Special Values of Anticyclotomic L-functions

V. Vatsal
Dept. of Mathematics
University of British Columbia
vatsal@math.ubc.ca

August 12, 2003

1 Introduction

The object of this paper is to extend the results and methods of [Vato1], where it was shown how cases of a conjecture of Mazur on the behavior of L-functions in an anticyclotomic $\mathbf{Z}_p$-extension could be deduced by studying the distribution of Heegner points associated to definite quaternion algebras. The main result of [Vato1] showed that when the sign in the functional equation is $+1$, then the special values of the L-functions in question are generically nonzero. In this paper we propose to study the special values modulo a prime λ of $\overline{\mathbf{Q}}$, and can offer three new theorems in this direction.

The first result (Theorem 1.1) determines the Iwasawa μ-invariant of the p-adic L-functions of Bertolini and Darmon. We show that μ is usually zero but not always; when $\mu \neq 0$, we give a precise formula for the value, and an interpretation of the positivity in terms of congruences.

The second result (Theorem 1.2) pertains to the case where λ has residue characteristic $\ell \neq p$. In this case, we show that the L-values are typically units, but, again, that this is not always the case. For technical reasons, this theorem applies only to a restricted class of ℓ, but it seems rather likely that the restrictions can be lifted.

Finally, we use the result of Theorem 1.2 to transfer our results from the case where the sign in the functional equation is $+1$ to the case of sign -1, and to *derivatives* of L-functions. This is achieved by using congruences and the sign-change phenomenon exploited by Bertolini-Darmon, namely, we prove a 'Jochnowitz congruence' which relates the nontriviality of a special value modulo λ to the nontriviality of a *classical* Heegner point on a modular curve. The result is stated in Theorem 1.4.

To describe these results more precisely, let g denote a newform on $\Gamma_0(N)$. Let K denote an imaginary quadratic field of discriminant D, such that D is prime to N. Write $N = N^+ \cdot N^-$, where N^+ is divisible only by those primes which are split in K, whereas N^- is divisible only by primes

which are inert. We make the assumption that N^- is square-free and divisible by an odd number of primes. Then the L-function $L(g, K, s)$ has a functional equation with sign $+1$. Furthermore, if χ is an anticyclotomic character with conductor $\mathfrak{f}$ prime to ND, then the twisted L-function $L(g, \chi, s)$ also has a functional equation with sign $+1$.

We are interested in studying the values $L(g, \chi, 1)$ as χ varies over characters of p-power conductor, for some fixed prime p. In our previous paper [Vato1], we showed that $L(g, \chi, 1) \neq 0$ for all but finitely many χ of p-power conductor. In this paper, we shall study the algebraic part of $L(g, \chi, 1)$ modulo a given prime λ of $\overline{\mathbf{Q}}$.

Thus, we fix a prime λ of $\overline{\mathbf{Q}}$, with residue characteristic ℓ. Then, following a construction of Hida, we define a canonical period Ω_g^{can} associated to g by saying

$$\Omega_g^{\mathrm{can}} = \frac{(g, g)}{\eta_0},$$

where (g, g) is the Petersson inner product on $\Gamma_0(N)$, and η_0 is Hida's congruence number associated to g. The precise definition is given in §2.4. Here we remark only that η_0 measures congruences modulo λ between g and modular forms of level dividing N on $\Gamma_0(N)$. It is known that the quantity

$$L^{\mathrm{al}}(g, \chi, 1) = \frac{L(g, \chi, 1)}{\Omega_g^{\mathrm{can}}} \tag{1}$$

is a λ-adic integer. We want to determine the valuation of $L^{\mathrm{al}}(g, \chi, 1)$ for χ of conductor p^n, as $n \to \infty$. To state the results, we need to introduce two further numbers C_{csp} and C_{Eis} associated to g. We will give the precise definitions of these in §2.4, and make some further comments in the discussion following Theorem 1.2 below. For the moment, we content ourselves with saying that C_{csp} measures congruences between g and cuspforms that do *not* occur on the quaternion algebra $B = B_{K,f}$, of discriminant N^-. On the other hand, C_{Eis} measure congruences between g and a space of Eisenstein series. Then we will show that the valuation of $L^{\mathrm{al}}(g, \chi, 1)$ approaches that of $C_{\mathrm{csp}} \cdot C_{\mathrm{Eis}}^2$ as $n \to \infty$.

