

Congruences between Modular Forms

M. RAM MURTY*

1. Introduction Recently, Goldfeld and Hoffstein [4] have shown, using the theory of L -functions that if f and g are two holomorphic Hecke newforms of weight k and *squarefree* levels N_1, N_2 respectively, then there is an $n = O(N \log N)$, with $N = \text{lcm}(N_1, N_2)$ so that

$$a_f(n) \neq a_g(n).$$

(Here, $a_f(n)$ denotes the n -th Fourier coefficient in the Fourier expansion of f at $i\infty$.) In other words, there is a constant c so that the first $cN \log N$ Fourier coefficients determine the newform. They obtain an analogous result if the weights are distinct. Assuming the generalized Riemann hypothesis for the Rankin-Selberg L -functions attached to these eigenforms, they deduce that the bound above can be improved to $O((\log N)^2 (\log \log N)^4)$.

We will show that these results can be established without the use of L -functions. Our approach leads to sharper results and is applicable in the wider context of two arbitrary cusp forms of any weight and level. In fact, we will prove a more general and sharper:

Theorem 1 *Let f and g be two distinct holomorphic modular forms of weight k and levels N_1 and N_2 respectively. Let $N = \text{lcm}(N_1, N_2)$. Then, for some*

$$n \leq \frac{k}{12} N \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

we must have $a_f(n) \neq a_g(n)$. (Here, the product is over primes p dividing N .)

Remark Note that we do not assume that f and g are Hecke eigenforms nor that they are of squarefree levels as in the Goldfeld - Hoffstein [4] paper. Moreover, let us observe that if $\nu(N)$ denotes the number of prime factors of N , and p_i denotes the i -th prime, then

$$\prod_{p|N} \left(1 + \frac{1}{p}\right) \leq \prod_{1 \leq i \leq \nu(N)} \left(1 + \frac{1}{p_i}\right) \leq \prod_{1 \leq i \leq \nu(N)} \left(1 - \frac{1}{p_i}\right)^{-1} \ll \log \log N$$

* Research partially supported by NSERC, FCAR and CICMA.

which is a sharper bound than the one given in [4, p. 387].

Proof Let $\phi = f - g$, and suppose $a_f(n) = a_g(n)$ for $n \leq M$. Then, ϕ has a zero of order $\geq M$ at $i\infty$. If Δ denotes Ramanujan's cusp form, then ϕ^{12}/Δ^k is of weight zero and hence a meromorphic function on the compact Riemann surface $X_0(N)$. Since Δ does not vanish on the upper half-plane, and has a simple zero at $i\infty$, the number of zeroes of ϕ , which is at least $12M - k$, is equal to the number of poles, which cannot exceed k times the index of $\Gamma_0(N)$ in $\Gamma(1)$ minus one (to account for $i\infty$ which already contributed to the zero count). The index of $\Gamma_0(N)$ in $\Gamma(1)$ is equal to

$$N \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

The result is now immediate.

We can make a few remarks. The first is that the method can be applied to any discrete subgroup contained in $\Gamma(1)$ to get an analogous result. One can also adapt it to deal with f and g of different weights.

The proof of Theorem 1 can be modified to handle different weights. Indeed, if

$$a_n(f) = a_n(g)$$

for all $n \leq M$, then

$$\phi = (f^{k_2} - g^{k_1})^{12} / \Delta^{k_1 k_2}$$

is a function on $X_0(N)$. The order of the zero at $i\infty$ is $\geq 12M - k_1 k_2$. The number of poles, on the other hand is $\leq k_1 k_2 ([\Gamma(1) : \Gamma_0(N)] - 1)$ by an analogous argument as before.

Let us introduce the following notation. Suppose

$$f(z) = \sum_{n=1}^{\infty} a_n(f) e^{2\pi i n z}$$

is the Fourier expansion of f at $i\infty$. Then, define

$$\text{ord}_{\infty}(f) = \min\{n : a_n(f) \neq 0\}.$$

We have therefore proved:

Theorem 2 *If f and g are holomorphic modular forms such that*

$$\text{ord}_{\infty}(f - g) > \frac{k_1 k_2}{12} ([\Gamma(1) : \Gamma_0(N)])$$

then $f = g$.

