9-2006

Congruences for the Coefficients of Weakly Holomorphic Modular Forms

Stephanie Treneer
Western Washington University, trenees@wwu.edu

CONGRUENCES FOR THE COEFFICIENTS OF WEAKLY HOLOMORPHIC MODULAR FORMS

STEPHANIE TRENEER

Abstract. Recent works have used the theory of modular forms to establish linear congruences for the partition function and for traces of singular moduli. We show that this type of phenomenon is completely general, by finding similar congruences for the coefficients of any weakly holomorphic modular form on any congruence subgroup $\Gamma_0(N)$. In particular, we give congruences for a wide class of partition functions and for traces of CM values of arbitrary modular functions on certain congruence subgroups of prime level.

1. Introduction and Statement of Results

Let $p(n)$ be the number of ways to write n as the sum of a nonincreasing sequence of positive integers. Ramanujan proved the following well-known congruences for the partition function $p(n)$:

$$p(5n+4) \equiv 0 \pmod{5},$$
$$p(7n+5) \equiv 0 \pmod{7},$$
$$p(11n+6) \equiv 0 \pmod{11}.$$

Ramanujan's work inspired a wealth of research into other congruences of the partition function (see [13] and [3] for references). Recently, Ahlgren and Ono (in [12], [1], and [2]) showed that if M is any positive integer coprime to 6, then there exist infinitely many congruences of the form

$$p(An+B) \equiv 0 \pmod{M}. \tag{1.1}$$

Their method in [2] explains every known linear congruence for $p(n)$. Results for other partition functions include Lovejoy's congruences for the number of partitions of n into distinct parts [10], and Swisher's congruences for the Andrews-Stanley partition function [20].

Linear congruences were also found for traces of singular moduli. Let D be a positive integer, and let $\mathcal{Q}_D$ be the set of positive definite integral binary quadratic forms

$$F(x,y) = ax^2 + bxy + cy^2$$

of discriminant $-D = b^2 - 4ac$. The modular group $\overline{\Gamma} := \mathrm{PSL}_2(\mathbb{Z})$ acts on $\mathcal{Q}_D$ with finitely many equivalence classes. For each $F \in \mathcal{Q}_D$, define α_F to be the unique root of $F(x,1)$ in the complex upper half-plane $\mathbb{H}$. Then the singular modulus $j(\alpha_F)$ is an algebraic integer, where

$$j(z) := \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots,$$

with $q := e^{2\pi i z}$, is the usual elliptic modular function on $\mathrm{SL}_2(\mathbb{Z})$.

2000 *Mathematics Subject Classification.* Primary: 11F37; Secondary: 11F33.

Following Zagier [21], we set $J(z) := j(z) - 744$ and consider the sequence of modular functions defined as follows. Let $T_0(m)$ be the normalized weight zero Hecke operator of index m. Set $J_0(z) := 1$, and for each positive integer m, define

$$J_m(z) := J(z)|T_0(m).$$

Then the mth Hecke trace of the singular moduli of discriminant $-D$ is

$$t_m(D) := \sum_{F \in \mathcal{Q}_D/\overline{\Gamma}} \frac{J_m(\alpha_F)}{w_F},$$

where w_F is the size of the stabilizer of F under the action of $\overline{\Gamma}$. Ahlgren and Ono [4] showed that if p is an odd prime with $p \nmid m$ and s is any positive integer, then a positive proportion of primes ℓ have the property that

$$t_m(\ell^3 n) \equiv 0 \pmod{p^s} \tag{1.2}$$

for every positive integer n coprime to ℓ such that p is inert or ramified in $\mathbb{Q}(\sqrt{-n\ell})$.

The methods for each of these results rely on the ability to realize both $\{p(n)\}$ and $\{t_m(n)\}$ as the coefficients of certain meromorphic half-integral weight modular forms. It is natural, then, to ask how common such phenomena are. We answer this question by proving a general result for weakly holomorphic modular forms. We show that an infinite number of linear congruences exist for the coefficients of every weakly holomorphic modular form of any weight, on any congruence subgroup $\Gamma_0(N)$, and with any character χ. This includes every form which can be written as a quotient of eta-functions. In particular, we can find linear congruences for a wide class of partition functions.

Suppose N and k are integers with N positive and $4 \mid N$, and let χ be a Dirichlet character modulo N. Let $\mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(N)}, \chi)$ be the space of weakly holomorphic modular forms of weight $\frac{k}{2}$ on the congruence subgroup $\Gamma_0(N)$ with character χ. For a more complete definition, see Section 2 below. Our main result shows that the phenomena in (1.1) and (1.2) are quite general.

Theorem 1.1. *Suppose that p is an odd prime, and that k and m are integers with k odd. Let N be a positive integer with $4 \mid N$ and $(N,p) = 1$, and let χ be a Dirichlet character modulo N. Let K be an algebraic number field with ring of integers $\mathcal{O}_K$, and suppose $f(z) = \sum a(n)q^n \in \mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(N)}, \chi) \cap \mathcal{O}_K((q))$. If m is sufficiently large, then for each positive integer j, a positive proportion of the primes $Q \equiv -1 \pmod{Np^j}$ have the property that*

$$a(Q^3 p^m n) \equiv 0 \pmod{p^j}$$

for all n coprime to Qp.

For completeness, we record the analogous result for integer weight modular forms. We denote the space of weakly holomorphic modular forms of integer weight k on $\Gamma_0(N)$ with character χ by $\mathcal{M}_k(\Gamma_0(N), \chi)$.

Theorem 1.2. *Suppose that p is an odd prime, and that k and m are integers. Let N be a positive integer with $(N,p) = 1$, and let χ be a Dirichlet character modulo N. Let K be an algebraic number field with ring of integers $\mathcal{O}_K$, and suppose $f(z) = \sum a(n)q^n \in \mathcal{M}_k(\Gamma_0(N), \chi) \cap \mathcal{O}_K((q))$. If m is sufficiently large, then for each positive integer j,*

(i) $a(p^m n) \equiv 0 \pmod{p^j}$ for almost all n coprime to p, and

(ii) a positive proportion of the primes $Q \equiv -1 \pmod{Np^j}$ *have the property that*

$$a(Qp^m n) \equiv 0 \pmod{p^j}$$

for all n *coprime to* Qp.

Remark 1. In Theorem 1.2 (i), we mean "almost all" in the sense of density (i.e. $\#\{n \leq x : a(p^m n) \equiv 0 \pmod{p^j}\} \sim x$ as $x \to \infty$). In light of part (i) of Theorem 1.2, the conclusion of part (ii) is less surprising, so the most interesting result is really Theorem 1.1.

Remark 2. In each theorem, the integer m is determined by the order of vanishing of f at the cusps $\frac{a}{c}$ of $\Gamma_0(Np^2)$ with $p^2 \mid c$. If there is a pole at a particular cusp, the corresponding order of vanishing is negative.

Remark 3. Note that Theorems 1.1 and 1.2 together with the Chinese Remainder Theorem imply linear congruences for all odd moduli M coprime to N.

Dedekind's eta-function, $\eta(z)$, is the weight one-half modular form defined by the infinite product

$$\eta(z) := q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n). \tag{1.3}$$

An eta-quotient is any function $f(z)$ of the form

$$f(z) = \prod_{\delta \mid N} \eta^{r_\delta}(\delta z) \tag{1.4}$$

where $N \geq 1$ and each r_δ is an integer. We will require, in addition, that

$$\sum_{\delta \mid N} r_\delta \delta \equiv 0 \pmod{24}. \tag{1.5}$$

This ensures that f has a Fourier expansion of the form $f(z) = \sum a(n) q^n$. Any eta-quotient can be made to satisfy condition (1.5) by replacing each δ with 24δ. The following corollary gives linear congruences for the coefficients of any eta-quotient.

Corollary 1.3. *Suppose* p *is an odd prime and* N *is an integer with* $(N, p) = 1$. *Let* $f(z)$ *as in (1.4) satisfy (1.5), and suppose that* $f(z)$ *has Fourier expansion* $f(z) = \sum a(n) q^n$. *Set* $k := \sum_{\delta \mid N} r_\delta$, *and let* m *be a sufficiently large integer.*

(a) If k *is odd, then for each positive integer* j, *a positive proportion of the primes* $Q \equiv -1 \pmod{Np^j}$ *have*

$$a(Q^3 p^m n) \equiv 0 \pmod{p^j}$$

for all n *coprime to* Qp.

