THE EFFECTIVE CHEBOTAREV DENSITY THEOREM
AND MODULAR FORMS MODULO 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 $O_K$ of a number field $K$. For any ideal $m \subset O_K$, we bound the first prime $p$ for which $f \mid T_p$ (resp. $g \mid T_{p^2}$) is zero (mod $m$). Applications include the solution to a question of Ono (2001) concerning partitions.

1. Introduction and statement of results

The existence of $\ell$-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

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

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

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

$$\rho_{\lambda,f} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(O_{\lambda})$$

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

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

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. $E_k(N,\chi)$] to denote the space of modular forms [resp. cusp
forms, resp. Eisenstein series] of weight $k$, level $N$, and Nebentypus $\chi$. We omit $\chi$ from the notation when it is trivial, and $N$ when it is 1.)

**Theorem** (Serre, [11], §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 $f(z) \mid T_p \equiv 0 \pmod{m}$ for every $f(z) \in M_k(N, \chi)$ with coefficients in $\mathcal{O}_K$.

Remark. Similarly, a positive density of primes satisfies $f(z) \mid T_p \equiv 2f(z) \pmod{m}$, and likewise for any other eigenvalue $\lambda \neq 0, 2 \pmod{m}$ which occurs.

As observed by Ono [12], Shimura’s correspondence can be used to extend Serre’s theorem to forms $f$ of half-integral weight $\kappa + \tfrac{1}{2} \geq \tfrac{1}{2}$, and the result is trivial if $\kappa + \tfrac{1}{2} = \tfrac{1}{2}$ by the Serre-Stark basis theorem. In these cases the theorem says that a positive density of primes $p \equiv -1 \pmod{NM}$ satisfy $f(z) \mid \Delta(z)$, and likewise for any other eigenvalue $\kappa$.

Serre’s theorem and its extension to half-integral weight hold for all modular forms, not just eigenforms. However, for a generic modular form $f$, the first prime $p$ such that $f(z) \mid T_p \equiv 0 \pmod{m}$ 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 $\mathbb{C}$.)

- $\delta = \delta(V) := \dim(V)$.
- $d = d(V) := \dim(\mathcal{E}_k(N, \chi) \cap V) + \sum \dim(S_{k,\new}^M(M, \chi))$, summing over all $M|N$ such that $f(tz) \in V$ for some $t \frac{N}{M}$ and some nonzero element $f(z) \in S_{k,\new}^M(M, \chi)$.
- $s = s(V) := \frac{k}{2} N \prod (1 + p^{-1})$, the product taken over primes $p|N$.
- A basis $f_1, \ldots, f_d$ of Hecke eigenforms for $(\mathcal{E}_k(N, \chi) \cap V) \oplus \bigoplus S_{k,\new}^M(M, \chi)$, 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 $\chi$ lie in $\mathcal{O}_K$. Let $K = K(V) := K_1K_2 \cdots K_d$ 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 $\mathfrak{m} = \prod \lambda_j^{\nu_j}$, where $\lambda_j$ has residue characteristic $\ell_j$. For each $j$, $V$ and $\mathfrak{m}$ determine further data:

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

Finally, using these data we define quantities

\[
B(V, \mathfrak{m}) := \prod_j \ell_j^{\nu_j\delta + \nu_j}, \text{ and}
\]

\[
(1.1) \quad \mathcal{L}(V, \mathfrak{m}) := \text{the product of the } \ell_j \text{ and any other primes dividing } N.
\]
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 $O_F$ of norm $m$. With notation as above, set $B = B(V, \mathfrak{m})$ and $L = L(V, \mathfrak{m})$. There is an absolute, effectively computable constant $A_1$ (defined in [LMO]) such that for some prime $p \equiv -1 \pmod{Nm}$ satisfying
\begin{equation}
  p \leq 2L^{A_1(B^{-1})}B^{A_1B},
\end{equation}
we have $f(z) | T_p \equiv 0 \pmod{m}$ for all $f \in V \cap F[[q]]$ whose coefficients are $p$-integral for each prime $p$ of $F$ dividing $\mathfrak{m}$. Assuming the Generalized Riemann Hypothesis, the same holds for some prime $p \equiv -1 \pmod{Nm}$ satisfying
\begin{equation}
  p \leq 280B^2(\log B + \log L)^2.
\end{equation}

