

CONGRUENCE FORMULA FOR CERTAIN DIHEDRAL TWISTS

SUDHANSHU SHEKHAR AND R. SUJATHA

ABSTRACT. In this article we prove a congruence formula for the special values of certain dihedral twists of two primitive modular forms of weight two with isomorphic residual Galois representation at a prime p .

1. INTRODUCTION

Let p be a prime number. Given two normalized Hecke eigenforms whose Fourier coefficients are integral and congruent modulo p , the congruence properties between the special values of their associated L -functions have been an important area of study. In particular, Greenberg and Vatsal [GV], and Vatsal [V] show under certain hypotheses that when the forms are twisted by Dirichlet characters, the associated twisted L -values are congruent. It is natural to investigate such congruences when we consider twists of the L -values for Artin representations of the Galois group of \mathbb{Q} . The aim of this article is to consider some simple Artin representations of dihedral type and prove congruence properties between the associated twisted p -adic L -values. Our results should be viewed as a mix of the congruence results for special algebraic L -values for congruent modular forms and congruence between p -adic L -values, the latter being predicted by non-commutative Iwasawa theory.

We now explain our results in greater detail. Let $f = \sum_n a(n, f)q^n$ and $g = \sum_n a(n, g)q^n$ be two new normalized Hecke eigenforms of weight 2 and level N_f and N_g respectively such that $a(n, f)$ and $a(n, g)$ are integers in \mathbb{Q} for each n . Let \bar{N}_f and \bar{N}_g denote the conductor of the residual Galois representation associated to f and g respectively. Fix an odd prime p and a positive square free integer d . We shall assume throughout this article that f and g are p -ordinary. Put $K = \mathbb{Q}(\sqrt{-d})$. Let F be a finite Galois extension of \mathbb{Q} such that $K \subset F$, with $\text{Gal}(F/\mathbb{Q})$ isomorphic to the dihedral group of order $2p^s$ for some integer $s \geq 1$. Let $\chi : \text{Gal}(F/K) \rightarrow \mathbb{C}^\times$ be an odd character of conductor \mathfrak{f}_χ and order p^s . This in particular implies that χ does not factor through a subextension of F/K . Put $\rho = \text{Ind}_{G_K}^{G_\mathbb{Q}} \chi$. We shall assume that ρ is irreducible. Let N_ρ denote the conductor of ρ , D denote the discriminant of K over \mathbb{Q} and D' denote the prime to p part of D . We define the quantity $R_*^S(\rho)$ by the formula

$$(1) \quad R_*^S(\rho) := \epsilon_p(\rho) \times u_*^{-v_p(N_\rho)} \times \frac{P_p(\hat{\rho}, u_*^{-1})}{P_p(\rho, w_*^{-1})} \times \frac{L_S(*, \rho, 1)}{(-2\pi i \Omega_*^+)(-2\pi i \Omega_*^-)}.$$

Received by the editors October 27, 2012 and, in revised form, July 2, 2013.

2010 *Mathematics Subject Classification.* Primary 14H52, 11F80, 11F11, 11F33.

Key words and phrases. Elliptic curve, Galois representation, modular forms, congruences for modular forms, special values of L -series, periods of modular forms.

Here $*$ denotes either f or g , $\epsilon_p(\rho)$ is the local epsilon factor of ρ defined as in [DD], $P_p(\hat{\rho}, X)$ and $P_p(\rho, X)$ respectively are the usual characteristic polynomials associated with the dual representation $\hat{\rho}$ and ρ at p , Ω_*^+ and Ω_*^- denote the canonical periods associated to $*$ as defined in [V], and u_* and w_* are p -adic numbers defined by

$$1 - a(p, *)X + pX^2 = (1 - u_*X)(1 - w_*X), \quad u_* \in \mathbb{Z}_p^\times.$$

Further, the subscript L_S denotes that in the corresponding twisted L -function, we have removed the Euler factors at the finite set of primes S . The finite set S shall always be assumed to contain the set

$$(2) \quad S_{min} = \{p, q | N_{K/\mathbb{Q}}(\mathfrak{f}_\chi), q | N/\bar{N}_*\},$$

where N denotes the least common multiple of N_f and N_g , and $N_{K/\mathbb{Q}}$ is the norm map. If $S = S_{min}$, then for simplicity, we shall remove the superscript S from the notation of $R_*^S(\rho)$ and write $R_f(\rho)$.

Suppose that $|a(n, f) - a(n, g)|_p < 1$ for each n coprime to N , where $|\cdot|_p$ is the p -adic norm normalized such that $|p|_p = p^{-1}$. Then, our aim is to show that $R_f^S(\rho)$ and $R_g^S(\rho)$ are p -adic integers satisfying the inequality

$$(3) \quad |R_f^S(\rho) - R_g^S(\rho)|_p < 1.$$

We in fact prove a more general result. For a Dirichlet character ϕ of p power conductor, we consider the special values of the L -functions associated to $f \otimes \rho \otimes \phi$ and $g \otimes \rho \otimes \phi$, and prove an analogous congruence formula. We shall prove the above inequality under certain assumptions made in section 3.

Our proof of (3) relies on the results proved in [B], [V] and [GV]. We make use of an auxiliary Artin representation σ which is congruent to ρ modulo p that has the virtue of being much simpler as it splits into a sum of two Dirichlet characters. We then use the congruence formula proved by Bouganis in [B] to obtain a congruence between the special values of $f \otimes \rho$ and $f \otimes \sigma$. A similar result holds for the form g as well. In [B], the results are proved for the prime $p = 3$, $K = \mathbb{Q}(\mu_3)$ and $[F : K] = 3$, as the author was mainly interested in the special value of L -functions in the first layer of the false Tate extensions. Using the ideas of *loc.cit.*, we extend the results to all odd primes and for other dihedral extensions F/\mathbb{Q} of degree $2p^s$. Additionally, it is assumed in [B] that the conductor of the modular form and its residual representation are equal and square free. Our results hold under a weaker hypothesis, and we make use of the results proved in [DDT] which gives a nice account of some of the techniques used by Wiles in the proof of Fermat's last theorem. We then use the results of [GV] to complete the proof of our main result. Our method requires a finer analysis of periods of modular forms as considered in [DDT] and a comparison with the 'canonical period' that appears in the work of Vatsal. This is discussed in section 4.

Even though the Artin representations considered here are of a rather special kind, such questions of course can be posed for more general Artin representations. We believe that our idea of using an auxiliary simple Artin representation like σ to prove the congruence formula involving twists by more general representations should be applicable in this larger setting. But this is contingent on proving subtle results of the kind stated in section 3. This is presently a topic of study in non-commutative Iwasawa theory, and we hope to address this theme in future works.

Another crucial ingredient in the proof here and also in [B] is the use of Hida's arithmetic measures in the dihedral context.

2. p -ADIC MODULAR FORMS AND ARITHMETIC MEASURE

In this section, we briefly recall the definition of the space of p -adic modular forms. For more details we refer the reader to [H]. We fix an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p \hookrightarrow \mathbb{C}_p$, where \mathbb{C}_p is the p -adic completion of $\bar{\mathbb{Q}}_p$ under the normalized p -adic absolute value $|p|_p = p^{-1}$.

In this section J will denote any positive integer. Let ψ be a Dirichlet character of conductor dividing J . For any subring $R \subset \bar{\mathbb{Q}}$, we consider the R -modules

$$M_k(\Gamma_0(J), \psi; R) := \{f \in M_k(\Gamma_0(J), \psi) \mid f(z) = \sum a(n, f)q^n, a(n, f) \in R\},$$

$$M_k(\Gamma_1(J); R) := \{f \in M_k(\Gamma_1(J)) \mid f(z) = \sum a(n, f)q^n, a(n, f) \in R\},$$

where $M_k(\Gamma_0(J), \psi)$ (resp. $M_k(\Gamma_1(J))$) denotes the space of modular forms with character ψ , the congruence subgroup $\Gamma_0(J)$ (resp. the congruence subgroup $\Gamma_1(J)$) and Fourier coefficients in the field of complex numbers \mathbb{C} . Let $H_k(\Gamma_0(J), \psi; R)$ (resp. $H_k(\Gamma_1(J), R)$) denote the Hecke algebra corresponding to the space $M_k(\Gamma_0(J), \psi; R)$ (resp. $M_k(\Gamma_1(J); R)$). The space of cusp forms with coefficients in R are defined as

$$S_k(\Gamma_0(J), \psi; R) := S_k(\Gamma_0(J), \psi) \cap M_k(\Gamma_0(J), \psi; R),$$

$$S_k(\Gamma_1(J); R) := S_k(\Gamma_1(J)) \cap M_k(\Gamma_1(J); R).$$

Let $h_k(\Gamma_0(J), \psi; R)$ (resp. $h_k(\Gamma_1(J), R)$) denote the Hecke algebra corresponding to the space $S_k(\Gamma_0(J), \psi; R)$ (resp. $S_k(\Gamma_1(J); R)$) of cusp forms. The p -adic norm of a modular form $f \in M_k(\Gamma_0(J), \psi; R)$ is defined as $|f|_p = \sup_n |a_n|_p$. Let K_0 be a finite extension of \mathbb{Q} and K be the closure of K_0 in \mathbb{C}_p with respect to the p -adic topology. Let $M_k(\Gamma_0(J), \psi; K)$ and $M_k(\Gamma_1(J); K)$ denote the p -adic completion of $M_k(\Gamma_0(J), \psi; K_0)$ and $M_k(\Gamma_1(J); K_0)$ respectively with respect to the norm $|\cdot|_p$ inside $K[[q]]$, where q is considered to be an indeterminate. Then it is known that

$$M_k(\Gamma_0(J), \psi; K) = M_k(\Gamma_0(J), \psi; K_0) \otimes_{K_0} K$$

and

$$M_k(\Gamma_1(J); K) = M_k(\Gamma_1(J), K_0) \otimes_{K_0} K.$$

Let \mathfrak{O}_K be the ring of integers in K and let A be either K or \mathfrak{O}_K . Then we also consider the spaces

$$M_k(J; A) := \bigcup_{n=0}^{\infty} M_k(\Gamma_1(Jp^n); A) \text{ and } M_k(J, \psi; A) := \bigcup_{n=0}^{\infty} M_k(\Gamma_0(Jp^n), \psi; A).$$

The spaces of the p -adic modular forms $\overline{M}_k(J; A)$ and $\overline{M}_k(J, \psi; A)$ of $\Gamma_1(J)$ and of $\Gamma_0(J)$ and character ψ are defined as the completion of the spaces $M_k(J; A)$ and $M_k(J, \psi; A)$ respectively with respect to the norm $|\cdot|_p$. The space of p -adic cusp forms are analogously defined.