Now let H_n denote the ring class field of K with conductor p^n, and let $H_\infty = \cup H_n$. Let $G_\infty = \mathrm{Gal}(H_\infty/K)$, and $G_n = \mathrm{Gal}(H_n/K)$. Then $G_\infty = G_1 \times \Delta_\infty$, where Δ_∞ is topologically isomorphic to $\mathbf{Z}_p$, and $G_n = G_1 \times \Delta_n$, where Δ_n is cyclic of order $p^{n+\delta-1}$, for some positive integer δ. We caution the reader that the normalization here is slightly different from that in [Vato1]; the H_n here corresponds to $H_{n-\delta}$ there. The present normalization is more convenient for our purposes here. Given any character χ of G_n, we may write $\chi = \chi_t \chi_w$, where χ_t is a tamely ramified character of G_1, and χ_w is a wildly ramified character of Δ_n. It will be convenient to study together all characters χ having the same tame part χ_t.

Let us first consider the case where λ is a prime of residue characteristic p. In this case, there are two very different possibilities, depending on whether $a_p = a_p(g)$ is a λ-adic unit or not. In the first

case we say that p is ordinary, and in the second we say that p is supersingular. In this paper, we will only consider the case where p is an ordinary prime (when considering primes λ such that $\lambda | p$). In this ordinary case, our question may be formulated in terms of p-adic L-functions. Let O denote a λ-adically complete discrete valuation ring containing the Fourier coefficients of g, as well as the values of a given tame character χ_t. Then there exists a p-adic L-function $\mathcal{L}(g, \chi_t, T) \in O[[T]]$ satisfying an interpolation property as follows. For every nontrivial root of unity ζ of p-power order, we have

$$\mathcal{L}(g, \chi_t, \zeta - 1) = \frac{1}{\alpha^{2n}} \frac{L(g, \chi, 1)}{\Omega_g^{\text{can}}} \cdot C_\chi,$$

where α is the unique unit root of the Hecke polynomial $X^2 - a_p X + p$, and the character $\chi = \chi_t \chi_w$ is determined by $\chi_w(u) = \zeta$, for some fixed topological generator u of Δ_∞. The integer n in the interpolation formula is defined so that the conductor of χ is p^n. The number C_χ is given by $C_\chi = \sqrt{D} p^n$. We will describe the construction of this p-adic L-function in §5 below, following a method of Bertolini-Darmon [BD96]. An alternative construction of the p-adic L-function was given by Perrin-Riou in [PR88].

According to the Weierstrass preparation theorem, we may write $\mathcal{L}(g, \chi_t, T) = \pi^\mu \cdot F(X) \cdot U(X)$, where π is a uniformizer in O, $F(X)$ is a distinguished polynomial, and $U(X)$ is an invertible power series. The number μ is called the μ-invariant of the p-adic L-function. Clearly, one has

$$\lim_{n \to \infty} \text{ord}_\lambda(L^{\text{al}}(g, \chi_t, 1)) = \mu.$$

Our first theorem may now be stated as follows.

