Canonical Periods and Congruence Formulae

V. Vatsal
Department of Mathematics
University of Toronto
100 St. George Street
Toronto M5S 1A1, Canada
vatsal@math.toronto.edu

July 19, 1999

0 Introduction

The purpose of this article is to show how congruences between the Fourier coefficients of Hecke eigenforms give rise to corresponding congruences between the algebraic parts of the critical values of the associated L-functions. This study was initiated by B. Mazur in his fundamental work on the Eisenstein ideal (see [Maz77] and [Maz79]) where it was made clear that congruences for analytic L-values were closely related to the integral structure of certain Hecke rings and cohomology groups. The results of [Maz79] also showed that congruences were useful in the study of nonvanishing of L-functions. This idea was then further developed by Stevens [Ste82] and Rubin-Wiles [RW82]. The work of Rubin and Wiles, in particular, used congruences to study the behavior of elliptic curves in towers of cyclotomic fields. A key ingredient here was a theorem of Washington, which states, roughly, that almost L-values in certain families are nonzero modulo p.

This theme has recently been taken up again, in the work of Ono-Skinner [OSa], [OSb], James [Jam], and Kohnen [Koh97]. While the earlier history was primarily concerned with cyclotomic twists, the current emphasis is on families of twists by quadratic characters. Here one wants quantitative estimates for the number of quadratic twists of a given modular form, which have nonvanishing L-function at $s = 1$. We continue this trend in the present work by using our general results to obtain a strong nonvanishing theorem for the quadratic twists of modular elliptic curves with rational points of order three. This generalizes a beautiful example due to Kevin James, and provides new evidence for a conjecture of Goldfeld [Gol79]. It should, however, be pointed out that even the study of quadratic twists may be traced back to Mazur: the reader is urged to look at pages 212–213 of [Maz79], and especially at the footnote at the bottom of page 213. The theorems of Davenport-Heilbronn [DH71] and Washington [Was78], which are crucial in this paper, are both mentioned in Mazur's article.

We want to begin by discussing the congruences that lie at the heart of this article. Thus let $f = \sum a_n q^n$ be an elliptic modular cuspform of level M and weight $k \geq 2$. Assume that f is a simultaneous eigenform for all the Hecke operators and that $a_1(f) = 1$. The L-function associated to f is defined by the Dirichlet series $L(s, f) = \sum a_n n^{-s}$, which converges for the real part of s sufficiently large, and has analytic continuation to $s \in \mathbf{C}$. A fundamental theorem of Shimura [Shi76] states that $L(s, f)$ enjoys the following algebraicity property:

Theorem (0.1) (Shimura). *There exist complex periods $\Omega_f^{\pm}$ such that, for each integer m satisfying $0 \leq m \leq k-2$, and every Dirichlet character χ, the quantity*

$$\tau(\overline{\chi}) \cdot m! \frac{L(m+1, f, \chi)}{(-2\pi i)^{m+1}\Omega_f^{\pm}}$$

is algebraic. Here the sign $\pm$ of $\Omega^{\pm}$ is determined by $\pm 1 = \chi(-1)$, and $\tau(\overline{\chi})$ denotes the Gauss sum of $\overline{\chi}$.

The integers m appearing in Shimura's theorem are said to be *critical* for $L(s, f)$.

Now consider another eigenform $g = \sum b_n q^n$, where the Fourier coefficients b_n are related to those of f by a congruence:

$$a_n \equiv b_n \pmod{\mathfrak{p}},$$

for a prime ideal $\mathfrak{p}$ in the ring of all algebraic integers (we need to fix an embedding of the algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$ into $\mathbf{C}$). Then general arguments from Iwasawa theory [Gre89], [Coa91], [BK90], suggest that algebraic parts of special values should reflect algebraic properties, so that for critical m, there should be a congruence

$$\tau(\overline{\chi}) \cdot m! \frac{L(m+1, f, \chi)}{(-2\pi i)^{m+1}\Omega_f^{\pm}} \equiv \tau(\overline{\chi}) \cdot m! \frac{L(m+1, g, \chi)}{(-2\pi i)^{m+1}\Omega_g^{\pm}} \pmod{\mathfrak{p}}. \tag{1}$$

Of course the crucial ingredient in proving such congruences is the determination of the periods $\Omega_*^{\pm}$, since Shimura's theorem only specifies them up to an algebraic constant. A related question arises in the definition of p-adic L-functions in Iwasawa theory, where one needs to specify these periods up to p-adic unit [Gre89], [Coa91].

In this article we show how to define canonical periods for cuspforms (canonical up to p-adic unit) and show how to derive the corresponding congruences. As we have already mentioned, results of this variety have been proven by a number of authors. However, we are able to subsume the previous works into a rather general frame: we show how all such congruences follow in a formal way from a sufficiently precise description of the Hecke-module structure of the cohomology with coefficients of the appropriate modular curves. The utility of these cohomology groups is already apparent in [AS86]. The specific condition we need is closely related to the 'multiplicity one' results introduced by Mazur, and, thanks to the work of Ribet, Wiles, and others, we are able to verify its validity in rather general situations. For example we have the following result:

Theorem (0.2). *Let p be an odd prime, and let $f = \sum a_n q^n$ and $g = b_n q^n$ be cuspidal newforms of weight 2 on $\Gamma_1(M)$, such that $a_n \equiv b_n \pmod{\mathfrak{p}^r}$, for some prime $\mathfrak{p}$ above p in $\overline{\mathbf{Q}}$. Assume that $(M, p) = 1$ and that the residual representation attached to f is irreducible. Fix an isomorphism $\mathbf{C}_p \cong \mathbf{C}$, such that the prime $\mathfrak{p}$ of $\overline{\mathbf{Q}} \subset \mathbf{C}$ induces the usual absolute value on $\mathbf{C}_p$. Then there exist canonical periods $\Omega_f^{\pm}$ and $\Omega_g^{\pm}$ such that the congruence (1) holds modulo $\mathfrak{p}^r$, for every character χ. There exists χ such that both sides of the congruence are nonzero modulo $\mathfrak{p}$.*

The organisation of this paper is as follows. The first section treats the case of residually irreducible forms, where there are no congruences with Eisenstein series. In an effort to obtain the most general statement, we state the hypothesis on the cohomology as an axiom, prove our main theorems under the this axiom, and conclude by giving a list of conditions under which the axiom is valid.

The second section is concerned with the case of residually reducible forms, where congruences with Eisenstein series may occur. The results in this setting are less satisfactory, as the Hecke-module structure of the cohomology is not well understood. Nevertheless, a considerable amount can be salvaged, and results similar to (0.2) are obtained. We conclude this section by showing that the L-values of a cuspform whose Fourier coefficients are congruent to those of an Eisenstein series has the property that its L-values are congruent to certain products of Bernoulli numbers. This is a refinement of a theorem due to Mazur and Stevens [Maz79], [Ste82].

The final section of the paper gives an application to nonvanishing theorems for modular L-functions. To state the problem we will investigate, let f be a modular cuspform even weight $k = 2m$. Let D be a square-free integer, and let χ_D denote the Kronecker character associated to the quadratic field $\mathbf{Q}(\sqrt{D})$. For a positive real number X, define the number

$$M_f(X) = \#\{D : |D| < X,\ L(m, f \otimes \chi_D) \neq 0\}.$$

Then a well-known conjecture in analytic number theory states that $M_f(X) \gg X$. There are a number of partial results in this direction, due to Murty-Murty [MM91], Iwaniec [Iwa90], and others; currently the best estimate is due to Ono and Skinner [OSb] who prove that $M_f(X) \gg X/\log(X)$.

In the case where f has weight 2 and corresponds to an elliptic curve over $\mathbf{Q}$, Goldfeld has conjectured that $M_f(X) \sim X/2$ (see [Gol79] for a more precise statement). A recent example due to Kevin James [Jam] shows that $M_f(X) \gg X$ for a certain elliptic curve of level 14. In this paper we will extend James' ideas to obtain the following result:

Theorem (0.3). *Let C be a modular elliptic curve over $\mathbf{Q}$ with a rational point of order three. Assume that C has good ordinary reduction at 3, and that the conductor N of C is square-free. Let f be the newform assosciated to C; then we have $M_f(X) \gg X$.*

The proof of the theorem is based on a mod 3 relationship between the algebraic part of $L(1, \chi_D)$ and the class-number of the field $\mathbf{Q}(\sqrt{D})$, which follows from the general congruence machinery developed in the second section. The estimate on $M_f(X)$ then follows from a theorem of Davenport and Heilbronn, as refined by Nakagawa and Horie [NH88]. This application of the Davenport-Heilbronn theorem is due to James, whose work gave a version of our theorem for the curve 14B in Cremona's tables. It should be pointed out that James relates the L-values to class numbers by using Waldspurger's theorem and the Shimura lift rather than the theory of congruences. His technique has also been exploited by Kohnen [Koh97] to obtain nonvanishing results for certain forms of level 1, including the Ramanujan Δ-function.

The author would like to thank K. Ono, C. Skinner, and A. Wiles for some useful conversations. Particular thanks are due to Ono, who brought the work of James to our attention.

Notation and Hypotheses

Let p be an odd prime, and N a positive integer prime to p. We set $M = Np^s$ for a non-negative integer s, and assume throughout that $M \geq 4$. Let Γ denote the group $\Gamma_1(M)$. Then our hypothesis that $M \geq 4$ implies that Γ is torsion-free. Let X be the Riemann surface given by the (complete) modular curve corresponding to Γ. Let C denote the set of cusps on X. We may identify C with the set $\mathbf{P}^1(\mathbf{Q})/\Gamma$. We will follow the notations and conventions of Stevens [Ste82], Chapter 1, in dealing with the cusps.

