PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 10, October 2008, Pages 3419–3428
S 0002-9939(08)09333-7
Article electronically published on May 7, 2008

THE EFFECTIVE CHEBOTAREV DENSITY THEOREM AND MODULAR FORMS MODULO $\mathfrak{m}$

SAM LICHTENSTEIN

(Communicated by Ken Ono)

ABSTRACT. Suppose that f (resp. g) is a modular form of integral (resp. half-integral) weight with coefficients in the ring of integers $\mathcal{O}_K$ of a number field K. For any ideal $\mathfrak{m} \subset \mathcal{O}_K$, we bound the first prime p for which $f \mid T_p$ (resp. $g \mid T_{p^2}$) is zero (mod $\mathfrak{m}$). Applications include the solution to a question of Ono (2001) concerning partitions.

1. Introduction and statement of results

The existence of ℓ-adic Galois representations attached to Hecke eigenforms entail congruence properties satisfied by their Fourier coefficients [SwD]. These in turn imply congruences for the Fourier coefficients of arbitrary integral weight modular forms, which may be extended to half-integral weight forms using the Shimura correspondence or the methods of [OSk]. For example, in the case of Ramanujan's cusp form

$$\Delta(z) = \sum \tau(n) q^n := q \prod (1-q^n)^{24} = q + 24q^2 + 252q^3 + \cdots, \quad \text{where } q = e^{2\pi i z},$$

these include well-known congruences such as $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$. We will be concerned with congruences of a different sort: the annihilation of modular forms modulo an ideal $\mathfrak{m}$ by Hecke operators.

Suppose $f(z) = \sum a(n) q^n$ is a normalized Hecke eigenform with integer weight k, level N and character χ, and with coefficients in the ring of integers $\mathcal{O}_K$ of a number field K. Let λ be a prime of $\mathcal{O}_K$ with residue characteristic ℓ, and let $\mathcal{O}_\lambda$ denote the λ-adic completion of $\mathcal{O}_K$. Work of Shimura, Deligne and Serre guarantees the existence of a continuous, semisimple, odd Galois representation

$$\rho_{\lambda,f} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_\lambda)$$

which is unramified at all primes $p \nmid N\ell$. (If $k = 1$, then in fact the representation is complex.) If Frob_p denotes a frobenius element corresponding to such a prime, these representations have the property that

$$\operatorname{tr} \rho_{\lambda,f}(\mathrm{Frob}_p) = a(p) \quad \text{and} \quad \det \rho_{\lambda,f}(\mathrm{Frob}_p) = \chi(p) p^{k-1}.$$

A consequence of this theory is a theorem of Serre concerning congruences for the coefficients of modular forms of the sort mentioned above. (We write $M_k(N,\chi)$ [resp. $S_k(N,\chi)$, resp. $\mathcal{E}_k(N,\chi)$] to denote the space of modular forms [resp. cusp

Received by the editors July 18, 2007, and, in revised form, August 25, 2007.
2000 *Mathematics Subject Classification.* Primary 11F33.

©2008 American Mathematical Society
Reverts to public domain 28 years from publication

forms, resp. Eisenstein series] of weight k, level N, and Nebentypus χ. We omit χ from the notation when it is trivial, and N when it is 1.)

Theorem (Serre, [S1], §6.4)**.** *Given a number ring $\mathcal{O}_K$ and an ideal $\mathfrak{m} \subset \mathcal{O}_K$ with norm M, a positive density of primes $p \equiv -1 \pmod{NM}$ satisfy $f(z) \mid T_p \equiv 0 \pmod{\mathfrak{m}}$ for every $f(z) \in M_k(N, \chi)$ with coefficients in $\mathcal{O}_K$.*

Remark. Similarly, a positive density of primes satisfies $f(z) \mid T_p \equiv 2f(z) \pmod{\mathfrak{m}}$, and likewise for any other eigenvalue $\lambda \not\equiv 0, 2 \pmod{\mathfrak{m}}$ which occurs.

As observed by Ono [O2], Shimura's correspondence can be used to extend Serre's theorem to forms f of half-integral weight $\kappa + \frac{1}{2} \geq \frac{3}{2}$, and the result is trivial if $\kappa + \frac{1}{2} = \frac{1}{2}$ by the Serre-Stark basis theorem. In these cases the theorem says that a positive density of primes $p \equiv -1 \pmod{NM}$ satisfy $f(z) \mid T_{p^2} \equiv 0 \pmod{\mathfrak{m}}$.

Serre's theorem and its extension to half-integer weight hold for all modular forms, not just eigenforms. However, for a generic modular form f, the first prime p such that $f(z) \mid T_p \equiv 0 \pmod{\mathfrak{m}}$ may be rather large. For example, consider powers of $\Delta(z)$. Whereas $\Delta(z) \mid T_{19} \equiv 0 \pmod 5$, the first Hecke operator T_p which annihilates $\Delta^3 \pmod 5$ is T_{149}. Here we use an effective version of the Chebotarev Density Theorem [LMO] to prove bounds for the first primes of the sort guaranteed by Serre's theorem, in terms of natural quantities depending on the space of modular forms and the ideal $\mathfrak{m}$.

