COEFFICIENTS OF HALF-INTEGRAL WEIGHT MODULAR FORMS

Jan H. Bruinier and Ken Ono

Appearing in the Journal of Number Theory

Abstract. In this paper we study the distribution of the coefficients $a(n)$ of half integral weight modular forms modulo odd integers M. As a consequence we obtain improvements of indivisibility results for the central critical values of quadratic twists of L-functions associated with integral weight newforms established in [O-S]. Moreover, we find a simple criterion for proving cases of Newman's conjecture for the partition function.

1. Introduction and Statement of Results

Suppose that $w \in \frac{1}{2}\mathbb{Z}$, that N is a positive integer (with $4 \mid N$ if $w \notin \mathbb{Z}$), and that χ is a Dirichlet character whose conductor divides N. Let $S_w(N, \chi)$ denote the space of weight w cusp forms with respect to the congruence subgroup $\Gamma_0(N)$ with Nebentypus character χ ([K, Sh] are standard references). As usual, we shall identify every such cusp form $f(z)$ with its Fourier expansion (where $q = e^{2\pi iz}$ throughout)

$$f(z) = \sum_{n=1}^{\infty} a(n)q^n.$$

Inspired by Kolyvagin's work on the Birch and Swinnerton-Dyer Conjecture and works of Kohnen, Zagier and Waldspurger relating the coefficients of half-integral weight Hecke eigenforms to values of modular L-functions, there have been a number of works on the indivisiblity of the coefficients of half-integral weight cusp forms. For example, works by Bruinier, Jochnowitz, McGraw, and Ono and Skinner [Br, J, M, O-S] imply that if $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(N, \chi) \cap \mathbb{Z}[[q]]$ is an eigenform which is not a single variable theta series, then every sufficiently large prime ℓ has the property that there are infinitely many

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

Key words and phrases. half-integral weight modular forms, the partition function.

The second author is grateful for the support of the Alfred P. Sloan, David and Lucile Packard, and H. I. Romnes Fellowships. Both authors thank the Number Theory Foundation and the National Science Foundation for their support.

square-free integers n for which $a(n) \not\equiv 0 \pmod{\ell}$. Although this result is satisfying, many questions remain. For example, it is natural to ask for a precise and natural arithmetic description of these primes ℓ.

Much more is known about the coefficients of integer weight cusp forms. The arithmetic of Galois representations and the combinatorics of Hecke operators dictate their behavior. For example, these arguments are very useful for studying the distribution of the coefficients modulo M. Using Galois representations and a delightfully simple argument, Serre observed [6.4, S] that there is a set of primes p with positive density with the property that

$$a(np^r) \equiv (r+1)a(n) \pmod{M} \tag{1.1}$$

for every pair of positive integers r and n. Obviously, (1.1) implies that each residue class modulo M contains infinitely many coefficients provided that there is an n for which $\gcd(a(n), M) = 1$.

Half-integral weight cusp forms do not necessarily enjoy this property. To see this, notice that Dedekind's function $\eta(24z) := q\prod_{n=1}^{\infty}(1-q^{24n}) \in S_{\frac{1}{2}}(576, \chi_{12})$ (here $\chi_{12} = \left(\frac{12}{\cdot}\right)$) has the q-expansion

$$\eta(24z) = \sum_{n=1}^{\infty} \chi_{12}(n) q^{n^2} = q - q^{25} - q^{49} + q^{121} + q^{169} - \cdots .$$

We begin by determining conditions which guarantee that a half-integral weight cusp form possesses this property modulo an odd integer M.

Theorem 1. *Let $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(N, \chi) \cap \mathbb{Z}[[q]]$ be a half-integral weight cusp form, and let χ be a real Dirichlet character. If M is an odd integer and there is a positive integer n for which $\gcd(a(n), M) = 1$, then at least one of the following is true:*

(1) *If $0 \le r < M$, then*

$$\#\{0 \le n \le X \ : \ a(n) \equiv r \pmod{M}\} \gg_{r,M} \begin{cases} \sqrt{X}/\log X & \text{if } 1 \le r < M, \\ X & \text{if } r = 0. \end{cases}$$

(2) *There are finitely many square-free integers, say $n_1, n_2, \dots, n_t$, for which*

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

Moreover if $\gcd(M, N) = 1$, $\epsilon \in \{\pm 1\}$ and $p \nmid NM$ is a prime with $\left(\frac{n_i}{p}\right) \in \{0, \epsilon\}$ for each $1 \le i \le t$, then $(p-1)f(z)$ is an eigenform modulo M of the half-integral weight Hecke operator $T(p^2, \lambda, \chi)$. In particular, we have

$$(p-1)f(z) \mid T(p^2, \lambda, \chi) \equiv \epsilon\chi(p)\left(\frac{(-1)^{\lambda}}{p}\right)(p^{\lambda} + p^{\lambda-1})(p-1)f(z) \pmod{M}.$$

Remarks.

(1) For simplicity, the results here are stated for cusp forms with integer coefficients and real Nebentypus character. However, we stress that Theorem 1 (2), and Corollaries 2 and 3 apply for any half-integral weight cusp form with algebraic integer coefficients. Theorem 1 (1) requires a minor modification. If α is a suitable algebraic integer and $\mathfrak{M}$ is a suitable ideal, then one obtains the frequency that $a(n) \equiv r\alpha \pmod{\mathfrak{M}}$, for every odd number r.