THEOREM 1.1 *Suppose that p is an ordinary prime for g. Then the μ-invariant is given by the formula*

$$\mu = \text{ord}_\lambda(C_{Eis}^2 \cdot C_{csp}).$$

To the best of our knowledge, this theorem provides the first class of examples beyond the classical results of Ferrero and Washington on cyclotomic fields, and those of Gillard and Schneps on elliptic curves with complex multiplication, where one can determine the μ-invariant of a broad class of p-adic L-functions. (H. Hida has recently announced a generalization of the latter to the context of Hecke L-functions of CM fields, see [Hid01].) Note here that it is *not* always true that $\mu = 0$. However, when $\mu \neq 0$, then the extra powers of p are accounted for by congruences, and the sign-change phenomenon studied by Bertolini and Darmon (see [BD96] and its various sequels). We will discuss this point further below.

Now we consider the case of $\ell \neq p$. In this case the results are not quite as satisfactory. Nevertheless, we can still offer the following

THEOREM 1.2 *Suppose that λ has residue characteristic $\ell \neq p$. Suppose that ℓ splits completely in the field $\mathbf{Q}(\chi_t)$ generated by the values of χ_t, and remains inert in $\mathbf{Q}(\mu_{p^\infty})$. Then*

$$\mathrm{ord}_\lambda\left(\frac{L(g,\chi,1)}{\Omega_g^{can}}\right) = \mathrm{ord}_\lambda(C_{Eis}^2 \cdot C_{csp}),$$

for all but finitely many $\chi = \chi_t\chi_w$.

It seems rather likely that one can remove the hypotheses on ℓ, at the cost of introducing some technical complications. As stated, the theorem requires in particular that the fields $\mathbf{Q}(\chi_t)$ and $\mathbf{Q}(\mu_{p^\infty})$ be linearly disjoint. This will be the case if and only if the character χ_t has order prime to p. In this case, the theorem holds for a positive proportion of λ. In particular, we see that $L(g,\chi,1) \neq 0$ for all but finitely many χ, provided that the tame group G_1 has order prime to p. This result was already proven in [Vato1]. Note that we do *not* require that p be an ordinary prime here.

We would like to point out that the proofs of Theorems 1.1 and 1.2 parallel quite closely the arguments of Ferrero and Washington [FW79] and [Was78] in the cyclotomic situation. In fact, it was an attempt to extend the method of Ferrero and Washington that was the motivation for the present work. For a discussion of the analogies, we refer the reader to the introduction of [Vato1].

It may sometimes be useful to invert the procedure of Theorem 1.2. Starting with a given ℓ, we want to know if there exist characters χ such that $\frac{L(g,\chi,1)}{\Omega_g^{\mathrm{can}}}$ is a unit. Then Theorem 1.2 is not so useful. Indeed, if λ is given, then it is rather hard to find primes p such that λ is inert even in $\mathbf{Q}(\mu_p)$: that infinitely many such p exist is the content of Artin's primitive root conjecture, which is still an open problem. Nevertheless, one can still resolve the question at hand, under a mild hypothesis on the form g.

To state the result, we let $\overline{\rho}$ denote the residual representation associated to g modulo λ. Thus $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(O/\lambda)$ is such that $\mathrm{Tr}(\overline{\rho}(\mathrm{Frob}(q)) = a_q$, for all primes $q \nmid N\ell$. We let $\overline{N}$ denote the Artin conductor for $\overline{\rho}$, so that $\overline{N}$ is the so-called minimal level for $\overline{\rho}$, in the sense of Serre's conjectures. Then we have

THEOREM 1.3 *Let the prime ℓ be given. Suppose that $\overline{\rho}$ is irreducible, and that there exists some prime q dividing $\overline{N}$ which divides N precisely to the first power. Then there exist infinitely many quadratic fields K and Hecke characters χ of K such that $\frac{L(g,\chi,1)}{\Omega_g^{can}}$ is a λ-adic unit.*

The proof of this theorem boils down to finding conditions that force the numbers C_{csp} and C_{Eis} to be λ-adic units, and making a convenient choice of p. We will give the argument in Section 4.3. We remark that it applies, in particular, when the level N is squarefree.