The result which we state below will be proved by a different method in Section 5 as an application of the Riemann-Roch theorem and is a small improvement of Theorem 2.

Theorem 3 *Suppose that f and g are two holomorphic cusp forms of weights k_1 and k_2 and levels N_1 and N_2 respectively. If*

$$\text{ord}_\infty(f - g) > k_1 k_2 (\mu - 1),$$

where μ is the genus of $X_0(N)$ and $N = \text{lcm}(N_1, N_2)$, then $f = g$.

Let us note that the genus μ satisfies the inequality

$$\mu \leq 1 + \frac{N}{12} \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

and thus, the bound of Theorem 3 is comparable to the one of Theorem 1.

In case that f and g are normalized newforms of distinct weights k_1 and k_2 and levels N_1 and N_2 respectively, we can in fact do better and derive an estimate superior to the *conditional* estimate of Goldfeld and Hoffstein [4, p. 386].

Theorem 4 *Let f and g be two holomorphic Hecke newforms of distinct weights k_1 and k_2 on $\Gamma_0(N_1)$ and $\Gamma_0(N_2)$ respectively. Then, there is an $n < 4(\log N)^2$ with $N = \text{lcm}(N_1, N_2)$ so that*

$$a_n(f) \neq a_n(g).$$

Proof We can view f and g as cusp forms on $\Gamma_0(N)$. Let us first note that there is a $p < 2 \log N$ which is coprime to N for otherwise N would be divisible by all the primes $< 2 \log N$ and hence by their product. By a classical estimate of Chebycheff, this product is

$$\prod_{p < 2 \log N} p = \exp \left(\sum_{p < 2 \log N} \log p \right) > N,$$

which is a contradiction. Thus, fixing such a prime p , and observing that

$$a_{p^2}(f) = a_p^2(f) - p^{k_1-1}$$

and

$$a_{p^2}(g) = a_p^2(g) - p^{k_2-1}$$

we deduce that $k_1 = k_2$. Noting that $p^2 < 4 \log^2 N$, we have a contradiction.

If we view Theorems 1, 2 and 3 as statements at the “infinite prime” then it is natural to ask for analogous results at the “finite primes”. That is, if we have a congruence between coefficients of modular forms (mod p) up to a certain natural number, can we conclude that the coefficients are always congruent? In the case the two forms have equal weight, such a result was first established by Sturm [12]. Sturm’s proof is sketchy in some places and therefore, for the sake of clarity of exposition and emphasis with the analogy above, we give the complete proof in Sections 2, 3 and 4. Sturm’s argument however cannot be easily modified to handle different weights. In Section 5, we therefore take a different approach through the Riemann-Roch theorem. This has the merit of being conceptually simple and at the same time working (mod p) (for p not dividing $N = \text{lcm}(N_1, N_2)$, however) thanks to the algebro-geometric generalization of the Riemann-Roch theorem. Recently, K. Ono [7] applied the theorem of Sturm in investigating the parity of the partition function.

2. Preliminaries In our paper [8], we indicated how the celebrated ABC conjecture leads naturally to the problem of congruences between modular forms. We will not discuss this connection here, but refer the reader to the forthcoming paper [8] for a detailed derivation. The purpose of this paper is to determine the (finite) amount of calculation necessary in order to establish a congruence between two modular forms.