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 $V \subset S_{k+\frac{1}{2}}(4N, \chi)$ is a Hecke-invariant subspace of $S_{2k}(2N, \chi^2)$, 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 $O_F$ of norm $m$. If $B = B(V, \mathfrak{m})$ and $L = L(V, \mathfrak{m})$ are defined by (1.1), where $V = S_{2k}(2N, \chi^2)$, then for some prime $p \equiv -1 \pmod{2Nm}$ satisfying the bound (1.2) we have $f(z) | T_p \equiv 0 \pmod{m}$ for all $f \in S_{\kappa+\frac{1}{2}}(4N, \chi) \cap F[[q]]$ whose Fourier coefficients are $p$-integral for each prime $p$ 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 $d$, $\delta$ and $s$ are elementary to calculate (cf. e.g. [OI]), the quantities $\mu_j$, $\nu_j$ 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 $\ell$ be any prime. Define quantities $B = B(\ell) := (\ell^2 - 1)(\ell^2 - \ell) = \# \text{GL}_2(\mathbb{F}_\ell)$ and $L = L(\ell, N) = \prod p$, 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 $\ell$-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
\begin{equation}
  j(z) = \sum c(n)q^n := \frac{E_4(z)^3}{\Delta(z)} = q^{-1} + 744 + 196884q + \cdots.
\end{equation}
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 $\sum a(ℓn)q^n$.

**Corollary 1.3.** Let $ℓ ≥ 13$ be a prime number. A positive density of primes $p$ satisfy $(j(z)|U_ℓ) | T_p \equiv 0 \pmod{ℓ}$. If $B = B(M_ℓ−1, ℓZ)$ and $L = L(M_ℓ−1, ℓZ) = ℓ$ 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 $α ≥ 1$ is an integer, then a positive density of primes $p$ satisfy

$$\left(\sum_{n=0}^{∞} c(n)q^n + 2\sum_{\left(\frac{q}{ℓ}\right) = -1} c(n)q^n\right) \mid T_p \equiv 0 \pmod{ℓ^α}.$$  

Let

$$V_{ℓ,α} := \begin{cases} M_{ℓ−1/2}, & α = 1, \\
M_{ℓ−1(ℓ−1)/2}^{2α−2(ℓ−1)/2}, & α > 1. \end{cases}$$

If $B = B(V_{ℓ,α}, ℓ^αZ)$ and $L = L(V_{ℓ,α}, ℓ^αZ) = ℓ$ are defined by (1.1), then the first such $p$ 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 $2 < ℓ ≤ 11$, $j(z)|U_ℓ \equiv 744 \pmod{ℓ}$, 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 $F(x) ∈ ℤ[x]$. For these forms, $F(j(z))|U_ℓ$ is constant (mod $ℓ$) for small $ℓ$, and for larger $ℓ$, $F(j(z))|U_ℓ$ is congruent (mod $ℓ$) 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 $ℓ ≥ 5$; this answers a question of Ono [AO].

**Corollary 1.5.** If $ℓ ≥ 5$ is prime and $α ≥ 1$ is an integer, then for any $c > 0$, for sufficiently large $X$ we have

$$\frac{\# \{0 ≤ n ≤ X : p(n) \equiv 0 \pmod{ℓ^α}\}}{X} ≥ (1−c)C(ℓ, α)^{-1},$$

for a constant $C(ℓ, α) > 0$. Set

$$κ = κ(ℓ, α) = \begin{cases} \frac{ℓα−1(ℓ−1)}{2} - 1, & α \text{ is odd}, \\
\frac{ℓα(ℓ−1)}{2} - 1, & α \text{ is even}, \end{cases}$$

and let $V_{ℓ,α} = S_{2κ}(288)$. If $B = B(V_{ℓ,α}, ℓ^αZ)$ and $L = L(V_{ℓ,α}, ℓ^αZ) = 6ℓ$ are defined by (1.1), then $C(ℓ, α) ≤ \frac{κ}{4}ℓ^αp^3$ 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 \(4.06 \times 10^{13}\), for the first prime \(Q\) such that there is a congruence of the form \(p(13Q^3 n + \beta) \equiv 0 \pmod{13}\). 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 \(1/14137 = 17303^{-1}\).

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 \(\{f_i(tz) : t \mid N\}_{\lambda_i}\) contains a basis for \(V\), where \(M_t\) denotes the level of \(f_i\).

**Lemma 2.1.** Suppose that \(f(z) \in V \cap \mathcal{F}[\mu]\) has \(\lambda_j\)-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 \(\nu_{\eta_j}(\alpha_{i,t}) \geq -\delta\nu_j\).

