(s - \lambda + 1, \chi\chi_t\chi_{-1}^{\lambda}) \cdot \sum_{n=1}^{\infty} a(tn^2)n^{-s};$$

here χ_{-1} and χ_t denote the Kronecker characters for the fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{t})$, respectively. The Shimura correspondence commutes with the action of the Hecke operators $T(p^2, \lambda, \chi)$ and $T(p, 2\lambda, \chi^2)$ (where the latter denotes the Hecke operator of index p on the integral weight space $S_{2\lambda}(\Gamma_0(N), \chi^2)$).

We next record some facts about modular forms modulo ℓ. Suppose that K is an algebraic number field and that $\mathcal{O}$ is its ring of integers. Let ℓ be a rational prime and let v be a place of

K over ℓ. Let $\mathcal{O}_v$ be the corresponding valuation ring and let $\mathfrak{m}_v$ be its maximal ideal. Then for any N we define the $\mathcal{O}_v$-module

$$M_k(\Gamma_1(N))_v := M_k(\Gamma_1(N)) \cap \mathcal{O}_v[[q]].$$

We also define

$$\mathbb{F}_v := \mathcal{O}_v/\mathfrak{m}_v$$

(by a standard abuse of notation we will write $\pmod v$ to mean $\pmod{\mathfrak{m}_v}$). Then, given a modular form

$$f = \sum a(n)q^n \in M_k(\Gamma_1(N))_v,$$

we may consider its reduction

$$\overline{f} := \sum \overline{a(n)}q^n \in \mathbb{F}_v[[q]].$$

Given a form $f \in M_k(\Gamma_1(N))_v$ whose reduction is non-zero, we define the *filtration* $w(\overline{f})$ by

$$w(\overline{f}) := \min\{k' \ : \ \text{there exists } g \in M_{k'}(\Gamma_1(N))_v \text{ such that } \overline{f} = \overline{g}\}.$$

Then we have

$$w(\overline{f}) \equiv k \pmod{\ell - 1}. \tag{2.4}$$

We define the theta operator by its effect on Fourier expansions:

$$\Theta\left(\sum a(n)q^n\right) = \sum na(n)q^n.$$

A well-known result of Serre and Swinnerton-Dyer [SwD, S1] describes the effect of Θ on the reduction modulo ℓ of a modular form of level one. The results of Serre and Swinnerton-Dyer have been generalized by Katz [Ka] and Gross [G] to forms of higher level. In particular, we have the following (see [G, §4]).

Proposition 2.1. *Suppose that $k \geq 2$, that $N \geq 4$, and that $\ell \nmid N$. With the above notation, suppose that $f \in M_k(\Gamma_1(N))_v$ is a form whose reduction $\pmod v$ is non-zero. Then*

$$w(\overline{\Theta f}) \leq w(\overline{f}) + \ell + 1,$$

with equality if $w(\overline{f}) \not\equiv 0 \pmod \ell$.

3. Proof of Theorem 1.

As mentioned above, this result is proved by the arguments of [B-O 1]; therefore we give only a brief account of the proof here. To begin, suppose that $F(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \cap \mathbb{Z}[[q]]$ is a modular form as given in the hypotheses. If M is a positive integer, then define the set of prime numbers

$$S(F, M) := \{p \ : \ p \equiv 1 \pmod{NM},\ F(z)|T(p^2, \lambda, \chi) \equiv 2F(z) \pmod M\}.$$

Combining properties of the Shimura correspondence with a result of Serre (see, for example, Lemma 2.2 of [B-O 1]) it can be shown that the set $S(F, M)$ contains a positive proportion of the primes.

Lemma 3.1. *Suppose that M is an odd positive integer. If there exists $p_0 \in S(F, M)$ and a positive integer n_0 for which $\left(\frac{n_0}{p_0}\right) = -1$ and $\gcd(a(n_0), M) = 1$, then the coefficients of $F(z)$ are well-distributed modulo M.*

Proof. By Lemma 2.1 of [B-O 1], it follows under these hypotheses that, for every integer r, there exists an integer n_r for which $a(n_r) \equiv r \pmod{M}$. The lemma now follows as in the proof of Theorem 1 of [B-O 1]. $\square$

Suppose that a modular form $F(z)$ as in Theorem 1 does not have well-distributed coefficients modulo ℓ^j. Then we may, after Lemma 3.1, suppose that every $p \in S(F, \ell^j)$ and every integer n with $a(n) \not\equiv 0 \pmod{\ell}$ have the property that $\left(\frac{n}{p}\right) \in \{0, 1\}$. Following the argument in the proof of Theorem 2.3 of [B-O 1], we conclude that there are finitely many square-free integers $n_1, n_2, \dots, n_t$ for which

$$F(z) \equiv \sum_{i=1}^{t} \sum_{m=1}^{\infty} a(n_i m^2) q^{n_i m^2} \pmod{\ell}.$$

This proves Theorem 1. $\square$

4. Proof of Theorem 2.

The proof of Theorem 2 is much more involved. As in the hypotheses, assume that $F(z) \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N), \chi) \cap \mathbb{Z}[[q]]$ and that ℓ is a prime with $\ell \nmid N$ and $\ell \geq 5$ such that $F(z)$ has the form (1.4). Given such a modular form, we may, after reordering the n_i, assume that there exists an integer m_1 for which

$$a(n_1 m_1^2) \not\equiv 0 \pmod{\ell}.$$

We begin with a lemma.