More precisely, let us fix an algebraic number field F with ring of integers \mathcal{O}_F . Fix a prime ideal \mathfrak{p} of \mathcal{O}_F and for a formal power series

$$s = \sum_{n=0}^{\infty} c_s(n)q^n, \quad c_s(n) \in \mathcal{O}_F,$$

define

$$\text{ord}_{\mathfrak{p}}(s) = \min\{n : \mathfrak{p} \nmid c_s(n)\}$$

with the convention that $\text{ord}_{\mathfrak{p}}(s) = \infty$ if $\mathfrak{p} \mid c_s(n)$ for all n . Recall that $k[[q]]$ with $k = \mathcal{O}_F/\mathfrak{p}$ is a discrete valuation ring. In particular, this implies the following. Notice that if

$$f = \sum_{n \geq 0} c_f(n)q^n$$

$$g = \sum_{n \geq 0} c_g(n)q^n$$

then

$$c_{fg}(n) = \sum_{i+j=n} c_f(i)c_g(j),$$

so that, if $\text{ord}_{\mathfrak{p}}(f) = n_f < \infty$ and $\text{ord}_{\mathfrak{p}}(g) = n_g < \infty$, then from the above formula, we see

$$\begin{aligned} c_{fg}(n_f + n_g) &\equiv c_f(n_f)c_g(n_g) \pmod{\mathfrak{p}} \\ &\not\equiv 0 \pmod{\mathfrak{p}}. \end{aligned}$$

We also note that $c_{fg}(n) \equiv 0 \pmod{\mathfrak{p}}$ if $n < n_f + n_g$. Hence,

$$\text{ord}_{\mathfrak{p}}(fg) = \text{ord}_{\mathfrak{p}}(f) + \text{ord}_{\mathfrak{p}}(g)$$

when each of the terms on the right hand side is finite. By the convention made above, the equality also holds if either one of $\text{ord}_{\mathfrak{p}}(f)$ or $\text{ord}_{\mathfrak{p}}(g)$ is infinity.

For each positive integer N , let

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

and fix Γ , a subgroup of $\Gamma(1)$ containing $\Gamma(N)$. As usual, \mathfrak{h} will denote the upper half-plane, k will be a positive integer and we will consider functions

$$f : \mathfrak{h} \rightarrow \mathbb{C}$$

satisfying certain conditions. $M_k(\Gamma)$ will denote the \mathbb{C} -vector space of modular forms of weight k for Γ . To be precise, let us define for each $\gamma \in GL_2^+(\mathbb{R})$, the function

$$(f|\gamma)(z) = f\left(\frac{az+b}{cz+d}\right)(cz+d)^{-k}(ad-bc)^{k/2}$$

where

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is a matrix of $GL_2(\mathbb{R})$ of positive determinant. Then $M_k(\Gamma)$ consists of holomorphic functions of the extended upper half-plane:

$$f : \mathfrak{h}^* = \mathfrak{h} \cup \mathbb{Q} \cup \{i\infty\} \rightarrow \mathbb{C}$$

satisfying $f|\gamma = f$ for all $\gamma \in \Gamma$.

Since

$$\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma,$$

such an $f \in M_k(\Gamma)$ has a Fourier expansion of the following type:

$$f(z) = \sum_{\substack{n \geq 0 \\ n \in N^{-1}\mathbb{Z}}} a_f(n)e(nz)$$

where $e(x) = e^{2\pi ix}$. If R is a subring of \mathbb{C} , we denote by $M_k(\Gamma, R)$ those forms of $M_k(\Gamma)$ whose Fourier coefficients lie in R . That is, $a_f(n) \in R$ for all n .

Our purpose now is to explain in some detail a fundamental result of Sturm [12] regarding congruences between modular forms. To this end, let us fix as before an algebraic number field F and let \mathcal{O}_F be the ring of integers of F . Let \mathfrak{p} be a prime ideal of \mathcal{O}_F . We will explain the following:

Theorem 5 (Sturm) *Let $f, g \in M_k(\Gamma, \mathcal{O}_F)$. Suppose $\text{ord}_{\mathfrak{p}}(f - g) > k[\Gamma(1) : \Gamma]/12$. Then $f \equiv g \pmod{\mathfrak{p}}$ with Γ a congruence subgroup.*

Notice that the bound does not depend on \mathfrak{p} .