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

By the theory of the Smith normal form, there is an \(\mathcal{O}_\mu\)-basis \(g_1, \ldots, g_\delta\) for \(M_k(N,\chi) \cap \mathcal{O}_\mu[\mu]\) 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 \(\mu\) of \(\mathcal{O}_\mu\), then all of the first \(s\) coefficients of the corresponding basis element \(g_i\) lie in \(\mu\) as well. If \(\pi\) is a uniformizer for \(\mathcal{O}_\mu\), this implies (by Sturm’s theorem again) that \(\pi^{-1} g_i \in M_k(N,\chi) \cap \mathcal{O}_\mu[\mu]\), which is a contradiction. Consequently, the elementary divisors are in \(\mathcal{O}_\mu^s\). Writing \(g_i(z) = \sum \gamma_i(n)q^n\), it follows that for some choice of \(\delta\) indices \(0 \leq n_1, \ldots, n_\delta < s\), the matrix \(G = (\gamma_i(n_j)) \in \text{Mat}_s(\mathcal{O}_\mu)\) is nonsingular over \(\mathcal{O}_\mu\).

Let \(A\) be the matrix with entries \(a_{i,t}(n_i)\), where \(i\) and \(t\) range through the \(\delta\) 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 \(n_i\)th coefficient of \(f_{i,t}\), we have \(a_{i,t}(n_i) = \sum \beta_{i,t,j} \gamma_j(n_i)\), yielding an equality \(A = B\). Taking valuations at \(\mu\), we find \(\nu_\mu(\det B) = \nu_\mu(\det A) \leq \delta\nu\). Since \(f = \sum a_{i,t} f_{i,t} = \sum \alpha_{i,t} \beta_{i,t,j} g_j\) 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 \(\nu_\mu(\alpha_{i,t}) \geq -\delta\nu\). \(\square\)

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 $\text{Gal}(L/K)$. 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 $N_{K/Q}\mathfrak{p}$ satisfies the following bounds:

(a) There is an absolute, effectively computable constant $A_1$ such that

$$N_{K/Q}\mathfrak{p} \leq 2d_L^{A_1}.$$ 

(b) Under GRH, there is an absolute, effectively computable constant $b$ such that

$$N_{K/Q}\mathfrak{p} \leq b(d_L)^2.$$ 

By work of Oesterlé [Oc], 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 $\text{Gal}(L/\mathbb{Q})$, 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 [111] and [112]

Proof of Theorem 1.1. Recall the notation in the statement of Theorem 1.1. For each prime $\lambda_j$, and each newform $f$, let $\rho_{i,j} := \rho_{f_i,\lambda_j}$ be the corresponding odd, continuous, semisimple $\mu_j$-adic Galois representation $\rho_{i,j} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\hat{\mathbb{O}}_j)$, where $\hat{\mathbb{O}}_j$ denotes the $\mu_j$-adic completion of $\mathcal{O}_{K/F}$. Composing with the natural projection $\text{GL}_2(\hat{\mathbb{O}}_j) \to \text{GL}_2(\mathcal{O}_{K/F}/\mu_j^{\nu_j^{+\alpha_j}})$, we obtain a reduced representation

$$\overline{\rho}_{i,j} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathcal{O}_{K/F}/\mu_j^{\nu_j^{+\alpha_j}}),$$ 

such that for any $p \nmid N\ell_j$ and any Frobenius element $\text{Frob}_p$,

$$\text{tr} \overline{\rho}_{i,j}(\text{Frob}_p) \equiv a_i(p) \pmod{\mu_j^{\nu_j^{+\alpha_j}}}.$$ 

Consider the direct sum

$$\overline{\rho} := \bigoplus_{i,j} \overline{\rho}_{i,j} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \bigoplus_{i,j} \text{GL}_2(\mathcal{O}_{K/F}/\mu_j^{\nu_j^{+\alpha_j}}).$$ 

Let $L/\mathbb{Q}$ be the Galois extension cut out by $\overline{\rho}$, which is unramified outside of $NL$. Using the elementary bound $\# \text{GL}_2(\mathcal{O}_{K/F}/\mu_j^{\nu_j^{+\alpha_j}}) \leq \ell_{\nu_j^{+\alpha_j}}^{\nu_j^{+\alpha_j}}$, we obtain the bound

$$(3.2) \quad [L : \mathbb{Q}] \leq \prod_j \ell_{\nu_j^{+\alpha_j}}^{\nu_j^{+\alpha_j}} = B(V,m).$$ 