The p -adic Hecke algebras $H_k(J, \psi; \mathfrak{O}_K)$ and $H_k(J; \mathfrak{O}_K)$ are defined respectively as the inverse limit $\varprojlim_n H_k(\Gamma_0(Jp^n), \psi; \mathfrak{O}_K)$ and $\varprojlim_n H_k(\Gamma_1(Jp^n); \mathfrak{O}_K)$. Similarly, the spaces $h_k(J, \psi; \mathfrak{O}_K)$ and $h_k(J; \mathfrak{O}_K)$ are defined. For each n , we also consider the idempotent operators $e_n = \varinjlim_m U(p)^{m!}$ in $H_k(\Gamma_0(Jp^n), \psi; \mathfrak{O}_K)$, where

$U(p)$ is the p -th Hecke operator. The idempotent operator e in $H_k(J, \psi; \mathfrak{O}_K)$ and $H_k(J; \mathfrak{O}_K)$ is defined as $\varprojlim_n e_n$.

Let $C(\mathbb{Z}_p^\times; \mathbb{Z}_p)$ and $LC(\mathbb{Z}_p^\times; \mathbb{Z}_p)$ denote the space of continuous (respectively locally constant) functions of \mathbb{Z}_p^\times with values in \mathbb{Z}_p . Now consider a modular form $h \in M_1(\Gamma_0(J), \psi; \mathfrak{O}_K)$ with q -expansion $h(z) = \sum_{n \geq 0} a(n, h)q^n$. Put $J = J_0 p^\beta$, where J_0 is prime to p . Then we consider the cuspidal arithmetic measure μ_h of weight one defined by

$$\mu_h(\phi) = \sum_{n \geq 1} \phi(n) a(n, h) q^n, \quad \phi \in C(\mathbb{Z}_p^\times; \mathbb{Z}_p).$$

For the definition of arithmetic measure we refer the reader to [H, page 36]. It is known that $\mu_h(\phi) \in \bar{S}_1(J; \mathbb{Z}_p)$ (see [H, Corollary 2.3]). For every positive integer L such that $J_0 | L$, we have a modified arithmetic measure defined as $\mu_h^L(\phi) := \mu_h(\phi)[L/J_0]$, where the linear map

$$[L/J_0] : \bar{S}_1(J_0; \mathbb{Z}_p) \longrightarrow \bar{S}_1(L; \mathbb{Z}_p)$$

is defined by

$$[L/J_0] \left(\sum_{n \geq 1} a(n, h) q^n \right) \mapsto \sum_{n \geq 1} a(n, h) q^{nL/J_0}.$$

Put $Z_L = \mathbb{Z}_p^\times \times (\mathbb{Z}/L\mathbb{Z})^\times$. For z in Z_L , we denote the summand in \mathbb{Z}_p^\times by z_p . The group Z_L acts on $C(\mathbb{Z}_p^\times; \mathbb{Z}_p)$ by the formula $(z \star \phi)(x) := \psi(z) z_p \phi(z_p^2 x)$ for $z \in Z_L$ and $\phi \in C(\mathbb{Z}_L; \mathbb{Z}_p)$. We also consider the arithmetic measure of weight one defined by

$$2E(\phi) = \sum_{\substack{n=1 \\ (n,p)=1}}^{\infty} \left(\sum_{\substack{d|n \\ (d,L)=1}} \text{sgn}(d) \phi(d) \right) q^n \in \mathbb{Z}_p[[q]].$$

Following [B] we call it the Eisenstein-Katz measure. For a finite order character $\eta : Z_L \rightarrow \mathbb{C}^\times$, we consider the arithmetic measure

$$(\mu_h^L * E)_\eta : C(\mathbb{Z}_p^\times; \mathbb{Z}_p) \rightarrow \bar{S}_2(L; \mathbb{Z}_p)$$

of weight 2 defined by the convolution of μ_h^L and E as follows:

$$(\mu_h^L * E)_\eta(\phi) := \int_{\mathbb{Z}_p^\times} \int_{Z_L} \eta(z) z_p (z^{-1} \star \phi)(x) dE(z) d\mu_h^L(x).$$

If η is the trivial character, then we shall drop it from the notation and just write $\mu_h^L * E$. For a finite order character $\phi \in C(Z_L; \mathbb{Z}_p)$ we have (cf. [B, Section 2])

$$(\mu_h^L * E)(\phi) = \mu_h^L(\phi) \cdot E(\psi^{-1} \cdot (\phi_p^{-2})),$$

where $\phi_p(z) = \phi(z_p)$.

3. p -ADIC RANKIN-SELBERG CONVOLUTION

In this section, we will use the p -adic Rankin-Selberg convolution considered by Hida in [H]. We shall use the results proved in this section in the subsequent ones to prove inequality (3). Let h be a new normalized Hecke eigenform of weight 2, level N_h and trivial character. Suppose that h is ordinary at p . Then we denote by

h_0 the p -stabilization of h which is a normalized Hecke eigenform of weight 2, level N_0 and trivial character defined by

$$h_0(z) = \begin{cases} h(z) & \text{if } p \text{ divides } N; \\ h(z) - wh(pz) & \text{otherwise;} \end{cases}$$

here w is the unique non-unit root of the Hecke polynomial of h at p , $N_0 := N_h p$ if $p \nmid N_h$ and $N_0 = N_h$ if $p \mid N_h$. Note that $a(p, f_0) = u_f$ is the unique p -adic unit root of the Hecke polynomial of f_0 at p . We shall sometimes drop the subscript f from the notation and just write u . Let D denote the discriminant of the quadratic imaginary extension $K = \mathbb{Q}(\sqrt{-d})$ and ϵ be the quadratic character of K . Recall that F/\mathbb{Q} is a dihedral Galois extension of \mathbb{Q} of degree $2p^s$ for some $s \geq 1$ such that $K \subset F$. Also,

$$\chi : \text{Gal}(F/K) \rightarrow \mathbb{C}^\times$$

is an odd character of conductor \mathfrak{f}_χ and order p^s . Now consider the series $h_\rho = \sum_{\mathfrak{a} \in \mathcal{O}_K} \chi(\mathfrak{a}) q^{N_{K/\mathbb{Q}}(\mathfrak{a})}$, where $\chi(\mathfrak{a}) = 0$ if $(\mathfrak{a}, \mathfrak{f}_\chi) \neq 1$. Here we have used the same notation for the Galois character χ and the associated ideal character via class field theory. Since χ is non-trivial, we have that $h_\rho \in S_1(|D|N_{K/\mathbb{Q}}(\mathfrak{f}_\chi), \epsilon\chi|_{\mathbb{Z}})$ is a primitive form.

Lemma 3.1. *We have*

- (i) $\chi|_{\mathbb{Z}}$ is a trivial character.
- (ii) Fourier coefficients of h_ρ are real numbers.

Proof. Let l be a prime of \mathbb{Z} . If l is not coprime to \mathfrak{f}_χ , then $\chi(l) = 0$. Therefore we may assume that χ is unramified at l . In particular, this implies that l is coprime to \mathfrak{f}_χ . Let \mathfrak{l} be a prime of K lying over l . Suppose that l is inert in K . This implies that the decomposition subgroup $D_{\mathfrak{l}}$ of a prime of F lying above l in $\text{Gal}(F/\mathbb{Q})$ maps onto $\text{Gal}(K/\mathbb{Q})$. If \mathfrak{l} does not split completely in F , then $D_{\mathfrak{l}}$ is a subgroup of $\text{Gal}(F/\mathbb{Q})$ of order $2p^r$ for some $r > 0$. Since p is odd, $D_{\mathfrak{l}}$ is a dihedral group, and therefore it cannot be cyclic. This implies that l must ramify in F . Being an inert prime, l is unramified in K/\mathbb{Q} , and hence \mathfrak{l} ramifies in F/K . This implies that l is not coprime to \mathfrak{f}_χ , and this is a contradiction. Therefore we see that l must split completely in F/K and the residue field extension at \mathfrak{l} corresponding to F is trivial. Hence, $\chi(\mathfrak{l}) = \chi(\text{Frob}_{\mathfrak{l}}^{-1}) = 1$, where $\text{Frob}_{\mathfrak{l}}$ is the Frobenius at \mathfrak{l} . Thus $\chi(l) = 1$.

Now assume that l is ramified in K , i.e. $l = \mathfrak{l}^2$ in K . If \mathfrak{l} splits completely in F , then as above $\chi(\mathfrak{l}) = 1$. If \mathfrak{l} does not split completely in F , then by a similar argument as above we get that the decomposition subgroup $D_{\mathfrak{l}}$ maps onto $\text{Gal}(K/\mathbb{Q})$ and the order of $D_{\mathfrak{l}}$ is equal to $2p^r$ for some $r > 0$. Since \mathfrak{l} remains unramified in F/K the residue field extension of F/\mathbb{Q} at l will have degree p^r but the decomposition group at l is of order $2p^r$. We hence get a normal subgroup of $D_{\mathfrak{l}}$ of order 2 as an inertia subgroup, which is impossible. Therefore this case cannot occur and we have $\chi(l) = \chi(\mathfrak{l}) = 1$.

Now suppose that $l = \mathfrak{l}\bar{\mathfrak{l}}$ in K . In this case, the action of $\text{Gal}(K/\mathbb{Q})$ takes the Frobenius at \mathfrak{l} to its inverse as $\text{Gal}(F/\mathbb{Q})$ is a dihedral extension. Therefore $\chi(\bar{\mathfrak{l}}) = \chi(\mathfrak{l})^{-1}$. Thus $\chi(l) = \chi(\mathfrak{l})\chi(\bar{\mathfrak{l}}) = 1$. This proves assertion (i).

Let $a(l, \rho)$ denote the l -th Fourier coefficient of h_ρ . If l is not coprime to \mathfrak{f}_χ , then $a(l, \rho) = 0$. We assume that l is coprime to \mathfrak{f}_χ . If l remains inert in K or ramifies in K , then we have already seen that $\chi(\mathfrak{l}) = 1$ for $\mathfrak{l} \mid l$ in K . Therefore we can assume

that $l = \bar{l}$. But in this case $a(l, h_\rho) = \chi(\mathfrak{l}) + \chi(\bar{\mathfrak{l}}) = \chi(\mathfrak{l}) + \chi(\mathfrak{l})^{-1}$, and this is a real number. \square

To prove the congruence (3), we need to consider one more Artin representation. Put $\sigma = \text{Ind}_{G_K}^{G_{\mathbb{Q}}} \mathbf{1}$, where $\mathbf{1}$ denotes the trivial representation. Then we have that

$$h_\sigma := \frac{1}{2}L(0, \epsilon) + \sum_{\mathfrak{a} \subset \mathfrak{O}_K} q^{N_{K/\mathbb{Q}}(\mathfrak{a})} \in M_1(\Gamma_0(D), \epsilon).$$

To prove the inequality stated in section 1 we need to make the following assumptions:

- (i) $N := \text{l.c.m.}(N_f, N_g)$ is coprime to p and N_ρ .
- (ii) \mathfrak{f}_χ is coprime to D' .
- (iii) N/\bar{N}_f and \bar{N}_f are coprime and \bar{N}_f is square free.
- (iv) The residual representation of the Galois representation associated to f is absolutely irreducible.