We want to explain how the numbers C_{csp} and C_{Eis} may be explained in terms of congruences, starting with C_{Eis}, since it is rather less surprising. As we have already remarked, C_{Eis} measures con-

gruences modulo λ between g and the space of Eisenstein series. In terms of Galois representations, this means that the residual representation $\overline{\rho}$ associated to g modulo λ is *reducible*. In this case, it is a well-known phenomenon that the L-values are often non-units. This seems to have first been observed by Mazur for the unique cuspform on $\Gamma_0(11)$, with $\ell = 5$. This observation was further pursued by Stevens [Ste89]. On the side of Selmer groups (about which we say nothing here), Greenberg [Gre89] has observed that an analogous phenomenon holds.

The quantity C_{csp} is perhaps more interesting. It will turn out that C_{csp} is a nonunit if and only if there exists no congruence between g and another form h whose level is *not* divisible by all the primes in N^-. To explain why the existence of such a form h *forces* the L-values of g to be nonunits, we may argue as follows. Suppose that there is a congruence $g \equiv h \pmod{\lambda}$, and that there is some prime q dividing N^- such that the level M of h is prime to q. For the purposes of this introduction, we shall assume that there is a unique such prime q. Under this hypothesis, we see that the number of primes dividing M that are inert in K is *even*. (This follows from the fact that N^- was assumed at the outset to have an odd number of prime factors.) It follows then that $L(h, \chi, s)$ has functional equation with sign -1. In particular, the L-functions $L(g, \chi, s)$ and $L(h, \chi, s)$ have functional equations with opposite signs for any anticyclotomic character χ of conductor p^n. Indeed, we find that $L(h, \chi, 1)$ vanishes trivially, while $L(g, \chi, 1)$ is expected to be nonzero. Since the general philosophy of congruences [Vat99] suggests that the algebraic parts of $L(g, \chi, 1)$ and $L(h, \chi, 1)$ should be congruent, we are led to expect that the algebraic part of $L(g, \chi, 1)$, being congruent to zero, is a non-unit, and this is precisely what our theorem says.

The sign-change phenomenon described above was first suggested in [Joc94]. It was further studied and refined by Bertolini and Darmon, in the paper [BD96] and its various sequels, especially [BD99a]. We will exploit a variant of this notion to transfer our results to the case of forms with functional equation having sign -1. To state the result, let g now denote a form of level N, where all primes dividing N are *split* in K. (This is the classical Heegner hypothesis.) Then $L(g, K, s)$ has functional equation with sign -1. If χ is a character of conductor p^n, with $(p, ND) = 1$, then $L(g, \chi, s)$ has sign -1 as well. In this case, a conjecture of Mazur (see [Maz84], or [Vato1]) asserts that $L'(g, \chi, 1)$ is nonzero for almost all χ.

In attempting to prove this conjecture, our only sign-post is the Gross-Zagier theorem, which states that if χ_0 is the trivial character, then $L'(g, \chi_0, 1)$ is, up to a simple constant, the height of a classical Heegner point Q on the modular curve $X_0(N)$. In particular, if E denotes the abelian variety quotient of $J_0(N)$ associated to g by Shimura, and $\pi : J_0(N) \to E$ is the modular parametrization, then the Gross-Zagier theorem states that $L'(g, \chi_0, 1)$ is nonzero if and only if $\tilde{Q} = \pi(Q)$ has infinite order in $E(K)$. On the algebraic side, Kolyvagin showed that if $\tilde{Q}$ has infinite order, then $E(K)$ has

rank 1.