We also fix an isomorphism $\mathbf{C}_p \cong \mathbf{C}$, together with an embedding $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$. We let K denote a finite extension of the field $\mathbf{Q}_p$ and write $\mathcal{O}$ for the ring of integers in K. We write π for a generator of the maximal ideal of $\mathcal{O}$, and put $\mathbf{F} = \mathcal{O}/\pi$. We will write $\mathbf{F}_p$ for the field with p elements.

We also want to recall some notation from Eichler-Shimura theory, as it is fundamental to what follows. For a ring A and a non-negative integer n we denote by $L_n(A)$ the symmetric polynomial algebra over A of of degree n. Thus $L_n(A)$ consists of the homogeneous polynomials of degree n, with coefficients in A. The group $\Sigma = GL_2(\mathbf{Q}) \cap M_2(\mathbf{Z})$ acts on $L_n(A)$ by

$$\gamma : P(X, Y) \mapsto P((X, Y) \det(\gamma)\gamma^{-1}).$$

Thus we may form the Eichler-Shimura cohomology groups $H^1(\Gamma, L_n(A))$ and the parabolic subgroups $H^1_p(\Gamma, L_n(A))$ (see [DI95], §12). Now let $k \geq 2$ be an integer, and let A be a subring of $\mathbf{C}$ (or $\mathbf{C}_p$). Let $S_k(A)$ denote the space of cusp forms on Γ with Fourier coefficients in A. Then $S_k(A)$ is stable under the Hecke operators. If we write $\mathbf{T}_k = \mathbf{T}(A)$ for the A-algebra generated by the Hecke operators in the endomorphism ring of $S_k(A)$, then $\mathbf{T}_k$ acts on the torsion-free parts of $H^1(\Gamma, L_n(A))$ and $H^1_p(\Gamma, L_n(A))$, for $n = k - 2$.

Given a weight k modular form $f(z)$ for Γ, we define a differential form with values in $L_n(\mathbf{C})$ by

$$\omega_f = f(z)(zX + Y)^n dz. \tag{2}$$

Then

$$\gamma \mapsto \int_{z_o}^{\gamma z_0} \omega_f$$

defines a 1-cocycle on Γ, with values in $L_n(\mathbf{C})$. If $f(z)$ is a cuspform then the class of ω_f is lies in the parabolic subgroup. Here z_0 is any basepoint in the upper half-plane $\mathcal{H}$.

1 The Irreducible Case

(1.1). Let $f = \sum a_n q^n$, $g = \sum b_n q^n$ be normalized Hecke eigenforms on Γ of weight $k \geq 2$, with coefficients in $\mathcal{O}$, and such that

$$a_n \equiv b_n \pmod{\pi^r}$$

for some integer $r \geq 1$. We do *not* assume at present that either f or g is a newform; the reasons for this will become clear in the sequel. Let $\mathbf{T}_k$ denote the $\mathcal{O}$-algebra generated by the Hecke operators acting on $S_k = S_k(\Gamma, \mathcal{O})$. Then the congruence class of f and g in S_k determines a maximal ideal $\mathfrak{m}$ of $\mathbf{T}_k$, and a residual representation

$$\rho_{\mathfrak{m}} : \mathrm{Gal}\,(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{T}_k/\mathfrak{m})$$

such that $\mathrm{Tr}\,(\mathrm{Frob}\,(q)) = T_q$ for all primes q with $(Np, q) = 1$. In this section we assume that $\rho_{\mathfrak{m}}$ is *irreducible*. This implies in particular that f and g are both cuspidal. The ring $\mathbf{T}_{k,\mathfrak{m}} \otimes \mathbf{Q}$ is an Artin algebra, and there are surjective K-algebra homomorphisms

$$\pi_f, \pi_g : \mathbf{T}_{k,\mathfrak{m}} \otimes \mathbf{Q} \to K$$

determined by f and g. The ring $\mathbf{T}_{k,\mathfrak{m}} \otimes \mathbf{Q}$ decomposes as a product of local Artin rings, and there are unique local factors R_f and R_g such that π_f, π_g factor through R_f, R_g respectively.

The Hecke algebra $\mathbf{T}_k$ acts on $H^1(\Gamma, L_n(\mathcal{O}))$, and we write $H^1(\Gamma, L_n(\mathcal{O}))_{\mathfrak{m}}$ for the localization at $\mathfrak{m}$. We may decompose $H^1(X, L_n(\mathcal{O}))$ further as $H^1(\Gamma, L_n(\mathcal{O})) = H^1(\Gamma, L_n(\mathcal{O}))^+ \oplus H^1(\Gamma, L_n(\mathcal{O}))^-$, according to the action of complex conjugation.

(1.2). In this section we describe the axioms under which we will prove our main theorem. Here we will simply state the conditions: a diverse list of hypotheses under which they may be verified is given at the end of this section. It is our hope that this sort of axiomatization will make clear the structure of the proof, and facilitate the applications.

The conditions are

1. $R_f = R_g = K$, and
2. There exist isomorphisms of $\mathbf{T}_k$-modules

$$\varphi^{\pm} : H^1(\Gamma, L_n(\mathcal{O}))^{\pm}_{\mathfrak{m}} = H^1_p(\Gamma, L_n(\mathcal{O}))^{\pm}_{\mathfrak{m}} \cong \mathbf{T}^*_{k,\mathfrak{m}} = \mathrm{Hom}_{\mathcal{O}}(\mathbf{T}_{k,\mathfrak{m}}, \mathcal{O})_{\mathfrak{m}}.$$

In particular, $H^1(\Gamma, L_n(\mathcal{O}))$ is torsion-free.

The first condition will be satisfied if, for example, both f and g are new of level M, but can often be checked in other situations. The second condition however is more delicate, and may fail for the simple reason that there is nontrivial $\mathcal{O}$-torsion in the cohomology group. It may therefore be preferable to modify Condition 2 by replacing $H^1(\Gamma, L_n(\mathcal{O}))$ with its image in $H^1(\Gamma, L_n(K))$. The arguments in this paper will then go through with only minor modifications. However, we are not aware of any examples where the weaker condition holds but the stronger one does not. Note also that the identification of group cohomology and parabolic cohomology at $\mathfrak{m}$ is a consequence of the irreducibility of $\rho_{\mathfrak{m}}$.

We assume from now on that these conditions hold.

(1.3). We now need to recall the duality between cusp forms and the Hecke rings, referring the reader to [DI95], §12 for details. With notation as in [DI95], there is a natural pairing $\mathbf{T}_k \times S_k \to \mathcal{O}$ given by $(t, h) \mapsto a_1(,h|t)$, and it can be shown ([DI95], Prop 12.4.13) that this pairing induces an isomorphism of $\mathbf{T}_k$-modules

$$S_k(\mathcal{O}) \cong \mathbf{T}^*_k = \mathrm{Hom}_{\mathcal{O}}(\mathbf{T}_k, \mathcal{O}).$$

We may therefore reformulate condition 2 above as follows: there exist isomorphisms

$$\theta^{\pm} : H^1(\Gamma, L_n(\mathcal{O}))^{\pm}_{\mathfrak{m}} \cong S_k(\mathcal{O})_{\mathfrak{m}}. \tag{3}$$

Given a modular form h in $S_k(\mathcal{O})_{\mathfrak{m}}$, we define cocycles $\delta^{\pm}_h$ by $\theta^{\pm}(\delta^{\pm}_h) = h$. Since we have $f \equiv g \pmod{\pi^r}$, we will have

$$\delta^{\pm}_f \equiv \delta^{\pm}_g \pmod{\pi^r} \tag{4}$$

for each choice of sign.

On the other hand, the recipe given in (2) shows that the modular forms f and g give rise to certain vector-valued differential forms on $\mathcal{H}$ and cohomology classes ω_f and ω_g in $H^1(\Gamma, L_n(\mathbf{C}))$. The cohomology classes ω_f and ω_g will be eigenvectors for the Hecke operators, with the same eigenvalues as f and g respectively. If we write $\omega^{\pm}_*$ for the projection to the $\pm$-part (here the star denotes either f or g) our Condition 1 then implies that there exist complex numbers $\Omega^{\pm}_f$ and $\Omega^{\pm}_g$ such that

$$\omega^{\pm}_* = \Omega^{\pm}_* \delta^{\pm}_*. \tag{5}$$

The numbers $\Omega^{\pm}_*$ are the canonical periods alluded to in the title. We note, however, they are only determined up to p-adic units, the dependence coming from the choice of isomorphism in Condition 2. Strictly speaking, the periods also depend on the maximal ideal $\mathfrak{m}$. It can be shown, however, that if the cuspform f corresponds to a modular elliptic curve E, then the canonical periods coincide with the usual Néron periods on E.

