Congruence primes for cusp forms of weight $k \geq 2$

FRED DIAMOND

§1. Introduction

This paper generalizes to higher weights a result of Ribet [R1] on congruences between weight two newforms of different levels. If $f = \sum a_n q^n$ and $g = \sum b_n q^n$ are newforms with the $a_n, b_n \in K$, and $\mathfrak{p}$ is a prime of K over the rational prime p, we say $f \equiv g \mod \mathfrak{p}$ if $a_n \equiv b_n$ for all n prime to the levels of f and g. If f has weight k, character χ and level N, then for a prime ℓ not dividing Np, denote by R_ℓ the set of newforms of weight k, character χ, but of level $d\ell$ with d dividing N (thus "new at ℓ").

THEOREM (RIBET). *For f as above, with $k = 2$, trivial χ, sufficiently large K and $p \nmid \frac{1}{2}\phi(N)N\ell$, there exist $g \in R_\ell$ with $g \equiv f \mod \mathfrak{p}$ if and only if*

$$a_\ell^2 \equiv (\ell+1)^2 \mod \mathfrak{p}.$$

In [D], it is observed that Ribet's proof requires neither trivial character nor p prime to N. Consequently an analogue [D, Th. 6] is proven for Λ-adic forms ([H2], [W]) which p-adically interpolate classical forms. This provides a result for p-stabilized newforms of any weight $k \geq 2$ [D, Cor. 6.9]. However, inherent in the definition of a p-stabilized newform is that it is ordinary at p. In §2 below, we dispense with this hypothesis and prove:

THEOREM 1. *For f as above, with $k \geq 2$, arbitrary χ, sufficiently large K and $p \nmid \frac{1}{2}\phi(N)N\ell(k-2)!$, there exist $g \in R_\ell$ with $g \equiv f \mod \mathfrak{p}$ if and only if*

$$a_\ell^2 \equiv \chi(\ell)\ell^{k-2}(\ell+1)^2 \mod \mathfrak{p}.$$

This is proved by applying Ribet's method directly to the parabolic cohomology groups associated to forms of higher weight. Decomposing the space of cusp forms into subspaces which are old and new at ℓ yields a cohomology congruence module which can be computed using the ingredients of a result of Ihara [I, Lemma 3.2]. For $k = 2$, Ihara's result may be viewed (via the exact sequence of Lyndon) as the vanishing of the parabolic cohomology group, with coefficients in $\mathbb{F}_p$, of a principal congruence subgroup of level N in $PSL_2(\mathbb{Z}[\ell^{-1}])$. We generalize this to cohomology with weight k coefficients in the proof of Lemma 3.2 below by noting that the restriction of a parabolic cocycle to the principal congruence subgroup of level Np vanishes, as does the kernel of this restriction homomorphism if $p \nmid N(k-2)!$ (Lemma 3.1).

Theorem 1 may be regarded in terms of raising the level of the modular representation $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_K/\mathfrak{p})$ associated to f. It has already been proved in some cases of higher weight in work of Jordan and Livné [J-L]. Their method requires that a prime q divide N exactly, and the result is needed to lower the level of the representation if it is unramified at q (from N to N/q). This also is a generalization of a weight two result of Ribet [R2] relating the Artin conductor of the representation to the level of some form from which it arises, as conjectured by Serre [S]. Theorem 1 is shown to be similarly useful in lowering the level of a modular representation (when q^r divides N, but not the Artin conductor) in recent work of Carayol [C].

This research was completed while visiting Ohio State University. I would like to thank Avner Ash for many suggestions, especially regarding the proof of Lemma 3.1, whose ingredients can be found in [A-S]. I would also like to thank Richard Taylor for helpful correspondence.

§2. Congruences

We fix a rational prime p and a finite extension K of $\mathbb{Q}_p$. Let $\mathcal{O}_K$ be the integral closure of $\mathbb{Z}_p$ in K and denote by $\mathfrak{p}$ its maximal ideal. We also fix embeddings of K into the algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, and of $\bar{\mathbb{Q}}$ into $\bar{\mathbb{Q}}_p$ and $\mathbb{C}$.