Lemma 4.1. *Suppose that $F(z) = \sum_{n=1}^{\infty} a(n) q^n$ is a modular form as in the hypotheses of Theorem 2. Suppose that $F(z)$ has the form (1.4), and that there exists an integer $n_1 m_1^2$ such that*

$$a(n_1 m_1^2) \not\equiv 0 \pmod{\ell}. \tag{4.1}$$

Then there exist primes $p_1, \dots, p_s$, distinct from ℓ, and a modular form

$$G(z) \in S_{\lambda+\frac{1}{2}}(\Gamma_0(N p_1^2 \dots p_s^2), \chi) \cap \mathbb{Z}[[q]]$$

with

$$G(z) \equiv \sum_{\substack{m=1 \\ \gcd(m, \prod p_i)=1}}^{\infty} a(n_1 m^2) q^{n_1 m^2} \not\equiv 0 \pmod{\ell}.$$

Proof. Select a prime $p_1 > \ell$ for which $\left(\frac{n_1}{p_1}\right) = -1$, but for which $\left(\frac{n_t}{p_1}\right) = 1$. We may clearly suppose that $p_1 > n_1 m_1^2$. Let $\chi_{p_1}^{\text{triv}}$ denote the trivial character modulo p_1; then we define the

modular form $G_1(z) \in S_{\lambda+\frac{1}{2}}(\Gamma_0(Np_1^2), \chi) \cap \mathbb{Z}[[q]]$ by

$$\begin{aligned} G_1(z) :&= \frac{F(z) \otimes \chi_{p_1}^{triv} - F(z) \otimes \left(\frac{\bullet}{p_1}\right)}{2} \\ &\equiv \sum_{\substack{i=1 \\ \left(\frac{n_i}{p_1}\right)=-1}}^{t-1} \sum_{\substack{m=1 \\ p_1 \nmid m}}^{\infty} a(n_i m^2) q^{n_i m^2} \pmod{\ell}. \end{aligned}$$

If we iterate this process (at most) $t-1$ times, we obtain primes $p_1, \dots, p_s$ as described in the lemma and a modular form

$$G(z) \in S_{\lambda+\frac{1}{2}}(\Gamma_0(Np_1^2 \dots p_s^2), \chi) \cap \mathbb{Z}[[q]],$$

with

$$G(z) \equiv \sum_{\substack{m=1 \\ \gcd(m, \prod p_i)=1}}^{\infty} a(n_1 m^2) q^{n_1 m^2} \pmod{\ell}.$$

Since $\gcd(n_1 m_1^2, \prod p_i) = 1$, we see from (4.1) that $G(z) \not\equiv 0 \pmod{\ell}$. $\square$

An important tool in our proof is a result of Bruinier and Ono which gives information about the possible images of modular forms $F(z)$ of the form (1.4) under the half-integral weight Hecke algebra. Here we record this result.

Theorem 4.2 ([B-O 1, Thm. 3.1]). *Let $F(z)$ be as in (1.1), and suppose that M is a positive odd integer which is coprime to N. Suppose that $p \nmid NM$ is prime, and that there exists a number $\epsilon_p \in \{-1, 1\}$ such that*

$$F(z) \equiv \sum_{\left(\frac{n}{p}\right) \in \{0, \epsilon_p\}} a(n) q^n \pmod{M}.$$

Then

$$(p-1)F(z) \big| T(p^2, \lambda, \chi) \equiv \epsilon_p \chi^*(p)(p^\lambda + p^{\lambda-1})(p-1)F(z) \pmod{M}.$$

Given a form $F(z)$ of the form (1.4) and a prime $\ell \nmid N$, we let $G(z) \in S_{\lambda+\frac{1}{2}}(\Gamma_0(Np_1^2 \dots p_s^2), \chi)$ be the modular form given by Lemma 4.1. For convenience, we define

$$N_0 := Np_1^2 \cdots p_s^2.$$

Then for every prime $p \nmid N_0 n_1 \ell$, Theorem 4.2 applies to the modular form $G(z)$ with $M = \ell$ and $\epsilon_p = \left(\frac{n_1}{p}\right)$. We conclude, for every prime $p \nmid N_0 n_1 \ell$ with $p \not\equiv 1 \pmod{\ell}$, that

$$G(z) \big| T(p^2, \lambda, \chi) \equiv \epsilon_p \chi^*(p)(p^\lambda + p^{\lambda-1}) G(z) \pmod{\ell}. \tag{4.2}$$

Recalling from §2 the definition of the Shimura lifting (and the assumption that $\lambda \geq 2$), we define the integral weight modular form

$$f(z) := \mathrm{Sh}_{n_1}(G) \in S_{2\lambda}(\Gamma_0(N_0)) \cap \mathbb{Z}[[q]].$$

It is clear that $f(z) \not\equiv 0 \pmod{\ell}$. Using (4.2) and the fact that the Shimura correspondence commutes with the action of the Hecke operators, we find, for every prime $p \nmid N_0 n_1 \ell$ with $p \not\equiv 1 \pmod{\ell}$, that

$$f\big|T(p, 2\lambda) \equiv \epsilon_p \chi^*(p)(p^\lambda + p^{\lambda-1})f \pmod{\ell}. \tag{4.3}$$