(1.4). Now we make explicit the connection with L-values. Roughly speaking, the algebraic parts of the L-functions attached to f and g are given by the integrals of the classes $\delta_*^\pm$ against suitable homology classes, and the congruence (4) we have exhibited between $\delta_f^\pm$ and $\delta_g^\pm$ leads to the congruences for the special values. To make this explicit, we introduce some notation. Let χ be a nontrivial Dirichlet character, of conductor D, and let $\mathbf{Z}(\chi)$ denote the ring obtained by adjoining to $\mathbf{Z}$ the values of χ. We define a *relative* homology class

$$\Lambda(\chi) \in H_1(X, \mathrm{Cusps}; \mathbf{Z}(\chi))$$

as follows. For a pair x, y of cusps we let $\{x, y\}$ denote the relative homology class generated by the projection to X of the geodesic path in the upper-half-plane joining x and y. Then the class $\Lambda(\chi)$ is defined by the formula

$$\Lambda(\chi) = \sum_{a=0}^{D-1} \overline{\chi}(a) \cdot \{\frac{a}{D}, i\infty\} \tag{6}$$

The paths $\{a/D, i\infty\}$ are vertical lines. There is a natural injection

$$H_1(X, \mathbf{Z}(\chi)) \hookrightarrow H_1(X, \mathrm{Cusps}; \mathbf{Z}(\chi)),$$

and a simple computation using the relative homology sequence and the boundary operator (see [Ste82], page 28) shows that $\Lambda(\chi)$ actually represents a class in $H_1(X, \mathbf{Z}(\chi))$ when the conductor D is prime to the level. The action of complex conjugation on homology gives a splitting

$$H_1(X, \mathbf{Z}(\chi)) = H_1(X, \mathbf{Z}(\chi))^+ \oplus H_1(X, \mathbf{Z}(\chi))^-,$$

and if $\alpha = \pm$ is such that $\chi(-1) = (-1)^\alpha$, then one checks without difficulty that $\Lambda(\chi)$ lies in $H_1(X, \mathbf{Z}(\chi))^\alpha$. When the weight $k = 2$, an easy computation shows that for any χ we have

$$\int_{\Lambda(\chi)} \omega_*^\pm = \tau(\overline{\chi}) \cdot \frac{L(1, *, \chi)}{(-2\pi i)}. \tag{7}$$

Here the number $L(1, *, \chi)$ is the value at $s = m$ of the L-function of $*$, twisted by the character χ, and $\tau(\overline{\chi})$ denotes the Gauss sum of $\overline{\chi}$. Note also that the integral is zero if the parity of χ does not agree with that of ω_*.

It is convenient to take an alternative approach when dealing with forms of higher weight. The key tool is the theory of modular symbols, as described in [GS93] §4. The following discussion is only a summary, and we refer the reader to [GS93] for a more detailed discussion and [AS86] for the proofs.

(1.5). Let R be a ring, and let A be an $R[\Gamma]$-module with Hecke action (this amounts to the restriction that R be a contravariant $R[\Sigma]$-module, in the notation of [GS93]). Let $\mathcal{D}$ denote the group of divisors supported on the cusps $\mathbf{P}^1(\mathbf{Q})$. Let $\mathcal{D}_0$ denote the subgroup of divisors of degree zero. Let $S_\Gamma(A) = \mathrm{Hom}_\Gamma(\mathcal{D}_0, A)$ denote the group of modular symbols, and let $B_\Gamma(A) = \mathrm{Hom}_\Gamma(\mathcal{D}, A)$ denote the boundary symbols. There is an isomorphism

$$H_c^1(Y, \tilde{A}) = S_\Gamma(A), \tag{8}$$

where $\tilde{A}$ is the local coefficient system associated to A on $Y = \Gamma/\mathcal{H}$, and the subscript 'c' denotes cohomology with compact supports. Furthermore, there is an exact sequence

$$0 \to H^0(\Gamma, A) \to B_\Gamma(A) \to S_\Gamma(A) \to H^1_p(\Gamma, A) \to 0. \tag{9}$$

Here $H^1_p(\Gamma, A)$ denotes the parabolic cohomology group Recall that $H^1_p(\Gamma, A)$ coincides with the image of the compactly supported cohomology under the composite $H^1_c(Y, \tilde{A}) \to H^1(Y, \tilde{A}) = H^1(\Gamma, A)$.

Given a modular symbol $\Phi \in S_\Gamma(A)$, we define the *special value* $L(\Phi) \in A$ by

$$L(\Phi) = \Phi(\{i\infty\} - \{0\}).$$

If χ is a primitive Dirichlet character with conductor $m \geq 1$, we define the twisted special value $L(\Phi, \chi)$ by $L(\Phi, \chi) = L(\Phi|R_\chi)$, where the twist operator is defined by

$$\Phi|R_\chi = \sum_{a=0}^{m-1} \overline{\chi}(a)\Phi| \begin{pmatrix} 1 & a/m \\ 0 & 1 \end{pmatrix} \in S_{\Gamma'(A)},$$

for a suitable group Γ'. Given a cuspform f for Γ, we may define a modular symbol Φ_f with values in $L_n(\mathbf{C})$ by the formula

$$\Phi_f(\{c_1\} - \{c_2\}) = \int_{c_2}^{c_1} \omega_f.$$

(1.6). Now we want to specialize this to the case of interest. Let $*$ denote either of the modular forms f or g as before. Then the differential forms $\omega_*^\pm$ define parabolic group cohomology classes with values in $L_n(\mathbf{C})$. We want to use (9) to lift these to modular symbols. To do this we use the Manin-Drinfeld argument. Let q be a prime congruent to 1 modulo Np, and let η_q denote the Hecke operator $T_q - 1 - < q >$. Arguing as in [GS93], Lemma 6.9b, we see that η_q kills the boundary symbols. Thus we define a modular symbol by lifting $\omega_*^\pm$ to S_Γ and then applying η_q. We obtain a modular symbol $\Phi_*^\pm$ with values in $L_n(\mathbf{C})$, whose special values are given by

$$\eta_q(*) \cdot L(\Phi_*^\pm, \chi) = L(*, \chi) = \left(\ldots, \tau(\overline{\chi}) \begin{pmatrix} k-2 \\ m \end{pmatrix} m! \frac{L(m+1, f, \chi)}{(-2\pi i)^{m+1}\Omega^\alpha}, \ldots \right) \tag{10}$$

We now repeat this procedure with the cohomology classes $\delta_*^\pm$. Since η_q is an integral Hecke operator, it acts on integral cohomology, and we obtain modular symbols $\Delta_*^\pm$ with values in $L_n(\mathcal{O})$, and we will have $\Delta_f^\pm \equiv \Delta_g^\pm \pmod{\pi^r}$. Naturality of the sequence (9) then implies the following algebraicity result:

$$\eta_q(*) \frac{L(*, \chi)}{\Omega_*^\pm} = L(\Delta_*^\pm, \chi) \in L_n(\mathcal{O}). \tag{11}$$

Observe that the quantity $\eta_q(*)$ is algebraic. Under the hypothesis that the maximal ideal $\mathfrak{m}$ is residually irreducible, it is easy to see that we may choose q so that $\eta_q(*)$ is a p-adic unit, for both f and g. Since we clearly have $\eta_q(f) \equiv \eta_q(g) \pmod{\pi^r}$, and both sides are p-adic units, we obtain the following proposition:

Proposition (1.7). *Let f and g be as above, so that $f \equiv g \pmod{\pi^r}$ and the maximal ideal $\mathfrak{m}$ is irreducible. Let χ be a Dirichlet character (we do not assume that the conductor is prime to the level), and let the sign $\alpha = \pm$ be determined by $\pm 1 = \chi(-1)$. Then for each integer m satisfying $0 \leq m \leq k-2$, we have the congruence*

$$\tau(\overline{\chi}) \cdot \begin{pmatrix} k-2 \\ m \end{pmatrix} m! \frac{L(m+1, f, \chi)}{(-2\pi i)^{m+1}\Omega_f^\alpha} \equiv \tau(\overline{\chi}) \cdot \begin{pmatrix} k-2 \\ m-1 \end{pmatrix} m! \frac{L(m+1, g, \chi)}{(-2\pi i)^{m+1}\Omega_g^\alpha} \pmod{\pi^r}.$$

Remark (1.8). The reader will note that the binomial coefficients in the formulae above are not generally p-adic units, except when $m = 0$. However, we can refine the congruences to obtain more precise information at the points $m > 1$ in the *ordinary* case by using properties of p-adic L-functions, as we now explain.

(1.9). We want to prove that the p-adic L-functions for f and g satisfy a congruence modulo π^r. We assume that f and g are p-stabilized newforms of level Np^r, so that $r \geq 1$ and the eigenvalue of U_p is a unit in $\mathbf{T}_{k,\mathfrak{m}}$. Let u be a topological generator of the multiplicative group $1 + p\mathbf{Z}_p$. Let χ be a nontrivial character, with conductor prime to N. Let ζ be a p-power root of unity, and define a Dirichlet character ξ by putting $\xi(u) = \zeta$ and $\xi((\mathbf{Z}/p\mathbf{Z})^\times) = 1$. Finally, for $* = f$ or $* = g$, define a quantity $\beta_p(*)$ as the (unit) eigenvalue of U_p on $*$. Then the p-adic L-function for $*$ and χ is a power series $L_p(*, \chi, X) \in \mathcal{O}(\chi)[[X]]$ characterised by the following interpolation formula: for all pairs ζ, m such that the p-part of $\chi\xi\omega^{-m}$ is nontrivial, we have

$$L_p(f, \chi, \zeta u^{m+1} - 1) = \tau(\overline{\chi\xi}\omega^m) \cdot \left(\frac{p^m}{\beta_p(*)}\right)^t \cdot m! \frac{L(m+1, *, \chi\xi\omega^{-m})}{(-2\pi i)^{m+1} \cdot \Omega_*^\alpha}. \tag{12}$$

Here p^t is the p-part of the conductor of $\chi\xi\omega^{-m}$. If on the other hand the p-part of $\chi\xi\omega^{-m}$ is trivial, then, letting $(\chi\xi\omega^{-m})_0$ denote the associated primitive character, we have

$$L_p(*, \chi, \zeta u^{m+1} - 1) = (1 - (\chi\xi\omega^{-m})_0(p)\beta_p(*)^{-1}p^m) \frac{L(m+1, *, \chi\xi\omega^{-m})}{(-2\pi i)^{m+1}\Omega_*^\alpha}. \tag{13}$$

Since $L_p(*, \chi, X)$ is an integral power series, it is completely characterised by the above formulae. We refer the reader to [MTT86] for a proof of the existence. Note also that there is a choice of complex period implicit in the definition, and that choosing a different period scales the function by a constant; one has to choose the periods correctly if one wants to have a congruence. At any rate, our main result is the following:

Theorem (1.10). *The p-adic L-functions of f and g are congruent in the sense that*

$$\Phi(X) = L_p(f, \chi, X) - L_p(g, \chi, X)$$

is divisible by π^r in $\mathcal{O}(\chi)[[X]]$.