(2) In view of the single variable theta series and those forms congruent to such series, it turns out that the estimates in Theorem 1 (1) are nearly optimal. However, apart from such forms, it is plausible that each residue class r contains a positive proportion of $a(n) \pmod{M}$.

(3) Conclusions (1) and (2) in Theorem 1 are not necessarily mutually exclusive. In fact, one may often employ Theorem 1 (2) to prove Theorem 1 (1) (see Theorem 4).

(4) Suppose that $f(z)$ is a Hecke eigenform which is not a single variable theta series. If $f(z)$ satisfies Theorem 1 (2) and $\gcd(p-1, M) = 1$, then Deligne's theorem bounding Hecke eigenvalues requires that $M \leq 2p^{\lambda-\frac{1}{2}}$.

Theorem 1 has a variety of number theoretic applications, and we begin with the arithmetic of the Shimura correspondence. If $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(N, \chi) \cap \mathbb{Z}[[q]]$ is a Hecke eigenform, then we address the problem described at the outset (i.e. that of obtaining a precise and purely arithmetic description of those primes ℓ for which there are only finitely many square-free n with $a(n) \not\equiv 0 \pmod{\ell}$).

To motivate our result, we recall an example of Kohnen and Zagier [K-Z]. If $\Delta(z) = \sum_{n=1}^{\infty} \tau(n)q^n = q - 24q^2 + \cdots \in S_{12}(1, \chi_0)$, then Kohnen and Zagier proved that the function $f_\Delta(z) \in S_{13/2}(4, \chi_0)$ defined by

$$f_\Delta(z) = \sum_{n=1}^{\infty} a(n)q^n = \frac{60}{2\pi i}\left(2G_4(4z)\Theta'(z) - G_4'(4z)\Theta(z)\right) = q - 56q^4 + 120q^5 - \dots$$

(throughout χ_0 denotes the trivial character) is a preimage of $\Delta(z)$ under the Shimura correspondence. Here $G_4(z)$ is the usual weight 4 Eisenstein series on $\mathrm{SL}_2(\mathbb{Z})$ and $\Theta(z) = 1 + 2\sum_{n=1}^{\infty} q^{n^2}$. It turns out that

$$f_\Delta(z) = \sum_{n=1}^{\infty} a(n)q^n \equiv \sum_{n=1}^{\infty} \left(\frac{n}{5}\right) q^{n^2} \pmod{5}. \tag{1.2}$$

Obviously $n = 1$ is the only square-free integer for which $a(n) \not\equiv 0 \pmod{5}$. Ramanujan proved that if p is prime, then

$$\tau(p) \equiv p + p^2 \pmod{5}. \tag{1.3}$$

In view of Theorem 1 (2), it is natural to suspect a strong relationship between congruences (1.2) and (1.3).

In the late 1960s and early 1970s, Serre and Swinnerton-Dyer [SwD] employed Deligne's theory of Galois representations to 'explain' congruences such as (1.3). Suppose that $F(z) = \sum_{n=1}^{\infty} A(n)q^n \in S_{2\lambda}(N_1, \chi_0) \cap \mathbb{Z}[[q]]$ is a normalized Hecke eigenform. If ℓ is prime, then Deligne proved that there is a Galois representation

$$\rho_{\ell,F} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \tag{1.4}$$

such that for every prime $p \nmid N_1\ell$ we have

$$\begin{aligned} \mathrm{Tr}(\rho_{\ell,F}(\mathrm{Frob}_p)) &\equiv A(p) \pmod{\ell}, \\ \det(\rho_{\ell,F}(\mathrm{Frob}_p)) &\equiv p^{2\lambda-1} \pmod{\ell}. \end{aligned}$$

A prime $\ell \geq 5$ is called *exceptional* if $\mathrm{Im}(\rho_{\ell,F}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ does not contain $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. The Serre and Swinnerton-Dyer theory [SwD, R1, R2, R3] implies that congruences like (1.3) hold precisely for exceptional primes ℓ. Combining these ideas with Theorem 1, we obtain:

Corollary 2. *Suppose that $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(N_0, \chi) \cap \mathbb{Z}[[q]]$ is an eigenform that is a preimage of a newform $F(z) = \sum_{n=1}^{\infty} A(n)q^n \in S_{2\lambda}(N_1, \chi_0) \cap \mathbb{Z}[[q]]$ under the Shimura correspondence.*

(1) *If $\ell \geq 5$ is a non-exceptional prime for which $\ell \nmid N_0$ and $f(z) \not\equiv 0 \pmod{\ell}$, then there are infinitely many square-free integers n for which $a(n) \not\equiv 0 \pmod{\ell}$.*

(2) *If $F(z)$ has complex multiplication and $\ell \nmid N_0$ is a prime for which $f(z) \not\equiv 0 \pmod{\ell}$, then there are infinitely many square-free integers n for which $a(n) \not\equiv 0 \pmod{\ell}$.*

Remark. Every $F(z)$ without complex multiplication has at most finitely many exceptional primes ℓ, and they are easily determined (see [SwD], [Th. 2.1, R3]).