Let $M := |D|N_{K/\mathbb{Q}}(\mathfrak{f}_\chi) = Jp^\delta$ for some integer J coprime to p . By [EK, Theorem 15(a)] there exists a positive integer m such that $M = D'p^\delta m^2$. In particular, m^2 is the prime to p part of $N_{K/\mathbb{Q}}(\mathfrak{f}_\chi)$, and we have

$$(4) \quad S_{min} = \{p, q|m, q|n\},$$

where n denotes the product of prime divisors of N/\bar{N}_f and S_{min} is the set of primes defined in (2). Note that assumption (ii) implies that m is coprime to D' and assumption (iii) implies that n is coprime to \bar{N} . Also note that $J = D'm^2$. Since f is congruent to g modulo p , we have $\bar{N}_f = \bar{N}_g$. Thus we shall drop the subscript f (resp. g) from \bar{N}_f (resp. \bar{N}_g) and write \bar{N} .

For every integer k , let i_k denote the trivial Dirichlet character mod k . For a modular form $h = \sum_n a(n, h)q^n$, let $h|i_k := \sum_n i_k(n)a(n, h)q^n$ be the modular form obtained by removing the Euler factors of h at the primes $l|k$. Then $\tilde{f}_0 := f_0|i_{mn} \in S_2(\Gamma_0(\bar{N}n^2m^2p), \mathbb{Q}_p)$ is a normalized Hecke eigenform. Now consider the \mathbb{Z}_p -algebra homomorphism $h_2(\Gamma_0(\bar{N}n^2m^2p); \mathbb{Z}_p) \rightarrow \mathbb{Z}_p$ induced by $T(n) \mapsto a(n, \tilde{f}_0)$. This map induces a decomposition

$$h_2(\Gamma_0(\bar{N}n^2m^2p); \mathbb{Q}_p) = \mathbb{Q}_p \times A.$$

For a proof of the above statement see [B, Section 4] and section 4 below in this article. Let $1_{\tilde{f}_0}$ denote the idempotent attached to the first summand. We fix a constant $c(f) \in \mathbb{Z}_p$ such that $c(f)1_{\tilde{f}_0} \in h_2(\Gamma_0(\bar{N}n^2m^2p); \mathbb{Z}_p)$. The idempotent $1_{\tilde{f}_0}$ induces a map

$$\ell_{\tilde{f}_0} : e\bar{S}_2(\bar{N}_f n^2 m^2 p, \mathbb{Q}_p) \rightarrow \mathbb{Q}_p$$

defined as $\ell_{\tilde{f}_0}(eh) = a(1, h|e|1_{\tilde{f}_0})$, where e is the idempotent operator defined in section 2. It follows from [H1, Lemma 4.1] that this map is well-defined. Now consider the measure

$$\mu_{\tilde{f}_0 \times h} := c(f) \circ \ell_{\tilde{f}_0} \circ e \circ (\mu_h^L * E),$$

where h can take the values h_ρ and $h_\sigma|i_m$ and $L = \bar{N}_f n^2 m^2$. Here \circ denotes the composition of maps. Note that $h_\sigma|i_m \in M_1(\Gamma_0(Dm^2), \epsilon)$.

Below we state a theorem of Hida which we shall use to prove our result. Before that we recall some notation. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a real matrix with positive

determinant. Then for a modular form G of weight k we shall denote by $G|_k\gamma$ the function defined by

$$G|_k\gamma(z) = \det(\gamma)^{k/2} G(\gamma(z))(cz + d)^{-k},$$

where $\det(\gamma)$ denotes the determinant of γ . For an integer Q we shall denote by τ_Q the matrix $\begin{pmatrix} 0 & -1 \\ Q & 0 \end{pmatrix}$. However, to simplify notation, in the special case when $Q = Jp^\beta$ for some $\beta \geq 0$, then following [H] and [B] we shall also use the notation τ_β to denote the matrix τ_{Jp^β} . We then have the following theorem.

Theorem 3.2 (cf. [H, Section 8], [B, Theorem 2.9]). *For every finite order character $\phi \in C(\mathbb{Z}_p^\times; \mathbb{Z}_p)$,*

$$\mu_{\tilde{f}_0 \times h}(\phi) = c(f)tp^{\beta/2}a(\tilde{f}_0, p)^{1-\beta} \frac{D(\tilde{f}_0, \mu_h(\phi)|_{1\tau_\beta}, 1)}{2^3\pi^2 i^3 \langle \tilde{f}_0|_{2\tau_{Nn^2m^2p}}, \tilde{f}_0 \rangle_{Nn^2m^2p}},$$

where $t = \text{l.c.m.}(L, J)LJ^{1/2}$, h can take the value h_ρ or $h_\sigma|m$, β is the smallest exponent such that $\mu_h(\phi) \in M_1(\Gamma_1(Jp^\beta))$, $D(\tilde{f}_0, \mu_{h_\rho}(\phi)|_{1\tau_\beta}, s)$ is the standard Rankin-Selberg L -function, $\tau_\beta = \begin{pmatrix} 0 & -1 \\ Jp^\beta & 0 \end{pmatrix}$ and $\langle, \rangle_{Nn^2m^2p}$ is the Petersson inner product.

The above theorem will be used to prove the congruence between the special values of $f \otimes \rho$ and $f \otimes \sigma$. The crucial point used in the proof is the linearity of the function $\mu_{\tilde{f}_0 \times h}$ in the variable h .

Let $W(h_\rho)$ denote the root number of h_ρ and $W(h_\rho) = \prod W_q(h_\rho)$ be the decomposition of $W(h_\rho)$ into local factors. We denote by $W'(h_\rho)$ the prime to p part of $W(h_\rho)$. We regard i_p as a character of \mathbb{Z}_p^\times and extend it to a function on \mathbb{Z}_p by defining it to be 0 outside \mathbb{Z}_p^\times . Let $P_p(\rho, X)$ denote the characteristic polynomial of ρ at p and h denote h_σ or h_ρ . Then the subscript $\{p, q|mn\}$ in $D_{\{p, q|mn\}}(f, h, 1)$ denotes that in the corresponding Rankin-Selberg L -function $D(f, h, 1)$, we have removed the Euler factors at p and at the prime divisors of mn .

In the following lemma, we shall evaluate the measure $\mu_{\tilde{f}_0 \times h}$ at the character i_p , and express it in terms of the Rankin-Selberg L -values $D_{p, q|nm}(f, h_\rho, 1)$ along with some other factors which occur in the formula for $R_f(\rho)$ in section 1. This mainly consists of unraveling the action of the operator $|_{1\tau_\beta}$ on the modular form $\mu_{h_\rho}(i_p)$. In carrying this out, we also isolate a power of p that occurs in the epsilon factor $\epsilon_p(\rho)$.

Lemma 3.3. *We have*

$$\begin{aligned} \mu_{\tilde{f}_0 \times h_\rho}(i_p) &= c(f)utW'(h_\rho)u^{-v_p(N_\rho)}\epsilon_p(\rho) \\ &\quad \times \frac{P_p(\rho, u^{-1})}{P_p(\rho, w^{-1})} \frac{D_{\{p, q|nm\}}(f, h_\rho, 1)}{2^3\pi^2 i^3 \langle \tilde{f}_0|_{2\tau_{Nn^2m^2p}}, \tilde{f}_0 \rangle_{Nn^2m^2p}}. \end{aligned}$$

Proof. We consider the case when $\delta > 0$. First we suppose that p is coprime to \mathfrak{f}_χ . Then χ is unramified at p . Therefore $\delta = 1$ and $\beta = 2$ [H, Lemma 5.2(i)]. In this case, the proof of Lemma 3.1 shows that $a(p, h_\rho) = 1$. Now from a similar computation as done in [B, Theorem 3.2] we get that

$$D(\tilde{f}_0, \mu_{h_\rho}(i_p)|_{1\tau_\beta}, 1) = p^{-1/2}W(h_\rho)uP_p(\rho, u^{-1})D(\tilde{f}_0, h_\rho, 1).$$

The p -part of the conductor of ρ is p . Therefore $\epsilon_p(\rho) = W_p(\rho)p^{1/2}$. Thus we get

$$u^{-\beta}p^{\beta/2}D(\tilde{f}_0, \mu_{h_\rho}(i_p)|_{1\tau_\beta}, 1) = u^{-v_p(N_\rho)}W'(h_\rho)\epsilon_p(\rho)P_p(\rho, u^{-1})D(\tilde{f}_0, h_\rho, 1),$$

where $W'(h_\rho)$ denotes the prime to p part of $W(h_\rho)$. Suppose that χ is ramified at p . In this case $a(p, h_\rho) = 0$ and $h_\rho|_{i_p} = h_\rho$. Therefore $\beta = \delta$. Again, by an argument similar to [B] we have

$$D(\tilde{f}_0, \mu_{h_\rho}(i_p)|_{1\tau_\beta}, 1) = W(h_\rho)P_p(\rho, u^{-1})D(\tilde{f}_0, h_\rho, 1).$$

Now the p -part of the conductor of ρ is p^β . We get

$$u^{-\beta}p^{\beta/2}D(\tilde{f}_0, \mu_{h_\rho}(i_p)|_{1\tau_\beta}, 1) = u^{-v_p(N_\rho)}W'(h_\rho)\epsilon_p(\rho)P_p(\rho, u^{-1})D(\tilde{f}_0, h_\rho, 1).$$

Next, suppose that $\delta = 0$. In this case $\beta = 2$. From [H, Lemma 5.2(i)] we have

$$\begin{aligned} u^{-\beta}p^{\beta/2}D(\tilde{f}_0, \mu_{h_\rho}(i_p)|_{1\tau_\beta}, 1) &= u^{-2}\epsilon_\chi|_{\mathbb{Z}}(p)W(h_\rho) \\ &\quad \times (1 - \overline{\epsilon_\chi}|_{\mathbb{Z}}(p)a(p, h_\rho)u + \overline{\epsilon_\chi}|_{\mathbb{Z}}(p)u^2)D(\tilde{f}_0, h_\rho, 1). \end{aligned}$$

Note that in the above formula we have used the fact that the Fourier coefficients of h_ρ are all real numbers. We have

$$(1 - \overline{\epsilon_\chi}|_{\mathbb{Z}}(p)a(p, h_\rho)u + \overline{\epsilon_\chi}|_{\mathbb{Z}}(p)u^2) = \overline{\epsilon_\chi}|_{\mathbb{Z}}(p)u^2P_p(\rho, u^{-1}).$$

Therefore we obtain

$$u^{-\beta}p^{\beta/2}D(\tilde{f}_0, \mu_{h_\rho}(i_p)|_{1\tau_\beta}, 1) = W'(h_\rho)D(\tilde{f}_0, h_\rho, 1).$$

In this case $W_p(h_\rho) = \epsilon_p(\rho) = 1$, as p does not divide N_ρ . Now the lemma follows from Theorem 3.2 and the fact that

$$D(\tilde{f}_0, h_\rho, 1) = P_p(h_\rho, w^{-1})^{-1}D_{\{p, q|nm\}}(f, h_\rho, 1).$$

□

The following lemma is the analogue of Lemma 3.3 for the representation σ . We remark that the form h_ρ is primitive, and hence one could directly apply [H, Lemma 5.2] in the above lemma. As $h_\sigma|i_m$ is not primitive, we need to argue differently in the next lemma.