We now apply a general result of Deligne and Serre [D-S, Lemme 6.11]. Using this result, we conclude that there exists a number field K and a place v over ℓ, together with a non-zero modular form $f'(z) \in S_{2\lambda}(\Gamma_0(N_0)) \cap \mathcal{O}_v[[q]]$, such that for all primes $p \nmid N_0 n_1 \ell$ with $p \not\equiv 1 \pmod{\ell}$, there exists $b(p) \in \mathcal{O}_v$ with

$$f'(z)|T(p, 2\lambda) = b(p)f'(z), \tag{4.4}$$

and

$$b(p) \equiv \epsilon_p \chi^*(p)(p^\lambda + p^{\lambda-1}) \pmod{v}. \tag{4.5}$$

By the theory of newforms, we may write

$$f'(z) = \sum_{j=1}^{n} \alpha_j f_j(\delta_j z), \tag{4.6}$$

where each f_j is a newform of weight 2λ and level dividing N_0, each δ_j is a divisor of N_0, and the α_j are non-zero algebraic numbers. For convenience, let us set

$$g(z) := f_1(z). \tag{4.7}$$

From (4.4) and (4.6) we conclude, for each prime p with $p \nmid N_0 n_1 \ell$ and $p \not\equiv 1 \pmod{\ell}$, that

$$g(z)|T(p, 2\lambda) = b(p)g(z). \tag{4.8}$$

After enlarging K if necessary, we may suppose that it contains the coefficients of g as well as all of the N_0-th roots of unity. We fix for the duration a place v of K over ℓ. As in the second section, we denote by $\mathbb{F}_v$ the residue field of $\mathcal{O}_v$, and we write

$$g(z) := \sum_{n=1}^{\infty} b(n)q^n$$

(note that the definition of the numbers $b(p)$ for primes p with $p \nmid N_0 n_1 \ell$ and $p \not\equiv 1 \pmod{\ell}$ is consistent with (4.8)). By the work of Deligne and Serre (see Thm. 6.7 of [D-S]) there is attached to $g(z)$ a semisimple residual Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_v), \tag{4.9}$$

unramified outside of $N_0\ell$, such that for all primes $p \nmid N_0\ell$, we have

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) \equiv b(p) \pmod{v}, \tag{4.10}$$

$$\mathrm{Det}(\rho(\mathrm{Frob}_p)) \equiv p^{2\lambda-1} \pmod{v}. \tag{4.11}$$

We let $G_v \subseteq \mathrm{GL}_2(\mathbb{F}_v)$ be the image of ρ, and we let $P_v \subset \mathrm{PGL}_2(\mathbb{F}_v)$ be the projectivization of G_v. Given the information (4.5), we will investigate the possibilities for G_v and P_v.

We begin with a lemma whose proof follows arguments of Swinnerton-Dyer [SwD, Lemma 2] and Ribet [R2, Thm. 2.1].

Lemma 4.3. *Let ρ be a representation as in* (4.9)*, and suppose that $\ell \mid \left|G_v\right|$. Then either ρ is reducible or G_v contains a conjugate of $\mathrm{SL}_2(\mathbb{F}_\ell)$.*

Proof of Lemma 4.3. We view $\mathrm{GL}_2(\mathbb{F}_v)$ as acting on a two-dimensional vector space V over $\mathbb{F}_v$, and we choose $\sigma \in G_v$ of exact order ℓ. Then there is a unique one-dimensional subspace W of V which is an eigenspace of σ with eigenvalue 1. If every element of G_v has W as an eigenspace, then ρ is upper-triangular (i.e. reducible). If this is not the case, then let $\sigma_1 \in G_v$ map W to another one-dimensional subspace W_1. After a suitable change of basis, we may suppose that for some $\gamma \in \mathbb{F}_v$ we have

$$\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1\sigma\sigma_1^{-1} = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}.$$

A classical result of Dickson (see Thm. 2.8.4 of [Go]), implies that

$$\mathrm{SL}_2(\mathbb{F}_\ell) \subseteq \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix} \right\rangle.$$

It follows in this case that G_v contains a conjugate of $\mathrm{SL}_2(\mathbb{F}_\ell)$; this proves the lemma. □

Lemma 4.4. *Suppose that $g(z)$ is the newform given in* (4.7)*, and let ρ be the representation attached to g as in* (4.9)*. Then G_v does not contain a conjugate of $\mathrm{SL}_2(\mathbb{F}_\ell)$.*

Proof of Lemma 4.4. After replacing ρ if necessary by a conjugate representation, it suffices to show that G_v does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$. Suppose by way of contradiction that $\mathrm{SL}_2(\mathbb{F}_\ell) \subseteq G_v$. Let χ_ℓ be the mod ℓ cyclotomic character, and consider the representation

$$\rho \times \chi_\ell \ : \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_v) \times \mathbb{F}_\ell^*.$$

Since the projection of the image onto the first factor contains $\mathrm{SL}_2(\mathbb{F}_\ell)$, and $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is simple, it follows that

$$\mathrm{SL}_2(\mathbb{F}_\ell) \times 1 = \mathrm{Comm}(\mathrm{SL}_2(\mathbb{F}_\ell)) \times 1 \subseteq (\rho \times \chi_\ell)(\mathrm{Comm}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))) \subseteq \mathrm{Im}(\rho \times \chi_\ell).$$