By Kolyvagin's celebrated work on the Birch and Swinnerton-Dyer Conjecture, it is well known that results like Corollary 2 have many consequences for elliptic curves. For example, recent similar works [Br, J, O-S] contain, for sufficiently large primes ℓ, results regarding the frequency of quadratic twists of elliptic curves with analytic rank 0 whose Tate-Shafarevich groups lack ℓ-torsion, as well as effective upper bounds for the order of the ℓ-part of the Tate-Shafarevich group of elliptic curves with analytic rank 1. Corollary 2 in the present work yields more precise versions of these results by clarifying what is meant for a prime ℓ to be sufficiently large. Since the consequences (i.e. [Cor. 2-5, O-S]) follow from [Cor. 1, O-S] in a straightforward way, here we content ourselves by stating its improvement.

We begin with some notation. Suppose that $F(z) = \sum_{n=1}^{\infty} A(n)q^n \in S_{2k}(N, \chi_0)$ is an even integer weight newform. If D is the fundamental discriminant of a quadratic field which is coprime to N, then let $(F \otimes \chi_D)(z)$ denote the quadratic twist of $F(z)$ defined by

$$(F \otimes \chi_D)(z) = \sum_{n=1}^{\infty} \left(\frac{D}{n}\right) A(n)q^n. \tag{1.5}$$

Moreover, let D_0 be defined by

$$D_0 := \begin{cases} |D| & \text{if } D \text{ is odd,} \\ |D|/4 & \text{if } D \text{ is even.} \end{cases} \tag{1.6}$$

A non-zero complex number $\Omega \in \mathbb{C}^\times$ is a *nice period for* $F(z)$ if

$$\frac{L(F \otimes \chi_D, k) D_0^{k-\frac{1}{2}}}{\Omega}, \quad \epsilon D > 0, \tag{1.7}$$

is always an algebraic integer. Here $L(F \otimes \chi_D, s)$ denotes the L-function of $(F \otimes \chi_D)(z)$, and $\epsilon \in \{\pm 1\}$ denotes the sign of the functional equation of $L(F, s)$, the L-function of $F(z)$. If ℓ is prime and $|\cdot|_\ell$ denotes the usual multiplicative valuation at ℓ extended to the algebraic closure of $\mathbb{Q}$, then we obtain the following improvement of [Cor. 1, O-S]:

Corollary 3. *Let $F(z) = \sum_{n=1}^{\infty} A(n) q^n \in S_{2k}(N, \chi_0) \cap \mathbb{Z}[[q]]$ be an even integer weight newform, and let ϵ be the sign of the functional equation for $L(F, s)$. There is a nice period Ω for $F(z)$ with the property that every non-exceptional prime $\ell \geq 5$ with $\ell \nmid N$ has infinitely many fundamental discriminants D for which*

$$\epsilon D > 0 \quad \textit{and} \quad \left| \frac{L(F \otimes \chi_D, k) D^{k-\frac{1}{2}}}{\Omega} \right|_\ell = 1.$$

Theorem 1 also applies to a classical conjecture in additive number theory. A *partition* of a positive integer n is any non-increasing sequence of positive integers whose sum is n. Let $p(n)$ denote the number of partitions of n (as usual, we adopt the convention that $p(0) = 1$ and $p(\alpha) = 0$ if $\alpha \notin \mathbb{N}$). If $\ell \geq 5$ is prime, then define $1 \leq \gamma_\ell < 24$ by the condition

$$24\gamma_\ell \equiv 1 \pmod{\ell}. \tag{1.8}$$

If $\ell = 5, 7$ or 11, then Ramanujan proved for every non-negative integer n that

$$p(\ell n + \gamma_\ell) \equiv 0 \pmod{\ell}. \tag{1.9}$$

Recently we have learned that similar, but more complicated congruences, are quite common (see [A, O]). For example if M is coprime to 6, then there are integers A and B such that for every n we have

$$p(An + B) \equiv 0 \pmod{M}.$$

The congruence

$$p(59^4 \cdot 13n + 111247) \equiv 0 \pmod{13}$$

is a typical example. Although there are many congruences, numerical evidence suggests that congruences of the special form (1.9) only hold for $\ell = 5, 7$ and 11.

Conjecture R. *If $\ell \geq 13$ is prime, then there are infinitely many integers n for which*

$$p(\ell n + \gamma_\ell) \not\equiv 0 \pmod{\ell}.$$

The following classical conjecture of Newman [N] concerns the distribution of the partition function among the complete set of residue classes modulo an integer M.

Conjecture N. (Newman) *If M is a positive integer, then for every integer $0 \leq r < M$ there are infinitely many non-negative integers n for which $p(n) \equiv r \pmod{M}$.*

Works by Atkin, Kolberg and Newman [At, Ko, N] verified the conjecture for $M = 2, 5, 7$ and 13 (note: the $M = 11$ case follows similarly). More recently, the second author and Ahlgren [A, O] obtained an algorithm which presumably proves the truth of the conjecture for any given M coprime to 6.

Theorem 1 leads to an interesting connection between Conjectures R and N, one which produces a simpler algorithm for testing Newman's Conjecture for prime moduli.