(b) If k *is even, then for each positive integer* j,
- *(i)* $a(p^m n) \equiv 0 \pmod{p^j}$ *for almost all* n *coprime to* p, *and*
- *(ii) a positive proportion of the primes* $Q \equiv -1 \pmod{Np^j}$ *have*

$$a(Qp^m n) \equiv 0 \pmod{p^j}$$

for all n *coprime to* Qp.

Corollary 1.3 may be applied to many partition functions. We mention only three examples here for brevity.

Example 1. Let k be a positive integer, and let $p_k(n)$ be the number of k-colored partitions of n, that is, the number of partitions of n where each part is assigned one of k colors. The generating function for $p_k(n)$ is given by

$$\sum_{n=0}^{\infty} p_k(n)q^n = \prod_{n=1}^{\infty} \frac{1}{(1-q^n)^k}. \tag{1.6}$$

Using (1.3) and (1.6), we can write

$$f(z) := \frac{1}{\eta^k(24z)} = \sum p_k\left(\frac{n+k}{24}\right) q^n.$$

Since $f(z)$ is an eta-quotient satisfying (1.5), Corollary 1.3 may be applied. Let $\ell \geq 5$ be prime. If k is odd, we get congruences of the form

$$p_k\left(\frac{Q^3\ell^m n+k}{24}\right) \equiv 0 \pmod{\ell^j},$$

and if k is even, we get

$$p_k\left(\frac{Q\ell^m n+k}{24}\right) \equiv 0 \pmod{\ell^j}.$$

Note that when $k = 1$ we recover the function $p(n)$, and get congruences of the form

$$p\left(\frac{Q^3\ell^m n+1}{24}\right) \equiv 0 \pmod{\ell^j},$$

which are guaranteed by the work of Ahlgren [1] and Ono [12].

Example 2. An *overpartition* of n is a partition in which the first occurrence of a number may be overlined. The number of overpartitions of n is denoted $\overline{p}(n)$. See Corteel-Lovejoy [6] for more about overpartitions. We apply Corollary 1.3(a) to the generating function

$$\sum_{n=0}^{\infty} \overline{p}(n)q^n = \prod_{n=1}^{\infty} \frac{1+q^n}{1-q^n} = \frac{\eta(2z)}{\eta^2(z)}$$

to get congruences of the form

$$\overline{p}(Q^3\ell^m n) \equiv 0 \pmod{\ell^j},$$

for primes $\ell \geq 5$. When the modulus is 5, we find an explicit infinite family of such congruences. In Section 5 we will prove the following.

Proposition 1.4. *Let $Q \equiv -1 \pmod 5$ be prime. Then*

$$\overline{p}(5Q^3 n) \equiv 0 \pmod 5$$

for all n coprime to Q.

Example 3. Let $D(n)$ be the number of partitions of n into distinct parts. Then

$$\sum_{n=0}^{\infty} D(n)q^n = \prod_{n=1}^{\infty}(1+q^n),$$

so we can write

$$\frac{\eta(48z)}{\eta(24z)} = \sum_{n=0}^{\infty} D\left(\frac{n-1}{24}\right) q^n.$$

By Corollary 1.3(b)(i), we see that for each prime $p \geq 5$ and integer $j \geq 1$, we have

$$D\left(\frac{p^m n - 1}{24}\right) \equiv 0 \pmod{p^j}$$

for almost all n coprime to p. Part (ii) of Corollary 1.3(b) yields congruences of the form

$$D\left(\frac{Qp^m n - 1}{24}\right) \equiv 0 \pmod{p^j},$$

for primes $p \geq 5$. These phenomena are guaranteed by the work of Lovejoy [10].

For our final application of Theorem 1.1, we obtain linear congruences for the trace of an arbitrary weakly holomorphic modular function on $\Gamma_0^*(p) = \langle \Gamma_0(p), W_p \rangle$, where p is prime (or $p = 1$) and $W_p = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$ is the Fricke involution. Following Bruinier and Funke [5], let D be a positive integer, and let $\mathcal{Q}_{D,p}$ be the subset of quadratic forms $F(x,y) = ax^2 + bxy + cy^2$ in $\mathcal{Q}_D$ with $a \equiv 0 \pmod{p}$. Then $\Gamma_0^*(p)$ acts on $\mathcal{Q}_{D,p}$ with finitely many equivalence classes. For any weakly holomorphic modular function f on $\Gamma_0^*(p)$, define the modular trace function

$$t_f^*(D) := \sum_{F \in \mathcal{Q}_{D,p}/\Gamma_0^*(p)} \frac{1}{|\Gamma_0^*(p)_F|} f(\alpha_F), \tag{1.7}$$

where $\Gamma_0^*(p)_F$ is the stabilizer of F in $\Gamma_0^*(p)$. Note that if $p = 1$ and $f = J_m$, the trace function $t_m(n)$ from (1.2) is recovered. Using Theorem 1.1 and recent work of Bruinier and Funke [5], we have the following corollary.

Corollary 1.5. *Suppose that p is prime (or $p = 1$), k is an integer and $\zeta_p := e^{\frac{2\pi i}{p}}$. Let f be a weakly holomorphic modular function on $\Gamma_0^*(p)$ with Fourier expansion $f(z) = \sum a(n)q^n \in \mathbb{Q}(\zeta_p)((q))$, and suppose $a(0) = 0$. Let ℓ be an odd prime with $\ell \neq p$. Then*

(a) There exists an integer M such that $Mt_f^*(D)$ is an algebraic integer for each $D > 0$.
(b) Let M be as in (a). If m is a sufficiently large integer, then for each positive integer j, a positive proportion of the primes $Q \equiv -1 \pmod{4p^2\ell^j}$ have the property that

$$Mt_f^*(Q^3 \ell^m D) \equiv 0 \pmod{\ell^j}$$

for each D coprime to $Q\ell$.

Remark 4. There is no control over the principal part of the function $f(z)$, so a result as general as Theorem 1.1 is required in order to get linear congruences for $t_f^*(D)$.

In Section 2 we state the remaining facts which we will require. We begin Section 3 with our key technical result. Starting with the weakly holomorphic form $f(z)$ on $\Gamma_0(N)$, we construct a cusp form for each positive integer j that preserves coefficients of $f(z)$ modulo p^j. Results of Shimura and Serre are then applied to this sequence of cusp forms to prove Theorem 1.1. A slight modification of this proof is then made to prove Theorem 1.2 in Section 4. In Sections 5 and 6, we prove the corollaries.

2. Preliminaries

Here we review some basic facts about half-integral weight modular forms. For a more detailed treatment, see for example [18], [8] or [14].

The usual action of $\Gamma_0(N)$ on the cusps $\mathbb{Q} \cup \{\infty\}$ yields a finite set of equivalence classes. A complete set of representatives for these classes is given in [11] as

$$\left\{\frac{a_c}{c} \in \mathbb{Q} : c|N,\ 1 \le a_c \le N,\ (a_c, N) = 1, a_c \equiv a_{c'} \pmod{(c, N/c)} \iff a_c = a_{c'}\right\}. \tag{2.1}$$

The set

$$G := \left\{(\alpha, \phi(z)) : \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q}) \text{ and } \phi^2(z) = \frac{\pm(cz+d)}{\sqrt{\det \alpha}}\right\}$$

is a group under the operation

$$(\alpha, \phi(z))(\beta, \psi(z)) = (\alpha\beta, \phi(\beta z)\psi(z)), \tag{2.2}$$

with identity $\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 1\right)$ and inverse $(\alpha, \phi(z))^{-1} = \left(\alpha^{-1}, \frac{1}{\phi(\alpha^{-1}z)}\right)$ for each $(\alpha, \phi(z)) \in G$. Restriction to matrices in $\Gamma := \mathrm{SL}_2(\mathbb{Z})$ yields the subgroup

$$G' := \{(\alpha, \phi(z)) \in G : \alpha \in \Gamma\}.$$

For each meromorphic function f on $\mathbb{H}$ and each integer k, the slash operator is defined for $\xi = (\alpha, \phi(z)) \in G$ as

$$f(z)|_{\frac{k}{2}}\xi := \phi(z)^{-k} f(\alpha z). \tag{2.3}$$

If $\xi \in G'$, then the Fourier expansion of $f(z)|_{\frac{k}{2}}\xi$ has the form

$$f(z)|_{\frac{k}{2}}\xi = \sum_{n \ge n_\xi} a_\xi(n) q_{h_\xi}^{n + \frac{r_\xi}{4}}, \qquad \text{with } r_\xi \in \{0, 1, 2, 3\}, \tag{2.4}$$

where $h_\xi \mid N$ and $q_{h_\xi} := e^{\frac{2\pi i z}{h_\xi}}$. The integers n_ξ, r_ξ and h_ξ are determined by the equivalence class of the cusp $\alpha\infty$ (see, e.g., §IV.1 of [8]).