Now choose $\gamma \in \mathrm{SL}_2(\mathbb{F}_\ell)$. In view of the assertion above, we may find $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that

$$(\rho \times \chi_\ell)(\sigma) = (\gamma, 1).$$

Fix any prime p with $p \nmid N_0 n_1 \ell$ and $p \not\equiv 1 \pmod{\ell}$. By the Chebotarev Density Theorem, there are infinitely many primes q for which

$$(\rho \times \chi_\ell)(\mathrm{Frob}_q) = (\rho \times \chi_\ell)(\mathrm{Frob}_p\, \sigma). \tag{4.12}$$

Notice that $\chi_\ell(\mathrm{Frob}_q) \equiv q \pmod{\ell}$ and that $\chi_\ell(\mathrm{Frob}_p\, \sigma) = \chi_\ell(\mathrm{Frob}_p)\chi_\ell(\sigma) \equiv p \mod \ell$. Therefore, it follows from (4.12) that

$$p \equiv q \pmod{\ell}. \tag{4.13}$$

Using (4.13) together with (4.10) and (4.5), we conclude that

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = \pm \mathrm{Tr}(\rho(\mathrm{Frob}_q)). \tag{4.14}$$

On the other hand, from (4.12) we see that

$$\mathrm{Tr}(\rho(\mathrm{Frob}_q)) = \mathrm{Tr}(\rho(\mathrm{Frob}_p\, \sigma)) = \mathrm{Tr}(\rho(\mathrm{Frob}_p) \cdot \gamma).$$

If we set $A := \rho(\mathrm{Frob}_p) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_v)$, then the last line together with (4.14) implies that

$$\mathrm{Tr}(A\gamma) = \pm \mathrm{Tr}(A). \tag{4.15}$$

Notice that (4.15) holds for all $\gamma \in \mathrm{SL}_2(\mathbb{F}_\ell)$. From this it is easy to get a contradiction. For example, setting $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and successively $\gamma = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ in (4.15) shows that $c = 0$. By symmetry we see that $b = 0$. Finally, setting $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ in (4.15) shows that $d = 0$; this proves the lemma. $\square$

After the last two lemmas, we may conclude that ρ is reducible in the case when $\ell \mid |G_v|$. If, on the other hand, $\ell \nmid |G_v|$, then we have the following possibilities for P_v (see [S2, Prop. 16]):

(1) P_v is cyclic.
(2) P_v is dihedral.
(3) P_v is isomorphic to A_4, S_4, or A_5.

To examine these cases, we argue as in [R2, p. 189]. If P_v is cyclic, then we find that ρ is reducible. If P_v is dihedral, then there is a non-trivial quadratic character ϕ modulo $N_0\ell$ such that

$$\phi(p) = -1 \implies b(p) \equiv 0 \pmod{v}. \tag{4.16}$$

Using (4.5), we conclude from (4.16) that for primes $p \nmid n_1$ we have

$$\phi(p) = -1 \implies p + 1 \equiv 0 \pmod{\ell},$$

which is clearly false. Therefore P_v is not dihedral.

If P_v is A_4, S_4, or A_5, then for each prime $p \nmid N_0\ell$, we have either

$$\frac{b(p)^2}{p^{2\lambda-1}} \equiv 0, 1, 2, 4 \pmod{v},$$

or

$$b(p)^4 - 3p^{2\lambda-1}b(p)^2 + p^{4\lambda-2} \equiv 0 \pmod{v}.$$

A case-by-case calculation using (4.5) shows that if $\ell \geq 5$, then each of these possibilities leads to a contradiction. (For example, the second displayed congruence together with (4.5) implies that $p^4 + p^3 + p^2 + p + 1 \equiv 0 \pmod{\ell}$ for all $p \nmid N_0 n_1 \ell$ with $p \not\equiv 1 \pmod{\ell}$, which is clearly false.) It follows that P_v is neither A_4, S_4, nor A_5 when $\ell \geq 5$.

After Lemmas 4.3 and 4.4 and the above discussion, we may assume, under the hypotheses of Theorem 2, that ρ is reducible. Recall that the field K contains all N_0-th roots of unity. Since ρ is semisimple, we may conclude that there are Dirichlet characters ψ_1 and ψ_2 modulo N_0 (viewed as characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in the usual way, and with values in $\mathbb{F}_v$) and that there are integers $0 \leq m, m' \leq \ell - 2$ for which

$$\rho = \psi_1 \chi_\ell^{m'} \oplus \psi_2 \chi_\ell^m. \tag{4.17}$$

In particular, for all primes $p \nmid N_0\ell$, (4.17) implies that

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) \equiv \psi_1(p)p^{m'} + \psi_2(p)p^m \pmod{v}, \tag{4.18}$$

$$\mathrm{Det}(\rho(\mathrm{Frob}_p)) \equiv \psi_1(p)\psi_2(p)p^{m'+m} \pmod{v}. \tag{4.19}$$

Comparing (4.11) and (4.19) for sufficiently many p, we find that

$$m' + m \equiv 2\lambda - 1 \pmod{\ell - 1},$$
$$\psi_2 = \psi_1^{-1}.$$

Therefore, $m' + m$ is odd, so we may assume that $m' > m$.