3. Sturm's theorem: the level one case To prove the theorem, we first consider the level one case. That is, $N = 1$. Recall that Ramanujan's cusp form

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n)e(nz) \in M_{12}(\Gamma(1), \mathbb{Z})$$

and can be written in terms of the standard Eisenstein series:

$$\Delta(z) = \frac{1}{1728}(E_4^3 - E_6^2)$$

with

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)e(nz),$$

$$E_6(z) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n)e(nz)$$

and

$$\sigma_k(n) = \sum_{\substack{d|n \\ d>0}} d^k.$$

Also, the modular function $j(z)$ is

$$j(z) = E_4^3/\Delta.$$

We reproduce below a result that is well-known for $M_k(\Gamma(1))$. We adapt it to the case $M_k(\Gamma(1), \mathcal{O}_F)$.

Proposition 6 *Let $\Phi \in M_{12k}(\Gamma(1), \mathcal{O}_F)$, satisfying $\text{ord}_{\mathfrak{p}}(\Phi) > k$. Then*

$$\Phi/\Delta^k \in \mathfrak{p}[j]$$

is a polynomial in j of degree at most k , all of whose coefficients are divisible by \mathfrak{p} .

Remark This fact is stated without proof in [12]. It is more or less evident from the fact that any modular function with only a pole at infinity must be a polynomial in j . However, the divisibility of the coefficients is not so clear. One can see this by comparing q -expansions. For the sake of completeness, we give a proof that assumes minimal background.

Proof We induct on k . For $k = 1$, Φ has weight 12 and so we can write it as an \mathcal{O}_F -linear combination of E_4^3 and Δ , as is easily checked. Dividing by Δ gives the result. Since $\text{ord}_{\mathfrak{p}}\Phi/\Delta > 0$, we observe that writing

$$\Phi/\Delta = \sum_{n \geq -1} c(n)e(nz),$$

we have $c(n) \in \mathcal{O}_F$ and $\mathfrak{p}|c(n)$ if $n \leq 0$.

For general k , let us find i and j so that

$$12k = 4i + 6j.$$

Then for some $c \in \mathcal{O}_F$,

$$\Phi - cE_4^i E_6^j$$

is a cusp form of weight $12k$.

Thus, we can write

$$\Phi = cE_4^i E_6^j + \Delta f_1$$

with $f_1 \in M_{12(k-1)}(\Gamma(1), \mathcal{O}_F)$. Dividing by Δ^k yields

$$\Phi/\Delta^k = cE_4^i E_6^j/\Delta^k + f_1/\Delta^{k-1}.$$

By induction hypothesis,

$$f_1/\Delta^{k-1} \in \mathfrak{p}[j].$$

Noting that $4i + 6j = 12k$ implies that $i \equiv 0 \pmod{3}$ and $j \equiv 0 \pmod{2}$ we can write $i = 3i_0$, $j = 2j_0$ so that

$$E_4^i E_6^j/\Delta^k = (E_4^3/\Delta)^{i_0} (E_6^2/\Delta)^{j_0}$$

and $E_4^3/\Delta = j$, $E_6^2/\Delta = j - 1728$. This completes the proof of the proposition.

We can now prove the theorem in the level one case. Let $\phi = f - g$. Then, $\text{ord}_{\mathfrak{p}}(\phi^{12}) > k$ implies

$$\phi^{12}/\Delta^k = \sum_{n \geq -k} c(n)e(nz)$$

with $c(n) \in \mathcal{O}_F$ and $\mathfrak{p} | c(n)$ if $n \leq 0$. By the proposition, $\phi^{12}/\Delta^k \in \mathfrak{p}[j]$ is a polynomial in j of degree at most k . Thus, $\phi^{12} \in \Delta^k \mathfrak{p}[j]$ implies $\text{ord}_{\mathfrak{p}} \phi^{12} = \infty$ so that $\text{ord}_{\mathfrak{p}} \phi = \infty$, as desired.