For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$ and $z \in \mathbb{H}$, define

$$j(\gamma, z) := \left(\frac{c}{d}\right) \varepsilon_d^{-1} \sqrt{cz + d}, \tag{2.5}$$

where $\left(\frac{c}{d}\right)$ is the extended Jacobi symbol and

$$\varepsilon_d := \begin{cases} 1 & \text{if } d \equiv 1 \pmod 4, \\ i & \text{if } d \equiv 3 \pmod 4, \end{cases} \tag{2.6}$$

and set $\tilde{\gamma} := (\gamma, j(\gamma, z))$. For any congruence subgroup $\Gamma' \le \Gamma_0(4)$, let $\widetilde{\Gamma'} := \{\tilde{\gamma} : \gamma \in \Gamma'\}$.

Let k be an integer. A function f on $\mathbb{H}$ is called a *weakly holomorphic modular form* of weight $\frac{k}{2}$ for $\widetilde{\Gamma'}$ if it is holomorphic on $\mathbb{H}$, meromorphic at the cusps and satisfies the property

$$f|_{\frac{k}{2}}\tilde{\gamma} = f \qquad \text{for all } \tilde{\gamma} \in \widetilde{\Gamma'}. \tag{2.7}$$

We say f is a *holomorphic modular form* if it is holomorphic at the cusps, and a *cusp form* if it vanishes at the cusps. The spaces of weight $\frac{k}{2}$ weakly holomorphic, holomorphic and cusp forms for $\widetilde{\Gamma'}$ are denoted by $\mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma'})$, $M_{\frac{k}{2}}(\widetilde{\Gamma'})$ and $S_{\frac{k}{2}}(\widetilde{\Gamma'})$, respectively.

Let N be a positive integer with $4 \mid N$, and let χ be a Dirichlet character modulo N. Then
$$\mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(N)}, \chi) := \left\{ f \in \mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_1(N)}) : f|_{\frac{k}{2}}\tilde{\gamma} = \chi(d) f \text{ for all } \tilde{\gamma} \in \widetilde{\Gamma_0(N)} \text{ with } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\}.$$
Each $f \in \mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(N)}, \chi)$ has a Fourier expansion $f(z) = \sum a(n) q^n$, where $q := e^{2\pi i z}$.

We have the following correspondence between integral and half-integral weight modular forms on $\Gamma_0(N)$ with character χ. Let
$$\chi_t(n) = \left(\frac{D}{n}\right) \qquad \text{for } D = \operatorname{disc}\left(\mathbb{Q}\left(\sqrt{t}\right)\right).$$
Then if $\frac{k}{2} \in \mathbb{Z}$, we have
$$\mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(N)}, \chi) = \mathcal{M}_{\frac{k}{2}}(\Gamma_0(N), \chi\chi_{-4}^{k/2}). \tag{2.8}$$
Suppose v and t are integers with $t \geq 1$. Set
$$\sigma_{v,t} := \left(\begin{pmatrix} 1 & v \\ 0 & t \end{pmatrix}, t^{1/4} \right) \in G. \tag{2.9}$$
The linear operator $U_t : \mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(N)}, \chi) \to \mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0([N,t])}, \chi\chi_t^k)$ is defined by
$$f(z)|U_t = t^{\frac{k}{4}-1} \sum_{v=0}^{t-1} f(z)|_{\frac{k}{2}} \sigma_{v,t} = t^{-1} \sum_{v=0}^{t-1} f\left(\frac{z+v}{t}\right) = \sum a(tn) q^n. \tag{2.10}$$
A second operator $V_t : \mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(N)}, \chi) \to \mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(Nt)}, \chi\chi_t^k)$ is defined by
$$f(z)|V_t = t^{-\frac{k}{4}} f(z)|_{\frac{k}{2}} \left(\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}, t^{-1/4} \right) = f(tz) = \sum a(n) q^{tn}. \tag{2.11}$$
These facts are stated in [18] (see Propositions 1.3 and 1.4) for holomorphic modular forms of weight $\frac{k}{2}$ with $k \geq 1$. However, one can verify with the same argument that these properties are true for weakly holomorphic modular forms of weight $\frac{k}{2}$ for any integer k. Set
$$\tau_{v,t} := \left(\begin{pmatrix} 1 & v/t \\ 0 & 1 \end{pmatrix}, 1 \right). \tag{2.12}$$
Putting the two operators together,
$$f(z)|U_t|V_t = t^{-1} \sum_{v=0}^{t-1} f(z)|_{\frac{k}{2}} \tau_{v,t} = \sum a(tn) q^{tn}. \tag{2.13}$$

If $f(z) = \sum a(n) q^n \in \mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(N)}, \chi)$ and ψ is a Dirichlet character modulo m, then the twist of f by ψ is given by
$$f \otimes \psi := \sum \psi(n) a(n) q^n \in \mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(Nm^2)}, \chi\psi^2). \tag{2.14}$$

For each prime $p \nmid N$, the integral weight Hecke operator $T_{k,N,\chi}(p)$ preserves the space $\mathcal{M}_k(\Gamma_0(N), \chi)$. The effect of $T_{k,N,\chi}(p)$ on the Fourier expansion of $f(z) = \sum a(n) q^n \in \mathcal{M}_k(\Gamma_0(N), \chi)$ is given by
$$f(z)|T_{k,N,\chi}(p) = \sum \left[a(pn) + \chi(p) p^{k-1} a\left(\frac{n}{p}\right) \right] q^n. \tag{2.15}$$

In the half-integral weight case, for each prime $p \nmid N$, the Hecke operator $T_{\frac{k}{2},N,\chi}(p^2)$ preserves the space $\mathcal{M}_{k/2}(\widetilde{\Gamma_0(N)},\chi)$. The effect of $T_{\frac{k}{2},N,\chi}(p^2)$ on the Fourier expansion of $f(z) = \sum a(n)q^n \in \mathcal{M}_{k/2}(\widetilde{\Gamma_0(N)},\chi)$ is

$$(2.16) \quad f(z)|T_{\frac{k}{2},N,\chi}(p^2) = \sum \left[a(p^2n) + \chi(p)\left(\frac{(-1)^{\frac{k-1}{2}}n}{p}\right)p^{\frac{k-3}{2}}a(n) + \chi(p^2)p^{k-2}a\left(\frac{n}{p^2}\right)\right]q^n.$$

3. Proof of Theorem 1.1

The following result is critical for proving Theorem 1.1.

Theorem 3.1. *Suppose that p is an odd prime, k, m and N are integers with $(N,p)=1$, and χ is a Dirichlet character modulo N. Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. Let $f(z) = \sum a(n)q^n \in \mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(N)},\chi) \cap \mathcal{O}_K((q))$. If m is sufficiently large, then for every positive integer j, there is an integer $\beta \geq j-1$ and a cusp form*

$$g_{p,j}(z) \in S_{\frac{k}{2}+\frac{p^\beta(p^2-1)}{2}}(\widetilde{\Gamma_0(Np^2)},\chi\chi_p^{km})$$

with the property that

$$g_{p,j}(z) \equiv \sum_{\substack{n=1 \\ p\nmid n}}^{\infty} a(p^m n)q^n \pmod{p^j}.$$

To prove Theorem 3.1, we show that we can pick an integer m large enough so that $f(z)|U_{p^m} = \sum a(p^m n)q^n$ is holomorphic at every cusp $\frac{a}{c}$ of $\Gamma_0(Np^2)$ with $p^2 \mid c$. We then define the modular form $f_m(z) := \sum_{p\nmid n} a(p^m n)q^n$, which vanishes at each of these cusps. Finally for each $j \geq 1$, we form $g_{p,j}(z)$ by multiplying $f_m(z)$ by an eta-quotient which vanishes at all of the cusps with $p^2 \nmid c$, and is congruent to 1 modulo p^j. The product $g_{p,j}(z)$ is then a cusp form congruent to $f_m(z)$ modulo p^j.

First we need to know the explicit form of the Fourier expansion of $f(z)|U_{p^m}$ at a cusp $\frac{a}{c}$ with $p^2 \mid c$.