If χ is a Dirichlet character and k is a positive integer, then we define the multiplicative function $\sigma_{k,\chi}$ by

$$\sigma_{k,\chi}(n) := \sum_{d|n} \chi(d)d^k.$$

For convenience, we denote by ψ the Dirichlet character $\pmod{N_0}$ with values in $\mathcal{O}_v$ whose reduction modulo v is ψ_1. The proof of Theorem 2 requires Lemma 4.5, whose proof follows the lines of [SwD, Lemma 8] and [R1, Lemma 4.6].

Lemma 4.5. *Suppose that $g(z)$ is the newform given by (4.7) and that the representation ρ attached to $g(z)$ is given by (4.17) with $m' > m$. Then we have $m' + m\ell + 1 \leq 2\lambda$.*

Proof. Recall that the newform g given by (4.7) has Fourier coefficients $b(n) \in \mathcal{O}_v$. Using (4.10) and (4.18) we find, for all primes $p \nmid N_0 n_1 \ell$, that

$$b(p) \equiv \psi^{-1}(p)p^m \sigma_{m'-m,\psi^2}(p) \pmod{v}. \tag{4.20}$$

Since g is a newform, it follows that for all primes $p \nmid N_0 n_1 \ell$ and all integers $j \geq 2$, we have

$$b(p^j) = b(p^{j-1})b(p) - p^{2\lambda-1}b(p^{j-2}). \tag{4.21}$$

Using (4.20), (4.21), and the multiplicativity of the Fourier coefficients of g, it follows by induction that for all n with $\gcd(n, N_0 n_1 \ell) = 1$, we have

$$b(n) \equiv \psi^{-1}(n) n^m \sigma_{m'-m,\psi^2}(n) \pmod{v}. \tag{4.22}$$

To complete the proof we require the following fact.

Lemma 4.6. *Suppose that $N \geq 2$ is an integer, that χ is an even Dirichlet character modulo N, and that $k \geq 2$ is an even integer. Then there is a modular form $F_{N,k,\chi}(z) \in M_k(\Gamma_0(N^2), \chi)$ whose Fourier expansion at infinity is given by*

$$F_{N,k,\chi}(z) = \sum_{\substack{n=1 \\ \gcd(n,N)=1}}^{\infty} \sigma_{k-1,\chi}(n) q^n.$$

Proof. Let χ_N^{triv} denote the trivial character modulo N. If $k = 2$ and $\chi = \chi_N^{\text{triv}}$, then we may take

$$F_{N,2,\chi_N^{\text{triv}}}(z) := \frac{1}{24} \cdot (NE_2(Nz) - E_2(z)) \otimes \chi_N^{\text{triv}},$$

where $E_2(z)$ is the usual quasi-modular Eisenstein series of weight 2 on $\mathrm{SL}_2(\mathbb{Z})$. If $k \geq 4$ and $\chi = \chi_N^{\text{triv}}$, then we may take

$$F_{N,k,\chi_N^{\text{triv}}}(z) := -\frac{B_k}{2k} E_k(z) \otimes \chi_N^{\text{triv}},$$

where $E_k(z)$ is the normalized Eisenstein series of weight k on $\mathrm{SL}_2(\mathbb{Z})$ and B_k is the kth Bernoulli number. Suppose that χ is non-trivial and primitive. Then, by the work of Hecke, (see, for example, [H, Proposition 5.1.2]) we have Eisenstein series

$$E_{N,k,\chi}(z) := 1 - \frac{2k}{B_{k,\chi}} \sum_{n=1}^{\infty} \sigma_{k-1,\chi}(n) q^n \in M_k(\Gamma_0(N), \chi),$$

where $B_{k,\chi}$ is the kth generalized Bernoulli number associated to χ. In this case, we may take

$$F_{N,k,\chi} := -\frac{B_{k,\chi}}{2k} \cdot E_{N,k,\chi} \otimes \chi_N^{\text{triv}}.$$

Finally, suppose that χ is non-trivial and imprimitive; we may then write $\chi = \chi_M \chi_N^{\text{triv}}$, where χ_M is a primitive character with conductor $M \mid N$. In this case we take

$$F_{N,k,\chi} := -\frac{B_{k,\chi_M}}{2k} \cdot E_{M,k,\chi_M} \otimes \chi_N^{\text{triv}}.$$

□

We now return to the proof of Lemma 4.5. Set $n_1' := n_1/\gcd(n_1, \ell)$. Recalling that $N_0 \geq 2$, let $F_{N_0, m'-m+1, \psi^2}(z) \in M_{m'-m+1}(\Gamma_0(N_0^2), \psi^2)$ be the modular form given in Lemma 4.6. We define

$$E := F_{N_0, m'-m+1, \psi^2} \otimes \psi^{-1}\chi_{n'}^{\text{triv}} = \sum_{\substack{n=1 \\ \gcd(n, N_0 n_1')=1}}^{\infty} \psi^{-1}(n)\sigma_{m'-m, \psi^2}(n)q^n.$$