Lemma 3.4. *We have*

$$\begin{aligned} \mu_{\tilde{f}_0 \times h_\sigma|i_m}(i_p) &= c(f)utW'(h_\sigma)m^{-1}\epsilon(m)u^{-v_p(N_\rho)}\epsilon_p(\sigma) \\ &\quad \times \frac{P_p(\sigma, u^{-1})}{P_p(\sigma, w^{-1})} \frac{D_{\{p, q|nm\}}(f, h_\sigma, 1)}{2^3\pi^2 i^3 \langle \tilde{f}_0|_{2\tau_{Nn^2m^2p}}, \tilde{f}_0 \rangle_{Nn^2m^2p}}. \end{aligned}$$

Proof. The proof of this lemma is analogous to the proof of [B, Theorem 3.2], where the special case when $p = D = 3$ is considered. We shall explain how the same can be derived in this general case. The problem can be divided into two cases. The first case is when $p|D$ and the second when $p \nmid D$. We shall explain the second case, as the first case is identical to [B, Theorem 3.2]. If $p \nmid D$, then $h_\sigma|i_m|i_p \in M_1(\Gamma_0(Dp^2m^2), \epsilon)$, that is, $\delta = 0$ and $\beta = 2$. Then for every $d|m^2$ there exists a constant c_d such that

$$h_\sigma|i_p|i_m = \sum_{d|m^2} c_d h_\sigma|i_p|[d_i],$$

where $[d_i]$ denotes the matrix $\begin{pmatrix} d_i & 0 \\ 0 & 1 \end{pmatrix}$. Now by a computation similar to [B, Theorem 3.2] we have

$$h_\sigma|[p^j d]|_{1\tau_{Dp^2m^2}} = p^{1-j}md^{-1}W(h_\sigma)h_\sigma|[p^{2-j}m^2/d],$$

where j can take values from 0 to 2. We also have

$$\begin{aligned} & h_\sigma |i_p|[d]|_1 \tau_{Dp^2m^2} \\ &= (h_\sigma - a(p, h_\sigma)h_\sigma|[p] + \epsilon(p)h_\sigma|[p^2])|[d]|_1 \tau_{Dp^2m^2} \\ &= p^{-1}d^{-1}mW(h_\sigma)(p^2h_\sigma|[p^2m^2/d] - pa(p, h_\sigma)h_\sigma|[pm^2/d] + \epsilon(p)h_\sigma|[m^2/d]). \end{aligned}$$

Using the fact that \tilde{f}_0 has no Euler factor at primes dividing m , it can be shown that the Rankin-Selberg convolution $D(\tilde{f}_0, h_\sigma |i_p|[d_i]|_1 \tau_{Dp^2m^2}, 1)$ is non-zero only if $d = m^2$. Also an easy computation shows that $c_{m^2} = \epsilon(m)$. Therefore we have

$$\begin{aligned} & D(\tilde{f}_0, h_\sigma |i_p|i_m|_1 \tau_{Dp^2m^2}, 1) \\ &= \epsilon(m)D(\tilde{f}_0, h_\sigma |i_p|[m^2]|_1 \tau_{Dp^2m^2}, 1) \\ &= \epsilon(m)p^{-1}m^{-1}W(h_\rho)D(\tilde{f}_0, p^2h_\sigma|[p^2] - pa(p, h_\sigma)h_\sigma|[p] + \epsilon(p)h_\sigma, 1) \\ &= \epsilon(m)p^{-1}m^{-1}W(h_\rho)(u^2 - a(p, h_\sigma)u + \epsilon(p))D(\tilde{f}_0, h_\sigma, 1) \\ &= \epsilon(m)p^{-1}m^{-1}W(h_\rho)u^2P_p(h_\sigma, u^{-1})D(\tilde{f}_0, h_\sigma, 1). \end{aligned}$$

Since $p \nmid D$ we have $W_p(h_\sigma) = 1$. Therefore we can write

$$u^{-\beta}p^{\beta/2}D(\tilde{f}_0, h_\sigma |i_m|i_p|_1 \tau_{Dp^2m^2}, 1) = m^{-1}\epsilon(m)W'(h_\rho)P_p(h_\sigma, u^{-1})D(\tilde{f}_0, h_\sigma, 1).$$

Now the result follows by using the formula

$$D(\tilde{f}_0, h_\rho, 1) = P_p(h_\sigma, w^{-1})^{-1}D_{\{p, q|m\}}(f, h_\sigma, 1)$$

and the fact that $\epsilon_p(h_\sigma) = 1$ and $v_p(N_\sigma) = 0$. \square

Remark 3.5. So far we have assumed that p does not divide N_f . But we remark that a similar congruence formula holds under the weaker assumption that $p|N_f$ (resp. $p|N_g$) but $p^2 \nmid N_f$ (resp. $p^2 \nmid N_g$). We still need to assume that f is ordinary at p . In this case $f_0 = f$ and $\tilde{f}_0 = f|i_{nm}$, where n is defined to be the prime to p part of N/\bar{N}_f . Further,

$$D(\tilde{f}_0, h_\rho, 1) = D_{\{q|nm\}}(f, h_\rho, 1)$$

and

$$D(\tilde{f}_0, h_\sigma, 1) = D_{\{q|nm\}}(f, h_\sigma, 1).$$

Thus in this case the denominator $P_p(\rho, w_f)$ (resp. $P_p(\rho, w_g)$) and $P_p(\sigma, w_f)$ (resp. $P_p(\sigma, w_g)$) will not appear in the formula for $\mu_{\tilde{f}_0 \times h_\rho}(i_p)$ (resp. $\mu_{\tilde{f}_0 \times h_\sigma}(i_p)$). Furthermore, we need not remove the Euler factors at p in this case. In the rest of the paper, for simplicity we shall continue to assume that the level of the modular forms f and g are coprime to p .

Let ϕ be a primitive Dirichlet character of conductor p^γ for some integer $\gamma \geq 1$ and $\bar{\phi}$ be its complex conjugation. Let γ' denote the conductor of $\epsilon\chi|_{\mathbb{Z}}$. For a Dirichlet character η and a modular form h let $h|\eta := \sum_n \eta(n)a(n, h)q^n$ denote the twist of h by η . In the rest of this section we shall compute the value of $\mu_{\tilde{f}_0 \times h_\rho}(\bar{\phi})$ and $\mu_{\tilde{f}_0 \times h_\sigma|i_m}(\bar{\phi})$. First, we suppose that $\phi = (\epsilon\chi|_{\mathbb{Z}})_p$, i.e. the p -part of the character $\epsilon\chi|_{\mathbb{Z}}$. Note that $(\epsilon\chi|_{\mathbb{Z}})_p$ is non-trivial only if $p|D$, where we recall that D denotes the discriminant of K/\mathbb{Q} . Let $r = r_1r_2$ be a positive integer prime to p , where r_1 is the product of primes which split in K and r_2 is the product of primes which remain inert in K . Then $(\epsilon\chi|_{\mathbb{Z}})_p(r) = -1$ if and only if r_2 is not a square. If r_2 is not a square, then there is no ideal of K whose norm is r_2 . This

shows that $a(r, h_\rho) = a(r, h_\sigma) = 0$. We also have that $(\epsilon\chi|_{\mathbb{Z}})_p(r) = 1$ if and only if r_2 is a square. This shows that $h_\rho|_\phi = h_\rho|_{i_p}$ and $h_\sigma|_\phi = h_\sigma|_{i_p}$. Thus in this case the value $\mu_{\tilde{f}_0 \times h_\rho}(\bar{\phi}) = \mu_{\tilde{f}_0 \times h_\rho}(i_p)$ and $\mu_{\tilde{f}_0 \times h_\sigma|_{i_m}}(\bar{\phi}) = \mu_{\tilde{f}_0 \times h_\sigma|_{i_m}}(i_p)$. Therefore in the rest of this section we shall assume that $\phi \neq (\epsilon\chi|_{\mathbb{Z}})_p$. First we need the following definition. Let h be a Hecke eigenform and π_p be the local automorphic representation associated to h at p . Then we say that h is p -minimal if either π_p is supercuspidal or the conductor of h is minimal among all its twists by a character of p -power conductor. In the next two lemmas, we evaluate the measure $\mu_{\tilde{f}_0 \times h_\rho}$ (respectively $\mu_{\tilde{f}_0 \times h_\sigma}$) at the Dirichlet character $\bar{\phi}$.

Lemma 3.6. *Suppose that h_ρ is p -minimal, and let $\bar{\phi}$ be the complex conjugate of ϕ . Then we have*

$$\begin{aligned} \mu_{\tilde{f}_0 \times h_\rho}(\bar{\phi}) &= c(f)utW'(h_\rho|\bar{\phi})u^{-v_p(N_{\rho\bar{\phi}})}\epsilon_p(\rho\bar{\phi}) \\ &\quad \times \frac{D_{\{p,q|nm\}}(f, h_\rho|\phi, 1)}{2^3\pi^2 i^3 \langle \tilde{f}_0|_{2\tau N n^2 m^2 p}, \tilde{f}_0 \rangle_{N n^2 m^2 p}}. \end{aligned}$$

Proof. Let π_p denote the local automorphic representation associated to h_ρ at p . We first assume that π_p is either a principal series representation $\pi_p(\alpha, \alpha')$ with α unramified or a special representation $\sigma(\alpha, \alpha')$ for quasi-characters α, α' of \mathbb{Q}_p^\times . Then it is shown in [H, Lemma 5.2(i)] that $\beta = \gamma + \gamma'$ and

$$(h_\rho|\bar{\phi})|_{1\tau_\beta} = W(h_\rho|\bar{\phi})\bar{h}_\rho|\phi,$$

where \bar{h}_ρ denote the complex conjugate of h_ρ . From Lemma 3.1 we have that $\bar{h}_\rho = h_\rho$. Thus we have

$$(h_\rho|\bar{\phi})|_{1\tau_\beta} = W(h_\rho|\bar{\phi})h_\rho|\phi.$$

From [H, 5.4(c)] we have that

$$W(h_\rho|\bar{\phi}) = W'(h_\rho)\phi(J)W_p(h_\rho|\bar{\phi}).$$

Therefore we get

$$p^{\beta/2}D(\tilde{f}_0, \mu_h(\phi)|_{1\tau_\beta}, 1) = W'(h_\rho)\phi(J)p^{\beta/2}W_p(h_\rho|\bar{\phi})D(\tilde{f}_0, h_\rho|\phi, 1).$$

Since we have assumed that $\bar{\phi} \neq \epsilon\chi|_{\mathbb{Z}}$ and ϕ is non-trivial, we have $\gamma > 0$, $\gamma' > 0$ and $h_\rho|\bar{\phi}$ is primitive. Thus the conductor $N_{\rho\bar{\phi}}$ of $\rho\bar{\phi}$ is $Jp^\gamma p^{\gamma'}$, and therefore $v_p(N_{\rho\bar{\phi}}) = \beta = \gamma + \gamma'$. Further, we also have that $\epsilon_p(\rho\bar{\phi}) = p^{\beta/2}W_p(h_\rho|\bar{\phi})$. Therefore we get that

$$u^{-\beta}p^{\beta/2}D(\tilde{f}_0, \mu_h(\phi)|_{1\tau_\beta}, 1) = W'(h_\rho)\phi(J)u^{-v_p(N_{\rho\bar{\phi}})}\epsilon_p(\rho\bar{\phi})D(\tilde{f}_0, h_\rho|\phi, 1).$$