We are interested in generalizations of this result to twisted Heegner points of higher level. On the algebraic side, the result is due to Bertolini-Darmon. To state their result, let χ denote an anticyclotomic character of conductor c, and let $Q \in J_0(N)$ be the CM point defined by a pair $(A, \mathfrak{n})$, where A is an elliptic curve with complex multiplications by the order $\mathfrak{o}_c$, and $\mathfrak{n}$ is a fractional ideal of $\mathfrak{o}_c$ with norm N. Then Q is defined over $K(c)$. By abuse of notation, we shall continue to write Q for the point $(Q - \infty) \in J_0(N)$, where ∞ denotes the cusp at infinity on $X_0(N)$. Then Bertolini and Darmon [BD90] have shown that, if $\sum_\sigma \chi(\sigma)Q^\sigma$ is nonzero in $E(K(c)) \otimes \mathbf{C}$, then the χ-eigenspace of $E(K(c))$ has rank 1. Their result is purely algebraic, and makes no reference to the derivative of the L-series.

On the other hand, the Gross-Zagier formula has recently been generalized by Zhang to give a formula for $L'(g, \chi, 1)$, if χ is a ramified character satisfying some very mild conditions (see [Zha01] for a very general statement, valid for automorphic forms over totally real fields). In particular, Zhang's generalization holds for characters of conductor p^n, where p is as above. It follows from his results that $L'(g, \chi, 1)$ is nonzero if and only if $\sum_\sigma \chi(\sigma)Q^\sigma$ has nonzero height.

In this paper, we will study the question of whether $\sum_\sigma \chi(\sigma)Q^\sigma$ is nonzero in $E(K(c)) \otimes \mathbf{Q}(\chi)$, as χ varies over anticyclotomic characters of p-power conductor. In view of Zhang's results, this may be viewed as statement about the derivatives $L'(g, \chi, 1)$.

THEOREM 1.4 *Suppose that all primes dividing N are split in K. Let χ vary over the set of anticyclotomic characters of p-power conductor. Then $\sum_\sigma \chi(\sigma)Q^\sigma$ and $L'(g, \chi, 1)$ are nonzero in $E(K(H_n)) \otimes \mathbf{Q}(\chi)$ and $\mathbf{C}$ respectively, for all but finitely many χ.*

As we have already remarked, this theorem is proven by the method of Jochnowitz congruences. Specifically, we introduce another form h of level Nq, such that $g \equiv h \pmod{\lambda}$, where λ is a suitably chosen prime of $\overline{\mathbf{Q}}$ (with characteristic ℓ), and q is a prime such that $q \nmid NDp\ell$ which is inert in K. Then g and h have opposite signs in their functional equations. Specifically, g has sign $+1$ and h has sign -1. We then prove the Jochnowitz congruence, which implies that $\sum_\sigma \chi(\sigma)Q^\sigma$ is indivisible by λ if $L(h, \chi, 1)$ is a λ-adic unit. This latter hypothesis is satisfied for almost all χ in view of Theorem 1.2. Then we deduce Theorem 1.4 from the fact that the torsion subgroup of $E(H_\infty)$ is finite, so that a point that is nonzero modulo $\lambda|\ell$, for ℓ sufficiently large, must have infinite order. Note that we do not require that p be an ordinary prime here.

We want to mention that Cornut [Cor01] has given a proof of a similar result which works directly with classical Heegner points, and avoids the machinery of Jochnowitz congruences (at least when p is an ordinary prime; if p is supersingular, it does not seem possible to obtain from his method

the fact that all but finitely many points are nontrivial). His work relies on the results of this paper, especially Lemma 5.13 below, in an essential way. On the other hand, our analysis of the so-called genus subgroup (see Proposition 5.3 below) follows fairly closely ideas introduced in his work.

We would like now to describe the proof of the Jochnowitz congruence, since that part of the argument may perhaps be quite novel. In particular, our method avoids the analysis of component groups that occurs in [BD99a]. For simplicity, we assume that g has rational Fourier coefficients, and so corresponds to an elliptic curve E. We select the prime $\lambda | \ell$ such that $E[\ell]$ is irreducible as a Galois module. The prime q is chosen to be a Kolyvagin prime, so that q is inert in K, and $\mathrm{Frob}(q)$ acts via complex conjugation on $E[\ell]$. In particular, we have $E[\ell] = V_+ \oplus V_-$, where $V_\pm$ is the $\pm$-eigenspace for $\mathrm{Frob}(q)$, and each $V_\pm$ is one-dimensional over $\mathbf{F}_\ell$.