Proof. The easiest way to see this is via the Weierstrass preparation theorem. We may write

$$\Phi(X) = B \cdot U(X) \cdot F(X),$$

where B is a constant, $U(X)$ is an invertible power series, and $F(X)$ is a distinguished polynomial (note $\mathcal{O}(\chi)$ may be ramified over $\mathcal{O}$, so that π need not be a uniformizer). We have to show that π^r divides B, under the hypothesis that $\Phi(X)$ takes on values divisible by π^r for all but finitely many points $X = \zeta u - 1$ (this follows from the congruences already proven at $s = 1$). By changing variables we may assume that $\Phi(\zeta - 1)$ is divisible by π^r for all but finitely many ζ.

Suppose B is not divisible by π^r; then since $\mathcal{O}(\chi)$ is a DVR, B must divide π^r. Dividing out by B, we may assume that $\Phi(X) = U(X) \cdot F(X)$, for a unit $U(X)$ and a distinguished polynomial $F(X)$, where F is such that it takes on values divisible by some nonunit $A = \pi^r b^{-1}$ at all but finitely many points $X = \zeta - 1$. Since $U(X)$ is a unit, we may even assume that $\Phi(X) = X^s + a_1 X^{s-1} + \cdots + a_s$, where the a_i all have positive valuation. One checks easily that if the order of ζ is sufficiently large, then the valuation of such a polynomial at $\zeta - 1$ coincides with that of the leading term $(\zeta - 1)^s$, and this approaches zero as the order of ζ approaches infinity. This is a contradiction, and proves the contention. □

Corollary (1.11). *Let the hypotheses on f and g be as in the above propostition. Then, for each χ with conductor prime to N, we have*

$$\tau(\overline{\chi}) \cdot m! \frac{L(m+1, f, \chi)}{(-2\pi i)^{m+1} \Omega_f^\alpha} \equiv \tau(\overline{\chi}) \cdot m! \frac{L(m+1, f, \chi)}{(-2\pi i)^{m+1} \Omega_g^\alpha} \pmod{\pi^r}$$

for each integer m satisfying $0 \leq m \leq k-2$.

Proof. Apply the theorem to $L_p(f, \chi\omega^r)$ and $L_p(g, \chi\omega^r)$ for suitable r, and use the interpolation property of the p-adic L-function. Note that the Euler factor in (13) is a p-adic unit. □

Remark (1.12). We want to show that our results are non-vacuous, in the sense that, for any choice of α of sign, there exists at least one twist χ of parity α with

$$\tau(\overline{\chi}) \cdot \frac{L(1, *, \chi)}{-2\pi i \cdot \Omega_*^\alpha} \neq 0 \pmod{\pi}.$$

When the weight k is two, this will follow from a result of Stevens (see [Ste85], Thm. 2.1). To state this result, recall the homology class $\Lambda(\chi) \in H_1(X, \mathbf{Z}(\chi))$ defined in (1.4), and let $\lambda(\chi)$ denote the image in $H_1(X, \overline{\mathbf{F}})$. Then Stevens' theorem states that the classes $\lambda(\chi)$ generate $H_1(X, \overline{\mathbf{F}})$. Since we have $H^1(\Gamma, \mathcal{O}) \otimes \mathcal{O}/\pi = H^1(\Gamma, \mathcal{O}/\pi)$ (see [Hid81], (1.10a)), and since we are in weight two, we can use the cap product to see that the special value is given by

$$\tau(\overline{\chi}) \cdot \frac{L(1, *, \chi)}{-2\pi i \cdot \Omega_*^\alpha} \neq 0 \pmod{\pi} = \delta_*^\pm \cap \Lambda(\chi).$$

Thus one has only to check that the cocycle $\delta_*^\pm$ is nonzero in $H^1(\Gamma, A) \otimes \mathcal{O}/\pi$. But this follows from Condition 2, as the form $*$ is not divisible by π in $S_2(\mathcal{O})$.

If $k \geq 3$, and $\mathfrak{m}$ is ordinary, we may use the techniques of Hida theory, as follows. Let $\mathbf{F} = \mathcal{O}/\pi$, and assume that f is a p-stabilized newform of level Np, and weight $k \geq 3$.Let $\Gamma = \Gamma_1(Np)$, and let e denote Hida's idempotent, giving the projection to the ordinary part of the Hecke algebra. Then Hida has shown that there is an isomorphism $j : eH_p^1(\Gamma, L_k(\mathbf{F})) = eH_p^1(\Gamma, \mathbf{F})$, induced by projection onto the coefficient of Y^n (see [Hid85], where it is assumed that $p \geq 5$, or the lemma on page 539 of [Wil88]). Let $\overline{\delta}$ denote the image of $\delta_f^\pm$ in $H^1(\Gamma, \mathbf{F})$; since j is an isomorphism it follows from condition 2 that $\overline{\delta}$ is nonzero. One then checks as in [AS86] that

$$\tau(\overline{\chi}) \cdot \frac{L(1, *, \chi)}{-2\pi i \cdot \Omega_*^\alpha} \neq 0 \pmod{\pi} \equiv \overline{\delta} \cap \Lambda(\chi),$$

and the the result follows from Stevens' theorem as before.

Now we give criteria for Condition 2 to be valid.

Theorem (1.13). *Condition 1 is valid in each of the following situations:*

- *$M = N$ is prime to p and $p > k$*
- *$M = Np$, $\mathfrak{m}$ is ordinary, and the Jordan-Holder factors of $\rho_\mathfrak{m}$ are distinct on a decomposition group D_p.*

Proof. It suffices work with a suitable maximal ideal in the Hecke ring with coefficients in $\mathbf{Z}_p$. The first statement then follows from the results of Faltings and Jordan, [FJ95], Thm. (2.1). The second statement follows, when $M = Np$ and $k = 2$, from [Wil95] Thm. 2.1. To extend to the higher weight, we briefly sketch how this follows from Hida's results on ordinary forms and cohomology groups [Hid85]. Hida has shown that there exists an isomorphism

$$eH_p^1(\Gamma_1(Np), L_n(\mathbf{F}_p)) = eH_p^1(\Gamma_1, \mathbf{F}_p), \tag{14}$$

where e is the idempotent giving the projection to the ordinary part. On the other hand, it follows from the properties of the universal Hecke ring $\mathbf{T}_\infty$ that

$$e\mathbf{T}_k/p = e\mathbf{T}_2/p, \tag{15}$$

where for each integer $k \geq 2$, $\mathbf{T}_k$ denotes the Hecke ring generated in the endomorphisms of $S_k(\mathbf{Z}_p)$. We may choose compatible maximal ideals at weight two and weight k so that the residual representations coincide; then the weight two result already verified shows that $H^1(\Gamma_1(Np), \mathbf{F}_p)^{\pm}$ is locally free of rank 1 over $\mathbf{T}_2/p$, for each choice of sign. But now the result follows upon combining (15) and (14). Note also that it follows from Hida's results the higher weight Hecke rings are Gorenstein, so that $\mathbf{T}_k^* \cong \mathbf{T}_k$ as $\mathbf{T}_k$-modules. $\square$

2 The Eisenstein case

In this section we show how to extend the foregoing results to the case of maximal ideal $\mathfrak{m}$ whose associated representation is *reducible*. To fix notation, we consider a normalized Hecke eigenform f of weight $k \geq 2$ as before. Given our fixed embedding $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}_p$, the form f defines a maximal ideal $\mathfrak{m}$ of residue characteristic p in $\mathbf{T}_k$ and a semisimple representation $\rho_\mathfrak{m} : \mathrm{Gal}\,(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{T}_k/\mathfrak{m})$ such that $\mathrm{Tr}\,(\mathrm{Frob}\,q) = a_q(f)$ for primes q not dividing Np. Our assumption is that $\rho_\mathfrak{m}$ is reducible, in the sense that there exist characters ξ_i such that

$$\rho_\mathfrak{m} = \xi_1 \oplus \xi_2.$$

Now let g be another eigenform satisfying $f \equiv g \pmod{\pi^r}$. There are two rather different possibilities here, depending on whether or not g is assumed to be an Eisenstein series. We will show how, in either of these two cases results similar to those previously obtained continue to hold. In addition to the elementary fact that the Mellin transforms of Eisenstein series are not neccesarily holomorphic, there are two technical difficulties in the present situation: the first is that the (co)-freeness of the cohomology is much more delicate, and the second is that the Manin-Drinfeld splitting will no-longer respect integral structures, as elements of the Eisenstein ideal do not act as units.