To state these bounds we require some notation. Given a Hecke-invariant subspace $V \subset M_k(N, \chi)$ we define the following quantities. (All dimensions are over $\mathbb{C}$.)

- $\delta = \delta(V) := \dim(V)$.
- $d = d(V) := \dim(\mathcal{E}_k(N, \chi) \cap V) + \sum \dim(S_k^{\text{new}}(M, \chi))$, summing over all $M|N$ such that $f(tz) \in V$ for some $t|\frac{N}{M}$ and some nonzero element $f(z) \in S_k^{\text{new}}(M, \chi)$.
- $s = s(V) := \frac{k}{12} N \prod(1 + p^{-1})$, the product taken over primes $p|N$.
- A basis $f_1, \ldots, f_d$ of Hecke eigenforms for $(\mathcal{E}_k(N, \chi) \cap V) \oplus \bigoplus S_k^{\text{new}}(M, \chi)$, the direct sum ranging over the same M from the definition of $d(V)$. Let $f_i(z) = \sum a_i(n) q^n$, normalizing so that $a_i(1) = 1$.
- Number fields K_i such that the coefficients of f_i and the values of the Nebentypus χ lie in $\mathcal{O}_{K_i}$. Let $K = K(V) := K_1 K_2 \cdots K_d$ be their compositum.

Now let F be a number field, and let $\mathfrak{m}$ be an ideal of the ring of integers $\mathcal{O}_F$ with prime factorization $\mathfrak{m} = \prod \lambda_j^{\alpha_j}$, where λ_j has residue characteristic ℓ_j. For each j, V and $\mathfrak{m}$ determine further data:

- Primes μ_j of KF lying over λ_j such that $\nu_j := \max\{\nu_{\mu_j}(a_i(n)) : 1 \leq i \leq d, 1 \leq n \leq s\}$ are as small as possible. (Here $\nu_\mu(a)$ denotes the μ-adic valuation of a, for a prime μ of $\mathcal{O}_F$ and an element $a \in F$. That is, $(a) = \mu^{\nu_\mu(a)} \cdot \mathfrak{b}$ for some fractional ideal $\mathfrak{b}$ relatively prime to μ.) Let $r_j := [\mathcal{O}_{KF}/\mu_j : \mathbb{F}_{\ell_j}]$.

Finally, using these data we define quantities

$$\begin{aligned} B(V, \mathfrak{m}) &:= \prod_j \ell_j^{4dr_j(\nu_j \delta + \alpha_j)}, \text{ and} \\ \mathcal{L}(V, \mathfrak{m}) &:= \text{ the product of the } \ell_j \text{ and any other primes dividing } N. \end{aligned} \tag{1.1}$$

Our main result is the following.

Theorem 1.1. *Let V be a Hecke-invariant subspace of $M_k(N,\chi)$, let F be a number field, and let $\mathfrak{m}$ be an ideal of $\mathcal{O}_F$ of norm m. With notation as above, set $B = B(V,\mathfrak{m})$ and $\mathcal{L} = \mathcal{L}(V,\mathfrak{m})$. There is an absolute, effectively computable constant A_1 (defined in* [LMO]*) such that for some prime $p \equiv -1 \pmod{Nm}$ satisfying*

$$p \leq 2\mathcal{L}^{A_1(B-1)}B^{A_1 B}, \tag{1.2}$$

we have $f(z) \mid T_p \equiv 0 \pmod{\mathfrak{m}}$ for all $f \in V \cap F[[q]]$ whose coefficients are λ-integral for each prime λ of $\mathcal{O}_F$ dividing $\mathfrak{m}$. Assuming the Generalized Riemann Hypothesis, the same holds for some prime $p \equiv -1 \pmod{Nm}$ satisfying

$$p \leq 280B^2\left(\log B + \log \mathcal{L}\right)^2. \tag{1.3}$$

An extension of Theorem 1.1 to half-integral weight forms follows via the Shimura correspondence. Since the Shimura lift of a Hecke-invariant subspace $V \subset S_{\kappa+\frac{1}{2}}(4N,\chi)$ is a Hecke-invariant subspace of $S_{2\kappa}(2N,\chi^2)$, in fact a statement slightly stronger than Theorem 1.2 as stated holds. We will see an example of this in Section 4.2.

Theorem 1.2. *Let $\kappa \geq 1$ be an integer, and consider the space of cusp forms $S_{\kappa+\frac{1}{2}}(4N,\chi)$. Let $\mathfrak{m}$ be an ideal of a number ring $\mathcal{O}_F$ of norm m. If $B = B(V,\mathfrak{m})$ and $\mathcal{L} = \mathcal{L}(V,\mathfrak{m})$ are defined by* (1.1)*, where $V = S_{2\kappa}(2N,\chi^2)$, then for some prime $p \equiv -1 \pmod{2Nm}$ satisfying the bound* (1.2) *we have $f(z) \mid T_{p^2} \equiv 0 \pmod{\mathfrak{m}}$ for all $f \in S_{\kappa+\frac{1}{2}}(4N,\chi) \cap F[[q]]$ whose Fourier coefficients are λ-integral for each prime λ of F dividing $\mathfrak{m}$. Under GRH, the same holds for some prime $p \equiv -1 \pmod{2Nm}$ satisfying the bound* (1.3)*.*

Remarks. (1) The data which contribute to the explicit bounds in Theorems 1.1 and 1.2 are not necessarily easy to compute. While the quantities d, δ and s are elementary to calculate (cf. e.g. [O1]), the quantities μ_j, ν_j and r_j can be difficult to compute for spaces of forms of large weight or level.