Now fix an embedding $L \hookrightarrow \mathbb{C}$ and the element $c \in \text{Gal}(L/\mathbb{Q})$ corresponding to complex conjugation. Since each $\overline{\rho}_{i,j}$ is odd, we have $\det \overline{\rho}_{i,j}(c) \equiv -1 \pmod{\mu_j^{\nu_j^{+\alpha_j}}}$. Because $c^2 = id$ and $\overline{\rho}_{i,j}(c)$ satisfies its own characteristic polynomial, this implies that $\text{tr} \overline{\rho}_{i,j}(c) = 0$ for each $i,j$. Therefore if $\text{Frob}_p$ is in the conjugacy class $C$ of
Gal(L/Q) containing c, then by (3.1) we have \(a_i(p) \equiv 0 \mod \mu_j^{\nu_j \delta + \alpha_i})\), for each \(i, j\). Consequently,

\[
f_i(z) | T_p \equiv 0 \mod \mu_j^{\nu_j \delta + \alpha_j})
\]

for each \(i\) and \(j\), and each \(t \mid N\). Moreover, since Frob\(_p\) acts as conjugation (i.e. inversion) on the \(N\)th and \(\ell\)th power roots of unity in \(\overline{Q}\), we must have \(p \equiv -1 \mod (\mu_n M)\).

Now suppose \(f(z) = \sum a(n)q^n\) is any element of \(M_k(N, \chi)\) with coefficients in \(KF\) which are \(\mu_j\)-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 \(f(z) | T_p \equiv 0 \mod \mu_j^{\nu_j \delta}\) for each \(j\). In particular, if \(f\) has coefficients in \(F\) which are \(\lambda_j\)-integral for each \(j\), then \(f(z) | T_p \equiv 0 \mod (\mu n M)\). 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 \(L/Q\), 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 \(\ell\) be a positive square-free integer, and define the Dirichlet character \(\psi_t\) by \(\psi_t(n) = \chi(n)\left(\frac{4}{n}\right)^{\kappa}\). If a sequence \(A_t(n)\) is defined by

\[
\sum A_t(n) = L(s - \kappa + 1, \psi_t) \cdot \sum b(tn^2) = S_{t,\kappa}(g(z)) := \sum A_t(n)q^n \text{ is a weight } 2\kappa \text{ modular form in } M_{2\kappa}(2N, \chi^2).
\]

In particular, the Shimura correspondence commutes with Hecke operators:

\[
S_{t,\kappa}(g(z) | T_p) = S_{t,\kappa}(g(z)) | T_p.
\]

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 \(\mod (\mu n M)\). For some \(p\) satisfying the bounds 1.2 and 1.3 we have \(g(z) \mod (\mu n M)\) for all \(g(z) \in V \cap F[[q]]\) which can be reduced \(\mod (\mu n M)\). If \(f(z) \in S_{\kappa + \frac{1}{2}}(N, \chi) \cap F[[q]]\) can be reduced \(\mod (\mu n M)\), then \(0 \equiv S_{t,\kappa}(f(z)) | T_p = S_{t,\kappa}(f(z) | T_p) \mod (\mu n M)\) for every square-free \(t\). By the definition of the Shimura lift \(S_{t,\kappa}(f(z) | T_p)\), this implies \(f(z) | T_p \equiv 0 \mod (\mu n M)\).

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 \(\ell\), the following hold:

(a) There is a modular form \(f_\ell(z) \in M_{\ell - 1}\) with \(\ell\)-integral coefficients such that \(j(z) | U_\ell \equiv f_\ell(z) \mod \ell\).
(b) There is a modular form \( g_\ell(z) \in M_{(\ell-1)^2} \) such that
\[
\sum_{n \equiv 0 \pmod{\ell}} c(n)q^n + 2 \sum_{(\frac{\ell}{n}) = -1} c(n)q^n \equiv g_\ell(z) \pmod{\ell}.
\]

(c) For any \( \alpha \geq 1 \) there are modular forms \( h_{\ell, \alpha} \in M_{\ell^{\alpha-1}(\ell-1)^2+2(n-2(\ell-1)^2)} \) such that
\[
\sum_{n \equiv 0 \pmod{\ell}} c(n)q^n + 2 \sum_{(\frac{\ell}{n}) = -1} c(n)q^n \equiv h_{\ell, \alpha}(z) \pmod{\ell^\alpha}.
\]

Applying Theorem 1.1 to the space \( V = M_k \), Corollaries 1.3 and 1.4 follow from Proposition 4.2.

4.2. **Proof of Corollary 1.5.** We now turn to the subject of the partition function \( p(n) \). Let \( \chi_2 \) denote the quadratic character \( \left( \frac{\cdot}{2} \right) \). 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 \( \eta(24z) \in S_2(576, \chi_2) \).