Theorem 4. *If $\ell \geq 5$ is prime, then at least one of the following is true:*

(1) *Newman's Conjecture is true for $M = \ell$, and*

$$\#\{0 \leq n \leq X \ : \ p(n) \equiv r \pmod{\ell}\} \gg_{r,\ell} \begin{cases} \sqrt{X}/\log X & \text{if } 1 \leq r < \ell, \\ X & \text{if } r = 0. \end{cases}$$

(2) *For every integer n we have*

$$p(\ell n + \gamma_\ell) \equiv 0 \pmod{\ell}.$$

In view of this result, Newman's Conjecture for a prime modulus $M = \ell \geq 5$ follows from the existence of a single n for which $p(\ell n + \gamma_\ell) \not\equiv 0 \pmod{\ell}$.

Corollary 5. *Conjectures N and R are true for every prime $13 \leq M < 2 \times 10^5$.*

The proof of Theorem 1 requires Shimura's theory of half-integral weight modular forms, a result of Serre on the coefficients of integer weight cusp forms, and some commutation relations for half-integral weight Hecke operators. In §2 we make some preliminary reductions for the proof of Theorem 1, and in §3 we conclude the proof with an analysis of the action of the half-integral weight Hecke operators modulo M. In §4 we prove Theorem 4 and Corollaries 2, 3 and 5.

2. Preliminary reductions

Throughout this section let M denote an odd integer, and let

$$f(z) = \sum_{n=1}^{\infty} a(n) q^n \in S_{\lambda+\frac{1}{2}}(N, \chi) \cap \mathbb{Z}[[q]] \tag{2.1}$$

be a half-integral weight cusp form with integer coefficients and real Dirichlet character χ. If $p \nmid N$ is prime, then the half-integral weight Hecke operator $T(p^2, \lambda, \chi)$ is a linear endomorphism on the space $S_{\lambda+\frac{1}{2}}(N, \chi)$ which is defined by

$$f(z) \mid T(p^2, \lambda, \chi) := \sum_{n=1}^{\infty} \left(a(p^2 n) + \chi^*(p) \left(\frac{n}{p}\right) p^{\lambda-1} a(n) + \chi^*(p^2) p^{2\lambda-1} a(n/p^2) \right) q^n. \tag{2.2}$$

Here χ^* is the Dirichlet defined by $\chi^*(n) := \left(\frac{(-1)^\lambda}{n}\right)\chi(n)$.

Lemma 2.1. *Suppose that M is an odd integer and $p_0 \equiv 1 \pmod{NM}$ is a prime for which*

$$f(z) \mid T(p^2, \lambda, \chi) \equiv 2f(z) \pmod{M}.$$

If there is a positive integer n_0 for which $\left(\frac{n_0}{p_0}\right) = -1$ and $\gcd(a(n_0), M) = 1$, then for every $0 \le r < M$ there are infinitely many integers n with $a(n) \equiv r \pmod{M}$.

Proof. By hypothesis, we see that $\chi(p_0) = 1$ and $p_0 \equiv 1 \pmod 4$. Therefore (2.2) implies, for every positive integer n, that

$$a(np_0^2) \equiv \left(2 - \left(\frac{n}{p_0}\right)\right) a(n) - a(n/p_0^2) \pmod{M}. \tag{2.3}$$

Therefore we find that

$$a(n_0 p_0^2) \equiv 3a(n_0) \pmod{M}. \tag{2.4}$$

Since $\left(\frac{n}{p_0}\right) = 0$ if $p_0 \mid n$, (2.3) and (2.4) imply that

$$\begin{aligned} a(n_0 p_0^4) &\equiv 2a(n_0 p_0^2) - a(n_0) \equiv 5a(n_0) \pmod{M}, \\ a(n_0 p_0^6) &\equiv 2a(n_0 p_0^4) - a(n_0 p^2) \equiv 7a(n_0) \pmod{M}, \end{aligned}$$

Generally, if k is a positive integer, then

$$a(n_0 p_0^{2k}) \equiv (2k+1)a(n_0) \pmod{M}.$$

Since $\gcd(a(n_0), M) = 1$, the result follows by varying k.

□

We now turn to the existence of such primes p_0. The next result, which follows from an observation of Serre and the arithmetic of the Shimura correspondence, proves that there is a vast supply of such primes.

Lemma 2.2. *A positive proportion of the primes $p \equiv 1 \pmod{NM}$ have the property that*

$$f(z) \mid T(p^2, \lambda, \chi) \equiv 2f(z) \pmod{M}.$$

Proof. By replacing $f(z)$ by any congruent form modulo M, we may assume that $f(z)$ is not a linear combination of single variable theta series. Hence its image, say $F(z)$, under the Shimura correspondence (see [K, Sh]) is an even integral weight cusp form in the space $S_{2\lambda}(N, \chi_0) \cap \mathbb{Z}[[q]]$. Serre observed [6.4, S] that a subset of primes $p \equiv 1 \pmod{NM}$ with positive density have the property that

$$F(z) \mid T_p(2\lambda, \chi_0) \equiv 2F(z) \pmod{M}. \tag{2.5}$$

Here $T_p(2\lambda, \chi_0)$ denotes the usual pth Hecke operator on the space $S_{2\lambda}(N, \chi_0)$. Denote this set of primes by $S(f, M)$. Since the Shimura correspondence commutes with the Hecke operators for the spaces $S_{\lambda+\frac{1}{2}}(N, \chi)$ and $S_{2\lambda}(N, \chi_0)$, if $p \in S(f, M)$, then (2.5) implies that

$$f(z) \mid T(p^2, \lambda, \chi_{12}) \equiv 2f(z) \pmod{M}.$$

□

Using Lemma 2.2 and Lemma 2.1, we now make an important observation.