Let us consider the general problem of showing that a Heegner point $Q \in E(H_n)$ is indivisible by ℓ. The basic fact we use is that if $\mathfrak{Q}$ is a prime of $\overline{\mathbf{Q}}$ over q, then the reduction $\overline{Q}$ of Q modulo $\mathfrak{Q}$ is a supersingular point defined over $\mathbf{F}_{q^2}$. Furthermore, since q splits completely in H_n, any other point in $E(H_n)$ reduces to a point in $E(\mathbf{F}_{q^2})$. To show that $\overline{Q}$ is not divisible by ℓ in $E(\mathbf{F}_{q^2})$, it is therefore enough to exhibit an isogeny $E' \to E$, defined over $\mathbf{F}_{q^2}$, and with kernel isomorphic to $\mathbf{F}_\ell$, such that there does *not* exist $y \in E'(\mathbf{F}_{q^2})$ which projects to $\overline{Q}$ in E. Such a isogeny may be constructed as follows. Let $E_\pm = E/V_\pm$, and let $E_\pm \to E$ denote the dual isogeny. Let $W_\pm \subset E_\pm$ denote the Cartier dual of $V_\pm$, which is the kernel of the dual isogeny. Note that, under our hypotheses, the group schemes $W_\pm$ and $V_\pm$ become constant, isomorphic to $\mathbf{F}_\ell$, over F_{q^2}. Thus, given $x \in E(\mathbf{F}_{q^2})$, we may form $F_\pm(x) \in W_\pm$ via the mechanism of the Frobenius substitution of geometric class field theory. One could also describe $F_\pm(x)$ more concretely in terms of Kummer theory. Applying this to the reduction of the CM points, we may conclude that Q is indivisible by ℓ if the number $F_\pm(\overline{Q})$ is nonzero in $W_\pm$.

In our applications, we would like to study divisibility of the twisted Heegner points. Namely, we want to show that $\sum_\sigma \chi(\sigma) F_\pm(\overline{Q^\sigma}) \in W_\pm \otimes k$ is nonzero. To analyze this, we view $F_\pm$ as defining a function $\mathbf{Z}[\Sigma] \to W_\pm \cong \mathbf{F}_\ell$, where Σ denotes the set of supersingular points on $X_0(N)$. The function $F_\pm$ enjoys a certain compatibility with respect to the Hecke operators, coming from its very definition. Furthermore, one has an evident compatibility with the action of $\mathrm{Frob}(q)$, which is the nontrivial automorphism of $\mathrm{Gal}(\mathbf{F}_{q^2}/\mathbf{F}_q)$.

But there is another way of constructing such a homomorphism $\mathbf{Z}[\Sigma] \to \mathbf{F}_\ell$, this time starting from the modular form h of level Nq which is congruent to g. Namely, one views $\mathbf{Z}[\Sigma]$ as the Picard group $\mathcal{M}$ of a Gross curve of level N, associated to the quaternion algebra B of discriminant q, as in Gross' special value formula (see §1 below, and [Vato1]). The form h, being new at q, defines a homomorphism $\psi : \mathcal{M} \to \mathbf{F}_\ell$, and one checks easily that, with a judicious normalization and choice

of sign in $F_\pm$, that one has the same Hecke compatibility. It follows now from a multiplicity-one theorem, due in this case to Mazur, that $F_\pm$ is *equal* to ψ. Thus we get

$$\sum_\sigma \chi(\sigma) F_\pm(Q^\sigma) \equiv \sum_\sigma \chi(\sigma)\psi(\overline{Q}^\sigma) \pmod{\lambda}.$$

The Jochnowitz congruence follows directly from this, since Gross' special value formula states that the right-hand-side of the congruence above is a 'square root' of the algebraic part of $L(h, \chi, 1)$, and our previous results show that the latter is a λ-adic unit for almost all χ.