Now using Theorem 3.2 and the fact that

$$D(\tilde{f}_0, h_\rho|\phi, 1) = D_{\{p,q|nm\}}(f, h_\rho|\phi, 1),$$

we get the desired formula. We mention that due to our assumption ϕ is non-trivial and $\bar{\phi} \neq (\epsilon\chi|_{\mathbb{Z}})_p$, $P_p(h_\rho|\bar{\phi}, X) = 1$. Now we assume that π_p is supercuspidal at p . In this case $h_\rho|\bar{\phi}$ is primitive (see [H, Lemma 5.2(ii)]). The possible values of β can be obtained from loc. cit. Thus

$$(h_\rho|\bar{\phi})|_{1\tau_\beta} = W(h_\rho|\bar{\phi})\bar{h}_\rho|\phi = W'(h_\rho|\bar{\phi})W_p(h_\rho|\bar{\phi})\bar{h}_\rho|\phi.$$

Now the proof follows by a method similar to the previous case. \square

Lemma 3.7.

$$\begin{aligned} \mu_{\tilde{f}_0 \times h_\sigma | i_m}(\bar{\phi}) &= c(f) utW'(h_\sigma | \bar{\phi}) u^{-v_p(N_{\sigma \bar{\phi}})} \epsilon_p(\sigma \bar{\phi}) \\ &\times \frac{D_{\{p, q | nm\}}(f, h_\sigma | \phi, 1)}{2^3 \pi^2 i^3 \langle \tilde{f}_0 |_{2\tau_{Nn^2m^2p}}, \tilde{f}_0 \rangle_{Nn^2m^2p}}. \end{aligned}$$

Proof. Let β be the smallest integer such that $h_\sigma | \bar{\phi} | i_m \in S_1(\Gamma_1(D'p^\beta m^2))$. Recall that D' denotes the prime to p part of D . Since we have assume that $\bar{\phi}$ is non-trivial and $\bar{\phi} \neq (\epsilon\chi|_{\mathbb{Z}})_p$, $\gamma \geq 1$ and $\gamma' \geq 1$. Therefore $\beta = \gamma + \gamma'$ and

$$h_\sigma | \bar{\phi} |_{1\tau_{D'p^\beta}} = W(h_\sigma | \bar{\phi}) h_\sigma | \phi.$$

For every $d|m^2$ there exist constants c_d such that

$$h_\sigma | i_m = \sum_{d|m^2} c_d h_\sigma | [d].$$

Therefore,

$$h_\sigma | i_m | \bar{\phi} = \sum_{d|m^2} c_d h_\sigma | \bar{\phi} | [d].$$

By a computation similar to [B, Theorem 3.2] we have

$$h_\sigma | \bar{\phi} | [d] |_{1\tau_{Dp^\beta m^2}} = d^{-1} m W(h_\sigma | \bar{\phi}) h_\sigma | \phi | [m^2/d].$$

Since \tilde{f}_0 has no Euler factor at primes dividing m , we have that the Rankin-Selberg L -function $D(\tilde{f}_0, h_\sigma | \phi | [d_i] |_{1\tau_{Dp^2m^2}}, 1)$ is non-zero only when $d = m^2$. Therefore,

$$D(\tilde{f}_0, h_\sigma | i_m | \bar{\phi} |_{1\tau_{Dp^2m^2}}, 1) = \epsilon(m) m^{-1} W(h_\sigma | \bar{\phi}) D(\tilde{f}_0, h_\sigma | \phi, 1).$$

In the above formula we have used the fact that $c_{m^2} = \epsilon(m)$. The rest of the computation is analogous to the computations in the proof of Lemma 3.4 and Lemma 3.6, and we again have the desired formula. \square

4. PERIODS FOR MODULAR FORMS

Let Ω_h^+ and Ω_h^- denote the canonical periods associated to a Hecke eigenform h of level M and weight 2 satisfying conditions 1 and 2 stated in [V]. We recall these conditions now. Let \mathfrak{m} denote the maximal ideal of $h_2(\Gamma_1(M); \mathbb{Z}_p)$ associated to the congruence class of the form h . The form h induces a \mathbb{Q}_p -algebra homomorphism

$$\pi_h : h_2(\Gamma_1(M); \mathbb{Z}_p)_{\mathfrak{m}} \otimes \mathbb{Q}_p \longrightarrow \mathbb{Q}_p.$$

Let R_h denote the unique local factor of the Hecke algebra through which π_h factors. For any module B over the Hecke algebra $h_2(\Gamma_1(M); \mathbb{Z}_p)$, let $B_{\mathfrak{m}}$ denote the localization of B at \mathfrak{m} . We fix an isomorphism $\mathbb{C} \cong \mathbb{C}_p$. Let A be a subring of \mathbb{C} (or \mathbb{C}_p). The Hecke algebra $h_2(\Gamma_1(M); A)$ acts on the Eichler-Shimura cohomology group $H^1(\Gamma_1(M), A)$ and its parabolic subgroup $H_p^1(\Gamma_1(M), A)$. Let $H^1(\Gamma_1(M), \mathbb{Z}_p)_{\mathfrak{m}}$ denote the localization of $H^1(\Gamma_1(M), \mathbb{Z}_p)$ at \mathfrak{m} . The complex conjugation action on the group $H^1(\Gamma_1(M), A)$ decomposes it into the $+$ and $-$ eigenspaces, denoted respectively by $H^1(\Gamma_1(M), A)^+$ and $H^1(\Gamma_1(M), A)^-$. The conditions in [V] are:

1. $R_h = \mathbb{Q}_p$.

2. There exist isomorphisms of $h_2(\Gamma_1(M); \mathbb{Z}_p)$ -modules

$$\begin{aligned} \theta^\pm : H^1(\Gamma_1(M), \mathbb{Z}_p)_{\mathfrak{m}}^\pm &= H_p^1(\Gamma_1(M), \mathbb{Z}_p)_{\mathfrak{m}}^\pm \cong \text{Hom}_{\mathbb{Z}_p}(h_2(\Gamma_1(M); \mathbb{Z}_p), \mathbb{Z}_p)_{\mathfrak{m}} \\ &\cong S_2(\Gamma_1(M); \mathbb{Z}_p)_{\mathfrak{m}}. \end{aligned}$$

If we take $h = \tilde{f}_0$, then it follows from [Wi, Theorem 2.1] (see also, [V, Theorem 1.13]) that condition 2 is satisfied. Note that p is an odd prime and the weight of \tilde{f}_0 is 2; therefore the residual representation associated to \tilde{f}_0 is p -distinguished. The first equality in condition 2 is a consequence of the assumption that the residual representation is irreducible. Let \mathfrak{m}_0^ψ denote the restriction of the maximal ideal \mathfrak{m} of $h_2(\Gamma_1(\bar{N}pm^2n^2); \mathbb{Z}_p)$ in $h_2(\Gamma_0(\bar{N}pm^2n^2), \psi; \mathbb{Z}_p)$. Then we have the following isomorphism of \mathbb{Z}_p -algebras:

$$h_2(\Gamma_1(\bar{N}pm^2n^2); \mathbb{Z}_p)_{\mathfrak{m}} \cong h_2(\Gamma_0(\bar{N}pm^2n^2), \psi; \mathbb{Z}_p)_{\mathfrak{m}_0^\psi}.$$

This follows from the fact that the Hecke algebra $h_2(\Gamma_1(\bar{N}pm^2n^2); \mathbb{Z}_p)$ splits as a product of $h_2(\Gamma_0(\bar{N}pm^2n^2), \psi; \mathbb{Z}_p)$, where ψ varies over the finite set of characters of the group $(\mathbb{Z}/(\bar{N}pm^2n^2))^\times$. We shall drop the character ψ from the notation \mathfrak{m}_0^ψ if ψ is the trivial character. Thus condition 1 stated in [V] follows from the fact that the \mathbb{Q}_p -algebra homomorphism

$$h_2(\Gamma_0(\bar{N}pm^2n^2), \mathbb{Z}_p)_{\mathfrak{m}_0} \otimes \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$$

induces a splitting

$$h_2(\Gamma_0(\bar{N}pm^2n^2); \mathbb{Z}_p)_{\mathfrak{m}_0} \otimes \mathbb{Q}_p \cong \mathbb{Q}_p \times A$$

([B, Section 4]). We mention that in [B], this splitting is obtained under the assumption that N is square free by using results proved in [DDT, Section 4]. But it is not difficult to see that the same proof works under the weaker assumption that \bar{N} is square free, with N/\bar{N} and \bar{N} being mutually coprime. We briefly explain this fact. Following the notation of *loc. cit.*, let Σ denote the set of finite primes of \mathbb{Q} consisting of the prime divisors of N/\bar{N} and m . Let N_Σ denote the integer $\bar{N}p \prod_{q \in \Sigma} q^2$.

Let $\bar{\rho}$ and $\bar{\sigma}$ respectively denote the residual representation of ρ and σ at p with the prime to p part of their conductor $N_{\bar{\rho}}$ and $N_{\bar{\sigma}}$ respectively. Recall that $N_{\bar{\rho}} = |D|N_{K/\mathbb{Q}}(\mathfrak{f}_\chi)$ and D' is the prime to p part of D . By assumption (ii) it implies that the prime to p part of $N_{\bar{\rho}}/D'$ and D' are coprime. By the definition of χ we have that $\chi^{p^t} = \mathbf{1}$. Therefore $\chi \equiv \mathbf{1} \pmod{\mathfrak{p}}$, where \mathfrak{p} denotes the unique prime of $\mathbb{Q}(\mu^t)$ lying above p . This implies that $\bar{\rho} = \bar{\sigma}$. Therefore $N_{\bar{\rho}} = N_{\bar{\sigma}}$. Since σ is the sum of the trivial character and a quadratic character we have $N_{\bar{\sigma}} = D$. Further, the prime to p part of $N_{\bar{\sigma}}$ is $N_{\bar{\sigma}}$, and therefore $N_{\bar{\sigma}} = D'$. Now it follows from [DDT, Lemma 2.7] that $N_{\bar{\rho}}/N_{\bar{\rho}}$ is cube free. Therefore $N_{\bar{\rho}}/D'$ is cube free. But the prime to p part of $N_{\bar{\rho}}/D'$ is m^2 , and hence the integer m is square free. Further, the assumption that \bar{N} is coprime to N/\bar{N} implies that N/\bar{N} is cube free (See [DDT, Lemma 2.7]). Therefore N_Σ is the same as $\bar{N}pn^2m^2$. Consider the Hecke eigenform g' of level N_Σ defined by the following:

- $a(q, g') = a(q, f)$ if $q \nmid N_\Sigma/N$;
- $a(q, g') = 0$ if $q | N_\Sigma/N$;
- $a(q, g') = u_f$ if $q = p$.