(2.1). We begin by explaining what is known about the Hecke-module structure of the cohomology. Freeness assertions analogous to (1.2) have been proven in the case of prime level in [Maz77], but it is unclear whether or not they will hold in general. To state a condition that is valid more often, we need to introduce some notation. Let $H_p^1(\Gamma, L_n(\mathcal{O}))_\mathfrak{m}$ denote the of $H_p^1(\Gamma, L_n(\mathcal{O}))$ at $\mathfrak{m}$. We may decompose $H_p^1(\Gamma, L_n(\mathcal{O}))$ according to the action of complex conjugation as usual. Our freeness hypothesis may then be stated as follows: for *some* choice of sign $\alpha \in \{+, -\}$, we have an isomorphism

1. $H_p^1(\Gamma, L_n(\mathcal{O}))^\alpha \cong S_k(\mathcal{O})_\mathfrak{m} \cong \mathrm{Hom}_\mathcal{O}(\mathbf{T}_k, \mathcal{O})_\mathfrak{m}$

When $k = 2$, it then follows from duality that for the opposite choice $-\alpha$ of sign, we will have $H_p^1(\Gamma, L_n(\mathcal{O}))^{-\alpha} \cong \mathbf{T}_k$. To require (co)-freeness of *both* eigenspaces is equivalent to the requirement that $\mathbf{T}_2$

be Gorenstein. It turns out that Condition 1 above is often true for appropriate α (see (2.7)), but, as we have already remarked, it is not known whether these rings are Gorenstein in general. Thus the condition may not hold for $-\alpha$.

From now on we assume that Condition 1 above is valid for at least one choice of α.

(2.2). First we treat the case of congruences between cuspforms. Thus let $f = \sum a_n q^n$ and $g = \sum b_n q^n$ be cuspidal Hecke eigenforms of level M, and assume that $a_n \equiv b_n \pmod{\pi^r}$ for each n. Assume further that f and g have residually reducible representations at the maximal ideal $\mathfrak{m} \subset \mathbf{T}_{k,\mathfrak{m}}$, and that the local factors of $\mathbf{T}_{k,\mathfrak{m}}$ determined by f and g are each one-dimensional over K. Choosing a sign α in Condition 1 above, we may define cocycles $\delta_*^\alpha \in H^1(\Gamma, L_n(\mathcal{O}))$ and complex periods Ω_*^α such that

$$\Omega_*^\alpha \delta_*^\alpha = \omega_*^\alpha. \tag{16}$$

Evidently, we will again have the congruence $\delta_f^\alpha \equiv \delta_g^\alpha$. Consider the modular symbols

$$\Delta_*^\alpha = \frac{\omega_*^\alpha}{\Omega_*^\alpha} \in S_\Gamma(L_n(\mathbf{C})).$$

We know that the image of Δ_*^α in $H_p^1(\Gamma, L_n(\mathbf{C}))$ represents the integral class δ_*^α. Now let $\tilde{\delta}_*^\alpha$ denote a lift of δ_*^α to $S_\Gamma(L_n(\mathcal{O}))$. We can make the choices so that $\tilde{\delta}_f^\alpha \equiv \tilde{\delta}_g^\alpha \pmod{\pi^r}$ (check this). Then $b_* = \delta_*^\alpha - \tilde{\delta}_*^\alpha \in B_\Gamma(L_n(\mathbf{C}))$ is a boundary symbol. Applying the operator η_q, we obtain the following result:

Theorem (2.3). *Let the cuspforms f and g be as above. Let $0 \le m \le k-2$ be an integer and let χ be a Dirichlet character with parity α. The we have the following congruence formula:*

$$\eta_q(f) \cdot \tau(\overline{\chi}) \cdot \begin{pmatrix} k-2 \\ m \end{pmatrix} m! \frac{L(m+1, f, \chi)}{(-2\pi i)^{m+1}\Omega_f^\alpha}$$
$$\equiv \eta_q(g) \tau(\overline{\chi}) \cdot \begin{pmatrix} k-2 \\ m \end{pmatrix} m! \frac{L(m+1, g, \chi)}{(-2\pi i)^{m+1}\Omega_g^\alpha} \pmod{\pi^r}. \tag{17}$$

Remark (2.4). Note that the quantities $\eta_q(*)$ will *not* be p-adic units. In particular, it is not clear that the quantities appearing in the the congruences are non-zero even for a single χ. However, we can do better if the character χ has conductor prime to the level, as the next theorem demonstrates.

Theorem (2.5). *Let f and g be as before. Let χ be a Dirichlet character of parity α and conductor m prime to the level M. If $k = 2$ then we have the congruence*

$$\tau(\overline{\chi}) \cdot \frac{L(1, f, \chi)}{(-2\pi i)\Omega_f^\alpha} \equiv \tau(\overline{\chi}) \frac{L(1, g, \chi)}{(-2\pi i)\Omega_g^\alpha} \pmod{\pi^r}.$$

If $k > 2$ and $p|N$, then the same congruence holds modulo π.

Proof. Assume that $k = 2$. We contend then that the χ-twisted special values of the boundary symbols b_* vanish. This may be seen as follows. Observe that if m is an integer prime to M, then any two cusps of the form a/m with $(a, m) = 1$ are equivalent under $\Gamma = \Gamma_1(M)$. The definitions, together with the fact that χ is nontrivial, now imply that the special value of the boundary symbol vanishes. Going back to the definitions of the modular symbols $\tilde{\Delta}_\alpha^*$, we find that the twisted special values of Δ_*^α and $\tilde{\Delta}_*^\alpha$ are equal. The result for $k = 2$ is now immediate, since the lifts $\tilde{\Delta}_*^\alpha$ were chosen so that $\tilde{\Delta}_f^\alpha \equiv \tilde{\Delta}_g^\alpha$.

To obtain the assertion about higher weight, we consider the usual morphism $L_n(\mathcal{O}) \to \mathbf{F}$ given by projecting onto the coefficient of Y^n and reducing modulo π. Since $p|M$, this will be a Γ-morphism. Evidently this map commutes with the twist operator. The weight-two argument used above now implies that the Y^n component of the twisted boundary symbol vanishes modulo π. Thus we get the asserted congruence at $s = 1$. □

Remark (2.6). As in the previous section, it can be shown that there exists χ such that the quantities appearing in the congruences are nonzero.

Now we give conditions for the validity of Condition 1. I am grateful to Wiles for explaining his work to me in this context.

Theorem (2.7). *Let ξ_1 and ξ_2 be the characters appearing in the semisimple representation $\rho_{\mathfrak{m}}$. Then Condition 1 is satisfied, for suitable α, in each of the following situations:*

- *For $k = 2$, when $\Gamma = \Gamma_0(q)$ for a prime q, and p divides the numerator of $(q-1)/12$. In this case 1 is valid for both choices of α.*
- *when f is a p-stabilized newform of level Np, even weight $k \geq 2$, and the characters ξ_i are distinct on D_p. In this case we may take $\alpha = -\xi_1(-1)$, where the character ξ_1 is determined as follows. If both ξ_i are unramified then ξ_1 is determined by the requirement that the eigenvalue of U_p on f be congruent to $\xi_1(p) \pmod{\mathfrak{m}}$. Otherwise precisely one of the two characters in ramified at p, and we take ξ_1 to be the unramified one.*
- *For $k = 2$, and $\Gamma = \Gamma_1(N)$, with $(N,p) = 1$. In this case we take ξ_1 to be the unique unramified character appearing in $\rho_{\mathfrak{m}}$, and define α as above.*

Proof. The first statement follows from work of Mazur [Maz77]. We warn the reader that the group $\Gamma_0(q)$ may have non-zero torsion, so that the results of this paper are not directly applicable. The modifications are standard and we omit them.

As for the second assertion, we first treat the case of weight 2 and level Np. Once again, we may assume that $\mathcal{O} = \mathbf{Z}_p$. Let the character ξ_1 be as in the statement of the theorem. Let $\mathcal{D} = J_1(Np)[p^\infty]_{\mathfrak{m}}$, and let $\mathcal{D}^0$ and $\mathcal{D}^{\text{ét}}$ be the submodule and quotient respectively of $\mathcal{D}$ defined in (2.2) of [Wil95]. Then the action of a decomposition group D_p on $\mathcal{D}^{\text{ét}}$ is unramified, and $\mathrm{Frob}\,(p)$ acts via U_p. Assume now that ξ_2 is such that group $\Delta_{(p)}$ of [Wil95], page 483, is nontrivial (this amounts to the restriction that $\xi_2 \neq \omega$ on D_p). In this we may use the argument on pages 483-484 of [Wil95] to conclude that

$$\mathcal{D}^0[p] = \mathbf{T}_{\mathfrak{m}}/p, \quad \text{and} \quad \mathcal{D}^{\text{ét}}[p] = \mathrm{Hom}\,(\mathbf{T}_{\mathfrak{m}}/p, \mathbf{Z}/p\mathbf{Z}), \tag{18}$$

where the isomorphisms are as $\mathbf{T}_{\mathfrak{m}}$-modules. Note that this part of Wiles' argument does *not* require the hypothesis that $\rho_{\mathfrak{m}}$ be irreducible. Note also that the action of Galois on $\mathcal{D}^{\text{ét}}$ is via the character ξ_1, which has parity $-\alpha$. It follows now from (18) that $\mathrm{Ta}_p(J_1(Np))^{\alpha}_{\mathfrak{m}}$ is free as a $\mathbf{T}_m$-module. But now $\mathrm{Ta}_p(J_1(Np))_{\mathfrak{m}} = H_1(X_1(Np, \mathbf{Z}_p))_{\mathfrak{m}}$ canonically by the Albanese map, and an application of Poincaré duality (cap product with the orientation class in H^2) shows that $H^1(X, \mathbf{Z}_p)^{-\alpha}_{\mathfrak{m}} = H^1_p(\Gamma, \mathcal{O})^{-\alpha}_{\mathfrak{m}}$ is free as a $\mathbf{T}_{\mathfrak{m}}$-module. On the other hand cup-product gives a self-duality of $H^1_p(\Gamma, \mathbf{Z}_p) = H^1(X, \mathbf{Z}_p)$, and since the cup-product is alternating we find that $H^1_p(\Gamma, \mathcal{O})^{\alpha}_{\mathfrak{m}}$ is co-free, as asserted. Note that we have used the fact the the comparison isomorphisms between the étale, Betti, and group cohomologies preserve the action of complex conjugation.