Using the notation from Section 2, we see that

$$E(z) \in M_{m'-m+1}(\Gamma_1(N_0^2 n_1'^2))_v.$$

Since $0 \leq m, m' \leq \ell - 2$, we have $m' - m + 1 \leq \ell - 1$; it follows from (2.4) that

$$w(\overline{E}) = m' - m + 1.$$

Proposition 2.1 then implies that

$$\overline{\Theta^{m+1}E} = \sum_{\substack{n=1 \\ \gcd(n, N_0 n_1' \ell)=1}}^{\infty} \overline{\psi^{-1}(n) n^{m+1} \sigma_{m'-m, \psi^2}(n)} q^n \tag{4.23}$$

has filtration

$$w(\overline{\Theta^{m+1}E}) = m' - m + 1 + (m+1)(\ell+1). \tag{4.24}$$

We next observe that

$$\overline{\Theta(g \otimes \chi_{N_0 n_1'}^{\text{triv}})} = \sum_{\substack{n=1 \\ \gcd(n, N_0 n_1' \ell)=1}}^{\infty} \overline{nb(n)} q^n. \tag{4.25}$$

By Proposition 2.1, we have

$$w(\overline{\Theta(g \otimes \chi_{N_0 n_1'}^{\text{triv}})}) \leq 2\lambda + \ell + 1. \tag{4.26}$$

Using (4.23), (4.25), and (4.22), we see that $\overline{\Theta^{m+1}E} = \overline{\Theta(g \otimes \chi_{N_0 n_1'}^{\text{triv}})}$. Therefore, comparing (4.24) and (4.26), we find that

$$m' + m\ell + 1 \leq 2\lambda.$$

Lemma 4.5 follows. □

We are now in a position to finish the proof of Theorem 2. We recall that the modular form $G(z)$ given by Lemma 4.1 has the form

$$G(z) \equiv \sum_{\substack{m=1 \\ \gcd(m, N_0/N)=1}}^{\infty} a(n_1 m^2) q^{n_1 m^2} \pmod{\ell}.$$

For every prime $p \nmid N_0 n_1 \ell$ with $p \not\equiv 1 \pmod{\ell}$ we recall that $\epsilon_p = \left(\frac{n_1}{p}\right)$. For such primes p, (4.5) and (4.18) imply that

$$\psi(p)p^{m'} + \psi^{-1}(p)p^m \equiv \epsilon_p \chi^*(p)(p^\lambda + p^{\lambda-1}) \pmod{v}. \tag{4.27}$$

We also recall that $4 \mid N$, that $N \mid N_0$, that $\ell \nmid N_0$, and that χ^* is a Dirichlet character modulo N, while ψ is a Dirichlet character modulo N_0.

Proof of assertion (1) of Theorem 2. This assertion is trivially true for $\overline{\lambda} = 0, 1$; we will therefore suppose that $\overline{\lambda} \geq 2$. By the hypotheses in this case we may suppose without loss of generality that $\ell \nmid n_1$. Suppose that $p \neq \ell$ is a prime with $p \equiv 1 \pmod{N_0 n_1}$ and $p \not\equiv 1 \pmod{\ell}$. For such a p, (4.27) becomes

$$p^{m'} + p^m \equiv p^{\overline{\lambda}} + p^{\overline{\lambda-1}} \pmod{\ell}. \tag{4.28}$$

We now notice that we may find a prime p in each residue class modulo ℓ for which (4.28) holds. Since $\overline{\lambda - 1} < \overline{\lambda}$ and $m < m'$, it follows that $m = \overline{\lambda - 1}$ and $m' = \overline{\lambda}$. The result now follows from Lemma 4.5 and (1.3).

Proofs of assertions (2) and (3) of Theorem 2. The proof in these cases is similar. Under our assumption, we have $\ell \mid n_1$. We write $n_1 = \ell n_1'$ with $\ell \nmid n_1'$. If we let $p \neq \ell$ be a prime with $p \equiv 1 \pmod{N_0 n_1'}$ and $p \not\equiv 1 \pmod{\ell}$, then (4.27) becomes

$$p^{m'} + p^m \equiv p^{\overline{\lambda + \frac{\ell-1}{2}}} + p^{\overline{\lambda + \frac{\ell-3}{2}}} \pmod{\ell}. \tag{4.29}$$

Since (4.29) holds for some prime in each residue class modulo ℓ, we conclude that

$$\{m, m'\} = \{\overline{\lambda + \tfrac{\ell-1}{2}},\ \overline{\lambda + \tfrac{\ell-3}{2}}\}. \tag{4.30}$$

If $0 \leq \overline{\lambda} \leq \frac{\ell-3}{2}$, then (4.30) implies that

$$m = \overline{\lambda} + \frac{\ell - 3}{2}, \quad m' = \overline{\lambda} + \frac{\ell - 1}{2}.$$

Assertion (2) now follows from Lemma 4.5 and (1.3).