Now consider a level N, a weight $k \geq 2$ and a prime ℓ not dividing Np. Let $Z = S_k(\Gamma_1(N) \cap \Gamma_0(\ell); K)$, the cusp forms on $\Gamma_1(N) \cap \Gamma_0(\ell)$ of weight k with q-expansions having coefficients in K. Let $\mathcal{H}_Z$ be the $\mathcal{O}_K$-algebra of endomorphisms of Z generated by the Hecke operators T_n for $n \geq 1$ (e.g. [H2, §1]). We note that this algebra includes the endomorphisms S_m for m prime to N defined by $f \mid S_m = m^{k-2} f \mid \sigma_m$ where $\sigma_m \in \Gamma_0(N\ell)$ is congruent to $\begin{pmatrix} m^{-1} & 0 \\ 0 & m \end{pmatrix}$ mod N.

We have a decomposition of Z into its subspaces which are old and new at ℓ, $Z = X \oplus Y$ [R1, §2]. Here X is the direct sum of two copies of $S_k(\Gamma_1(N); K)$, and Y may be characterized as the kernel of $T_\ell^2 - S_\ell$. The newforms in X are those in Z of level dividing N, and those in Y have level divisible by ℓ. We will always assume $X \neq 0$ (in particular, if $N \leq 2$ then k is even and sufficiently large). This decomposition is stable under the action of $\mathcal{H}_Z$. We let $\mathcal{H}_X$ be the image of $\mathcal{H}_Z$ in the endomorphism ring of X and similarly define $\mathcal{H}_Y$. Then to prove the existence of non-trivial congruences between forms in X and forms in Y, we must show that $\mathcal{H}_{X,Y} = \mathcal{H}_X \oplus \mathcal{H}_Y / \mathcal{H}_Z$ is non-trivial. We do so (under suitable conditions) by using the cohomology to construct an $\mathcal{H}_{X,Y}$-module.

We now apply Ribet's analysis [R1, §3] of such a cohomology congruence module to the parabolic cohomology corresponding to cusp forms of weight k. For $n = k-2$, we define $L_n(\mathbb{Z}) = \mathbb{Z}^{n+1}$ with the action of $SL_2(\mathbb{Z})$ determined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}^n = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}^n,$$

where $\begin{pmatrix} x \\ y \end{pmatrix}^n = {}^t(x^n, x^{n-1}y, \ldots, y^n)$.

For any abelian group R, $SL_2(\mathbb{Z})$ then acts on $L_n(R) = L_n(\mathbb{Z}) \otimes R$. Then let $W(\mathcal{O}_K)$ be the image of $\mathrm{H}^1_P(\overline{\Gamma_1(N)}, L_n(\mathcal{O}_K))$ in $\mathrm{H}^1_P(\overline{\Gamma_1(N)}, L_n(K))$ and let $W(R) = W(\mathcal{O}_K) \otimes_{\mathcal{O}_K} R$ for any $\mathcal{O}_K$-module R. Similarly define $V(R)$ using the parabolic cohomology of $\overline{\Gamma_1(N) \cap \Gamma_0(\ell)}$. (For a subgroup G of $SL_2(\mathbb{Z})$, $\bar{G}$ will denote its image in $PSL_2(\mathbb{Z})$.) Following Hida, we can define a pairing on $W(\mathcal{O}_K)$ which is perfect if $p \nmid N(k-2)!$ [H1, Th. 3.2], as is the pairing defined analogously on $V(\mathcal{O}_K)$. (Note that the constraint on p, together with the assumption $X \neq 0$, ensures that there are no elliptic elements of order p.)

The inclusions of $\Gamma_1(N) \cap \Gamma_0(\ell)$ in $\Gamma_1(N)$ and in $\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(N) \begin{pmatrix} \ell^{-1} & 0 \\ 0 & 1 \end{pmatrix}$ naturally induce a homomorphism $W(R)^2 \to V(R)$. Let $A(K)$ be the image of $W(K)^2$ in $V(K)$, and $B(K)$ its orthogonal complement under the pairing (on $V(K)$). Then $V(K) = A(K) \oplus B(K)$, and under the natural action of the Hecke operators of level $N\ell$, $A(K)$, $B(K)$ and $V(\mathcal{O}_K)$ are respectively faithful $\mathcal{H}_X$, $\mathcal{H}_Y$ and $\mathcal{H}_Z$-modules (see [D, Prop. 3.1]). Therefore

$$\Omega = {[A(K) + V(\mathcal{O}_K)] \cap [B(K) + V(\mathcal{O}_K)]} \Big/ {V(\mathcal{O}_K)}$$

is an $\mathcal{H}_{X,Y}$-module.