Proposition 3.2. *Suppose that p is an odd prime, k and N are integers with $(N,p)=1$, and χ is a Dirichlet character modulo N. Let $f(z) = \sum a(n)q^n \in \mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(N)},\chi)$. Suppose $\mu \in \{\pm 1, \pm i\}$, and that $\xi := \left(\begin{pmatrix} a & b \\ cp^2 & d\end{pmatrix}, \mu\sqrt{cp^2z+d}\right) \in G'$, with $ac > 0$. Then there exists an integer n_0, a sequence $\{a_0(n)\}_{n\geq n_0}$, a positive integer $h_0|N$, and an $r_0 \in \{0,1,2,3\}$ such that for each $m \geq 1$, we have*

$$(f(z)|U_{p^m})|_{\frac{k}{2}}\xi = \sum_{\substack{n\geq n_0 \\ 4n+r_0\equiv 0 \pmod{p^m}}} a_0(n)q_{h_0p^m}^{n+\frac{r_0}{4}}.$$

Proof. Fix $m \geq 1$, and let $\sigma_{v,t}$ be defined as in (2.9). By (2.10),

$$(3.1) \qquad (f(z)|U_{p^m})|_{\frac{k}{2}}\xi = (p^m)^{\frac{k}{4}-1}\sum_{v=0}^{p^m-1} f(z)|_{\frac{k}{2}}\sigma_{v,p^m}\xi.$$

For each v appearing in (3.1), we choose an integer $s_v \equiv 0 \pmod 4$ so that

$$s_vN \equiv (a+vcp^2)^{-1}(b+vd) \,(\mathrm{mod}\, p^m), \tag{3.2}$$

and set

$$w_v := s_vN. \tag{3.3}$$

We can ensure that $4 \mid s_v$ since any integer s_v satisfying the congruence can be replaced by $(1-p^{2m})s_v$. We require a lemma to show that the w_v are distinct modulo p^m.

Lemma 3.3. *Let $w_v = s_vN$, with s_v defined as in* (3.2). *The integers w_v run through the residue classes mod p^m as v does.*

Proof. Suppose $w_v \equiv w_u \pmod{p^m}$. Then using (3.2) we have

$$(a+ucp^2)(b+vd) \equiv (a+vcp^2)(b+ud) \pmod{p^m}. \tag{3.4}$$

Expanding and simplifying (3.4) yields

$$avd + bucp^2 \equiv aud + bvcp^2 \pmod{p^m}. \tag{3.5}$$

If $u \neq v$ then write

$$u = v + v_1p^e \tag{3.6}$$

with $v_1 \neq 0$, $p \nmid v_1$ and $e \geq 0$. Substituting expression (3.6) in (3.5) and simplifying, we have

$$v_1bcp^{e+2} \equiv adv_1p^e \pmod{p^m}. \tag{3.7}$$

Since $p \nmid adv_1$, this gives a contradiction unless $e \geq m$. The lemma then follows from (3.6). □

Now we return to the proof of Proposition 3.2. Recall the definitions of w_v (3.3) and $\sigma_{v,t}$ (2.9). For each v, define

$$\gamma_v := \begin{pmatrix} a+vcp^2 & \frac{b+vd-aw_v-w_vvcp^2}{p^m} \\ cp^{m+2} & d-w_vcp^2 \end{pmatrix}, \tag{3.8}$$

and

$$\alpha_v := (\gamma_v, \mu\sqrt{cp^2(p^mz-w_v)+d}). \tag{3.9}$$

It is easy to verify that the determinant of γ_v is 1, and that the choice of w_v makes the upper right entry of γ_v an integer. Therefore γ_v is in $\mathrm{SL}_2(\mathbb{Z})$. A computation using (2.2) shows that

$$\sigma_{v,p^m}\xi = \alpha_v\sigma_{w_v,p^m}, \tag{3.10}$$

so from (3.1) and (3.10), we have

$$(f(z)|U_{p^m})|_{\frac{k}{2}}\xi = (p^m)^{\frac{k}{4}-1}\sum_{v=0}^{p^m-1} f(z)|_{\frac{k}{2}}\alpha_v\sigma_{w_v,p^m}. \tag{3.11}$$

For each v, some computations using (2.2) and (3.8) show that

$$\begin{aligned}
\alpha_v\alpha_0^{-1} &= \left(\gamma_v, \mu\sqrt{cp^2(p^m z - w_v)+d}\right)\left(\gamma_0, \mu\sqrt{cp^2(p^m z - w_0)+d}\right)^{-1} \\
&= \left(\gamma_v, \mu\sqrt{cp^2(p^m z - w_v)+d}\right)\left(\gamma_0^{-1}, \frac{1}{\mu\sqrt{cp^2(p^m(\gamma_0^{-1}z)-w_0)+d}}\right) \\
&= \left(\gamma_v\gamma_0^{-1}, \frac{\sqrt{cp^2(p^m(\gamma_0^{-1}z)-w_v)+d}}{\sqrt{cp^2(p^m(\gamma_0^{-1}z)-w_0)+d}}\right) \\
&= \left(\gamma_v\gamma_0^{-1}, \sqrt{(w_v-w_0)c^2p^{m+4}z+1+(w_0-w_v)acp^2}\right),
\end{aligned} \tag{3.12}$$

where

$$\gamma_v\gamma_0^{-1} = \begin{pmatrix} 1+(w_v-w_0)(acp^2+vc^2p^4) & \frac{v}{p^m}+(w_0-w_v)(\frac{a^2+avcp^2}{p^m}) \\ (w_v-w_0)c^2p^{m+4} & 1+(w_0-w_v)acp^2 \end{pmatrix}. \tag{3.13}$$

The next lemma shows that $\alpha_v\alpha_0^{-1} \in \widetilde{\Gamma_1(N)}$.

Lemma 3.4. *Let α_v and α_0 be defined as in* (3.9). *Then*

$$\alpha_v\alpha_0^{-1} = (\gamma_v\gamma_0^{-1}, j(\gamma_v\gamma_0^{-1}, z)) \in \widetilde{\Gamma_1(N)}.$$

Proof. By (3.3) we have $N|(w_v - w_0)$, so $\gamma_v\gamma_0^{-1} \in \Gamma_1(N)$. By (3.12) it remains to show that

$$j(\gamma_v\gamma_0^{-1}, z) = \sqrt{(w_v-w_0)c^2p^{m+4}z+1+(w_0-w_v)acp^2}.$$

By (2.5) and (3.13),

$$j(\gamma_v\gamma_0^{-1}, z) = \left(\frac{(w_v-w_0)c^2p^{m+4}}{1+(w_0-w_v)acp^2}\right)\varepsilon^{-1}_{1+(w_0-w_v)acp^2}\sqrt{(w_v-w_0)c^2p^{m+4}z+1+(w_0-w_v)acp^2}.$$

Each $w_v \equiv 0 \pmod 4$, so $\varepsilon_{1+(w_0-w_v)acp^2} = 1$ by (2.6). To evaluate the Jacobi symbol requires two cases: either $w_v > w_0$ or $w_v < w_0$. Note that the case $w_v = w_0$ is trivial. We will treat the case where $w_v > w_0$.

Define $\varepsilon := \{0,1\}$ by $\varepsilon \equiv m \pmod 2$. Since $ac > 0$, we have $1+(w_0-w_v)acp^2 < 0$, so

$$\left(\frac{(w_v-w_0)c^2p^{m+4}}{1+(w_0-w_v)acp^2}\right) = \left(\frac{(w_v-w_0)p^\varepsilon}{(w_v-w_0)acp^2-1}\right).$$

Set $w_v - w_0 = 2^e r$, where r is odd. Then using properties of Jacobi symbols, and the fact that $(w_v-w_0)acp^2 \equiv 0 \,(\mathrm{mod}\, 8)$, we find that

$$\begin{aligned}
\left(\frac{(w_v-w_0)p^\varepsilon}{(w_v-w_0)acp^2-1}\right) &= \left(\frac{2}{(w_v-w_0)acp^2-1}\right)^e\left(\frac{rp^\varepsilon}{(w_v-w_0)acp^2-1}\right) \\
&= \left(\frac{(w_v-w_0)acp^2-1}{rp^\varepsilon}\right)(-1)^{\left(\frac{rp^\varepsilon-1}{2}\right)} \\
&= \left(\frac{-1}{rp^\varepsilon}\right)(-1)^{\left(\frac{rp^\varepsilon-1}{2}\right)} \\
&= 1.
\end{aligned}$$