Then it is shown in [DDT, Lemma 4.6] that the maximal ideal \mathfrak{m}_0 of $h_2(N_\Sigma; \mathbb{Z}_p)$ determined by the form f corresponds to the congruence class of g' . Further it is also shown in [B, Section 4] that $h_2(N_\Sigma; \mathbb{Z}_p)_{\mathfrak{m}_0}$ is a reduced \mathbb{Z}_p -algebra, and that the \mathbb{Q}_p -algebra homomorphism

$$h_2(\Gamma_0(N_\Sigma), \mathbb{Z}_p)_{\mathfrak{m}_0} \otimes \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$$

induced by g' induces a splitting

$$h_2(\Gamma_0(N_\Sigma; \mathbb{Z}_p))_{\mathfrak{m}_0} \otimes \mathbb{Q}_p \cong \mathbb{Q}_p \times A.$$

Note that the form g' coincides with the modular form \tilde{f}_0 . Therefore the condition 1 of [V] holds, and we have

Lemma 4.1. *The canonical periods $\Omega_{\tilde{f}_0}^\pm$ exist.* □

Remark 4.2. We remark that for the existence of the above period, we have crucially used the fact that the algebra $h_2(N_\Sigma; \mathbb{Z}_p)_{\mathfrak{m}_0}$ is reduced. This in turn relies on the results proved in [DDT], [Wi] and [B]. The proof of these results depend on the assumption that \bar{N}_f is square free. But this assumption can be relaxed. In fact, the semisimplicity of this Hecke algebra is still true at weight two as long as N_Σ is cube free (see [CE]). But we shall continue to assume that \bar{N}_f is square free, as we need this assumption to compare the periods which appear in [V] and [B]. We strongly believe that it should be possible to remove this assumption, though we have been unable to do this at present.

Next we shall compare the period $\Omega_{\tilde{f}_0}^+ \Omega_{\tilde{f}_0}^-$ with the period $\Omega_f^+ \Omega_f^-$. We shall begin by recalling the definition of these periods. Let $h = \sum_n a(n, h) q^n$ be a Hecke eigenform of level M satisfying conditions 1 and 2 above, $\omega_h = \sum_n a(n, h) q^{n-1} dq$ be the holomorphic differential form in $H_p^1(\Gamma(M), \mathbb{C})$ associated to h and $\bar{\omega}_h = \sum_n a(n, h) \bar{q}^{n-1} d\bar{q}$, where the bar denotes complex conjugation. Put $\omega_h^+ = (\omega_h + \bar{\omega}_h)/2$ and $\omega_h^- = (\omega_h - \bar{\omega}_h)/2$. Consider the cocycles δ_h^\pm defined by $\theta^\pm(\delta_h^\pm) = h$. Then the periods Ω_h^\pm are defined as the scalars such that $\omega_h^\pm = \Omega_h^\pm \delta_h^\pm$. Such scalars exist by condition 1 (see [V]). These periods are well defined only up to a multiple of a p -adic unit which depends on the choice of the isomorphism in condition 2. Let A_h denote the complex matrix such that $(\omega_h, \bar{\omega}_h) = (\delta_h^+, \delta_h^-) A_h$. Then we have that $(-1/2) \det(A_h) = \Omega_h^+ \Omega_h^-$. To compare the two periods associated to $f|_{i_n}$ and \tilde{f}_0 , we need to compare $A_{f|_{i_n}}$ and $A_{\tilde{f}_0}$. But it follows from the proof of [DDT, Theorem 3.36] that in fact $A_{f|_{i_n}} = A_{\tilde{f}_0}$. We mention that in [DDT] the case of the congruence subgroup $\Gamma_0(M)$ is considered. But the same proof works for $\Gamma_1(M)$ as well. Now it is shown in [GV, Lemma 3.6] that up to a factor of a p -adic unit, $\Omega_{f|_{i_n}}^\pm$ is the same as Ω_f^\pm . Therefore we have,

Lemma 4.3. *The numbers $\Omega_f^+ \Omega_f^-$ and $\Omega_{\tilde{f}_0}^+ \Omega_{\tilde{f}_0}^-$ are equal up to a factor which is a p -adic unit.* □

Next we shall compare the periods considered in [V] with the periods considered in [B]. We recall the definition of the period considered in [B]. Let θ_0^\pm be the map considered in condition 2 after replacing the congruence subgroup $\Gamma_1(M)$ with $\Gamma_0(M)$. We mention that if $h = \tilde{f}_0$, then condition 2 holds even for $\Gamma_0(\bar{N}n^2m^2p)$. For a Hecke eigenform h in $S_2(M; \mathbb{Z})$ let x_h^\pm denote the image of h by the inverse of θ_0^\pm . Then there exists a complex matrix A_h^0 such that $(\omega_h, \bar{\omega}_h) = (x_h^+, x_h^-) A_h^0$. Then the period Ω_h considered in [B] is defined as the determinant of A_h^0 . Now

consider the following commutative diagram:

$$\begin{array}{ccc} H^1(\Gamma_0(\bar{N}n^2m^2p); \mathbb{Z}_p)_{\mathfrak{m}_0}^{\pm} & \xrightarrow{i} & H^1(\Gamma_1(\bar{N}n^2m^2p); \mathbb{Z}_p)_{\mathfrak{m}}^{\pm} \\ \downarrow \theta_0^{\pm} & & \downarrow \theta^{\pm} \\ S_2(\Gamma_0(\bar{N}n^2m^2p); \mathbb{Z}_p)_{\mathfrak{m}_0} & \xrightarrow{j} & S_2(\Gamma_1(\bar{N}n^2m^2p); \mathbb{Z}_p)_{\mathfrak{m}} \end{array}$$

The horizontal map j is an isomorphism. This follows from the fact that

$$h_2(\Gamma_0(\bar{N}n^2m^2p); \mathbb{Z}_p)_{\mathfrak{m}_0} \cong h_2(\Gamma_1(\bar{N}n^2m^2p); \mathbb{Z}_p)_{\mathfrak{m}}$$

is an isomorphism. Since the two vertical maps are isomorphisms, we get that the horizontal map i is also an isomorphism. It then follows from the above diagram that the image of $x_{f_0}^{\pm}$ under the inclusion i is the same as $\delta_{f_0}^{\pm}$. Therefore, up to an invertible element in $GL_2(\mathbb{Z}_p)$, which depends on the choice of the isomorphism θ^{\pm} , we have $A_{\tilde{f}_0}^0 = A_{f_0}$. Therefore we have

Lemma 4.4. *The numbers $\Omega_{\tilde{f}_0}$ and $\Omega_{f_0}^+ \Omega_{f_0}^-$ are the same up to a factor which is a p -adic unit.* \square

We end this section by mentioning that it is known that the period $\pi^2 \Omega_{\tilde{f}_0}$ is the same as $\Omega_{E_f}^+ \Omega_{E_f}^-$ up to a factor of a p -adic unit, where $\Omega_{E_f}^{\pm}$ are the Néron periods associated to the elliptic curve E_f associated to f (see [B, Theorem 4.8, 4.9]). This follows from the works of Wiles, Diamond-Flach-Guo and Hida (see [DFG], [H2] and [Wi]).

5. CONGRUENCE FORMULA

In this section we shall prove the inequality (3). Recall that f and g are p -ordinary weight 2 new Hecke eigenforms of level N_f and N_g respectively with equivalent residual representation at the odd prime p . The prime to p conductor of this residual representation is denoted by \bar{N} . The number u_f (resp. u_g) denotes the p -adic unit root of the Hecke polynomial of f (resp. g). The modular form f_0 (resp. g_0) is the p -stabilization of f (resp. g) and i_n denotes the trivial Dirichlet character mod n with $n = l.c.m.(N_f, N_g)/\bar{N}$. Also \tilde{f}_0 (resp. \tilde{g}_0) denotes the modular form $f_0|i_n$ (resp. $g_0|i_n$). Recall that the integer m^2 is the prime to p part of $N_{K/\mathbb{Q}}(\mathfrak{f}_{\chi})$.

In the theorem below, we prove the congruence between the special values of $f \otimes \rho$ and $f \otimes \sigma$ using the linearity of $\mu_{\tilde{f}_0 \times h}$ in the variable h and the congruence between h_{ρ} and h_{σ} . We continue with the notation as in the earlier section.

Theorem 5.1. *We have*

$$\begin{aligned} W'(h_{\rho}) u_f^{-v_p(N_{\rho})} \epsilon_p(\rho) &\times \frac{P_p(\rho, u^{-1})}{P_p(\rho, w^{-1})} \frac{L_{\{p, q|nm\}}(f, \rho, 1)}{2^3 \pi^2 i^3 \Omega_{\tilde{f}_0}} \\ &\equiv W'(h_{\sigma}) m^{-1} \epsilon(m) u_f^{-v_p(N_{\sigma})} \epsilon_p(\sigma) \times \frac{P_p(\sigma, u^{-1})}{P_p(\sigma, w^{-1})} \frac{L_{\{p, q|nm\}}(f, \sigma, 1)}{2^3 \pi^2 i^3 \Omega_{\tilde{f}_0}} \pmod{p}. \end{aligned}$$

Proof. Since $\bar{\rho} = \bar{\sigma}$, we have $a(q, h_{\sigma}) \equiv a(q, h_{\rho}) \pmod{p}$ for all q coprime to pm . Therefore $h_{\sigma}|i_m|i_p \equiv h_{\rho}|i_p \pmod{p}$. This shows that

$$\mu_{\tilde{f}_0 \times h_{\rho}}(i_p) \equiv \mu_{\tilde{f}_0 \times h_{\sigma}|i_m}(i_p) \pmod{p}.$$

From the discussion in [B, Section 4], we can choose $c(f)$ such that

$$\frac{c(f)}{\langle \tilde{f}_0 | 2\tau_{Nn^2m^2p}, \tilde{f}_0 \rangle_{Nn^2m^2p}} = \frac{1}{\Omega_{\tilde{f}_0}}.$$

Now we have

$$D_{\{p,q|nm\}}(f, \rho, 1) = L_{\{p,q|nm\}}(f, \rho, 1).$$

Note that here we have used the fact that N is coprime to N_ρ . Indeed, if there exists a prime q such that q^2 divides N_f and q divides N_ρ , then the above equality may not hold. Now the theorem follows by using Lemma 3.3, Lemma 3.4 and the fact that u_f is a p -adic unit. \square

The results proved so far for the modular form f can be similarly obtained for g as well. We now state our main result. Note that in the congruence formula (5) below, the left hand side is precisely the number $R_f(\rho)$ and the right hand side is the number $R_g(\rho)$.