4. Sturm's theorem: the general level case We begin by discussing some preliminaries.

Let Γ contain $\Gamma(N)$. We want to reduce the proof of the Theorem to the level one case by constructing a map:

$$T : M_{12k}(\Gamma(N), \mathcal{O}_F) \rightarrow M_{12k}(\Gamma(1), \mathcal{O}_F)$$

such that

$$\text{ord}_{\mathfrak{p}}(T(\phi)) \geq \text{ord}_{\mathfrak{p}}(\phi).$$

Theorem 3.52 of Shimura [10, p. 85] assures us that the space $S_k(\Gamma(N))$, the space of cusp forms of weight k for $\Gamma(N)$ has a basis of cusp forms whose Fourier coefficients at $i\infty$ are rational integers, provided $k \geq 2$. This means that any element of $S_k(\Gamma(N), F)$ has the bounded denominator property. That is, given an element $f \in S_k(\Gamma(N), F)$, there is an element $A \in F$ so that $Af \in S_k(\Gamma(N), \mathcal{O}_F)$.

By the theory of Eisenstein series, we conclude that $M_k(\Gamma(N))$ has a basis whose Fourier coefficients are rational over $\mathbb{Q}(\zeta_N)$ where ζ_N denotes a primitive N -th root of unity. (See also Theorems 6.6 and 6.9 of Shimura [10, pp. 136-140]).

Now we can prove the theorem in the general case. As in [12, p. 276], let $\phi = f - g$. Our aim is to show that under the hypotheses of the Theorem, $\text{ord}_{\mathfrak{p}}(\phi) = \infty$. Thus, replacing ϕ by ϕ^{12} if necessary, we may suppose $12|k$. Then, $\phi\Delta^{-k/12}$ is a modular function of level N . Since $\Gamma(N)$ is a normal subgroup of $\Gamma(1)$, we note that for any $\gamma \in \Gamma(1)$,

$$\phi|\gamma \in M_k(\Gamma(N), F(\zeta_N)).$$

By what we have said in the previous paragraph, $\phi|\gamma$ has bounded denominators. Now let K be the Hilbert class field of $F(\zeta_N)$. Then $\mathfrak{p}\mathcal{O}_K$ is a principal ideal in \mathcal{O}_K . Let \wp be a prime ideal of \mathcal{O}_K dividing $\mathfrak{p}\mathcal{O}_K$.

For every $\gamma \in \Gamma(1)$, we can clearly find $A(\gamma) \in K^*$ such that $\text{ord}_{\wp} A(\gamma)(\phi|\gamma)$ is finite, simply by dividing by a suitable power of \wp . Moreover, by the Chinese remainder theorem, we can arrange

$$A(\gamma)(\phi|\gamma) \in M_k(\Gamma(N), \mathcal{O}_K)$$

Now consider the “norm function from $\Gamma(N)$ to $\Gamma(1)$ ”, namely,

$$\Phi = \phi \prod_{i=2}^m A(\gamma_i)(\phi|\gamma_i)$$

where $1 = \gamma_1, \gamma_2, \dots, \gamma_m$ is a set of coset representatives of $\Gamma(N)$ in $\Gamma(1)$. Note that

$$\Phi \in M_{km}(\Gamma(1))$$

because if $\sigma \in \Gamma(1)$,

$$\Phi|\sigma = \left(\prod_{i=2}^m A(\gamma_i) \right) \prod_{i=1}^m (\phi|\gamma_i\sigma)$$

and $\gamma_1\sigma, \gamma_2\sigma, \dots, \gamma_m\sigma$ is again a set of coset representatives of $\Gamma(N)$ in $\Gamma(1)$ so that $\Phi|\sigma = \Phi$. Note also that

$$\text{ord}_\varphi(\Phi) \geq \text{ord}_\varphi\phi = \text{ord}_\mathfrak{p}\phi > km/12.$$

By the level one cases we deduce that $\text{ord}_\varphi\Phi = \infty$. Thus,

$$\text{ord}_\varphi\phi + \sum_{i=2}^m \text{ord}_\varphi(A(\gamma_i)\phi|\gamma_i) = \infty$$

Since $\text{ord}_\varphi(A(\gamma_i)\phi|\gamma_i) < \infty$ for $i = 2, \dots, m$, we conclude that $\text{ord}_\varphi\phi = \infty$. Hence $\text{ord}_\mathfrak{p}\phi = \infty$. This completes the proof.