(2) Theorem 1.1 is essentially a statement about the odd Galois representations mentioned above, and not about modular forms *per se*. Nowhere does modularity enter into the proof except in providing these representations. We have stated the result in the guise above because the coefficients of modular forms provide a wealth of arithmetically interesting sequences arising as traces of such representations. But odd Galois representations arise elsewhere in number theory as well, and the same methods produce similar results in these cases. For example the following fact can be proved in the same manner as Theorem 1.1. Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, and let ℓ be any prime. Define quantities $B = B(\ell) := (\ell^2-1)(\ell^2-\ell) = \#\,\mathrm{GL}_2(\mathbb{F}_\ell)$ and $\mathcal{L} = \mathcal{L}(\ell,N) = \prod p$, the product of all primes p dividing $N\ell$. A positive density of primes $Q \equiv -1 \pmod{N\ell}$ have the property that $E(\mathbb{F}_Q)$ has nontrivial ℓ-torsion. Moreover, the first such Q satisfies (1.2), and under GRH it satisfies (1.3).

One application of Theorem 1.1 is to the coefficients of the modular j-function

$$j(z) = \sum c(n)q^n := \frac{E_4(z)^3}{\Delta(z)} = q^{-1} + 744 + 196884q + \cdots.$$

Here $E_4(z)$ is the classical Eisenstein series of weight 4. Note that $j(z)$ is not a modular form, since it has a simple pole at infinity. Nevertheless, it is possible to

deduce the following from Theorem 1.1. Recall that U_ℓ is the operator on formal power series sending $\sum a(n)q^n$ to $\sum a(\ell n)q^n$.

Corollary 1.3. *Let $\ell \geq 13$ be a prime number. A positive density of primes p satisfy $(j(z) \mid U_\ell) \mid T_p \equiv 0 \pmod{\ell}$. If $B = B(M_{\ell-1}, \ell\mathbb{Z})$ and $\mathcal{L} = \mathcal{L}(M_{\ell-1}, \ell\mathbb{Z}) = \ell$ are defined by* (1.1)*, then the first such p satisfies* (1.2)*, and under GRH it satisfies* (1.3)*.*

Corollary 1.4. *If ℓ is a prime number and $\alpha \geq 1$ is an integer, then a positive density of primes p satisfy*

$$\left(\sum_{n \equiv 0 \pmod{\ell}} c(n)q^n + 2 \sum_{(\frac{-n}{\ell})=-1} c(n)q^n \right) \mid T_p \equiv 0 \pmod{\ell^\alpha}. \tag{1.4}$$

Let

$$V_{\ell,\alpha} := \begin{cases} M_{\frac{(\ell-1)^2}{2}}, & \alpha = 1, \\ M_{\ell^{\alpha-1}(\ell-1)+\frac{\ell^{2\alpha-2}(\ell-1)^2}{2}}, & \alpha > 1. \end{cases}$$

If $B = B(V_{\ell,\alpha}, \ell^\alpha\mathbb{Z})$ and $\mathcal{L} = \mathcal{L}(V_{\ell,\alpha}, \ell^\alpha\mathbb{Z}) = \ell$ are defined by (1.1)*, then the first p such that* (1.4) *holds satisfies the bound* (1.2)*. Under GRH, the first such p satisfies* (1.3)*.*

Remark. Serre showed [S1] that for $2 < \ell \leq 11$, $j(z)|U_\ell \equiv 744 \pmod{\ell}$, which is why these cases are excluded. Elkies, Ono and Yang [EOY] have generalized Serre's result to weakly holomorphic modular forms $F(j(z))$, where $F(x) \in \mathbb{Z}[x]$. For these forms, $F(j(z)) \mid U_\ell$ is constant $\pmod{\ell}$ for small ℓ, and for larger ℓ, $F(j(z)) \mid U_\ell$ is congruent $\pmod{\ell}$ to a genuine modular form of bounded weight. It is thus possible to obtain generalizations of Corollary 1.3 for generic $F(j(z))$.

As an application of Theorem 1.2, we obtain a lower bound on the proportion of integers n such that the partition function $p(n)$ vanishes modulo a power of a prime $\ell \geq 5$; this answers a question of Ono [AO].