Theorem 5.2. *We have*

$$\begin{aligned} u_f^{-v_p(N_\rho)} \epsilon_p(\rho) \frac{P_p(\rho, u_f^{-1})}{P_p(\rho, w_f^{-1})} \frac{L_{\{p,q|nm\}}(f, \rho, 1)}{(-2\pi i \Omega_f^+)(-2\pi i \Omega_f^-)} \\ (5) \quad \equiv u_g^{-v_p(N_\rho)} \epsilon_p(\rho) \frac{P_p(\rho, u_g^{-1})}{P_p(\rho, w_g^{-1})} \frac{L_{\{p,q|nm\}}(g, \rho, 1)}{(-2\pi i \Omega_g^+)(-2\pi i \Omega_g^-)} \pmod{p}. \end{aligned}$$

The proof of the above theorem is an immediate consequence of Theorem 5.1, Lemma 4.3, Lemma 4.4 and the next lemma. Note that in the formula for $R_f(\rho)$, $P_p(\hat{\rho}, u_f^{-1})$ appears in the numerator, whereas in Theorem 5.2, we have $P_p(\rho, u_f^{-1})$. But in our case, ρ is self-dual, and hence ρ and $\hat{\rho}$ are equivalent. Now, using the results in [GV] and [V] and the fact that σ is a sum of two Dirichlet characters, we show that the special values of $f \otimes \sigma$ and $g \otimes \sigma$ are congruent mod p .

Lemma 5.3. *We have*

$$\begin{aligned} W'(h_\sigma) m^{-1} \epsilon(m) u^{-v_p(N_\rho)} \epsilon_p(\sigma) \times \frac{P_p(\sigma, u_f^{-1})}{P_p(\sigma, w_f^{-1})} \frac{L_{\{p,q|nm\}}(f, \sigma, 1)}{(-2\pi i \Omega_{f_0}^+)(-2\pi i \Omega_{f_0}^-)} \\ \equiv W'(h_\sigma) m^{-1} \epsilon(m) u^{-v_p(N_\rho)} \epsilon_p(\sigma) \times \frac{P_p(\sigma, u_g^{-1})}{P_p(\sigma, w_g^{-1})} \frac{L_{\{p,q|nm\}}(g, \sigma, 1)}{(-2\pi i \Omega_{g_0}^+)(-2\pi i \Omega_{g_0}^-)} \pmod{p}. \end{aligned}$$

Proof. By assumption we have $a(q, f) \equiv a(q, g) \pmod{p}$ for all primes $q \nmid N$. This says that the residual representations associated to f and g are isomorphic and $\bar{N}_f = \bar{N}_g$. Now let q be a prime dividing \bar{N}_f . Then it follows from [DDT, Lemma 4.6] that $a(q, f) \equiv a(q, g) \pmod{p}$. Thus we have $a(q, f) \equiv a(q, g) \pmod{p}$ for all primes q not dividing nm . Therefore $a(q, \tilde{f}_0) \equiv a(q, \tilde{g}_0) \pmod{p}$ for all primes q .

Consider the Artin representation $\sigma = \mathbf{1} \oplus \epsilon$ where ϵ is the non-trivial quadratic character of $\text{Gal}(K/\mathbb{Q})$. We first assume that $p \nmid D$. Then we have

$$u^{-v_p(N_\epsilon)} \tau_p(\epsilon^{-1}) \frac{L(\tilde{f}_0, \epsilon, 1)}{(-2\pi i \Omega_{\tilde{f}_0}^-)} \equiv u^{-v_p(N_\epsilon)} \tau_p(\epsilon^{-1}) \frac{L(\tilde{g}_0, \epsilon, 1)}{(-2\pi i \Omega_{\tilde{g}_0}^-)} \pmod{p},$$

where $\tau_p(\epsilon^{-1})$ is the local Gauss sum for ϵ^{-1} at p and N_ϵ denotes the conductor of ϵ . The above statement follows from [V, Theorem 1.10]. We also have

$$(1 - u_f^{-1}) \frac{L(\tilde{f}_0, 1)}{(-2\pi i \Omega_{\tilde{f}_0}^+)} \equiv (1 - u_g^{-1}) \frac{L(\tilde{g}_0, 1)}{(-2\pi i \Omega_{\tilde{g}_0}^+)} \pmod{p}.$$

Further, $\epsilon^{-1} = \epsilon$ and $\tau_p(\epsilon) = \epsilon_p(\sigma)$. Since $P_p(\sigma, T) = 1 - T$ and $N_\epsilon = N_\sigma$,

$$\begin{aligned} u^{-v_p(N_\rho)} \epsilon_p(\rho) P_p(\sigma, u_f^{-1}) \frac{L(\tilde{f}_0, \epsilon, 1)}{(-2\pi i \Omega_{\tilde{f}_0}^-)} \frac{L(\tilde{f}_0, 1)}{(-2\pi i \Omega_{\tilde{f}_0}^+)} \\ \equiv u^{-v_p(N_\rho)} \epsilon_p(\rho) P_p(\sigma, u_g^{-1}) \frac{L(\tilde{g}_0, \epsilon, 1)}{(-2\pi i \Omega_{\tilde{g}_0}^-)} \frac{L(\tilde{g}_0, 1)}{(-2\pi i \Omega_{\tilde{g}_0}^+)} \pmod{p}. \end{aligned}$$

We have $L(\tilde{f}_0, 1)L(\tilde{f}_0, \epsilon, 1) = L(\tilde{f}_0, \sigma, 1)$ and

$$L(\tilde{f}_0, \sigma, 1) = \frac{L_{\{p, q|mn\}}(f, \sigma, 1)}{P_p(\sigma, w_f^{-1})}.$$

Now the lemma follows from the fact that $W'(h_\sigma)m^{-1}\epsilon(m)$ is a p -adic unit.

We next consider the case when $p \nmid D$. In this case p does not divide the conductor of ϵ . Therefore $v_p(N_\sigma) = 0$ and $\epsilon_p(\sigma) = 1$. Thus we have the following congruence formula:

$$(1 - \epsilon(p)u_f^{-1}) \frac{L(\tilde{f}_0, \epsilon, 1)}{(-2\pi i \Omega_{\tilde{f}_0}^-)} \equiv (1 - \epsilon(p)u_g^{-1}) \frac{L(\tilde{g}_0, \epsilon, 1)}{(-2\pi i \Omega_{\tilde{g}_0}^-)} \pmod{p}.$$

The rest of the argument is analogous to the previous case. Note that in this case

$$P_p(\sigma, u_f^{-1}) = (1 - u_f^{-1})(1 - \epsilon(p)u_f^{-1}).$$

□

Let ϕ be a non-trivial primitive Dirichlet character of a p -power conductor. Assume that $\phi \neq (\epsilon\chi|_{\mathbb{Z}})_p$. Then using Lemma 3.6 and Lemma 3.7 the following theorem can be proved using a method analogous to the proof of Theorem 5.1.

Theorem 5.4. *We have*

$$\begin{aligned} W'(h_\rho|\bar{\phi})u^{-v_p(N_{\rho\bar{\phi}})}\epsilon_p(\rho\bar{\phi}) \times \frac{L_{\{p, q|nm\}}(f, \rho\phi, 1)}{2^3\pi^2 i^3 \Omega_{\tilde{f}_0}} \\ \equiv W'(h_\sigma|\bar{\phi})m^{-1}\epsilon(m)u^{-v_p(N_{\sigma\bar{\phi}})}\epsilon_p(\sigma\bar{\phi}) \times \frac{L_{\{p, q|nm\}}(f, \sigma\phi, 1)}{2^3\pi^2 i^3 \Omega_{\tilde{f}_0}} \pmod{p}. \end{aligned}$$

□

Using [V, Theorem 1.10] the following lemma can be proved by an argument similar to proof of Lemma 5.3.

Lemma 5.5. *We have*

$$\begin{aligned} W'(h_\sigma|\bar{\phi})m^{-1}\epsilon(m)u_f^{-v_p(N_{\sigma\bar{\phi}})}\epsilon_p(\sigma\bar{\phi}) \times \frac{L_{\{p, q|nm\}}(f, \sigma\phi, 1)}{(-2\pi i \Omega_{\tilde{f}_0}^+)(-2\pi i \Omega_{\tilde{f}_0}^-)} \\ \equiv W'(h_\sigma|\bar{\phi})m^{-1}\epsilon(m)u_g^{-v_p(N_{\sigma\bar{\phi}})}\epsilon_p(\sigma\bar{\phi}) \times \frac{L_{\{p, q|nm\}}(g, \sigma\phi, 1)}{(-2\pi i \Omega_{\tilde{g}_0}^+)(-2\pi i \Omega_{\tilde{g}_0}^-)} \pmod{p}. \end{aligned}$$

□

As a consequence of Theorem 5.4 and Lemma 5.5 we obtain the following theorem which shows that $R_f(\rho \otimes \phi) \equiv R_g(\rho \otimes \sigma) \pmod{p}$.

Theorem 5.6. *We have*

$$(6) \quad \begin{aligned} u_f^{-v_p(N_\rho \bar{\phi})} \epsilon_p(\rho \bar{\phi}) \frac{L_{\{p,q|nm\}}(f, \rho \phi, 1)}{(-2\pi i \Omega_f^+)(-2\pi i \Omega_f^-)} \\ \equiv u_g^{-v_p(N_\rho \bar{\phi})} \epsilon_p(\rho \bar{\phi}) \frac{L_{\{p,q|nm\}}(g, \rho \phi, 1)}{(-2\pi i \Omega_g^+)(-2\pi i \Omega_g^-)} \pmod{p}. \end{aligned}$$

□

Recall that in section 1 we had considered a set S of primes containing the set S_{min} (see also (2) and (4)). In the formula $R_f(\rho)$ (see (1)) we have removed the local L -factors at primes in the set S from the L -function of f twisted by ρ . The congruence relation (5) in Theorem 5.2 between $R_f^S(\rho)$ and $R_g^S(\rho)$ has been proved in the special case where $S = S_{min}$. The congruence relation (5) is in fact valid for any set S containing S_{min} . We briefly explain this now.

Let l be a prime number not dividing nmp . If $l \nmid N = l.c.m.(N_f, N_g)$, then by the assumption that the residual Galois representations of f and g are equivalent, we get that the Fourier coefficient $a(f, l) \equiv a(g, l) \pmod{p}$. If $l|N$, then by the assumption that $l \nmid n$, we have that $l|\bar{N}$. Now, we have mentioned in the proof of Lemma 5.3 (see [DDT, Lemma 4.6]) that $a(l, f) \equiv a(l, g)$ modulo p . Let $L_l(f, \rho, s)$ (resp. $L_l(g, \rho, s)$) denote the local L -factor of f (resp. g) twisted by ρ at l . Then using the fact that $a(f, l) \equiv a(g, l) \pmod{p}$, it can easily be checked that $L_l(f, \rho, 1)^{-1} \equiv L_l(g, \rho, 1)^{-1} \pmod{p}$. Note that since $l \neq p$, the numbers $L_l(f, \rho, 1)^{-1}$ (resp. $L_l(g, \rho, 1)^{-1}$) are p -adic integers. Thus, multiplying the integers $L_l(f, \rho, 1)^{-1}$ (resp. $L_l(g, \rho, 1)^{-1}$) on the left (resp. right) hand side of the congruence relation (5) in Theorem 5.2 we get that

$$R_f^S(\rho) \equiv R_g^S(\rho) \pmod{p}$$

for the set $S = S_{min} \cup \{l\}$. Applying the above argument successively for the primes l in the enlarged set S , we can prove the inequality (3) stated in section 1. A similar argument works if we twist f (resp. g) with a $\rho \otimes \phi$ for some Dirichlet character ϕ of p -power conductor.