5. An application of the Riemann-Roch theorem

Theorem 7 *Suppose that f and g are holomorphic cusp forms on $\Gamma_0(N)$, of weight k and levels N_1, N_2 respectively. Let N be the lcm of N_1 and N_2 . Suppose that*

$$\text{ord}_\infty(f - g) > \frac{k}{2}(2\mu - 1)$$

where μ is the genus of $X_0(N)$. Then $f = g$.

Proof If $f \neq g$, then k is even since there are no non-zero odd weight forms. $\omega = (f - g)(dz)^{k/2}$ is a holomorphic differential $k/2$ -form on $X_0(N)$. Its degree is $(k/2)(2\mu - 2)$. On the other hand, the hypothesis means that at $i\infty$, $\text{ord}_{i\infty}(\omega) \geq (k/2)(2\mu - 1) - (k/2)$ where the extra $k/2$ comes from $(dz)^{k/2}$. Thus, (see for example, Shimura [10, Prop. 2.16, p. 39])

$$\frac{k}{2}(2\mu - 2) = \text{deg}(\omega) \geq \text{ord}_{i\infty}(\omega) \geq \frac{k}{2}(2\mu - 1) - \frac{k}{2},$$

which is a contradiction.

Proof of Theorem 3 It is now clear that Theorem 3 can be proved in an exactly similar manner. Indeed, as before, let us consider the differential $(f^{k_2} - g^{k_1})(dz)^{k_1 k_2/2}$ and proceed as in the previous proof.

Theorem 8 *Suppose f and g are cusp forms of even weight k and level N with coefficients lying in the ring of integers \mathcal{O}_F of some algebraic number field F . Suppose that for some prime ideal \mathfrak{p} coprime to the level N , we have*

$$\text{ord}_{\mathfrak{p}}(f - g) > \frac{k}{2}(2\mu - 1),$$

then, $f \equiv g \pmod{\mathfrak{p}}$.

Proof We apply the Riemann-Roch theorem valid in any field of characteristic p which is coprime to N . This uses the non-trivial fact that $X_0(N)$ has good reduction for all $p \nmid N$ and is due to Igusa [5] (see also Deligne–Rapoport [3]). Again, cusp forms of weight 2 can be interpreted as differentials on $X_0(N)$ over \mathbb{F}_p . The same argument as before is valid for arbitrary even weight k . (See Silverman [11, p. 39] and [2, p. 96], for example.)

This approach has the advantage that it can generalize to two different weights k_1 and k_2 .

Theorem 9 *Suppose that f and g are cusp forms of weights k_1 and k_2 and levels N_1 and N_2 respectively. Suppose further that at least one of k_1 or k_2 is even. As before, let us suppose the coefficients lie in the ring of integers \mathcal{O}_F of some algebraic number field. If \mathfrak{p} is a prime ideal of \mathcal{O}_F , and*

$$\text{ord}_{\mathfrak{p}}(f - g) > k_1 k_2 (\mu - 1)$$

then $f \equiv g \pmod{\mathfrak{p}}$.

We can derive better variations of Theorems 8 and 9 which are better for small primes, if we are willing to assume the generalized Riemann hypothesis for certain Dedekind zeta functions. In fact, if f and g are normalized Hecke eigenforms of level N , we know by Deligne [1] that there exists a Galois extension K_f/\mathbb{Q} and a representation

$$\rho_{\mathfrak{p},f} : \text{Gal}(K_f/\mathbb{Q}) \rightarrow \text{GL}_2(\mathcal{O}_{K_f}/\mathfrak{p})$$

such that for each prime $v \nmid \mathfrak{p}N$, we have

$$\text{tr}(\rho_{\mathfrak{p},f}(\sigma_v(K_f/\mathbb{Q}))) \equiv a_v(f) \pmod{\mathfrak{p}}$$

where σ_v denotes the Artin symbol of v . An identical result holds for g . Thus, we may consider the compositum $K_f K_g$ and deduce by the Chebotarev density theorem (see [6] or [9]) the following:

Theorem 10 *Assume that the Dedekind zeta function of $K_f K_g/\mathbb{Q}$ satisfies the analogue of the Riemann hypothesis and f and g are normalized Hecke eigenforms as above with Fourier coefficients lying in a field F . If \mathfrak{p} is a prime ideal of O_F coprime to N and*

$$\text{ord}_{\mathfrak{p}}(f - g) > (\log(\text{Norm}_{F/\mathbb{Q}}(\mathfrak{p})) + \log N)^4,$$

then $f \equiv g \pmod{\mathfrak{p}}$.

Proof By the Chebotarev density theorem and the Riemann hypothesis for the Dedekind zeta function of $K_f K_g/\mathbb{Q}$, we deduce that for any given conjugacy class C of $\text{Gal}(K_f K_g/\mathbb{Q})$, there is a prime v with

$$\text{Norm}(v) \leq (\log(\text{Norm}_{F/\mathbb{Q}}(\mathfrak{p})) + \log N)^4$$

so that $\sigma_v(K_f K_g/\mathbb{Q}) \in C$. Thus, if

$$a_v(f) \equiv a_v(g) \pmod{\mathfrak{p}}$$

for each v whose norm satisfies the last inequality, then by Deligne's theorem and the effective Chebotarev density theorem as cited above, we can conclude the desired result.

We can also remark that even if f and g are not Hecke eigenforms, a similar result can still be established. Note however, these bounds depend on \mathfrak{p} . Also worthy of contrast is that Theorem 5 is valid for all primes \mathfrak{p} whereas Theorems 8 and 9 are applicable only when \mathfrak{p} is coprime to N .

References

- [1] P. Deligne. Formes modulaires et représentations ℓ -adiques. *Séminaire Bourbaki, 1968–69, exposé 355*, Lect. Notes in Math., **179**, Springer-Verlag, Berlin, 1971, pp. 139–172.
- [2] K. Doi and M. Ohta. On some congruences between cusp forms on $\Gamma_0(N)$. *Modular Functions of one Variable. V, Bonn, 1976* (J.-P. Serre and D. Zagier, Eds.), Lect. Notes in Math., **601**, Springer-Verlag, Berlin, 1977.
- [3] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. *Modular Functions of one Variable. II*. Lect. Notes in Math., **349**, Springer-Verlag, Berlin, 1973, pp. 143–316.
- [4] D. Goldfeld and J. Hoffstein. On the number of terms that determine a modular form. *Contemp. Math.*, AMS, **143** (1993), 385–393.

- [5] J. Igusa. Kroneckerian model of fields of elliptic modular functions. *Amer. J. Math.*, **81** (1959), 561–577.
- [6] K. Murty, R. Murty and N. Saradha. Modular forms and the Chebotarev density theorem. *Amer. Journal of Math.*, **110** (1988), 253–281.
- [7] K. Ono. Parity of the Partition Function in Arithmetic Progressions. *J. reine angew. Math.*, **472** (1996), 1–15.
- [8] M.R. Murty. Bounds for congruence primes. Preprint.
- [9] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Etudes Sci. Publ. Math.*, **54** (1982), 123–201.
- [10] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Publ. Math. Soc. Japan, **11**, 1971.
- [11] J. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, **106**, Springer-Verlag, Berlin, 1986.
- [12] J. Sturm. On the congruence of modular forms. *Number Theory, New York, 1984–85*, Lect. Notes in Math., **1240**, Springer-Verlag, 1987, Berlin, pp. 275–280.

M. Ram Murty

Department of Mathematics and Statistics, Queen's University, Jeffery Hall
Kingston, Ontario K7L 3N6, Canada