Theorem 2.3. *If there is a positive integer n for which $\gcd(a(n), M) = 1$, then at least one of the following is true:*

1. *If $0 \le r < M$, then there are infinitely many integers n for which $a(n) \equiv r \pmod{M}$.*
2. *There are finitely many square-free integers, say $n_1 < n_2 < \cdots < n_t$, for which*

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

Proof. As in the proof of Lemma 2.2, let $S(f, M)$ denote the set of primes $p \equiv 1 \pmod{NM}$ for which

$$f(z) \mid T(p^2, \lambda, \chi) \equiv 2f(z) \pmod{M}.$$

Suppose that (1) is false. If $p \in S(f, M)$, then Lemma 2.1 implies that every $n \in \mathbb{Z}^+$ with $\gcd(a(n), M) = 1$ has the property that

$$\left(\frac{n}{p}\right) \in \{0, 1\}. \tag{2.6}$$

Let $n_1 < n_2 < \dots$ denote the sequence of square-free positive integers with the property there is an integer m_i for which $a(n_i m_i^2) \not\equiv 0 \pmod{M}$. By (2.6), each n_i has the property that $\left(\frac{n_i}{p}\right) \in \{0, 1\}$ for every prime $p \in S(f, M)$. By quadratic reciprocity, $S(f, M)$ cannot contain a positive proportion of the prime numbers if there are infinitely many such n_i's. Therefore there are finitely many square-free integers, say $n_1 < n_2 < \cdots < n_t$, such that

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

□

3. Hecke eigenvalues modulo M and the proof of Theorem 1

Here we consider the arithmetic of those modular forms $f(z)$ satisfying Theorem 2.3 (2). To do so, we prove a general statement regarding the eigenvalues of the half-integral weight Hecke operators modulo M. As in the last section, throughout we assume that M is an odd integer, and that

$$f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+\frac{1}{2}}(N, \chi) \cap \mathbb{Z}[[q]] \tag{3.1}$$

is a half-integral weight cusp form with integer coefficients and real character χ.

First we recall some operators on the space $S_{\lambda+\frac{1}{2}}(N, \chi)$ (see [S-St, Br]). The Fricke involution $W_N : S_{\lambda+\frac{1}{2}}(N, \chi) \to S_{\lambda+\frac{1}{2}}(N, (\frac{N}{\cdot})\chi)$ is defined by

$$f(z) \mid W_N = (-i\sqrt{N}z)^{-\lambda-1/2} f(-1/Nz). \tag{3.2}$$

If m is a positive integer, then let $B_m : S_{\lambda+\frac{1}{2}}(N, \chi) \to S_{\lambda+\frac{1}{2}}(Nm^2, \chi)$ be the projection defined by

$$f(z) \mid B_m = \sum_{n=1}^{\infty} a(mn)q^{mn}. \tag{3.3}$$

Finally, if ψ is a Dirichlet character with conductor m and $d(z) = \sum_{n=1}^{\infty} c(n)q^n \in S_{\lambda+\frac{1}{2}}(N, \chi)$, then let $d_\psi(z) \in S_{\lambda+\frac{1}{2}}(Nm^2, \chi\psi^2)$ denote the twist of $d(z)$ by ψ:

$$d_\psi(z) = \sum_{n=1}^{\infty} \psi(n)c(n)q^n. \tag{3.4}$$

These operators satisfy various commutation relations (see [S-St], [Br]). For instance, if $p \nmid N$ is prime, then the twist by the quadratic character $\varphi = \left(\frac{\cdot}{p}\right)$ and the Fricke involution W_{Np^2} satisfy [(3), Br]

$$f_\varphi \mid W_{Np^2} = \chi^*(p)\left(p^{1/2} f \mid W_N \mid B_p - p^{-1/2} f \mid W_N\right). \tag{3.5}$$

Theorem 3.1. *Let M be a positive integer that is coprime to N, and let $p \nmid NM$ be prime. If there is an $\epsilon \in \{\pm 1\}$ for which*

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

then

$$(p-1)f(z) \mid T(p^2, \lambda, \chi) \equiv \epsilon\chi^*(p)(p^\lambda + p^{\lambda-1})(p-1)f(z) \pmod{M}.$$

Proof of Theorem 3.1. We argue in a similar way as in the proof of [Th. 1, Br]. Without loss of generality we may assume that N is a square. Let $g(z) \in S_{\lambda+\frac{1}{2}}(N,\chi)$ be the cusp form defined by

$$g(z) = \sum_{n=1}^{\infty} b(n) q^n = f(z) \mid W_N. \tag{3.6}$$

Let $\varphi = \left(\frac{\cdot}{p}\right)$ and define

$$h(z) = f - f \mid B_p - \epsilon f_\varphi = 2 \sum_{\varphi(n)=-\epsilon} a(n) q^n. \tag{3.7}$$

By hypothesis, we have that $h(z) \equiv 0 \pmod{M}$.