Corollary 1.5. *If $\ell \geq 5$ is prime and $\alpha \geq 1$ is an integer, then for any $\epsilon > 0$, for sufficiently large X we have*

$$\frac{\#\{0 \leq n \leq X : p(n) \equiv 0 \pmod{\ell^\alpha}\}}{X} \geq (1-\epsilon)C(\ell,\alpha)^{-1},$$

for a constant $C(\ell, \alpha) > 0$. Set

$$\kappa = \kappa(\ell,\alpha) = \begin{cases} \frac{\ell^{\alpha-1}(\ell-1)}{2} - 1, & \alpha \text{ is odd}, \\ \ell^\alpha(\ell-1) - 1, & \alpha \text{ is even}, \end{cases}$$

and let $V_{\ell,\alpha} = S_{2\kappa}(288)$. If $B = B(V_{\ell,\alpha}, \ell^\alpha\mathbb{Z})$ and $\mathcal{L} = \mathcal{L}(V_{\ell,\alpha}, \ell^\alpha\mathbb{Z}) = 6\ell$ are defined by (1.1)*, then $C(\ell,\alpha) \leq \frac{5}{4}\ell^\alpha p^3$ for some prime p satisfying the bound* (1.2)*, and under GRH for some p satisfying* (1.3)*.*

Remark. Using the Chinese Remainder Theorem, it is not difficult to extend this result to obtain an explicit lower bound for the proportion of integers n such that $p(n)$ vanishes modulo *any* composite number M coprime to 6.

Example 1.6. As an illustration of the quality of the bounds produced using Corollary 1.5 and the discussion on Hecke-invariant subspaces immediately following Theorem 1.1, we consider the problem of finding congruences for $p(n)$ modulo 13.

Assuming GRH, and using considerations to be addressed in Section 4.2 (where this example will be discussed in more detail), we can obtain a bound of about 4.06×10^{13}, for the first prime Q such that there is a congruence of the form $p(13Q^3n + \beta) \equiv 0 \pmod{13}$. The corresponding lower bound $C(13, 1)^{-1}$ for the proportion of n such that $p(n) \equiv 0 \pmod{13}$ is about 10^{-42}. However, note that Atkin [At] found the congruence

$$p(11^3 \cdot 13n + 237) \equiv 0 \pmod{13},$$

so the actual proportion is at least $\frac{1}{11 \cdot 13^3} = 17303^{-1}$.

In Section 2 we give some preliminaries for the proofs of Theorems 1.1 and 1.2. Section 3 contains those proofs. In Section 4 we prove Corollaries 1.3 through 1.5.

2. Preliminaries for the proofs of Theorems 1.1 and 1.2

Assume the notation and hypotheses from Section 1. Recall that $\{f_i(tz) : t|\frac{N}{M_i}\}$ contains a basis for V, where M_i denotes the level of f_i.

Lemma 2.1. *Suppose that $f(z) \in V \cap F[[q]]$ has λ_j-integral coefficients and that*

$$f(z) = \sum a(n)q^n = \sum \alpha_{i,t} f_i(tz)$$

is the decomposition of $f(z)$ with respect to the $f_i(tz)$. Then each $\nu_{\mu_j}(\alpha_{i,t}) \geq -\delta\nu_j$.

Proof. Define the coefficients $a_{i,t}(m)$ by $f_i(tz) = \sum a_i(n)q^{tn} =: \sum a_{i,t}(m)q^m$. For notational convenience, let $\lambda = \lambda_j, \mu = \mu_j, \nu = \nu_j$, and denote the field KF by E. Write $\mathcal{O}_\mu$ for the localization of $\mathcal{O}_E$ at μ. By a theorem of Sturm [St], if the first s coefficients of a form in $M_k(N, \chi) \cap E[[q]]$ are μ-integral, then the form is in fact in $M_k(N, \chi) \cap \mathcal{O}_\mu[[q]]$. Thus there is an injective map φ from the free, rank δ $\mathcal{O}_\mu$-module $M_k(N, \chi) \cap \mathcal{O}_\mu[[q]]$ into $\mathcal{O}_\mu^s$ which sends a form to the vector consisting of its first s Fourier coefficients.

By the theory of the Smith normal form, there is an $\mathcal{O}_\mu$-basis $g_1, \ldots, g_\delta$ for $M_k(N, \chi) \cap \mathcal{O}_\mu[[q]]$ and an isomorphism $\psi : \mathcal{O}_\mu^s \to \mathcal{O}_\mu^s$ such that the composition $\psi \circ \varphi$ is diagonal with respect to the basis g_i. If an elementary divisor lies in the maximal ideal μ of $\mathcal{O}_\mu$, then all of the first s coefficients of the corresponding basis element g_i lie in μ as well. If π is a uniformizer for $\mathcal{O}_\mu$, this implies (by Sturm's theorem again) that $\pi^{-1}g_i \in M_k(N, \chi) \cap \mathcal{O}_\mu[[q]]$, which is a contradiction. Consequently, the elementary divisors are in $\mathcal{O}_\mu^\times$. Writing $g_i(z) = \sum \gamma_i(n)q^n$, it follows that for some choice of δ indices $0 \leq n_1, \ldots, n_\delta < s$, the matrix $G = (\gamma_i(n_j)) \in \mathrm{Mat}_\delta(\mathcal{O}_\mu)$ is nonsingular over $\mathcal{O}_\mu$.