In the case where the $\xi_2 = \omega$, we may may use Lemma 2.2 of [Wil95], which is valid even for reducible $\mathfrak{m}$, and once again deduce (18). This completes the proof of the theorem in weight two and level Np.

To extend to higher weights, we use Hida's theory as in (1.13) to show that

$$H^1_p(\Gamma, L_n(\mathbf{F}_p))^\alpha = H^1_p(\Gamma, \mathbf{F}_p)^\alpha = \mathrm{Hom}\,(\mathbf{T}_k/p, \mathbf{Z}/p).$$

The result now follows from the lemma on dualizing modules on page 249 of [MW86].

The final assertion of the theorem may be proven by using the q-expansion principle, as in the paper of Wiles already cited. The argument is similar but easier, owing to the the fact that we have good reduction at p. $\square$

(2.8). We now want to treat the case where g is assumed to be an Eisenstein series. This was already treated in [Maz79] for the case of $\Gamma_0(q)$ and in [Ste82] for more general groups. However the main result (4.2.3) in [Ste82] is subject to the unverified hypothesis (4.2.2). The proof of our theorem (2.10) is very similar to that of Stevens; the main advantage is that we are able to work with Eisenstein series rather than the cuspidal group. Furthermore, our Condition 1 which replaces the first part of Stevens' (4.2.2), may be verified in the cases of interest.

To state our theorem we need to recall some facts about Eisenstein series. Let ψ_1 and ψ_2 be (not neccesarily primitive) Dirichlet characters of conductors N_1 and N_2 respectively, such $\psi_1\psi_2(-1)$ is *even.* Let $M = N_1 \cdot N_2$; we assume that $N \geq 4$. Then there exists (see [Ste82] (3.4.2), where the normalization is somewhat different) a holomorphic Eisenstein series

$$E = \sum a_n(E)q^n = E(\psi_1, \psi_2)$$

of weight 2 on $\Gamma = \Gamma_1(M)$ whose associated Dirichlet series is given by $L(s, \psi_1) \cdot L(s-1, \psi_2)$.

For each integer $k \geq 1$, we let $\mathbf{B}_k$ denote the k-th Bernoulli polynomial. Then $\mathbf{B}_1 = X - 1/2$. For a Dirichlet character χ of conductor m we have

$$L(1-n, \chi) = m^{n-1} \cdot \sum_{a=1}^{m} \chi(a)\mathbf{B}_n\left(\frac{a}{m}\right). \tag{19}$$

Now let $f = \sum a_n(f)q^n$ be a weight two cuspform. We assume only that f is an eigenform for all the Hecke operators. Let $p \geq 3$ be a prime. We say that $f \equiv E \pmod{\pi^r}$ if $a_n(E) \equiv a_n(f) \pmod{\pi^r}$ for each $n > 0$ and if a certain condition on the constant terms of the q-expansions of E at the various cusps of Γ is satisfied. To state this condition, let ω_E denote the differential form on Y associated to E. Then, for each cusp s of Γ, we require that the quantity $2\pi i \cdot \mathrm{Res}_s(\omega_E)$ be an algebraic integer, divisible by π. We note that the cohomology class associated to E is algebraic by the Manin-Drinfeld argument, so that these residues are in fact algebraic. The number $2\pi i \cdot \mathrm{Res}_s(\omega_E)$ may also be described as the constant term of the q-expansion of E at the cusp s.

Remark (2.9). The condition on the residues is redundant if $p \geq 5$ and the level M is prime to p. This follows from the q-expansion principle in characteristic p. It is not redundant if $p = 3$, as the mod 3 Hasse invariant occurs in weight 2.

Theorem (2.10). *Let f be a p-stabilized cuspidal newform of weight 2 and level Np. Assume that there exists a p-stabilized Eisenstein series E as above such that $f \equiv E \pmod{\pi^r}$. Suppose that $\psi_2 \neq \psi_1$, and let $\alpha = -\psi_1(-1)$. Then Condition 1 holds for α, and for each nontrivial primitive Dirichlet character χ of* *conductor prime to Np there exists a period Ω_E which is a p-adic unit such that the following congruence holds:*

$$\tau(\overline{\chi}) \cdot \frac{L(1,f,\chi)}{(-2\pi i)\Omega_f^\alpha} \equiv \tau(\overline{\chi}) \cdot \frac{L(1,E,\chi)}{(-2\pi i)\Omega_E \pmod{\pi^r}} \tag{20}$$

Proof. The validity of Condition 1 is a direct application of (2.7). To prove the the rest of the theorem we will use the results of [Ste82] and [Ste85]. Let $\delta_E \in H^1(\Gamma, K)$ be the coycle defined by $\delta_E(\gamma) = \int_z^{\gamma z} \omega_E$, where $\gamma \in \Gamma$ and z is any point in the upper half-plane. As we have already remarked, the algebraicity of this cocycle follows from the Manin-Drinfeld argument. Then it follows from [Ste82], (3.2.5), that $\delta_E \in h^1(\Gamma, K)^\alpha$. Since $(N,p)=1$, it follows from [Ste85], Thm. 1.3 that δ_E takes values in $\mathcal{O}$. Indeed, the integrality of the residues is part of the hypothesis. As for the L-values, it suffices (since p is odd) to show that, for each nontrivial primitive character χ of parity α, that

$$\tau(\overline{\chi})\frac{L(1,E,\chi)}{2\pi i}$$

is integral. Note the normalization in [Ste85], (1.3) and (1.5); Stevens' $a_{nN}(E)$ is our $a_n(E)$. But now it follows from the definitions that

$$\tau(\overline{\chi}) \cdot \frac{L(1,E,\chi)}{2\pi i} = \tau(\overline{\chi})\frac{L(1,\psi_1\chi)}{2\pi i} \cdot L(0,\psi_2\chi).$$

Since E is p-stabilized, ψ_1 has conductor prime to p and ψ_2 is considered as having conductor divisible precisely by the first power of p. Then an explicit calculation with (19) shows that the second factor is integral. The integrality of the first factor follows from the functional equation, and the fact that the conductor is prime to p. Thus $\delta_E \in H^1(\Gamma, \mathcal{O})$.

Now let $R = \mathcal{O}/\pi^r$. Since we have assumed that the residual divisor is divisible by π^r, it follows that the image $\overline{\delta}_E$ of δ_E in $H^1(\Gamma, R)$ lies in the subgroup $H^1_p(\Gamma, R)$. Note that $\overline{\delta}_E \neq 0$; this follows from a theorem of Washington (see [Ste82], §3.5, and [Was78]). It even follows from Washington's result that $\overline{\delta}_E$ is not divisible by π; the point is that there exists a period which is a p-adic unit.

On the other hand, let $\delta_f^\alpha \in H^1_p(\Gamma, \mathcal{O})$ be the canonical cocycle attached to f, and let $\overline{\delta}_f^\alpha$ denote the reduction mod π^r. We contend that there exists a nonzero $u \in R^*$ such that

$$\overline{\delta}_E^\alpha = u \cdot \overline{\delta}_f^\alpha.$$

To see this we recall that $H^1_p(\Gamma, \mathcal{O})_\mathfrak{m} = \mathrm{Hom}\,(\mathbf{T}_\mathfrak{m}, \mathcal{O})$, and since we are working with constant coefficients and since $\mathbf{T}_\mathfrak{m}$ is a free $\mathcal{O}$-module we have

$$H^1_p(\Gamma, R)_\mathfrak{m} = H^1_p(\Gamma, \mathcal{O})_\mathfrak{m} \otimes R = \mathrm{Hom}\,(\mathbf{T}_\mathfrak{m} \otimes R, R)$$

as $\mathbf{T}_\mathfrak{m} \otimes R$-modules. Let $s \in \mathrm{Hom}\,(\mathbf{T}_\mathfrak{m} \otimes R, R)$ be the morphism that send the Hecke operator t onto the class of $a_1(f|t) \pmod{\pi^r}$. One checks easily that s is an eigenvector for the action of $\mathbf{T}_\mathfrak{m} \otimes R$ on $\mathrm{Hom}\,(\mathbf{T}_\mathfrak{m} \otimes R, R)$, with eigenvalues congruent to those of f. Furthermore, the space of such eigenvectors is obviously free of rank one (evaluate on the identity operator). Since both $\overline{\delta}_E^\alpha$ and $\overline{\delta}_f^\alpha$ have the same set of eigenvalues modulo π^r, and neither is divisible by π, the existence of the unit u follows.

Now we compute the special values. Let $\lambda(\chi) \in H_1(X, R[\chi])$ denote the homology class associated to χ. We would like to 'integrate' δ_E along $\lambda(\chi)$. However, the Eisenstein cohomology class does *not* extend to X, and so some care is required. The crucial point is that the 'mod p' cocycle $\overline{\delta}_E$ does extend: we have $\overline{\delta}_E \in H^1_p(\Gamma, R) = H^1(X, R)$. The cap-product $\overline{\delta}_E \cap \lambda(\chi)$, is well-defined, and takes the place of the integral.