We stress that it is necessary to assume that S contains S_{min} . In our recent work [SS] we have discussed a few numerical examples to show that if S does not contain these primes, then the congruence need not hold. However, under certain stronger assumptions, the congruence between special values of f (resp. g) twisted by ρ can be shown without removing the Euler factors at the primes dividing the integer nm . We discuss these cases below. In particular we now have the following improvement of Theorem 5.2.

Theorem 5.7. *For a prime factor q of m suppose that,*

- (i) $q + 1 + a(q, f)$ is coprime to p if q is inert in K and
- (ii) $q + 1 - a(q, f)$ is coprime to p if q is split in K .

Then we have

$$\begin{aligned} u_f^{-v_p(N_\rho)} \epsilon_p(\rho) \frac{P_p(\rho, u_f^{-1})}{P_p(\rho, w_f^{-1})} \frac{L_{\{p,q|n\}}(f, \rho, 1)}{(-2\pi i \Omega_f^+)(-2\pi i \Omega_f^-)} \\ \equiv u_g^{-v_p(N_\rho)} \epsilon_p(\rho) \frac{P_p(\rho, u_g^{-1})}{P_p(\rho, w_g^{-1})} \frac{L_{\{p,q|n\}}(g, \rho, 1)}{(-2\pi i \Omega_g^+)(-2\pi i \Omega_g^-)} \pmod{p}. \end{aligned}$$

Proof. Let q be a prime divisor of m . Then q is unramified in K and ramified in F . Let $M(f)$ be the p -adic Galois representation associated to f and $M(\rho)$ be the Galois representation associated to ρ . Therefore the Euler factor of the tensor product L -function associated to $M(f) \otimes M(\rho)$ at q is defined as

$$L_q(f, \rho, s) := (\det(1 - \text{Frob}_q^{-1} q^{-s} | (M(f) \otimes M(\rho))^{I_q}))^{-1}.$$

Since N_ρ is coprime to the conductor of f , $M(f)$ is unramified at q . Therefore we have

$$(M(f) \otimes M(\rho))^{I_q} \cong M(f) \otimes M(\rho)^{I_q}.$$

Since F is ramified at q , the inertia subgroup in $\text{Gal}(F/\mathbb{Q})$ at q is identified with $\text{Gal}(F/K)$. Thus the action of $\text{Gal}(F/\mathbb{Q})$ on $M(\rho)^{I_q}$ factors through $\text{Gal}(K/\mathbb{Q})$. Now suppose that q splits in K . Then Frob_q acts trivially on $M(\rho)^{I_q}$. Therefore the Euler factor for the tensor product L -function will be equal to the Euler factor of f at q . But the Euler factor of f evaluated at 1 is equal to $(q^{-1}(q+1-a(q, f)))^{-1}$. This shows that $L_q(f, \rho, 1)$ is a p -adic unit. Now suppose that q remains inert in K . Then the action on $\text{Gal}(K/\mathbb{Q})$ on $M(\rho)^{I_q}$ is non-trivial. Thus in this case we get

$$L_q(f, \rho, 1) = (q^{-1}(1 + a(f, q) + q))^{-1}.$$

Again, by assumption, $L_q(f, \rho, 1)$ is a p -adic unit. A similar formula holds for the modular form g . Since $a(q, f) \equiv a(q, g)$, we have

$$L_q(f, \rho, 1) \equiv L_q(g, \rho, 1) \pmod{p}.$$

By multiplying the Euler factors at primes dividing m on both side of the congruence stated in Theorem 5.2, we get the desired congruence. \square

We mention an example of congruence of modular forms satisfying the hypotheses of the previous theorem. Let f be the modular form associated to the isogeny class of the elliptic curve E_1 of conductor 11 and g be the modular form associated to the first isogeny class of elliptic curve E_2 of conductor 77 in Cremona's tables [Cr]. The minimal Weierstrass model of these two elliptic curves are given by the following equations

$$E_1 : y^2 + y = x^3 - x^2 - 10x - 20; \quad E_2 : y^2 + y = x^3 + 2x.$$

Then $a(n; f) \equiv a(n; g) \pmod{3}$ for all n coprime to 7 (see [D]). Also, the residual representation associated to f is irreducible at 3. Put $m = 13$, $K = \mathbb{Q}(\mu_3)$ and $F = K(13^{1/3})$. The 13th Fourier coefficient of f is 4 [WS]. Thus all the assumptions of Theorem 5.7 hold. Note that 13 splits in K . This is true because $36 = 6^2 \equiv -3 \pmod{13}$. Now using Theorem 5.7 we get that the special value of f twisted by any irreducible Artin representation ρ of $\text{Gal}(F/\mathbb{Q})$ is congruent to the special value of g twisted by ρ . Note that to get the congruence stated in Theorem 5.7, we need to remove the Euler factors at 3 and 7.

Corollary 5.8. *Suppose that $N_f = N_g = \bar{N}_f$. If the assumptions of Theorem 5.7 hold, then we have*

$$\begin{aligned} u_f^{-v_p(N_\rho)} \epsilon_p(\rho) \frac{P_p(\rho, u_f^{-1})}{P_p(\rho, w_f^{-1})} \frac{L_{\{p\}}(f, \rho, 1)}{(-2\pi i \Omega_f^+)(-2\pi i \Omega_f^-)} \\ \equiv u_g^{-v_p(N_\rho)} \epsilon_p(\rho) \frac{P_p(\rho, u_g^{-1})}{P_p(\rho, w_g^{-1})} \frac{L_{\{p\}}(g, \rho, 1)}{(-2\pi i \Omega_g^+)(-2\pi i \Omega_g^-)} \pmod{p}. \end{aligned} \quad \square$$

We now mention an example of congruence of modular forms where all the assumptions of the corollary above are satisfied. Let f be the modular form associated to the 3rd isogeny class of the elliptic curve of conductor 158 and g be the modular form associated to the 5th isogeny class of the elliptic curve of conductor 158 in Cremona's tables [Cr]. Then $a(n; f) \equiv a(n; g) \pmod{3}$ for all n . This can be shown using the Sturm bound and the table of Fourier coefficients of f and g obtained from [Cr]. Further, the members of the 3rd isogeny class of the elliptic curves of conductor 158 do not have any 3-isogeny, and therefore the residual representation of the form f at the prime 3 is irreducible. Also, in this case $N_f = N_g = \bar{N}_f$. Put $m = 5$, $K = \mathbb{Q}(\mu_3)$ and $F = K(5^{1/3})$. The 5th Fourier coefficient of f is 1 and $5 + 1 + 1 = 7$ is coprime to 3. Note that 5 remains inert in K . Thus the congruence stated in the above corollary holds for all irreducible Artin representations ρ of $\text{Gal}(F/\mathbb{Q})$. Finally, we mention that a source of infinitely many examples of congruence between elliptic curves is [RS] in the case when $p = 3$ and $p = 5$.

ACKNOWLEDGEMENTS

The authors would like to thank R. Greenberg and N. Vatsal for helpful discussions. The article of T. Bouganis was of great help, and we would like to thank him for answering our questions. The first author would like to thank L. Clozel, E. Ghate and C. S. Rajan for answering basic questions on modular forms. The second author gratefully acknowledges the support of an NSERC grant. The authors are also grateful to TIFRCAM, Bangalore for the hospitality provided while this work was in progress. Finally, we thank the referee for comments which helped improve the exposition of this paper.

REFERENCES

- [B] Thanasis Bouganis, *Special values of L-functions and false Tate curve extensions*, J. Lond. Math. Soc. (2) **82** (2010), no. 3, 596–620, DOI 10.1112/jlms/jdq041. With an appendix by Vladimir Dokchitser. MR2739058 (2012g:11120)
- [CE] Robert F. Coleman and Bas Edixhoven, *On the semi-simplicity of the U_p -operator on modular forms*, Math. Ann. **310** (1998), no. 1, 119–127, DOI 10.1007/s002080050140. MR1600034 (99b:11043)
- [Cr] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1992. MR1201151 (93m:11053)
- [D] Fred Diamond, *Congruences between modular forms: raising the level and dropping Euler factors*, Proc. Nat. Acad. Sci. U.S.A. **94** (1997), no. 21, 11143–11146, DOI 10.1073/pnas.94.21.11143. Elliptic curves and modular forms (Washington, DC, 1996). MR1491976 (98m:11033)
- [DD] T. Dokchitser and V. Dokchitser, *Computations in non-commutative Iwasawa theory*, Proc. Lond. Math. Soc. (3) **94** (2007), no. 1, 211–272, DOI 10.1112/plms/pdl014. With an appendix by J. Coates and R. Sujatha. MR2294995 (2008g:11106)
- [DDT] Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Int. Press, Cambridge, MA, 1994, pp. 1–154. MR1474977 (99d:11067a)
- [DFG] Fred Diamond, Matthias Flach, and Li Guo, *The Tamagawa number conjecture of adjoint motives of modular forms* (English, with English and French summaries), Ann. Sci. École Norm. Sup. (4) **37** (2004), no. 5, 663–727, DOI 10.1016/j.ansens.2004.09.001. MR2103471 (2006e:11089)
- [EK] E. Kani, *Binary theta series and modular forms with complex multiplication*, Int. J. Number Theory **10** (2014), no. 4, 1025–1042. MR3208873
- [GV] Ralph Greenberg and Vinayak Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), no. 1, 17–63, DOI 10.1007/s002220000080. MR1784796 (2001g:11169)

- [H] Haruzo Hida, *A p -adic measure attached to the zeta functions associated with two elliptic modular forms. II*, Ann. Inst. Fourier (Grenoble) **38** (1988), no. 3, 1–83. MR976685 (89k:11120)
- [H1] Haruzo Hida, *A p -adic measure attached to the zeta functions associated with two elliptic modular forms. I*, Invent. Math. **79** (1985), no. 1, 159–195, DOI 10.1007/BF01388661. MR774534 (86m:11097)
- [H2] Haruzo Hida, *Congruence of cusp forms and special values of their zeta functions*, Invent. Math. **63** (1981), no. 2, 225–261, DOI 10.1007/BF01393877. MR610538 (82g:10044)
- [RS] K. Rubin and A. Silverberg, *Families of elliptic curves with constant mod p representations*, Elliptic curves, modular forms, and Fermat’s last theorem (Hong Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 148–161. MR1363500 (96j:11078)
- [SS] Sudhanshu Shekhar and R. Sujatha, *Euler characteristic and congruences of elliptic curves*, Münster J. of Math. **7** (2014), 327–343.
- [V] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. **98** (1999), no. 2, 397–419, DOI 10.1215/S0012-7094-99-09811-3. MR1695203 (2000g:11032)
- [Wi] Andrew Wiles, *Modular elliptic curves and Fermat’s last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551, DOI 10.2307/2118559. MR1333035 (96d:11071)
- [WS] W. Stein, *Modular forms database*, modular.math.washington.edu/Tables.

SCHOOL OF MATHEMATICS, TATA INSTITUTE OF FUNDAMENTAL RESEARCH, MUMBAI-400005, INDIA

E-mail address: `sudhansu@math.tifr.res.in`

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BRITISH COLUMBIA, CANADA V6T 1Z2

E-mail address: `sujatha@math.ubc.ca`