Let A be the matrix with entries $a_{i,t}(n_j)$, where i and t range through the δ possibilities in an arbitrary but fixed order. Similarly, write $f_{i,t} = \sum \beta_{i,t,j} g_j$ and let B be the matrix with entries $\beta_{i,t,j}$. Examining the n_lth coefficient of $f_{i,t}$, we have $a_{i,t}(n_l) = \sum \beta_{i,t,j}\gamma_j(n_l)$, yielding an equality $A = BG$. Taking valuations at μ, we find $\nu_\mu(\det B) = \nu_\mu(\det A) \leq \delta\nu$. Since $f = \sum \alpha_{i,t} f_{i,t} = \sum \alpha_{i,t}\beta_{i,t,j} g_j$ has coefficients in $\mathcal{O}_\mu$, each sum $\sum \alpha_{i,t}\beta_{i,t,j} \in \mathcal{O}_\mu$. So by Cramer's rule, each $\alpha_{i,t} \in \det B^{-1}\mathcal{O}_\mu$, whence $\nu_\mu(\alpha_{i,t}) \geq -\delta\nu$. □

We next turn to effective forms of the Chebotarev Density Theorem.

Theorem 2.2 (Lagarias, Montgomery, Odlyzko [LMO]). *Let L/K be a finite Galois extension of number fields, and d_L the absolute value of the discriminant of L. Let C be a conjugacy class of $\mathrm{Gal}(L/K)$. There is a prime ideal $\mathfrak{p}$ of K such that the conjugacy class $\left(\frac{L/K}{\mathfrak{p}}\right) = C$, and such that $N_{K/\mathbb{Q}}\mathfrak{p}$ satisfies the following bounds:*

(a) *There is an absolute, effectively computable constant A_1 such that*
$$N_{K/\mathbb{Q}}\mathfrak{p} \leq 2d_L^{A_1}.$$
(b) *Under GRH, there is an absolute, effectively computable constant b such that*
$$N_{K/\mathbb{Q}}\mathfrak{p} \leq b(\log d_L)^2.$$

By work of Oesterlé [Oe], one may take $b = 70$. We will be interested in the case where $K = \mathbb{Q}$ and $L/\mathbb{Q}$ is a Galois extension of bounded degree n. Combining Theorem 2.2 with a discriminant bound [S2, §1.4, Prop. 6], Serre deduces the following bound.

Proposition 2.3 ([S2], §2.5, Théorème 6). *Let $L/\mathbb{Q}$ be a Galois extension of finite degree n, and S a set of prime numbers such that $L/\mathbb{Q}$ is unramified outside of S. Under GRH, for each conjugacy class C in $\mathrm{Gal}(L/\mathbb{Q})$, there exists a prime number $p \notin S$ such that the frobenius at p is in C, and such that*
$$p \leq 280n^2(\log n + \sum_{q\in S} \log q)^2.$$

3. Proofs of Theorems 1.1 and 1.2

Proof of Theorem 1.1. Recall the notation in the statement of Theorem 1.1. For each prime λ_j, and each newform f_i, let $\rho_{i,j} := \rho_{f_i,\lambda_j}$ be the corresponding odd, continuous, semisimple μ_j-adic Galois representation $\rho_{i,j} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\widehat{\mathcal{O}}_j)$, where $\widehat{\mathcal{O}}_j$ denotes the μ_j-adic completion of $\mathcal{O}_{KF}$. Composing with the natural projection $\mathrm{GL}_2(\widehat{\mathcal{O}}_j) \to \mathrm{GL}_2(\mathcal{O}_{KF}/\mu_j^{\nu_j\delta+\alpha_j})$, we obtain a reduced representation
$$\overline{\rho}_{i,j} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_{KF}/\mu_j^{\nu_j\delta+\alpha_j}),$$
such that for any $p \nmid N\ell_j$ and any frobenius element Frob_p,
$$\mathrm{tr}\,\overline{\rho}_{i,j}(\mathrm{Frob}_p) \equiv a_i(p) \pmod{\mu_j^{\nu_j\delta+\alpha_j}}. \tag{3.1}$$
Consider the direct sum
$$\overline{\rho} := \bigoplus_{i,j} \overline{\rho}_{i,j} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \bigoplus_{i,j} \mathrm{GL}_2(\mathcal{O}_{KF}/\mu_j^{\nu_j\delta+\alpha_j}).$$
Let $L/\mathbb{Q}$ be the Galois extension cut out by $\overline{\rho}$, which is unramified outside of $N\mathcal{L}$. Using the elementary bound $\#\,\mathrm{GL}_2(\mathcal{O}_{KF}/\mu_j^{\nu_j\delta+\alpha_j}) \leq \ell_j^{4r_j(\nu_j\delta+\alpha_j)}$, we obtain the bound
$$[L:\mathbb{Q}] \leq \prod_j \ell_j^{4dr_j(\nu_j\delta+\alpha_j)} = B(V,\mathfrak{m}). \tag{3.2}$$
Now fix an embedding $L \hookrightarrow \mathbb{C}$ and the element $c \in \mathrm{Gal}(L/\mathbb{Q})$ corresponding to complex conjugation. Since each $\overline{\rho}_{i,j}$ is odd, we have $\det\overline{\rho}_{i,j}(c) \equiv -1 \pmod{\mu_j^{\nu_j\delta+\alpha_j}}$. Because $c^2 = \mathrm{id}$ and $\overline{\rho}_{i,j}(c)$ satisfies its own characteristic polynomial, this implies that $\mathrm{tr}\,\overline{\rho}_{i,j}(c) = 0$ for each i,j. Therefore if Frob_p is in the conjugacy class C of