Finally, notice that the third assertion is trivially true for $\overline{\lambda} = \frac{\ell-1}{2}, \frac{\ell+1}{2}, \frac{\ell+3}{2}$. If $\overline{\lambda} \geq \frac{\ell+5}{2}$, then (4.30) implies that

$$m = \overline{\lambda} - \frac{\ell + 1}{2}, \quad m' = \overline{\lambda} - \frac{\ell - 1}{2},$$

from which the third assertion follows. □

5. The proof of Theorem 5.

We turn to the proof of Newman's Conjecture for prime power moduli ℓ^j with $\ell \geq 5$. We first suppose that

$$\ell \geq 13.$$

By Propositions 1 and 2 of [A], we see, for every integer $j \geq 1$, that there exists a modular form

$$F_{\ell,j} \in S_{\frac{\ell^j - \ell^{j-1}-1}{2}}(\Gamma_0(576\ell), \chi_{12})$$

with the property that

$$F_{\ell,j}(z) \equiv \sum_{n=0}^{\infty} p\left(\frac{\ell n+1}{24}\right) q^n \pmod{\ell^j}.$$

If the coefficients of $F_{\ell,j}(z)$ are well-distributed modulo ℓ^j, then Theorem 5 for the modulus ℓ^j follows immediately. If the coefficients are not well-distributed modulo ℓ^j, then by Theorem 1 we may conclude that $F_{\ell,j}(z)$ has the form (1.4). Now, using the $j = 1$ case of [A-B, Thm. 3], we find that there exists a modular form

$$F_\ell(z) \in S_{\frac{\ell-2}{2}}(\Gamma_0(576), \chi_{12})$$

such that

$$F_\ell(z) \equiv F_{\ell,j}(z) \equiv \sum p\left(\frac{\ell n+1}{24}\right) q^n \pmod{\ell}.$$

Moreover, Theorem 1 of [A-B] implies that for $\ell \geq 13$ we have

$$F_\ell(z) \not\equiv 0 \pmod{\ell}.$$

Writing $\frac{\ell-2}{2} = \lambda + \frac{1}{2}$, we have $\overline{\lambda} = \frac{\ell-3}{2}$ and $i_\lambda = 0$. This contradicts Corollary 3. Hence, Theorem 5 is true for each modulus ℓ^j with $\ell \geq 13$.

It remains to consider the cases when $\ell = 5$, 7, or 11. Here the argument above breaks down since the Ramanujan congruences imply that $F_\ell(z) \equiv 0 \pmod{\ell}$. Therefore, some additional work is necessary.

Suppose that $\ell = 5$, 7, or 11, and that $j \geq 1$ is an integer. Using a construction outlined in [A-O 1], we see that there exist positive integers $N_{\ell,j}$ and $\lambda_{\ell,j}$ together with a quadratic character $\chi_{\ell,j}$ modulo $N_{\ell,j}$ and a modular form

$$F_{\ell,j} := \sum_{n=1}^{\infty} a_{\ell,j}(n) q^n \in S_{\lambda_{\ell,j}+\frac{1}{2}}(\Gamma_0(N_{\ell,j}), \chi_{\ell,j}) \cap \mathbb{Z}[[q]]$$

with the property that

$$F_{\ell,j}(z) \equiv \sum_{\left(\frac{-n}{\ell}\right)=-1} p\left(\frac{n+1}{24}\right) q^n \pmod{\ell^j}. \tag{5.1}$$

If the coefficients of $F_{\ell,j}(z)$ are well-distributed modulo ℓ^j, then Theorem 5 for the modulus ℓ^j follows immediately.

Therefore, we will suppose by way of contradiction that the coefficients of $F_{\ell,j}(z)$ are not well-distributed modulo ℓ^j. Then Theorem 1 implies that there are finitely many square-free integers $n_1, n_2, \dots, n_r$ such that

$$\sum_{\left(\frac{-n}{\ell}\right)=-1} p\left(\frac{n+1}{24}\right) q^n \equiv \sum_{i=1}^{r}\sum_{m=1}^{\infty} a_{\ell,j}(n_i m^2) q^{n_i m^2} \pmod{\ell}. \tag{5.2}$$

On the other hand (see [A-O 2, (4.1), (4.2), (4.3)]), there are modular forms

$$f_\ell(z) := \sum_{n=1}^{\infty} a_\ell(n) q^n \in S_{\frac{\ell^2-2}{2}}(\Gamma_0(576), \chi_{12}) \cap \mathbb{Z}[[q]]$$

with

$$f_\ell(z) \equiv \sum_{\left(\frac{-n}{\ell}\right)=-1} p\left(\frac{n+1}{24}\right) q^n \not\equiv 0 \pmod{\ell}. \tag{5.3}$$

In particular we have

$$f_5(z) = \eta^{23}(24z), \tag{5.4}$$

$$f_7(z) = \eta^{23}(24z)E_4^3(24z) + 3\eta^{47}(24z), \tag{5.5}$$

$$\begin{aligned} f_{11}(z) =& \eta^{23}(24z)E_4^{12}(24z) + 5\eta^{47}(24z)E_4^9(24z) \\ &+ 4\eta^{71}(24z)E_4^6(24z) + \eta^{95}(24z)E_4^3(24z) + 8\eta^{119}(24z). \end{aligned} \tag{5.6}$$

Combining (5.2), and (5.3), we see that

$$f_\ell(z) \equiv \sum_{i=1}^{r}\sum_{m=1}^{\infty} a_\ell(n_i m^2) q^{n_i m^2} \pmod{\ell}.$$

Next, we note from (5.4), (5.5), and (5.6), that, for each $\ell \in \{5, 7, 11\}$ we have

$$a_\ell(23) = 1. \tag{5.7}$$

Hence, by Lemma 4.1, there are primes $p_1, \dots, p_s > 23$, distinct from ℓ, and a modular form $G_\ell(z) \in S_{\frac{\ell^2-2}{2}}(\Gamma_0(576 p_1^2 \cdots p_s^2), \chi_{12})$ with

$$G_\ell(z) \equiv \sum_{\substack{m=1 \\ \gcd(m, \prod p_i)=1}}^{\infty} a_\ell(23m^2) q^{23m^2} \not\equiv 0 \pmod{\ell}.$$