The other case is handled similarly. This proves Lemma 3.4. ∎

Returning to the proof of Proposition 3.2, we see that (3.11) and Lemma 3.4 yield

$$(f(z)|U_{p^m})|_{\frac{k}{2}}\xi = (p^m)^{\frac{k}{4}-1}\sum_{v=0}^{p^m-1} f(z)|_{\frac{k}{2}}\alpha_0\sigma_{w_v,p^m}. \tag{3.14}$$

Then using (2.4), we see that there exist integers $h_0 \mid N$, n_0 and r_0, and a sequence $\{a_0(n)\}_{n\geq n_0}$, such that

$$f(z)|_{\frac{k}{2}}\alpha_0 = \sum_{n\geq n_0} a_0(n)q_{h_0}^{n+\frac{r_0}{4}} = \sum_{n\geq n_0} a_0(n)q_{4h_0}^{4n+r_0}. \tag{3.15}$$

Now (2.3), (3.15) and (2.9) yield

$$\begin{aligned}\sum_{v=0}^{p^m-1} f(z)|_{\frac{k}{2}}\alpha_0\sigma_{w_v,p^m} &= \sum_{v=0}^{p^m-1} p^{-km/4}\sum_{n\geq n_0} a_0(n)e^{\left(\frac{2\pi i}{4h_0}\right)\left(\frac{z+w_v}{p^m}\right)(4n+r_0)}\\ &= p^{-km/4}\sum_{n\geq n_0} a_0(n)e^{\frac{2\pi i z}{4h_0p^m}(4n+r_0)}\sum_{v=0}^{p^m-1} e^{\frac{2\pi i w_v}{4h_0p^m}(4n+r_0)}.\end{aligned} \tag{3.16}$$

For each v, we have $4h_0 \mid 4N \mid w_v$ and $(4h_0, p^m) = 1$, so by Lemma 3.3, the numbers $\frac{w_v}{4h_0}$ run through the residue classes modulo p^m as v does. Therefore,

$$\sum_{v=0}^{p^m-1} e^{\frac{2\pi i w_v}{4h_0p^m}(4n+r_0)} = \sum_{v=0}^{p^m-1} e^{\frac{2\pi i v}{p^m}(4n+r_0)} = \begin{cases} p^m & \text{if } 4n+r_0\equiv 0 \pmod{p^m},\\ 0 & \text{else.}\end{cases} \tag{3.17}$$

Putting (3.16) and (3.17) together, we obtain

$$\sum_{v=0}^{p^m-1} f(z)|_{\frac{k}{2}}\alpha_0\sigma_{w_v,p^m} = p^{m(1-\frac{k}{4})}\sum_{\substack{n\geq n_0\\ 4n+r_0\equiv 0\,(\mathrm{mod}\, p^m)}} a_0(n)e^{\frac{2\pi i z}{4h_0p^m}(4n+r_0)}. \tag{3.18}$$

Finally, (3.14) and (3.18) imply

$$(f(z)|U_{p^m})|_{\frac{k}{2}}\xi = \sum_{\substack{n\geq n_0\\ 4n+r_0\equiv 0\,(\mathrm{mod}\, p^m)}} a_0(n)q_{h_0p^m}{}^{(n+\frac{r_0}{4})}. \tag{3.19}$$

This concludes the proof of Proposition 3.2. ◻

Proposition 3.5. *Suppose that p is an odd prime, k and N are integers with $(N,p) = 1$, and χ is a Dirichlet character modulo N. Let $f(z) = \sum a(n)q^n \in \mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(N)}, \chi)$. For each nonnegative integer m, define*

$$f_m(z) := f(z)|U_{p^m} - f(z)|U_{p^{m+1}}|V_p \in \mathcal{M}_{\frac{k}{2}}(\widetilde{\Gamma_0(Np^2)}, \chi\chi_p^{km}).$$

Then for m sufficiently large, f_m vanishes at each cusp $\frac{a}{cp^2}$ of $\Gamma_0(Np^2)$ with $ac > 0$.

Proof. By Proposition 3.2, for each m and each

$$\xi := \left(\begin{pmatrix} a & b\\ cp^2 & d\end{pmatrix}, \mu\sqrt{cp^2z+d}\right) \in G' \tag{3.20}$$

with $ac > 0$ and $\mu \in \{\pm 1, \pm i\}$, we have

$$(f(z)|U_{p^m})|_{\frac{k}{2}}\xi = \sum_{\substack{n \geq n_0 \\ 4n+r_0 \equiv 0 \pmod{p^m}}} a_0(n) q_{h_0 p^m}{}^{(n+\frac{r_0}{4})}.$$

Let γ_0 be defined as in (3.8). The integers n_0 and r_0 are determined by the equivalence class of the cusp $\gamma_0\infty$ under $\Gamma_0(N)$, so there are finitely many such distinct pairs (n_0, r_0) as $\frac{a}{cp^2}$ runs over all possible equivalence classes. If m is sufficiently large, then

$$-p^m < 4n_0 + r_0$$

for all such pairs. Fix such an m, and suppose ξ has the form (3.20). In the corresponding Fourier expansion, if $a_0(n) \neq 0$ and $4n + r_0 \equiv 0 \pmod{p^m}$, then $4n + r_0 \geq 4n_0 + r_0 > -p^m$, so $4n + r_0 \geq 0$, from which $n \geq 0$. Therefore,

$$(f(z)|U_{p^m})|_{\frac{k}{2}}\xi = \sum_{\substack{n \geq 0 \\ 4n+r_0 \equiv 0 \pmod{p^m}}} a_0(n) q_{h_0 p^m}^{n+\frac{r_0}{4}}, \tag{3.21}$$

so $f(z)|U_{p^m}$ is holomorphic at the cusp $\frac{a}{cp^2}$. Now

$$f_m(z)|_{\frac{k}{2}}\xi = (f(z)|U_{p^m})|_{\frac{k}{2}}\xi - (f(z)|U_{p^m})|U_p|V_p|_{\frac{k}{2}}\xi. \tag{3.22}$$

Using (2.13), the second term in (3.22) becomes

$$(f(z)|U_{p^m})|U_p|V_p|_{\frac{k}{2}}\xi = p^{-1}\sum_{v=0}^{p-1}(f(z)|U_{p^m})|_{\frac{k}{2}}\tau_{v,p}\xi. \tag{3.23}$$

For each v, we choose an integer $s_v \equiv 0 \pmod 4$ so that

$$s_v N \equiv a^{-1}vd \pmod p, \tag{3.24}$$

and set

$$w_v := s_v N. \tag{3.25}$$

Define

$$\delta_v := \begin{pmatrix} 1 + aw_vcp + vw_vc^2p^2 & \frac{avd-a^2w_v}{p} - acvw_v - bvcp \\ w_vc^2p^3 & 1 - aw_vcp \end{pmatrix},$$

and

$$\beta_v := \left(\delta_v, \sqrt{w_vc^2p^3z + 1 - aw_vcp}\right).$$

A computation shows that

$$\tau_{v,p}\xi = \beta_v\xi\tau_{w_v,p}. \tag{3.26}$$

Using arguments similar to those used to prove Lemma 3.4, we find that

$$\beta_v = (\delta_v, j(\delta_v, z)) \in \widetilde{\Gamma_1(Np)}. \tag{3.27}$$

Then by (3.26) and (3.27), for each v appearing in (3.23), we have

$$(f(z)|U_{p^m})|_{\frac{k}{2}}\tau_{v,p}\xi = (f(z)|U_{p^m})|_{\frac{k}{2}}\beta_v\xi\tau_{w_v,p} = (f(z)|U_{p^m})|_{\frac{k}{2}}\xi\tau_{w_v,p}. \tag{3.28}$$