As a generalization of Ihara's result [I, Lemma 3.2], we will prove in §3 the injectivity (if $p \nmid N(k-2)!$) of the induced map

$$\alpha : W(K/\mathcal{O}_K)^2 \to V(K/\mathcal{O}_K).$$

As an immediate consequence $\Omega \cong \ker(\beta\circ\alpha)$, where $\beta : V(K/\mathcal{O}_K) \to W(K/\mathcal{O}_K)^2$ is the adjoint of α with respect to the above pairings. This isomorphism is $\mathcal{H}_Z$-linear where for m prime to ℓ, T_m acts as the matrix $\begin{pmatrix} T'_m & 0 \\ 0 & T'_m \end{pmatrix}$ on $W(K/\mathcal{O}_K)^2$ (using primes to denote Hecke operators of level N), and T_ℓ as $\begin{pmatrix} T'_\ell & \ell^{k-1} \\ -\ell^{2-k}S'_\ell & 0 \end{pmatrix}$.

A straightforward computation then yields

$$\beta\circ\alpha = \begin{pmatrix} \ell+1 & T'^*_\ell \\ T'_\ell & \ell^{k-2}(\ell+1) \end{pmatrix}$$

(where T'^*_ℓ is adjoint to T'_l and satisfies $\ell^{k-2}T'_\ell = S'_\ell T'^*_\ell$). Since $S_\ell = \begin{pmatrix} S'_\ell & 0 \\ 0 & S'_\ell \end{pmatrix}$ on $W(K/\mathcal{O}_K)^2$, we have

$$T_\ell^2 - S_\ell = \begin{pmatrix} -S'_\ell & T'_\ell \\ 0 & -\ell^{2-k}S'_\ell \end{pmatrix} \circ\beta\circ\alpha.$$

Since S'_ℓ is an automorphism, we have $\ker(\beta\circ\alpha) = \ker(T_\ell^2 - S_\ell)$. Using Ribet's argument ([R1, p. 510] or [D, Prop. 3.4]), we deduce that $\mathrm{Ann}_{\mathcal{H}_X}\,\Omega \subseteq (T_\ell^2 - S_\ell)\mathcal{I}_X$ where $\mathcal{I}_X$ is the integral closure of $\mathcal{H}_X$ in $\mathcal{H}_X \otimes_{\mathcal{O}_K} K$. Now since Ω is an $\mathcal{H}_{X,Y}$-module, this implies

$$(*) \qquad (T_\ell^2 - S_\ell)\mathcal{H}_X \subseteq \pi_X(\ker\pi_Y) \subseteq (T_\ell^2 - S_\ell)\mathcal{I}_X,$$

where π_X and π_Y denote the appropriate projection maps of $\mathcal{H}_Z$.

We can replace Z by $Z^{(\chi)} = S_k(\Gamma_0(N\ell),\chi\,; K)$, where χ is a Dirichlet character defined mod N with values in K and consider the decomposition $Z^{(\chi)} = X^{(\chi)}\oplus Y^{(\chi)}$. If $p \nmid \frac{1}{2}\phi(N)$, then $\mathcal{H}_{Z^{(\chi)}}$ is a direct summand of $\mathcal{H}_Z$, and we can replace X and Y by $X^{(\chi)}$ and $Y^{(\chi)}$ in $(*)$. Now suppose $f = \sum a_n q^n$ is a newform of level N, weight k, character χ and coefficients in K. Suppose further that $x^2 - a_\ell x + \ell^{k-1}\chi(\ell)$ has roots $\alpha,\beta \in K$. Then $f_\alpha = f - \beta f(\ell z)$ is an eigenform of T_ℓ, and applying π_{Kf_α} to $(*)$ we get

$$\pi_{Kf_\alpha}(\ker\pi_{Y^{(\chi)}}) = (\alpha^2 - \chi(\ell)\ell^{k-2})\mathcal{O}_K.$$

Using the duality between the Hecke algebra and the lattice in Z of forms with integral coefficients to compute the congruence module [D, §2], we find

$$C_{Kf_\alpha,Y^{(\chi)}} \cong (\alpha^2 - \chi(\ell)\ell^{k-2})^{-1}\mathcal{O}_K\,/\,\mathcal{O}_K.$$