We consider the twist of $g(z)$ with the Dirichlet character φ. The commutation relation (3.5) implies that

$$\begin{aligned} g_\varphi \mid W_{Np^2} &= \chi^*(p) \left(p^{1/2} f \mid B_p - p^{-1/2} f \right) \\ &= \chi^*(p) \left(p^{1/2} - p^{-1/2} \right) f - \epsilon \chi^*(p) p^{1/2} f_\varphi - \chi^*(p) p^{1/2} h. \end{aligned}$$

If we apply W_{Np^2} once again and use (3.5) for $f_\varphi(z)$, we get

$$g_\varphi = \chi^*(p) \left(p^{1/2} - p^{-1/2} \right) f \mid W_{Np^2} + \epsilon g - \epsilon p g \mid B_p - \chi^*(p) p^{1/2} h \mid W_{Np^2}.$$

We substitute

$$(f \mid W_{Np^2})(z) = p^{\lambda+1/2} (f \mid W_N)(p^2 z) = p^{\lambda+1/2} g(p^2 z)$$

and obtain the power series identity

$$\begin{aligned} \sum_{n=1}^{\infty} \varphi(n) b(n) q^n = \chi^*(p) \left(p^{\lambda+1} - p^\lambda \right) \sum_{n=1}^{\infty} b(n) q^{p^2 n} - \epsilon (p-1) \sum_{n=1}^{\infty} b(n) q^n \\ + \epsilon p \sum_{\gcd(n,p)=1} b(n) q^n - \chi^*(p) p^{1/2} h \mid W_{Np^2}. \end{aligned}$$

Since $f(z)$ has coefficients in $\mathbb{Z}$, the q-expansion principle on the modular curve $X_0(N)$ implies that the coefficients $b(n)$ of $g(z)$ are contained in $\mathbb{Z}[1/N, \zeta_N]$. Here ζ_N denotes a primitive N-th root of unity. Because $h(z) \equiv 0 \pmod{M}$, we find in the same way that the coefficients of $h \mid W_{Np^2}$ are contained in the principal ideal MA of the ring $A := \mathbb{Z}[1/Np^2, \zeta_{Np^2}]$ (see also [Lemma 1, Br]). Notice that the assumption $\gcd(M, Np) = 1$ is needed here.

For $b \in A$ we write $b \equiv 0 \pmod{M}$, if $b \in MA$. ¿From the identity (3.7) we obtain the following congruences for the coefficients $b(n)$ modulo M:

(1) If p does not divide n, then $b(n) \equiv \epsilon \varphi(n) b(n) \pmod{M}$.
(2) If $p|n$ and p^2 does not divide n, then $(p-1)b(n) \equiv 0 \pmod{M}$.
(3) If $p^2|n$, then $(p-1)b(n) \equiv \epsilon \chi^*(p) p^\lambda (p-1) b(n/p^2) \pmod{M}$.

Inserting these congruences into (2.2), the formula for $g(z) \mid T(p^2, \lambda, \chi)$, we find that

$$(p-1)g(z) \mid T(p^2, \lambda, \chi) \equiv \epsilon\chi^*(p)(p^\lambda + p^{\lambda-1})(p-1)g(z) \pmod{M}.$$

The theorem now follows from the fact that the Fricke involution W_N commutes with the Hecke operator $T(p^2, \lambda, \chi)$.

□

Proof of Theorem 1. In view of Theorems 2.3 and 3.1, it suffices to prove the estimates in Theorem 1 (1). By Theorem 2.3, for each $0 \le r < M$, there is a positive integer n_r for which

$$a(n_r) \equiv r \pmod{M}. \tag{3.8}$$

Obviously, we have $f(z) \in S_{\lambda+\frac{1}{2}}(2N\prod_r n_r, \chi)$. Hence arguing as before, [6.4, S] and the commutativity of Shimura's correspondence implies that a positive proportion of the primes $p \equiv -1 \pmod{2MN\prod_r n_r}$ have the property that

$$f(z) \mid T(p^2, \lambda, \chi) \equiv 0 \pmod{M}.$$

Call this set of primes $Z(f, M)$. If $p \in Z(f, M)$, then (2.2) implies for each n_r that

$$a(p^2 n_r) \equiv (-1)^\lambda \chi^*(-1)\left(\frac{n_r}{p}\right) r \pmod{M}. \tag{3.9}$$

Suppose that n_r has the prime factorization $n_r = 2^{e(r)}\prod_i p_{i,r}$, where each $p_{i,r}$ is odd. Since every $p \in Z(f, M)$ satisfies $p \equiv -1 \pmod 8$ and $p \equiv -1 \pmod{p_{i,r}}$, by quadratic reciprocity we have

$$\left(\frac{n_r}{p}\right) = \left(\frac{2}{p}\right)^{e(r)} \prod_i \left(\frac{p_{i,r}}{p}\right) = \left(\frac{2}{p}\right)^{e(r)} \prod_i \left(\frac{p}{p_{i,r}}\right)\left(\frac{-1}{p_{i,r}}\right) = \prod_i \left(\frac{1}{p_{i,r}}\right) = 1.$$

Therefore for every $p \in Z(f, M)$, (3.9) implies that

$$a(p^2 n_r) \equiv (-1)^\lambda \chi^*(-1) r \pmod{M}.$$

For each p these values constitute a complete set of representatives for the residue classes modulo M. By varying p, we find that

$$\#\{0 \le n \le X \ : \ a(n) \equiv r \pmod{M}\} \gg \sqrt{X}/\log X.$$

For the $r = 0$ estimate, notice that if $p \in Z(f, M)$, then for all n (2.2) implies that

$$a(p^2 n) \equiv -\chi^*(p)\left(\frac{n}{p}\right) p^{\lambda-1} a(n) - p^{2\lambda-1} a(n/p^2) \pmod{M}.$$

By replacing n by np where $p \nmid n$, this becomes

$$a(p^3 n) \equiv -p^{2\lambda-1} a(n/p) \equiv 0 \pmod{M}.$$

This immediately implies that a proportion of n have $a(n) \equiv 0 \pmod{M}$.