**Proposition 4.2 (Ahlgren-Boylan [AB]).** If \( \ell \geq 5 \) is prime and \( \alpha \) 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
\[
(4.1) \quad k := \begin{cases} 
\frac{\ell^{\alpha-1}(\ell-1)}{2} - \frac{1}{2} \left( \frac{24\beta - 1}{24\beta - 1} + 1 \right) & \ell \alpha \text{ odd}, \\
\frac{\ell^{\alpha-1}(\ell-1)}{2} - \frac{1}{2} \left( \frac{24\beta - 1}{24\beta - 1} + 1 \right) & \ell \alpha \text{ even}.
\end{cases}
\]

Then there exists a modular form \( F(z) \in M_k \cap \mathbb{Z}[q] \) such that
\[
\sum_{n=0}^\infty p(\ell^\alpha n + \beta)q^{24n+\frac{24\beta-1}{24\beta-1}} = \eta(24z)^{\frac{24\beta-1}{24\beta-1}} F(24z)
\]
\[=: G_{\ell, \alpha}(z) \in S_{k+\frac{24\beta-1}{24\beta-1}}(576, \chi_2) \pmod{\ell^\alpha}.
\]

Recall the notation from the statement of Corollary 1.3 and observe from (4.1) that \( k + \frac{1}{2} = \kappa(\ell, \alpha) + \frac{1}{2} = k + \frac{24\beta-1}{24\beta-1} \) is the weight of the modular form \( G(z) = G_{\ell, \alpha}(z) \) defined by Proposition 4.2.

**Proof of Corollary 1.3.** 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 \( \beta' \) such that \( p(Q^{2\ell^\alpha} + \beta') \equiv 0 \pmod{\ell^\alpha} \) for integers \( n \) in any of \( Q - 1 \) of the residue classes \( \pmod{\ell^\alpha} \). Since \( \frac{Q-1}{2} \geq \frac{1}{2} \), Corollary 1.3 follows easily from this fact by Theorem 1.2.

We can rewrite the statement of Proposition 4.2 as
\[
(4.2) \quad \sum_{n \equiv 24\beta-1 \pmod{24\ell}} p\left( \frac{\ell^\alpha n + 1}{24} \right) q^n \equiv G(z) \pmod{\ell^\alpha}.
\]

\(^1\)The referee points out that the bounds may be improved slightly using the fact that it is easy to establish when \( E_2 | T_p \equiv 0 \pmod{\ell} \). 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 \((n, Q) = 1\), \(Q^n \equiv \frac{24\beta - 1}{\ell} \pmod{24}\), and \(G(z) \mid T_{Q^2} \equiv 0 \pmod{\ell^n}\), then (1.2) and the definition of the action of half-integral weight Hecke operators on power series give

\[
p\left( \frac{Q^{1/\ell} n + 1}{24} \right) \equiv 0 \pmod{\ell^n}.
\]

Since \(Q \equiv -1 \pmod{24\ell}\) we have \(Q^2 \equiv 1 \pmod{24}\), so defining \(r = r(\ell, \alpha) := \frac{1 - 24\beta}{\ell^2}\), we have \(Q^n \equiv \frac{24\beta - 1}{\ell} \pmod{24}\) 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 \(\beta' = \frac{Q^{1/\ell} + 1}{24} - \beta\), (4.3) implies that \(p(Q^{1/\ell} n + n') \equiv 0 \pmod{\ell^n}\) for \(n\) in any of the \(Q - 1\) allowable residue classes \(\pmod{Q}\).

**Example 4.3.** We now revisit Example 4.3 above (congruences for \(p(n)\) modulo \(\ell^n = 13\)) in more detail. The bounds produced by a naïve, direct application of Corollary 4.3 are astronomical. To improve upon these, we make use of the discussion following Theorem 1.1. Recalling the notation of the proof of Corollary 4.3 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 \(S_{13}(576, \chi_{12})\).

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 \# \(\text{GL}_2(\mathbb{F}_{13}) \leq 13^4\), when in fact \# \(\text{GL}_2(\mathbb{F}_{13}) = (13^2 - 1)(13^2 - 13) = 26208\). 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 \(4.06 \times 10^{13}\), and the corresponding lower bound on the proportion of integers \(n\) such that \(p(n) \equiv 0 \pmod{13}\) is about \(9.19 \times 10^{-43}\).

**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**


3428 SAM LICHTENSTEIN


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