Now we rewrite (3.23) using (3.28), (3.21), (2.3) and (2.12) to get

$$(3.29)\quad (f(z)|U_{p^m})|U_p|V_p|_{\frac{k}{2}}\xi = p^{-1}\sum_{v=0}^{p-1}(f(z)|U_{p^m})|_{\frac{k}{2}}\xi\tau_{w_v,p}$$

$$= p^{-1}\sum_{v=0}^{p-1}\left(\sum_{\substack{n\geq 0\\ 4n+r_0\equiv 0\,(\mathrm{mod}\,p^m)}} a_0(n)q_{h_0p^m}^{n+\frac{r_0}{4}}\right)\Bigg|_{\frac{k}{2}}\tau_{w_v,p}$$

$$= p^{-1}\sum_{v=0}^{p-1}\sum_{\substack{n\geq 0\\ 4n+r_0\equiv 0\,(\mathrm{mod}\,p^m)}} a_0(n)\exp\left(\frac{2\pi i(z+\frac{w_v}{p})}{h_0p^m}\left(n+\frac{r_0}{4}\right)\right)$$

$$= p^{-1}\sum_{\substack{n\geq 0\\ 4n+r_0\equiv 0\,(\mathrm{mod}\,p^m)}} a_0(n)q_{h_0p^m}^{n+\frac{r_0}{4}}\sum_{v=0}^{p-1}\exp\left(\frac{2\pi i w_v}{4h_0p^{m+1}}(4n+r_0)\right)$$

$$= p^{-1}\sum_{\substack{n\geq 0\\ 4n+r_0\equiv 0\,(\mathrm{mod}\,p^m)}} a_0(n)q_{h_0p^m}^{n+\frac{r_0}{4}}\sum_{v=0}^{p-1}\exp\left(\frac{2\pi i w_v}{4h_0p}\left(\frac{4n+r_0}{p^m}\right)\right).$$

Recall the definition of w_v (3.25). Note that since a, d, h_0 and 4 are all coprime to p, the numbers $w_v/4h_0$ run through the residue classes modulo p as v does, so

$$(3.30)\quad \sum_{v=0}^{p-1}\exp\left(\frac{2\pi i w_v}{4h_0p}\left(\frac{4n+r_0}{p^m}\right)\right) = \sum_{v=0}^{p-1}\exp\left(\frac{2\pi i v}{p}\left(\frac{4n+r_0}{p^m}\right)\right) = \begin{cases} p & \text{if } p \mid \frac{4n+r_0}{p^m},\\ 0 & \text{otherwise.}\end{cases}$$

Putting together (3.29) and (3.30), we have

$$(3.31)\quad (f(z)|U_{p^m})|U_p|V_p|_{\frac{k}{2}}\xi = \sum_{\substack{n\geq 0\\ 4n+r_0\equiv 0\,(\mathrm{mod}\,p^{m+1})}} a_0(n)q_{h_0p^m}^{n+\frac{r_0}{4}}.$$

Now using (3.22), (3.21) and (3.31), we have

$$(3.32)\quad f_m(z)|_{\frac{k}{2}}\xi = \sum_{\substack{n\geq 0\\ 4n+r_0\equiv 0\,(\mathrm{mod}\,p^m)}} a_0(n)q_{h_0p^m}^{n+\frac{r_0}{4}} - \sum_{\substack{n\geq 0\\ 4n+r_0\equiv 0\,(\mathrm{mod}\,p^{m+1})}} a_0(n)q_{h_0p^m}^{n+\frac{r_0}{4}}.$$

If $r_0 \neq 0$ then neither series in (3.32) has a constant term, and if $r_0 = 0$, then the constant term in each expansion is $a_0(0)$, so they cancel. Therefore $f_m(z)$ vanishes at the cusp $\frac{a}{cp^2}$. This concludes the proof of Proposition 3.5. □

Now for each odd prime p, we define the eta-quotient

$$F_p(z) := \begin{cases} \frac{\eta^{p^2}(z)}{\eta(p^2z)} \in M_{\frac{p^2-1}{2}}(\Gamma_0(p^2)) & \text{if } p\geq 5,\\ \frac{\eta^{27}(z)}{\eta^3(9z)} \in M_{12}(\Gamma_0(9)) & \text{if } p=3.\end{cases}$$

Using a standard formula for the order of vanishing of an eta-quotient at a cusp (see [7]), we see that F_p vanishes at every cusp $\frac{a}{c}$ of $\Gamma_0(Np^2)$ with $p^2 \nmid c$. By the definition of $\eta(z)$, it is clear that $F_p(z) \equiv 1 \pmod{p}$, and an easy induction argument shows that $F_p(z)^{p^{s-1}} \equiv 1 \pmod{p^s}$ for any integer $s \geq 1$.

Proof of Theorem 3.1. Let f be as in the hypotheses of Theorem 3.1. Let m be chosen to satisfy Proposition 3.5 for f, and fix j. If $\beta \geq j-1$ is sufficiently large, then

$$g_{p,j}(z) := f_m(z) \cdot F_p(z)^{p^\beta} \equiv f_m(z) \pmod{p^j} \tag{3.33}$$

vanishes at all cusps $\frac{a}{c}$ of $\Gamma_0(Np^2)$ for which $p^2 \nmid c$. By Proposition 3.5, $g_{p,j}(z)$ vanishes at the cusps $\frac{a}{c}$ for which $p^2|c$, so we have

$$g_{p,j}(z) \in S_{\frac{k}{2}+\frac{p^\beta(p^2-1)}{2}}(\widetilde{\Gamma_0(Np^2)}, \chi\chi_p^{km}). \tag{3.34}$$

By (2.10) and (2.13), we have

$$g_{p,j}(z) \equiv f_m(z) \equiv \sum_{n=1}^{\infty} a(p^m n)q^n - \sum_{n=1}^{\infty} a(p^{m+1}n)q^{pn} \equiv \sum_{\substack{n=1 \\ p\nmid n}}^{\infty} a(p^m n)q^n \pmod{p^j}. \tag{3.35}$$

Combining (3.34) and (3.35) proves Theorem 3.1. □

The proof of Theorem 1.1 uses the following result of Ahlgren and Ono, which relies on Shimura's theory and a result of Serre (stated below as Proposition 4.2). The proof of Serre's theorem involves the theory of modular Galois representations and the Chebotarev density theorem.

Proposition 3.6. (Ahlgren-Ono [2], Lemma 3.1) *Suppose that $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\frac{k}{2}}(\widetilde{\Gamma_0(N)}, \chi)$ has coefficients in the ring of integers of some number field, and M is a positive integer. Furthermore, suppose that $k > 3$. Then a positive proportion of the primes $p \equiv -1 \pmod{MN}$ have the property that*

$$f(z)|T_{\frac{k}{2},N,\chi}(p^2) \equiv 0 \pmod{M}.$$

Proof of Theorem 1.1. Let f be as in the hypotheses of Theorem 1.1. Fix an odd prime p, and an integer $j \geq 1$, and let

$$g_{p,j}(z) \equiv \sum_{\substack{n=1 \\ p\nmid n}}^{\infty} a(p^m n)q^n \pmod{p^j}$$

be the cusp form guaranteed by Theorem 3.1, with β chosen so that $\kappa := k + p^\beta(p^2-1) > 3$. By Proposition 3.6, a positive proportion of the primes $Q \equiv -1 \pmod{Np^j}$ have

$$g_{p,j}(z)|T_{\frac{\kappa}{2},Np^2,\chi\chi_p^{km}}(Q^2) \equiv 0 \pmod{p^j}. \tag{3.36}$$

If we write $g_{p,j}(z) = \sum_{n=1}^{\infty} b(n)q^n$, then (2.16) and (3.36) yield

$$\begin{aligned} &g_{p,j}(z)|T_{\frac{\kappa}{2},Np^2,\chi\chi_p^{km}}(Q^2) \\ &= \sum_{n=1}^{\infty} \left(b(Q^2n) + \chi\chi_p^{km}(Q) \left(\frac{(-1)^{\frac{\kappa-1}{2}} n}{Q} \right) Q^{\frac{\kappa-3}{2}} b(n) + \chi\chi_p^{km}(Q^2)Q^{\kappa-2} b\left(\frac{n}{Q^2}\right) \right) q^n \equiv 0 \pmod{p^j}. \end{aligned} \tag{3.37}$$

Replacing n by Qn in (3.37), we have

(3.38)
$$\sum_{n=1}^{\infty}\left(b(Q^3n)+\chi\chi_p^{km}(Q)\left(\frac{(-1)^{\frac{\kappa-1}{2}}Qn}{Q}\right)Q^{\frac{\kappa-3}{2}}b(Qn)+\chi\chi_p^{km}(Q^2)Q^{\kappa-2}b\left(\frac{Qn}{Q^2}\right)\right)q^{Qn} \equiv 0 \pmod{p^j}.$$

If $(Q,n)=1$, then the coefficient of q^{Qn} in (3.38) is just $b(Q^3n)$. So

$$a(p^mQ^3n)\equiv b(Q^3n)\equiv 0 \,(\mathrm{mod}\, p^j)$$

for all n coprime to Qp. This completes the proof of Theorem 1.1. □

4. Proof of Theorem 1.2

For the integral weight case we use two results of Serre.