□

4. Number Theoretic Applications

Here we consider the number theoretic consequences of Theorem 1 described in §1.

Proof of Corollary 2. Begin by observing that if $f(z)$ is an eigenform, then (2.2) implies that for square-free n we have $a(n) \mid a(nm^2)$ for all m. Therefore, if $a(nm^2) \not\equiv 0 \pmod{\ell}$, then $a(n) \not\equiv 0 \pmod{\ell}$.

Suppose that there are finitely many square-free integers, say $n_1, n_2, \dots, n_t$, for which

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

By Theorem 1 (2), there are arithmetic progressions of primes $r_j \pmod{TN_0\ell}$, for some positive integer T, with the property that

$$f(z) \mid T(p^2, \lambda, \chi) \equiv \epsilon \chi^*(r_j)(r_j^{\lambda} + r_j^{\lambda-1}) f(z) \pmod{\ell}$$

for every prime $p \equiv r_j \pmod{\ell}$. Moreover, these residue classes $r_j \pmod{TN_0\ell}$ cover at least $(\ell - 3)/2$ many residue classes modulo ℓ (note. this depends on whether ℓ divides any n_i).

Since the coefficient $A(p)$ is the eigenvalue of $f(z)$ with respect to the Hecke operator $T(p^2, \lambda, \chi)$ (by the definition of Shimura's correspondence), for primes $p \equiv r_j \pmod{TN_0\ell}$ we obtain the congruence

$$A(p) \equiv \epsilon \chi^*(r_j)(r_j^{\lambda} + r_j^{\lambda-1}) \pmod{\ell}. \tag{4.1}$$

Case (1). If ℓ is non-exceptional, the Chebotarev Density Theorem, the uniform distribution of Frob_p in the Galois group, and an an easy generalization of [Lemma 7, SwD] implies that the $A(p)$ do not satisfy any congruences like (4.1). Therefore there are infinitely many square-free integers n with $a(n) \not\equiv 0 \pmod{\ell}$.

Case (2). Suppose that $F(z)$ has complex multiplication. By (4.1), it is easy to see that $A(p) \equiv 0 \pmod{\ell}$ only for those primes p above for which $p \equiv -1 \pmod{\ell}$. However, since $\ell \nmid N_0$, every residue class $r \pmod{N_0}$ with $\gcd(r, N_0)=1$ contains some such primes p with $p \not\equiv -1 \pmod{\ell}$. In particular, each class contains primes p for which $A(p) \not\equiv 0 \pmod{\ell}$. However this is a contradiction; for if $F(z)$ had complex multiplication, then there would be a discriminant D dividing N_0 with the property that $A(p) = 0$ for every prime p with $\left(\frac{D}{p}\right) = -1$. Hence there are infinitely many square-free n for which $a(n) \not\equiv 0 \pmod{\ell}$.

□

Proof of Corollary 3. There is a twist F_χ, $\chi(-1) = (-1)^k \epsilon$, satisfying Hypotheses H1 and H2 of [pp. 377-378 , Wal]. By [Théorème 1, Wal] there is an integer N', a non-zero eigenform $f(z) = \sum_{n=1}^{\infty} a(n) q^n \in S_{k+\frac{1}{2}}(N')$ such that $N | N'$, and a period Ω such that for each fundamental discriminant D for which $\epsilon D > 0$

$$a(D_0)^2 = \begin{cases} \varepsilon_D \frac{L(F \otimes \chi_D, k) D_0^{k-\frac{1}{2}}}{\Omega} & \text{if } D_0 \text{ is relatively prime to } 4N', \\ 0, & \text{otherwise,} \end{cases}$$

where ε_D is an algebraic integer with $|\varepsilon_D|_\ell = 1$. The result now follows from Corollary 2 by scaling Ω appropriately.

□

Proof of Theorem 4. By [Th. 8, O], there is a half-integral weight cusp form $F_\ell(z) = \sum_{n=1}^{\infty} a_\ell(n)q^n \in S_{\lambda_\ell+\frac{1}{2}}(576\ell, \chi_{12}) \cap \mathbb{Z}[[q]]$ for which

$$F_\ell(z) \equiv \sum_{\substack{n\geq 0,\\ \ell n \equiv -1 \pmod{24}}} p\left(\frac{\ell n+1}{24}\right) q^n \pmod{\ell}. \tag{4.2}$$

Here $\lambda_\ell = (\ell^2-\ell-2)/2$ and $\chi_{12} := \left(\frac{12}{\cdot}\right)$. This is the $k=1$ case of [Th. 8, O]. Although this theorem asserts that these forms are on the congruence subgroup $\Gamma_0(576\ell)$, the proof shows that they are indeed on $\Gamma_0(576)$. To see this, observe that the $U(\ell)$ operator modulo ℓ is the ℓth Hecke operator for modular forms on $SL_2(\mathbb{Z})$, and that $\eta(24\ell z) \equiv \eta(24z)^\ell \pmod{\ell}$. Now observe that the coefficients of $F_\ell(z) \pmod{\ell}$ are precisely the values $p(\ell n + \gamma_\ell) \pmod{\ell}$. Moreover, observe that if $a_\ell(n) \not\equiv 0 \pmod{\ell}$, then $\gcd(n, 24) = 1$.