$\mathrm{Gal}(L/\mathbb{Q})$ containing c, then by (3.1) we have $a_i(p) \equiv 0 \pmod{\mu_j^{\nu_j\delta+\alpha_j}}$, for each i, j. Consequently,

$$f_i(tz) \mid T_p \equiv 0 \pmod{\mu_j^{\nu_j\delta+\alpha_j}} \tag{3.3}$$

for each i and j, and each $t|\frac{N}{M_i}$. Moreover, since Frob_p acts as conjugation (i.e. inversion) on the Nth and ℓ_jth power roots of unity in $\overline{\mathbb{Q}}$, we must have $p \equiv -1 \pmod{Nm}$.

Now suppose $f(z) = \sum a(n)q^n$ is any element of $M_k(N,\chi)$ with coefficients in KF which are μ_j-integral for each j. Writing

$$f(z) = \sum_{i,t} c_{i,t} f_i(tz),$$

Lemma 2.1 implies that each $\nu_{\mu_j}(c_{i,t}) \geq -\nu_j\delta$. By linearity, this along with (3.3) entails that $f(z) \mid T_p \equiv 0 \pmod{\mu_j^{\alpha_j}}$ for each j. In particular, if f has coefficients in F which are λ_j-integral for each j, then $f(z) \mid T_p \equiv 0 \pmod{\mathfrak{m}}$. Thus, the theorem follows from (3.2) by applying Proposition 2.3 (resp. Theorem 2.2(a) and [S2, §1.4 Prop. 6]) to the extension $L/\mathbb{Q}$, to obtain the conditional (resp. unconditional) bound on p. □

The proof of Theorem 1.2 uses Shimura's correspondence between half-integral and integral weight modular forms, which we now recall. Suppose that $g(z) = \sum b(n)q^n \in M_{\kappa+\frac{1}{2}}(4N,\chi)$ is a half-integral weight modular form with $\kappa \geq 1$. Let t be a positive square-free integer, and define the Dirichlet character ψ_t by $\psi_t(n) = \chi(n)\left(\frac{-1}{n}\right)^{\kappa}\left(\frac{t}{n}\right)$. If a sequence $A_t(n)$ is defined by

$$\sum \frac{A_t(n)}{n^s} := L(s-\kappa+1,\psi_t) \cdot \sum \frac{b(tn^2)}{n^s},$$

then $S_{t,\kappa}(g(z)) := \sum A_t(n)q^n$ is a weight 2κ modular form in $M_{2\lambda}(2N,\chi^2)$. In particular, the Shimura correspondence commutes with Hecke operators:

$$S_{t,\kappa}(g(z) \mid T_{p^2}) = S_{t,\kappa}(g(z))|T_p.$$

Proof of Theorem 1.2. Let notation be as in the statement of Theorem 1.2, and apply Theorem 1.1 to the space $V = S_{2\kappa}(2N,\chi^2)$ and the ideal $\pmod{\mathfrak{m}}$. For some p satisfying the bounds (1.2) and (1.3) we have $g(z) \mid T_p \equiv 0 \pmod{\mathfrak{m}}$ for all $g(z) \in V \cap F[[q]]$ which can be reduced $\pmod{\mathfrak{m}}$. If $f(z) \in S_{\kappa+\frac{1}{2}}(N,\chi) \cap F[[q]]$ can be reduced $\pmod{\mathfrak{m}}$, then $0 \equiv S_{t,\kappa}(f(z)) \mid T_p = S_{t,\kappa}(f(z) \mid T_{p^2}) \pmod{\mathfrak{m}}$ for every square-free t. By the definition of the Shimura lift $S_{t,\kappa}(f(z) \mid T_{p^2})$, this implies $f(z) \mid T_{p^2} \equiv 0 \pmod{\mathfrak{m}}$. □

4. Proofs of corollaries

4.1. **Proof of Corollaries 1.3 and 1.4.** Here we examine the Fourier coefficients $c(n)$ of the j-function. The only obstacle to applying Theorem 1.1 directly is that $j(z)$ is not a modular form. However, we have the following fact.