Stevens has computed this cap-product explicitly by using the classical theory of Dedekind sums, and a suitable lift of $\lambda(\chi)$ to the space $H_1(Y, \mathbf{Z}[\chi])$, where the periods of the Eisenstein series are well-defined. This calculation is rather involved, and we will not attempt to reproduce it here (see [Ste82], Section (3.1.5) for the details). The result, however, may be simply stated: Stevens shows that

$$\delta_E^\alpha \cap \lambda(\chi) \equiv \tau(\overline{\chi}) \frac{L(1, E, \chi)}{2\pi i} \pmod{\pi^r}.$$

On the other hand, cap-product in characteristic zero reduces to integration upon scalar extension to the reals, and we have

$$\delta_f^\alpha \cap \lambda(\chi) = \left(\frac{\omega_f^\alpha}{\Omega_f^\alpha}\right) \cap \lambda(\chi) = \frac{1}{\Omega_f^\alpha} \int_{\lambda(\chi)} \omega_f^\alpha.$$

Since cap product commutes with reduction mod p, this evidently implies the theorem.

Remark (2.11). It would be interesting to extend the above results to Eisenstein series of higher weight. One can define algebraic cocycles $\delta_E \in H^1(\Gamma, L_n(K))$ as before, but in this case integrality properties become rather delicate. It seems rather likely that one can give a similar treatment to the one for weight two if one assumes that $p > k$, using, for instance, the results in [Ste89], §6, but we have not pursued the details.

Remark (2.12). The requirement in the theorem that f be p-stabilized is harmless, since Eisenstein primes at level N prime to p are ordinary. Given a form of level N, we may pass to a p-stabilized form of level Np and apply the theorem. However, it is important to note that the same theorem holds at level N (the proof is the same). This has the advantage that we may may consider characters of conductor divisible by p. We will use this variant in the next section.

3 An Application to Nonvanishing Theorems

(3.1). Let C be a modular elliptic curve with a rational point of order p (so $p = 3, 5$, or 7). Let $\rho_0 : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{F}_p)$ denote the representation on the p-division points of C. Then since C has a rational p-torsion point, we see that ρ_0 contains the trivial representation as a subobject. Since the determinant of ρ_0 is given by the mod p Teichmuller character $\omega : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{F}_p^*$, we find that the semisimplification ρ of ρ_0 is given by

$$\rho = 1 \oplus \omega. \tag{21}$$

Now let $f = \sum a_n q^n$ be the newform such that $L(s, f) = L(s, C)$. If $q \neq p$ is a prime of good reduction for C, then (21) shows that

$$a_q \equiv \omega(q) + 1 \pmod{p}. \tag{22}$$

Let E denote the non-holomorphic Eisenstein series of level 1 and weight 2. In the language of the previous section this is $E(1, 1)$, and we have

$$E(z) - \frac{1}{8\pi y} = \frac{-1}{24} + \sum_{n=1}^{\infty} \sigma(n) q^n$$

where $\sigma(n) = \sum_{d|n} d$. Thus we may restate (22) as follows: we have

$$a_q \equiv \sigma_q \pmod{p}.$$

In view of the results of section 2 above, this suggests strongly that there should be a mod p relationship between the L-values of f and those of E. Thus let D be a square-free negative integer and let χ_D be the odd quadratic character corresponding to the field $\mathbf{Q}(\sqrt{D})$. Then the twist of E by χ_D is the Eisenstein series $E_D = E(\chi_D, \chi_D)$, and we have

$$\tau(\chi_D)\frac{L(1, E_D)}{-2\pi i} = \tau(\chi_D)\frac{L(1, \chi_D)}{-2\pi i} \cdot L(0, \chi_D) = \frac{1}{2}L(0, \chi_D)^2.$$

But the analytic class-number formula states that $L(0, \chi_D)$ is essentially the class-number $h(D)$ of $\mathbf{Q}(\sqrt{D})$. Thus we expect a mod p relationship between $L(1, C \otimes \chi_D)$ and $h(D)$. In particular, we expect that $L(1, C \otimes \chi_D) \neq 0$ whenever $h(D) \neq 0 \pmod 3$. Results of this kind have been obtained by a number of authors, for instance Frey [Fre88], Nekovář, [Nek90], and James [Jam]. While Nekovář and James work with specific C, Frey proves a general result on the Selmer groups of such elliptic curves C, showing that under certain conditions the twisted 3-Selmer group $S(C \otimes \chi_D)$ is trivial if the class number $h(D)$ is prime to 3. Our result below may be viewed as a complement to the theorem of Frey, with the link being given by the Birch-Swinnerton-Dyer conjecture. It would be interesting to compare Frey's results to ours more explicitly; we note only that we can recover the triviality of the 3-Selmer groups in the present situation by invoking the theorem of Kolyvagin.

(3.2). To state the theorem we need some notation. Let C be a modular elliptic curve with a rational point of order p. Assume that C has good, ordinary reduction at p. Let q be any odd prime with $q \equiv 1 \pmod 9$ if $p = 3$ and $q \equiv 1 \pmod p$ if $p = 5, 7$, such that C has good reduction at q. Let N_1 the product of primes $\ell | N$ where C has either nonsplit multiplicative reduction or additive reduction, and let N_2 denote the product of primes of additive or split multiplicative reduction, together with the prime q.

Theorem (3.3). *Let the curve C be as above. Then there is a period Ω^- for C such that $\tau(\chi_D)\frac{L(1,E\otimes\chi_D)}{(-2\pi i)\Omega^-}$ is integral for any negative square-free integer D. Furthermore, if D is prime to Nq, we have the congruence*

$$\begin{aligned} &(1 - \chi_D(q)/q) \cdot \tau(\chi_D)\frac{L(1, C \otimes \chi_D)}{(-2\pi i)\Omega^-} \\ &\qquad \equiv \frac{1}{2}\prod_{\ell | N_1}(1 - \chi_D(\ell)/\ell)\prod_{\ell | N_2}(1 - \chi_D(\ell)) \cdot L(0, \chi_D)^2 \pmod{p}. \end{aligned} \tag{23}$$

Proof. The idea is of course to exhibit an Eisenstein series congruent to f, where f is the newform associated to C, and then apply (2.10), or, more precisely, the variant described in (2.12). We will only give the proof for $p = 3$, as the other cases are analogous. Let E^q be the unique holomorphic Eisenstein series on $\Gamma_0(q)$. Then the constant term of the q-expansion at infinity is given by $(q-1)/24$. Since there are only two cusps on $\Gamma_0(q)$ and since the sum of the residues is zero, we see that the residue at zero is given by $(1-q)/24$. Since $q \equiv 1 \pmod 9$ it follows that these residues are divisible by 3. Obviously the same is true for the residual divisor of E^q on $\Gamma_1(q)$. Furthermore, the same argument as in the proof of (2.10) shows that E^q represents an integral cohomology class. Observe that the eigenvalue for U_q on E^q is equal to 1.

Now since q is a prime of good reduction for C, we may use (22) to conclude that the roots of the Hecke polynomial at q for C has both roots congruent to 1 modulo 3. Let f^q denote the form obtained from f by removing one of the Euler factors at q arbitrarily. Then the eigenvalue of U_q on f^q is also congruent to 1 modulo 3.00

We would like to adjust E^q by removing Euler factors so that the resulting form has Hecke eigenvalues congruent to those of f^q. It is actually more convenient for the study of these Euler factors to work in a more general context. For a positive integer r let s_r denote the matrix

$$\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}.$$

Then, for any integer T, there is a map $\Gamma_1(Tr) \to \Gamma_1(T)$ defined by $\gamma \mapsto s_r\gamma s_r^{-1}$. This induces a map $\pi_r : Y_1(Tr) \to Y_1(T)$ given locally on $\mathcal{H}$ by $z \mapsto rz$. Then is $g(z)$ is a weight-two modular form of level R, we find that $\pi^*(g(z)dz) = rg(rz)dz$. Thus If we write φ_r for the cocycle on $\Gamma_1(Tr)$ obtained by integrating $rg(rz)$, then $\varphi_r(\gamma) = \varphi(s_r\gamma s_r^{-1})$, where φ is the cocycle on $\Gamma_1(T)$ attached to g. Thus $rg(rz)$ defines an integral class on $\Gamma_1(Tr)$ whenever $g(z)$ defines an integral class on $\Gamma_1(T)$. Furthermore, since conjugation by s_r takes parabolic elements to parabolic elements, we see that φ_r vanishes modulo 3 if on parabolic elements of $\Gamma_1(Tr)$ if φ has this property at level T. If r is not divisible by 3, then these conclusions are also valid for $g(rz)$.

We now iterate this, removing Euler factors as appropriate, at primes ℓ of bad reduction for C. We will only treat the nonsplit multiplicative case, as the other possibilities are similar but easier. Write the Fourier expansion of f as $f = \sum a_n(f)q^n$. In the nonsplit case it is known that that $a_\ell(f) = -1$. Furthermore, a theorem of Langlands and Deligne (see [Car86]) shows that $c_\ell(f)$ arises as the eigenvalue of $\mathrm{Frob}\,(\ell)$ on the maximal unramified quotient of $\mathrm{Ta}_3(C)$. It follows from the fact that the composition factors on the mod 3 representation for C are 1 and ω that ℓ must be such that $\omega(\ell) = -1$. Thus we may replace $E^q(z)$ by $E^q(z) - E^q(\ell z)$ to obtain a form with eigenvalue congruent to -1 at ℓ. Since ℓ is a 3-adic unit this form represents an integral class and has residues divisible by 3 in $\mathbf{Z}_3$.