Proof of Theorem 1.2. Let f and p be as in the hypotheses of Theorem 1.2, and fix $j\geq 1$. First, if $4\nmid N$, we may consider $f(z)$ as a modular form on $\Gamma_0(4N)$, so we will assume that $4\mid N$. Then by (2.8) and Theorem 3.1, there exists a cusp form $g_{p,j}$ of positive integral weight such that

$$g_{p,j}(z)\equiv \sum_{\substack{n=1\\ p\nmid n}}^{\infty} a(p^mn)q^n \pmod{p^j}. \tag{4.1}$$

The first assertion follows from (4.1) together with the following result of Serre [15].

Proposition 4.1. (Serre [15], Corollaire du Théorème 1) *Let*

$$f(z)=\sum_{n=0}^{\infty}c_nq_M^n, \quad M\geq 1,$$

be a modular form of integral weight $k\geq 1$ on a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, *and suppose that the coefficients c_n lie in the ring of integers of an algebraic number field K. Then for any integer $m\geq 1$,*

$$c_n\equiv 0 \pmod{m}$$

for almost all n.

For the second assertion, we use another result of Serre.

Proposition 4.2. (Serre [16], Exercise 6.4) *Suppose that* $f(z)=\sum_{n=1}^{\infty}a(n)q^n\in S_k(\Gamma_0(N),\chi)$ *has coefficients in $\mathcal{O}_K$, and M is a positive integer. Furthermore, suppose that $k>1$. Then a positive proportion of the primes* $p\equiv -1 \pmod{MN}$ *have the property that*

$$f(z)|T_{k,N,\chi}(p)\equiv 0 \pmod{M}.$$

It follows from (4.1) and Proposition 4.2 that if $g_{p,j}(z)$ has weight κ and character ψ, then a positive proportion of the primes $Q\equiv -1 \pmod{Np^j}$ have the property that

$$g_{p,j}(z)|T_{\kappa,Np^2,\psi}(Q)\equiv 0 \pmod{p^j}. \tag{4.2}$$

If we write $g_{p,j}(z) = \sum_{n=1}^{\infty} b(n)q^n$, then (2.15) and (4.2) imply that

$$g_{p,j}(z)|T_{\kappa,Np^2,\psi}(Q) = \sum_{n=1}^{\infty} \left(b(Qn) + \psi(Q)Q^{\kappa-1} b\left(\frac{n}{Q}\right)\right) q^n \equiv 0 \pmod{p^j}. \tag{4.3}$$

If $(Q,n)=1$, then the coefficient of q^n in (4.3) is just $b(Qn)$. Therefore

$$a(Qp^m n) \equiv b(Qn) \equiv 0 \pmod{p^j}$$

for all n coprime to Qp. This concludes the proof of Theorem 1.2. □

5. Eta-quotients

Here we prove Corollary 1.3 and Proposition 1.4. The first result concerning eta-quotients follows easily from the main theorems.

Proof of Corollary 1.3. Let f be as in the hypotheses of Corollary 1.3. It is clear by (1.3) that $\eta(z)$ is holomorphic and non-vanishing on $\mathbb{H}$, so f is also holomorphic on $\mathbb{H}$. Since $\eta(z)$ has integer coefficients, so does $f(z)$. Replace N by a power of N, if necessary, so that $f(z)$ satisfies

$$N \sum_{\delta|N} \frac{r_\delta}{\delta} \equiv 0 \pmod{24}. \tag{5.1}$$

Then f is a weakly holomorphic modular form of weight $\frac{k}{2}$ and some character χ with level N [7]. We may now apply either Theorem 1.1 or Theorem 1.2, depending on the parity of k, to complete the proof of Corollary 1.3. □

We now prove Proposition 1.4, which gives an infinite class of congruences for overpartitions modulo 5.

Proof of Proposition 1.4. Consider the theta functions

$$\Theta(z) := \sum_{n=-\infty}^{\infty} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + \cdots \in M_{\frac{1}{2}}(\widetilde{\Gamma_0(4)}),$$

and

$$\Theta_1(z) := \frac{\eta^2(z)}{\eta(2z)} = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2} = 1 - 2q + 2q^4 - 2q^9 + \cdots \in M_{\frac{1}{2}}(\widetilde{\Gamma_0(16)}).$$

Let χ_2^{triv} be the trivial character modulo 2. Using (2.14), it is easy to verify that these theta functions satisfy

$$\Theta_1(z)^3 = \Theta(z)^3 - 2\Theta(z)^3 \otimes \chi_2^{\text{triv}} \in M_{\frac{3}{2}}(\widetilde{\Gamma_0(16)}). \tag{5.2}$$

Recall that the generating function for overpartitions is

$$\sum_{n=0}^{\infty} \overline{p}(n) q^n = \frac{\eta(2z)}{\eta^2(z)} = \frac{1}{\Theta_1(z)}.$$

Let

$$\Delta(z) := q \prod_{n=1}^{\infty} (1-q^n)^{24} = \eta^{24}(z) \in S_{12}(\Gamma), \tag{5.3}$$

and set

$$f(z) := \frac{\frac{\Delta^2(z)}{\Delta(2z)} \Big| T_{12,2}(5)}{\frac{\eta^{10}(z)}{\eta^5(2z)}}. \tag{5.4}$$

Since the numerator is of level 2, and the 24th power of the denominator is also of level 2, it suffices to check holomorphicity at the two cusps of $\Gamma_0(2)$. It is clear by (1.3) and (2.15) that f is holomorphic at infinity. A computation using (2.15) shows that

$$\frac{\Delta^2(z)}{\Delta(2z)} \Big| T_{12,2}(5) = 48828126 \frac{\Delta^2(z)}{\Delta(2z)} + 2342387712\Delta(z) + 4630511616\Delta(2z). \tag{5.5}$$

Using the transformation formula

$$\eta\left(-\frac{1}{z}\right) = (-iz)^{\frac{1}{2}}\eta(z) \tag{5.6}$$

([14], Theorem 1.61) with (5.4) and (5.5), we calculate that the expansion of $f(z)$ at 0 has the form

$$c \cdot q^{\frac{3}{16}} + \cdots$$

for some constant $c \in \mathbb{C}$. Therefore

$$f(z) \in M_{\frac{19}{2}}(\widetilde{\Gamma_0(16)}). \tag{5.7}$$

Since $T_{12,2}(5)$ is the same as the operator U_5 modulo 5, it can be verified using (1.3) and (2.10) that

$$\begin{aligned} f(z) &\equiv \frac{\frac{\Delta^2(z)}{\Delta(2z)} \Big| U_5}{\frac{\eta^{10}(z)}{\eta^5(2z)}} \pmod 5 \\ &\equiv \frac{\left(\frac{\eta^{50}(z)}{\eta^{25}(2z)} \cdot \sum \overline{p}(n)q^n\right) \Big| U_5}{\frac{\eta^{10}(z)}{\eta^5(2z)}} \pmod 5 \\ &\equiv \sum \overline{p}(5n)q^n \pmod 5. \end{aligned} \tag{5.8}$$

The Eisenstein series

$$E_4(z) := 1 + 240\sum_{n=1}^{\infty} \sigma_3(n)q^n \in M_4(\Gamma) \tag{5.9}$$

clearly satisfies

$$E_4(z) \equiv 1 \pmod 5. \tag{5.10}$$

Using (5.2), (5.9) and (5.10), we have

$$\Theta_1(z)^3 \cdot E_4^2(z) \in M_{\frac{19}{2}}(\widetilde{\Gamma_0(16)}) \tag{5.11}$$

with

$$\Theta_1(z)^3 \equiv \Theta_1(z)^3 \cdot E_4^2(z) \pmod 5. \tag{5.12}$$

By a result of Sturm ([19], Theorem 1), two holomorphic modular forms in $M_{\frac{k}{2}}(\widetilde{\Gamma_0(N)}, \chi)$ are congruent modulo m if their coefficients are congruent modulo m for each index $n \leq \frac{k}{24}[\Gamma : \Gamma_0(N)]$. Using (5.12), the congruence

$$f(z) \equiv \Theta_1(z)^3 \pmod 5 \tag{5.13}$$

can be easily verified with a computer algebra system, well beyond the Sturm bound of 19. Then (5.8) and (5.13) imply that

$$\Theta_1(z)^3 \equiv \sum \overline{p}(5n)q^n \pmod 5. \tag{5.14}$$

It is well known that $\Theta^3(z)$, considered as a form of level 16, is a normalized eigenform for $T_{\frac{3}{2},16}(Q^2)$, satisfying

$$\Theta(z)^3 | T_{\frac{3}{2},16}(Q^2) = (Q+1)\Theta^3(z) \tag{5.15}$$

for each odd prime Q.