Proposition 4.1 (Serre, [S1], §§6.15-16)**.** *For any prime ℓ, the following hold:*

(a) *There is a modular form $f_\ell(z) \in M_{\ell-1}$ with ℓ-integral coefficients such that*

$$j(z) \mid U_\ell \equiv f_\ell(z) \pmod{\ell}.$$

(b) *There is a modular form* $g_\ell(z) \in M_{\frac{(\ell-1)^2}{2}}$ *such that*

$$\sum_{n\equiv 0 \pmod{\ell}} c(n)q^n + 2\sum_{\left(\frac{-n}{\ell}\right)=-1} c(n)q^n \equiv g_\ell(z) \pmod{\ell}.$$

(c) *For any* $\alpha \geq 1$ *there are modular forms* $h_{\ell,\alpha} \in M_{\ell^{\alpha-1}(\ell-1)+\frac{\ell^{2\alpha-2}(\ell-1)^2}{2}}$ *such that*

$$\sum_{n\equiv 0 \pmod{\ell}} c(n)q^n + 2\sum_{\left(\frac{-n}{\ell}\right)=-1} c(n)q^n \equiv h_{\ell,\alpha}(z) \pmod{\ell^\alpha}.$$

Applying Theorem 1.1 to the space $V = M_k$, Corollaries 1.3 and 1.4 follow from Proposition 4.1.[1]

4.2. **Proof of Corollary 1.5.** We now turn to the subject of the partition function $p(n)$. Let χ_{12} denote the quadratic character $\left(\frac{12}{\bullet}\right)$. Recall the Dedekind eta function

$$\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n).$$

It is well known (cf. e.g. [O1, Cor. 1.62]) that $\eta(24z) \in S_{\frac{1}{2}}(576, \chi_{12})$.

Proposition 4.2 (Ahlgren-Boylan [AB])**.** *If* $\ell \geq 5$ *is prime and* α *is a positive integer, let* $1 \leq \beta = \beta(\ell,\alpha) \leq \ell^\alpha - 1$ *denote the unique integer such that* $24\beta \equiv 1 \pmod{\ell^\alpha}$*. Define an even integer* $k = k(\ell,\alpha)$ *by*

(4.1)
$$k := \begin{cases} \frac{\ell^{\alpha-1}(\ell-1)}{2} - \frac{1}{2}\left(\frac{24\beta-1}{\ell^\alpha}+1\right) = \frac{(\ell^{\alpha-1}+1)(\ell-1)}{2} - 12(\lfloor \ell/24 \rfloor + 1), & \alpha \text{ odd}, \\ \ell^{\alpha-1}(\ell-1) - \frac{1}{2}\left(\frac{24\beta-1}{\ell^\alpha}+1\right) = \ell^{\alpha-1}(\ell-1) - 12, & \alpha \text{ even}. \end{cases}$$

Then there exists a modular form $F(z) \in M_k \cap \mathbb{Z}[[q]]$ *such that*

$$\sum_{n=0}^{\infty} p(\ell^\alpha n + \beta)q^{24n+\frac{24\beta-1}{\ell^\alpha}} \equiv \eta(24z)^{\frac{24\beta-1}{\ell^\alpha}}F(24z)$$
$$=: G_{\ell,\alpha}(z) \in S_{k+\frac{24\beta-1}{2\ell^\alpha}}(576,\chi_{12}) \pmod{\ell^\alpha}.$$

Recall the notation from the statement of Corollary 1.5, and observe from (4.1) that $\kappa + \frac{1}{2} = \kappa(\ell,\alpha) + \frac{1}{2} = k + \frac{24\beta-1}{2\ell^\alpha}$ is the weight of the modular form $G(z) = G_{\ell,\alpha}(z)$ defined by Proposition 4.2.

Proof of Corollary 1.5. We will show using Proposition 4.2 and arguments of Ono and Ahlgren-Boylan [O2, AB] that if $G_{\ell,\alpha}(z) \mid T_{Q^2} \equiv 0 \pmod{\ell^\alpha}$ and $Q \equiv -1 \pmod{24\ell}$, then there is an integer β' such that $p(Q^3\ell^\alpha n + \beta') \equiv 0 \pmod{\ell^\alpha}$ for integers n in any of $Q-1$ of the residue classes $\pmod{Q}$. Since $\frac{Q-1}{Q} \geq \frac{4}{5}$, Corollary 1.5 follows easily from this fact by Theorem 1.2.

We can rewrite the statement of Proposition 4.2 as

$$\sum_{n\equiv\frac{24\beta-1}{\ell^\alpha} \pmod{24}} p\left(\frac{\ell^\alpha n+1}{24}\right)q^n \equiv G(z) \pmod{\ell^\alpha}. \tag{4.2}$$

[1]The referee points out that the bounds may be improved slightly using the fact that it is easy to establish when $E_k|T_p \equiv 0 \pmod{\ell}$. For example, in the setting of Corollary 1.3 it actually suffices to take $V = S_k$, since for $p \equiv -1 \pmod{\ell}$ one automatically has $E_{\ell-1}|T_p = \sigma_{\ell-2}(p)E_{\ell-1} \equiv 0 \pmod{\ell}$.