Noting that

$$(\alpha^2 - \chi(\ell)\ell^{k-2})(\beta^2 - \chi(\ell)\ell^{k-2})\mathcal{O}_K = (a_\ell^2 - \chi(\ell)\ell^{k-2}(\ell+1)^2)\mathcal{O}_K,$$

we see that if $p \nmid \frac{1}{2}\phi(N)N(k-2)!$, and $a_\ell^2 \equiv \chi(\ell)\ell^{k-2}(\ell+1)^2 \mod \mathfrak{p}$, then there exists $g \in R_\ell$ congruent to f modulo the maximal ideal of the ring of integers of $\bar{\mathbb{Q}}_p$. Conversely, if such a g exists, we deduce from properties of the associated Galois representations that $a_\ell^2 \equiv \chi(\ell)\ell^{k-2}(\ell+1)^2 \mod \mathfrak{p}$ [R1, p. 506]. This proves Theorem 1.

We can sharpen this result by decomposing $Y^{(\chi)} = Y^+ \oplus Y^-$, computing the appropriate congruence modules and applying a method of Wiles using Fitting ideals. We thus obtain Theorem 2; for further details, see [D, §4].

THEOREM 2. *For f as above, K sufficiently large and $p \nmid N\ell(k-2)!$, there exist integers d_i and distinct newforms $g_i \in Y^{(\chi)}$ with*

$$g_i \equiv f \mod \mathfrak{p}^{d_i} \quad \textit{and} \quad \sum d_i \geq v_\mathfrak{p}(a_\ell^2 - \chi(\ell)\ell^{k-2}(\ell+1)^2) - 2v_\mathfrak{p}(2\phi(N)).$$

§3. Parabolic cohomology

In this section we prove the injectivity of α (Lemma 3.2). First recall that for a group G, a subset Q of G, and a G-module A, $\mathrm{H}^1_Q(G,A)$ is the subgroup of $\mathrm{H}^1(G,A)$ obtained from the cocycles u satisfying $u(\gamma) \in (\gamma-1)A$ for all $\gamma \in Q$. For a congruence subgroup of $PSL_2(\mathbb{Z})$, we write $\mathrm{H}^1_P(G,A)$ for $\mathrm{H}^1_Q(G,A)$ where Q is the set of parabolic elements of G. We begin by proving the vanishing of a finite cohomology group necessary to the proof of Lemma 3.2. In many cases this is a consequence of [K-P-S, Th. 1.5.3].

LEMMA 3.1. *Let Q be a p-sylow subgroup of $G = SL_2(\mathbb{F}_p)$, and $\mathbb{F}_q$ a finite field of characteristic p. Then $\mathrm{H}^1_Q(G, L_n(\mathbb{F}_q)) = 0$ for $0 \leq n \leq p-1$.*

PROOF: We let Q act trivially on $\mathbb{F}_q$ and consider the induced module $\mathrm{Ind}_Q^G(\mathbb{F}_q)$, the set of functions from G/Q to $\mathbb{F}_q$. Identifying G/Q with the punctured plane $\mathbb{F}_p{}^2 \setminus \{(0,0)\}$, and $L_n(\mathbb{F}_q)$ with the space of homogeneous polynomials of degree n in $\mathbb{F}_q[x,y]$, we have an injection of G-modules $\phi : L_n(\mathbb{F}_q) \to \mathrm{Ind}_Q^G(\mathbb{F}_q)$ [A-S, p. 855], which induces

$$\phi_* : \mathrm{H}^1_Q(G, L_n(\mathbb{F}_q)) \to \mathrm{H}^1_Q(G, \mathrm{Ind}_Q^G(\mathbb{F}_q)).$$

Since Shapiro's isomorphism,

$$\mathrm{H}^1(G, \mathrm{Ind}_Q^G(\mathbb{F}_q)) \cong \mathrm{H}^1(Q, \mathbb{F}_q),$$

sends $\mathrm{H}^1_Q(G, \mathrm{Ind}_Q^G(\mathbb{F}_q))$ to $\mathrm{H}^1_Q(Q, \mathbb{F}_q) = 0$, we conclude that $\mathrm{H}^1_Q(G, \mathrm{Ind}_Q^G(\mathbb{F}_q)) = 0$.