If Theorem 1 (1) is false for $F_\ell(z)$, then by Theorem 1 (2) there are finitely many square-free integers, say $n_1, n_2, \ldots, n_t$, for which

$$F_\ell(z) \equiv \sum_{i=1}^{t}\sum_{m=1}^{\infty} a_\ell(n_i m^2) q^{n_i m^2} \pmod{\ell}. \tag{4.3}$$

Without loss of generality, we may assume that

$$0 \not\equiv F_\ell(z) \equiv \sum_{m=1}^{\infty} a_\ell(n_1 m^2) q^{n_1 m^2} \pmod{\ell}. \tag{4.4}$$

This is easily accomplished by recursively replacing $F_\ell(z)$ by a suitable linear combination of trivial and quadratic twists.

Fix an integer n_0 for which $a_\ell(n_0) \not\equiv 0 \pmod{\ell}$. As before, we have that $\gcd(n_0, 24) = 1$. If P_ℓ denotes the set of primes that are primitive roots modulo ℓ, then for all but finitely many primes $p \in P_\ell$ we may apply Theorem 1 (2) with $\epsilon = \left(\frac{n_0}{p}\right)$.

If $p_0 \nmid n_0$ is such a prime, then we have

$$\begin{aligned} a_\ell(p_0^2 n_0) &\equiv -\left(\frac{n_0}{p_0}\right)\chi_{12}^*(p_0)p^{-1}a_\ell(n_0) \pmod{\ell},\\ a_\ell(p_0^4 n_0) &\equiv p^{-2}a_\ell(n_0) \pmod{\ell}. \end{aligned}$$

This follows from (2.2), Theorem 1 (2), the fact p_0 is a quadratic non-residue modulo ℓ, and the fact that $\lambda_\ell = \ell(\ell-1)/2 - 1$. More generally, for every positive integer k we have

$$a_\ell(p_0^{2k} n_0) \equiv \begin{cases} -\left(\frac{n_0}{p_0}\right)\chi_{12}^*(p_0)p_0^{-k}a_\ell(n_0) \pmod{\ell} & \text{if } k \text{ is odd},\\ p_0^{-k}a_\ell(n_0) \pmod{\ell} & \text{if } k \text{ is even}. \end{cases} \tag{4.5}$$

Since $\gcd(n_0, 24) = 1$, we may select such a prime p_0 with the additional property that $-\left(\frac{n_0}{p_0}\right)\chi_{12}^*(p_0) = 1$. Since p_0 is a primitive root modulo ℓ, (4.5) then implies that each non-zero residue class $r \pmod{\ell}$ contains infinitely many $a_\ell(n)$. One obtains estimates in these cases by arguing as in the proof of Theorem 1. Similarly, one obtains the $r \equiv 0 \pmod{\ell}$ case by arguing again in the proof of Theorem 1.

□

Proof of Corollary 5. By Theorem 4, if there is a single n for which $p(\ell n + \gamma_\ell) \not\equiv 0 \mod \ell$, then Newman's Conjecture is true for ℓ. Moreover, since $F_\ell(z) \pmod{\ell}$ cannot be a non-zero polynomial, there must be infinitely many n for which $p(\ell n + \gamma_\ell) \not\equiv 0 \pmod{\ell}$. A simple program yields this result.

□

References

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

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

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

[J] N. Jochnowitz, *Congruences between modular forms of half integral weights and implications for class numbers and elliptic curves*, preprint.

[K] N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer Verlag, 1984.

[K-Z] W. Kohnen and D. Zagier, *Values of $L-$series of modular forms at the center of the critical strip*, Invent. Math. **64** (1981), 173-198.

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

[M] W. McGraw, *On a theorem of Ono and Skinner*, J. Number Theory **86** (2001), 244-252.

[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*, Annals of Mathematics **151** (2000), 293-307.

[O-S] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo ℓ*, Annals of Mathematics **147** (1998), 453-470.

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

[R2] K. Ribet, *Galois representations attached to eigenforms with Nebentypus*, Springer Lect. Notes. **601** (1976), 17-51.

[R3] K. Ribet, *On $\ell-$adic representations attached to modular forms II*, Glasgow Math. J. **27** (1985), 185-194.

[S] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, L'Ensein. Math. **22** (1976), 227-260.

[S-St] J.-P. Serre and H. Stark, *Modular forms of weight 1/2*, Modular functions of one variable, VI, Springer Lect. Notes. **627** (1977), 27-67.

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

[SwD] H. P. F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms*, Springer Lect. Notes **350** (1973), 1-55.

[Wal] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures et Appl. **60** (1981), 375-484.

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: bruinier@math.wisc.edu

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: ono@math.wisc.edu