If $(n, Q) = 1, Q^3 n \equiv \frac{24\beta - 1}{\ell^\alpha} \pmod{24}$, and $G(z) \mid T_{Q^2} \equiv 0 \pmod{\ell^\alpha}$, then (4.2) and the definition of the action of half-integral weight Hecke operators on power series give

$$p\left(\frac{Q^3 \ell^\alpha n + 1}{24}\right) \equiv 0 \pmod{\ell^\alpha}. \tag{4.3}$$

Since $Q \equiv -1 \pmod{24\ell}$ we have $Q^2 \equiv 1 \pmod{24}$, so defining $r = r(\ell, \alpha) := \frac{1 - 24\beta}{\ell^\alpha}$, we have $Q^3 n \equiv \frac{24\beta - 1}{\ell^\alpha} \pmod{24}$ if and only if $n \equiv r \pmod{24}$. Replace n by $\frac{n-r}{24}$, and observe that $(r + 24n, Q) = 1$ provided $n \not\equiv -\frac{r}{24} \pmod{Q}$. Hence, setting $\beta' = \frac{Q^3+1}{24} - \beta$, (4.3) implies that $p(Q^3 \ell^\alpha n + \beta') \equiv 0 \pmod{\ell^\alpha}$ for n in any of the $Q - 1$ allowable residue classes $\pmod{Q}$. □

Example 4.3. We now revisit Example 1.6 above (congruences for $p(n)$ modulo $\ell^\alpha = 13$) in more detail. The bounds produced by a naïve, direct application of Corollary 1.5 are astronomical. To improve upon these, we make use of the discussion following Theorem 1.1. Recalling the notation of the proof of Corollary 1.5, the fact that $k(13, 1) = 0$ implies that $G_{13,1}(z) = \eta(24z)^{11}$. In fact, $\eta(24z)^{11}$ is a Hecke eigenform, so we may restrict our attention to a one-dimensional subspace of the 408-dimensional space $S_{\frac{11}{2}}(576, \chi_{12})$.

By examining the first few Fourier coefficients, it is possible to check that the Shimura lift $G^*_{13,1}(z)$ of $G_{13,1}(z)$ is a quadratic twist of the unique newform in $S_{10}(6)$ [GO, Prop. 6]. Since the coefficients of the newform in $S_{10}(6)$ are 13-integral rational numbers, so are the coefficients of $G^*_{13,1}$. Setting V to be the one-dimensional span of $G^*_{13,1}$, it is straightforward to compute from (1.1) that $B(V, 13) = 13^4$. In fact, we can do slightly better than this since the proof of Theorem 1.1 used the approximation $\#\,\mathrm{GL}_2(\mathbb{F}_{13}) \le 13^4$, when in fact $\#\,\mathrm{GL}_2(\mathbb{F}_{13}) = (13^2-1)(13^2-13) = 26208$. So we can take this value for B, and (1.3) remains valid. The resulting bound on the first prime Q such that $G_{13,1}(z) \mid T_{Q^2} \equiv 0 \pmod{13}$ is about 4.06×10^{13}, and the corresponding lower bound on the proportion of integers n such that $p(n) \equiv 0 \pmod{13}$ is about 9.19×10^{-43}.

Acknowledgments

The author is very grateful to Ken Ono for his invaluable assistance with every aspect of this project and to the anonymous referee for many helpful suggestions.

References

[AB] S. Ahlgren and M. Boylan, *Arithmetic properties of the partition function*, Invent. Math. (3) **153** (2003), 487-502. MR2000466 (2004e:11115)

[AO] 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, Contemp. Math. **291**, Amer. Math. Soc., Providence, RI, 2001, 1-10. MR1874518 (2002j:11120)

[At] A. O. L. Atkin, *Multiplicative congruence properties and density problems for $p(n)$*, Proc. London Math. Soc. (3) **18** (1968), 563-576. MR0227105 (37:2690)

[EOY] N.D. Elkies, K. Ono, and T. Yang, *Reduction of CM elliptic curves and modular function congruences*, Int. Math. Res. Not. **44** (2005), 2695-2707. MR2181309 (2006k:11076)

[GO] L. Guo and K. Ono, *The partition function and the arithmetic of certain modular L-functions*, Int. Math. Res. Not. 21 (1999), 1179-1197. MR1728677 (2000m:11102)

[LMO] J.C. Lagarias, H.L. Montgomery and A.M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. (3) **54** (1979), 271-296. MR553223 (81b:12013)

[Oe] J. Oesterlé, Versions effectives du théorème de Chebotarev sous l'hypothése de Riemann généralisée, *Astérisque* **61** (1979), 165-167.

[O1] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, CBMS **102**, American Math. Soc., 2004. MR2020489 (2005c:11053)

[O2] K. Ono, *Distribution of the partition function modulo m*, Ann. of Math. **151** (2000), 293-307. MR1745012 (2000k:11115)

[OSk] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo ℓ*, Ann. Math. (2) **147** (1998), 453-470. MR1626761 (99f:11059a)

[S1] J-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Enseignement Math. **22** (1976), 227-260. MR0434996 (55:7958)

[S2] J-P. Serre, *Quelque applications du théorème de densité de Chebotarev*, Publ. Math. IHES no. 54 (1981), 323-401. MR644559 (83k:12011)

[St] J. Sturm, *On the congruence of modular forms*, Lect. Notes in Math. **1240**, Springer, Berlin, 1987, 275-280. MR894516 (88h:11031)

[SwD] H.P.F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms*, Lect. Notes in Math. **350**, Springer, Berlin, 1973, 1-55. MR0406931 (53:10717a)

286 Adams House Mail Center, Harvard University, Cambridge, Massachusetts 02138
E-mail address: sflicht@fas.harvard.edu