Thus we finally obtain an Eisenstein series E of level qN, where N is the conductor of E, and such that $E \equiv f^q$, where f^q is the form previously defined. To check the eigenvalue at 3, we need Theorem 2.1.4 of [Wil88]. We may write $E = E(\psi_1, \psi_2)$ where each ψ_i is the trivial character, but viewed as having nontrivial conductors N_i, as follows. If ℓ is a prime of split multiplicative reduction, then we may assume that ℓ divides N_2. If ℓ is a prime of nonsplit multiplicative reduction then ℓ divides N_1. Primes of additive reduction divide both N_i, and q divides the conductor of N_2.

In view of (2.10), it remains only to compute the special values of E. A brief calculation shows that these are given explicitly as follows:

$$\tau(\chi_D)\frac{L(1, E, \chi_D)}{-2\pi i} = \frac{1}{2}\prod_{\ell|N_1}(1 - \chi_D(\ell)/\ell)\prod_{\ell|N_2}(1 - \chi_D(\ell)) \cdot L(0, \chi_D)^2. \tag{24}$$

This completes the proof of the theorem. □

Corollary (3.4). *Let C be as in the theorem. Assume that each prime of additive reduction is congruent to 1 modulo p. Let D be such that $\chi_D(\ell) = -1$ for primes ℓ of additive or split multiplicative reduction, and such that $\chi_D(\ell)/\ell \equiv -1 \pmod p$ for primes of nonsplit reduction. Then $L(1, C \otimes \chi_D) \neq 0$ if the class number $h(D)$ of $\mathbf{Q}(\sqrt{D})$ is prime to p.*

Proof. We note first of all the hypothesis on D ensures that the Euler factors at prime $\ell|Np$ on the right-hand-side of (23) are nonzero modulo p. Given D we may choose q so that the Euler q-factors on both sides are nonzero. The corollary now follows from the analytic class number formula. □

Corollary (3.5). *Take $p = 3$, and let C be as in the corollary. Then there exists an arithmetic progression S modulo N if N is odd and modulo l.c.m.$(N, 4)$ if N is even, such that, for all square-free integers $D < 0$ in S, the value $L(1, f \otimes \chi_D) \neq 0$ if the class number of $\mathbf{Q}(\sqrt{D})$ is prime to 3. Let T be the set of fundamental discriminants D in S; then the subset of D for which $L(1, C \otimes \chi_D) \neq 0$ has proportion at least $1/2$ in T.*

Proof. The existence of S follows from quadratic reciprocity. The last statement is a consequence of a theorem due to Nakagawa and Horie [NH88]; see [Jam], Thm. 3.4 and Cor. 3.5. One has to check that the conditions of James' Cor. 3.5 are satisfied but the verification is elementary.

Remark (3.6). It can be shown (see [Won]) that there are infinitely many nonisomorphic curves satisfying the conditions of (3.2), with $p = 3$. There are even infinitely many such curves whose conductor is square-free.

Example (3.7). Let C be the elliptic curve 19B in Cremona's tables [Cre92]. An equation for C is $y^2 + y = x^3 + x^2 - 9x - 15$. Then C has a rational point of order three and is of conductor 19. The associated modular form f is ordinary at three, so that C has ordinary reduction. The epsilon factor in the functional equation is 1 (all these facts can be checked in Cremona). We conclude that the epsilon factor for $C \otimes \chi_D$ is given by $\chi_D(-19)$, whenever D is prime to 19. This will be positive iff $\chi_D(19) = -1$. A conjecture of Goldfeld [Gol79] predicts that $L(1, C \otimes \chi_D) \neq 0$ for essentially 'all' such D; our theorem asserts that this is the case for a subset of D with proportion at least 1/2.

Remark (3.8). Given a cusp form f, one can attempt an analysis similar to that above whenever the p-adic Galois representation associated to f is reducible modulo p, for some prime p. The results of this paper show that one obtains a congruence between the special values of f and the class numbers of certain abelian number fields. It would be interesting to unwind the Cohen-Lenstra heuristics to obtain conditional results for nonvanishing. For example, one can work with elliptic curves with 5 or 7 torsion points. It is clear that one should get a better proportion of nonvanishing twists.

References

[AS86] A. Ash and G. Stevens, *Modular forms in characteristic ℓ and special values of their L-functions*, Duke Math. J. **53** (1986), no. 3, 849–868.

[BK90] S. Bloch and K. Kato, *L-functions and the Tamagawa numbers of motives*, Grothendieck Festschrift (P. Cartier *et al*, ed.), vol. 1, Birkhauser, 1990.

[Car86] H. Carayol, *Sur les représentations p-adiques attachées aux formes modulaires de Hilbert*, Ann. Sci. Ec. Nor. Sup. **IV, Ser. 19** (1986), 409–468.

[Coa91] J. Coates, *p-adic L-functions*, L-Functions and Arithmetic (J. Coates and M. Taylor, eds.), Cambridge University Press, 1991.

[Cre92] J. Cremona, *Algorithms for elliptic curves*, Cambridge University Press, 1992.

[DH71] H. Davenport and H. Heilbronn, *On the density of discriminants of a cubic fields II*, Proc. Roy. Soc. London, Ser. A **322**, 1971, 405–420.

[DI95] F. Diamond and J. Im, *Modular curves and modular forms*, Seminar on Fermat's last theorem, Toronto, 19993 (K. Murty, ed.), C.M.S. Conference Proceedings, Amer. Math. Soc., 1995, pp. 39–133.

[FJ95] G. Faltings and B. Jordan, *Crystalline cohomology and $GL_2(\mathbf{Q})$*, Israel J. Math. (1995).

[Fre88] G. Frey, *On the Selmer groups of twists of elliptic curves with $\mathbf{Q}$-rational torsion points*, Can. J. Math. **XL** (1988), no. 3, 649–665.

[Gol79] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory, Carbondale, Springer Lecture Notes, vol. 751, Springer Verlag, 1979, pp. 108–118.

[Gre89] R. Greenberg, *Iwasawa theory for p-adic representations*, Adv. Stud. Pure Math. (J. Coates, ed.), vol. 17, American Math. Soc., 1989.

[GS93] R. Greenberg and G. Stevens, *p-adic L-functions and p-adic periods of modular forms*, Invent. Math. **111** (1993), 407–447.

[Hid81] H. Hida, *Congruences of cusp forms and special values of their zeta functions*, Invent. Math. **63** (1981), 225–261.

[Hid85] H. Hida, *Galois representations into $GL_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms*, Invent. Math. **85** (1985), 545–613.

[Iwa90] H. Iwaniec, *On the order of nonvanishing of L-functions at the critical point*, Sem. Théorie des Nombres Bordeaux **2** (1990), 365–376.

[Jam] K. James, *L-series with nonzero central critical value*, to appear.

[Koh97] W. Kohnen, *On the proportion of quadratic twists of modular forms nonvanishing at the central critical point*, preprint, 1997.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Pub. Math. I.H.E.S. **47** (1977), 33–189.

[Maz79] B. Mazur, *On the arithmetic of special values of L-functions*, Invent. Math. **55** (1979), 207–240.

[MM91] M.R. Murty and V.K. Murty, *Mean values of derivatives of modular L-series*, Ann. Math. **133** (1991), 447–75.

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogs of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1–48.

[MW86] B. Mazur and A. Wiles, *On p-adic analytic families of Galois representations*, Compostio Math. **59** (1986), 231–264.

[NH88] J. Nakagawa and K. Horie, *Elliptic curves with no torsion points*, Proc. A.M.S. **104** (1988), 20–25.

[Nek90] J. Nekovář, *Class numbers of quadratic fields and Shimura's correspondence*, Math. Annalen **287** (1990), 577–594.

[OSa] K. Ono and C. Skinner, *Fourier coefficients of half-integer weight forms modulo ℓ*, To appear in *Ann. Math.*

[OSb] K. Ono and C. Skinner, *Nonvanishing of quadratic twists of modular L-functions*, preprint.

[RW82] K. Rubin and A. Wiles, *Mordell-Weil groups of elliptic curves over cyclotomic fields*, Number theory related to Fermat's last theorem (N. Koblitz, ed.), Birkhauser, 1982.

[Shi76] G. Shimura, *The special values of zeta functions associated with cusp forms*, Comm. Pure Applied Math. **29** (1976), 783–804.

[Ste82] G. Stevens, *Arithmetic on modular curves*, Progress. Math., vol. 20, Birkhauser, 1982.

[Ste85] G. Stevens, *The cuspidal group and special values of L-functions*, Trans. Amer. Math. Soc. **291** (1985), no. 2, 519–550.

[Ste89] G. Stevens, *The Eisenstein measure and real quadratic fields*, Théorie des nombres, Québec, 1987 (J.-M. de Koninck and J. Levesque, eds.), de Gruyter, 1989, pp. 887–927.

[Was78] L. Washington, *The non-p-part of the class number in a cyclotomic* $\mathbf{Z}_p$*-extension*, Invent. Math. **49** (1978), 87–97

[Wil88] A. Wiles, *On ordinary* λ*-adic representations associated to modular forms*, Invent. Math. **94** (1988), 529–573.

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's last theorem.*, Ann. Math. **141** (1995), 443–551.

[Won] S. Wong, *Elliptic curves of rank zero*, preprint.