Furthermore, by Theorem 4.2 and (2.1), we see that, for every prime $p \nmid 6 \cdot 23 \cdot p_1 \cdots p_s \ell$ with $p \not\equiv 1 \pmod{\ell}$, we have

$$a_\ell(23p^2) + \left(\frac{23}{p}\right)\chi_{12}^*(p) p^{\frac{\ell^2-5}{2}} a_\ell(23) \equiv \epsilon_p \chi_{12}^*(p)(p^{\frac{\ell^2-3}{2}} + p^{\frac{\ell^2-5}{2}}) a_\ell(23) \pmod{\ell}. \tag{5.8}$$

We observe that $\epsilon_p = \left(\frac{23}{p}\right)$ and that $\chi_{12}^*(p) = \left(\frac{-3}{p}\right)$. It is then easy to obtain the desired contradictions. In particular, if $\ell = 5$ and $p = 7$, then (5.8) becomes $3 \equiv 2 \pmod 5$. If $\ell = 7$ and $p = 5$, then (5.8) becomes $2 \equiv 5 \pmod 7$, while if $\ell = 11$ and $p = 5$ then (5.8) becomes $6 \equiv 2 \pmod{11}$. It follows that Theorem 5 holds also when $\ell = 5$, 7, or 11. $\square$

Acknowledgments. The authors thank the referee for suggestions which improved the exposition in this paper.

References

[A] S. Ahlgren, *The partition function modulo composite integers M*, Math. Ann. **318** (2000), 795-803.

[A-B] S. Ahlgren and M. Boylan, *Arithmetic properties of the partition function*, Invent. Math. **153** (2003), no. 3, 487-502.

[A-O 1] S. Ahlgren and K. Ono, *Congruence properties for the partition function*, Proc. Nat. Acad. Sci. **98** (2001), no. 23, 12882-12884.

[A-O 2] S. Ahlgren and K. Ono, *Congruences and conjectures for the partition function*, Contemp. Math. **291** (2001), 1-10.

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

[B-D-O] A. Balog, H. Darmon, and K. Ono, *Congruences for Fourier coefficients of half-integral weight modular forms and special values of L-functions*, Proceedings for a conference in honor of Heini Halberstam, vol. 1, Birkhäuser, Boston, MA, 1996, pp. 105-127.

[B] J. Bruinier, *Non-vanishing modulo ℓ of Fourier coefficients of half-integral weight modular forms*, Duke Math. J. **98** (1999), 595-611.

[B-O 1] J. Bruinier and K. Ono, *Fourier coefficients of half-integral weight modular forms*, J. Number Th. **99** (2003), 164-179.

[B-O 2] J. Bruinier and K. Ono, *Fourier coefficients of half-integral weight modular forms (corrigendum)*, J. Number Th. **104** (2004), 378-379.

[D-S] P. Deligne and J.-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. École Normale Sup. 4^e sér. 7 (1974), 507-530.

[G] B.H. Gross, *A tameness criterion for Galois representations attached to modular forms* (mod p), Duke Math. J. **61** (1990), no. 2, 445-517.

[Go] D. Gorenstein, *Finite Groups*, Chelsea Publishing Company, New York, 1980.

[H] H. Hida, *Elementary theory of L-functions and Eisenstein series*, London Mathematical Society Student Texts, vol. 26, Cambridge University Press, 1993.

[Ka] N. Katz, *A result on modular forms in characteristic p*, Lecture Notes in Math., vol. 601 (Modular functions of one variable, V) (1977), Springer Verlag Berlin, 53-61.

[Kl] T. Kløve, *Recurrence formulae for the coefficients of modular forms and congruences for the partition function and for the coefficients of $j(\tau)$, $(j(\tau)-1728)^{1/2}$, and $j(\tau)^{1/3}$*, Math. Scand. **23** (1969), 133-159.

[Kob] N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag, New York, Graduate Texts in Mathematics, No. 97, 1984.

[Kol] O. Kolberg, *Note on the parity of the partition function*, Math. Scand. **7** (1959), 377-378.

[N] M. Newman, *Periodicity modulo m and divisibility properties of the partition function*, Trans. Amer. Math. Soc. **97** (1960), 225-236.

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

[R1] K. Ribet, *On ℓ-adic representations attached to modular forms*, Invent. Math. **28** (1975), 245-275.

[R2] K. Ribet, *On ℓ-adic representations attached to modular forms, II*, Glasgow Math. J. **27** (1985), 185-194.

[S1] J.-P. Serre, *Congruences et formes modulaires (d'après Swinnerton-Dyer)*, Sém. Bourbaki **416** (1971-1972), 319-338.

[S2] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

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

[SwD] H. P. F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for modular forms*, Lecture Notes in Math., vol. 350 (Modular functions of one variable III) (1973), Springer-Verlag Berlin, 1-55.

[V] M. F. Vignéras, *Facteurs gamma et équations fonctionelles*, Lecture Notes in Math., vol. 627 (Modular functions of one variable VI) (1977), Springer-Verlag Berlin, 79-103.

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

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