The Hecke operator $T_{\frac{3}{2},16}(Q^2)$ commutes with the quadratic twist χ_2^{triv}, so using (5.2) and (5.15) we have

$$\Theta_1(z)^3 | T_{\frac{3}{2},16}(Q^2) \equiv (Q+1)\Theta_1(z)^3 \equiv 0 \pmod 5 \tag{5.16}$$

when $Q \equiv -1 \pmod 5$. Then using (5.14) and an argument as in (3.38), we have

$$\overline{p}(5Q^3n) \equiv 0 \pmod 5,$$

when n is coprime to Q. This concludes the proof of Proposition 1.4. □

6. Traces of CM values of modular functions

In [5], Bruinier and Funke realize the traces of arbitrary modular functions on any congruence subgroup as the Fourier coefficients of certain weakly holomorphic modular forms. These forms are obtained by integrating the modular functions against a theta series associated to a certain lattice and a certain Schwartz function. The authors give the following theorem as a concrete example of their more general result.

Recall the modular trace function for $\Gamma_0^*(p)$ given in (1.7). Define $\sigma_1(n) := \sum_{t|n} t$ for $n \in \mathbb{Z}_{>0}$, set $\sigma_1(0) := -\frac{1}{24}$, and let $\sigma_1(x) := 0$ for $x \notin \mathbb{Z}_{\geq 0}$.

Theorem 6.1. (Bruinier-Funke [5], Theorem 1.1) *Let $f \in \mathcal{M}_0(\Gamma_0^*(p))$ have Fourier expansion $f(z) = \sum a(n)q^n$ with $a(0) = 0$. Then*

$$G(z, f) := \sum_{D>0} t_f^*(D)q^D + \sum_{n \geq 0}(\sigma_1(n) + p\sigma_1(n/p))a(-n) - \sum_{m>0}\sum_{n>0} ma(-mn)q^{-m^2}$$

is a weakly holomorphic modular form of weight 3/2 for the group $\widetilde{\Gamma_0(4p)}$.

Proof of Corollary 1.5. For simplicity, let $G(z) := G(z, f)$ be the modular form guaranteed by Theorem 6.1. The following lemma shows that $G(z)$ has algebraic coefficients.

Lemma 6.2. *Let f be a weakly holomorphic modular function for $\Gamma_0^*(p)$ whose Fourier coefficients with respect to q_p lie in $\mathbb{Q}(\zeta_p)$. Then for each discriminant $D > 0$, $t_f^*(D)$ is algebraic.*

Proof. We can view f as a modular function for the principal congruence subgroup $\Gamma(p)$, which consists of matrices in Γ congruent to the identity modulo p. Let k_p be the field of modular functions for Γ_p whose Fourier expansions with respect to q_p have coefficients in $\mathbb{Q}(\zeta_p)$. Fix a discriminant $D > 0$ and a quadratic form $F \in \mathcal{Q}_{D,p}$, and let α_F be the associated root in $\mathbb{H}$. Set $K = \mathbb{Q}(\alpha_F)$. By the theory of complex multiplication, the field $Kk_p(\alpha_F)$, generated over K by all values $f(\alpha_F)$ with $f \in k_p$ and f defined at α_F, is the ray class field over K with conductor p (see [9], Ch. 10 §1, Corollary to Theorem 2). So in particular, $f(\alpha_F)$ is algebraic. Lemma 6.2 then follows from definition (1.7). □

By Lemma 6.2, we have $G(z) \in \overline{\mathbb{Q}}((q))$. The next lemma proves conclusion (a) of Corollary 1.5.

Lemma 6.3. *Let f be as in the hypotheses of Corollary 1.5, and let $G(z) := G(z, f)$ be the modular form guaranteed by Theorem 6.1. There exists an integer M and an algebraic number field L such that $MG(z) \in \mathcal{O}_L((q))$.*

Proof. Recall the function $\Delta(z)$ from (5.3). Since $G(z)$ is meromorphic at the cusps of $\Gamma_0(4p)$ and $\Delta(z)$ vanishes at each cusp, then for sufficiently large h, the function $\Delta^h(z)G(z)$ is a cusp form for $\Gamma_0(4p)$. Since $\Delta(z)$ has integer coefficients,

$$\Delta^h(z)G(z) \in \overline{\mathbb{Q}}[\![q]\!].$$

Hence $\Delta^h(z)G(z)$ has bounded denominators, that is, there is an algebraic number field L and an integer M such that

$$M\Delta^h(z)G(z) \in \mathcal{O}_L[\![q]\!]$$

(see Lemma 8 of [17]). But $\frac{1}{\Delta^h(z)}$ also has integer coefficients, so we have

$$MG(z) \in \mathcal{O}_L((q)).$$

□

Now we prove Corollary 1.5(b). By Lemma 6.3, we can apply Theorem 1.1 to $MG(z)$. Hence for each $j \geq 1$, a positive proportion of the primes $Q \equiv -1 \pmod{4p\ell^j}$ have

$$Mt_f^*(Q^3\ell^m D) \equiv 0 \pmod{\ell^j}$$

for all D coprime to $Q\ell$. This concludes the proof of Corollary 1.5. □

References

[1] S. Ahlgren, *Distribution of the partition function modulo composite integers M*, Math. Ann. **318** (2000), 795-803.

[2] S. Ahlgren and K. Ono, *Congruence Properties for the Partition Function*, Proc. Natl. Acad. Sci. USA **98** (2001), no. 23, 12882-12884.

[3] S. Ahlgren and K. Ono, *Congruences and conjectures for the partition function*, Proceedings of the Conference on q-series with Applications to Combinatorics, Number Theory and Physics, AMS Contemporary Mathematics, vol. 291, 2001, pp. 1-10.

[4] S. Ahlgren and K. Ono, *Arithmetic of Singular Moduli and Class Equations*, Compositio Math. **141** (2005), 293-312.

[5] J. H. Bruinier and J. Funke, *Traces of CM Values of Modular Functions*, J. Reine Angew. Math., to appear.

[6] S. Corteel and J. Lovejoy, *Overpartitions*, Trans. Amer. Math. Soc. **356** (2004), 1623-1635.

[7] B. Gordon and K. Hughes, *Multiplicative properties of eta-products*, Contemp. Math. **143** (1993), 415-430.
[8] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1993.
[9] S. Lang, *Elliptic Functions*, Springer-Verlag, New York, 1987.
[10] J. Lovejoy, *Divisibility and distribution of partitions into distinct parts*, Adv. Math. **158** (2001), 253-263.
[11] Y. Martin, *Multiplicative η-quotients*, Trans. Amer. Math. Soc. **348** (1996), 4825-4856.
[12] K. Ono, *Distribution of the partition function modulo m*, Ann. of Math. **151** (2000), 293-307.
[13] K. Ono, *Arithmetic of the partition function*, Proceedings of the NATO Advanced Study Institute on Special Functions, Special Functions 2000 (J. Bustoz, S. Suslov, eds.), Kluwer Academic Publishers, 2002, pp. 243-253.
[14] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, CBMS Regional Conference Series in Mathematics, vol. 102, American Mathematical Society, Providence, RI, 2004.
[15] J.-P. Serre, *Divisibilité des coefficients des formes modulaires de poids entier*, C. R. Acad. Sci. Paris Sèr. I Math. **279** (1974), 679-682.
[16] J.-P. Serre, *Divisibilité des certaines fonctions arithmétiques*, Enseign. Math. **22** (1976), 227-260.
[17] J.-P. Serre and H. M. Stark, *Modular forms of weight 1/2*, Modular functions of one variable VI (Proc. Second Internat. Conf., Univ. Bonn, Bonn 1976), Lecture Notes in Math, vol. 627, Springer, 1977, pp. 27-67.
[18] G. Shimura, *On modular forms of half-integral weight*, Ann. of Math. **97** (1973), 440-481.
[19] J. Sturm, *On the congruence of modular forms*, Springer Lect. Notes **1240** (1984), 275-280.
[20] H. Swisher, *The Andrews-Stanley partition function and $p(n)$*, Trans. Amer. Math. Soc., recommended for publication.
[21] D. Zagier, *Traces of singular moduli*, Motives, Polylogarithms and Hodge Theory, Part I. (F. Bogomolov and L. Katzarkov, eds.), International Press, Somerville, 2002, pp. 211-244.

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