Acknowledgements

It is a pleasure to thank H. Darmon for some useful conversations on the subject of this paper. Part of this research was supported by an NSERC grant. I am also indebted to C. Cornut for his careful examination of an earlier version of this paper. The formulation of Proposition 5.3 below borrows freely from his work [Cor01]. I would also like to thank an anonymous referee for some useful suggestions.

2 Gross' special value formula

We want to recall the special value formula of Gross, and the construction of the p-adic L-function. Since this is amply documented in the literature, we will be brief. For more details, we refer the reader to [BD96], [BD98], or [BD99b]. We will use the notations of [Vat01], Section 2.

2.1 Let $N = N^+ \cdot N^-$ as in the introduction, and fix an oriented Eichler order $R \subset B$ of level N^+. Then we have the isomorphism

$$\mathrm{Cl}(B) = B^\times \backslash \hat{B}^\times / \hat{R}^\times = B^\times \backslash \hat{B}^\times / \hat{\mathbf{Q}}^\times \hat{R}^\times$$

where $\mathrm{Cl}(B)$ denotes the set of conjugacy classes of oriented Eichler orders of level N^+. Here the second equality follows from the fact that $\mathbf{Q}$ has class number one, so that $\hat{\mathbf{Q}}^\times = \mathbf{Q}^\times \cdot \hat{\mathbf{Z}}^\times \subset \mathbf{Q}^\times \cdot \hat{R}^\times$. Let $\Gamma' = R[1/p]^\times$, viewed as a subgroup of $B \otimes \mathbf{Q}_p^\times \cong GL_2(\mathbf{Q}_p)$. Then strong approximation gives

$$\mathrm{Cl}(B) = \Gamma' \backslash G / K,$$

where $G = PGL_2(\mathbf{Q}_p)$, and $K = PGL_2(\mathbf{Z}_p)$ is a maximal compact subgroup.

Let X denote the Gross curve of level N^+ associated to the quaternion algebra B, and let $\mathcal{M} = \mathrm{Pic}(X)$. Thus $\mathcal{M}$ is the free $\mathbf{Z}$-module with basis elements given by $\mathrm{Cl}(B)$. Then $\mathcal{M}$ is a module for the Hecke ring $\mathbf{T}$. Let $\psi = \psi_g : \mathbf{T} \to O_g \subset \mathbf{R}$ denote the canonical homomorphism. Let

$$\mathcal{M}_g = \mathcal{M}_{\mathbf{R}} \otimes_{\mathbf{T}} \mathbf{R},$$

where the tensor product is taken with respect to the map $\psi_g : \mathbf{T} \to \mathbf{R}$. It is known that $\mathcal{M}_g$ is a $\mathbf{R}$-vector space of dimension one. Fix an identification $\mathcal{M}_g \cong \mathbf{R}$, or, equivalently, a nonzero element $v \in \mathcal{M}_g$. Then we may view ψ as a $\mathbf{R}$-valued function, also denoted by ψ, on $\mathcal{M}$ by requiring that $\psi(m) \cdot v = m \otimes 1$. Applying ψ to the basis elements $[R] \in \mathcal{M}$, we obtain a function $\psi' : \mathrm{Cl}(B) \to \mathbf{R}$. Choice of a different basis element v in the definition has the effect of scaling ψ' by a nonzero constant.

Since we are interested in studying special values modulo λ, we need to make our special values integral in some canonical way. Thus, it is important to specify the function ψ precisely. To do this, we let O denote a λ-adically complete discrete valuation ring, containing the Fourier coefficients of g. Let $\mathcal{M}^g$ denote the submodule of $M \otimes O$ where $\mathbf{T}$ acts via the character ψ. Then the multiplicity one theorem states that $\mathcal{M}^g$ is a free O-module of rank 1. Let w denote a generator of $\mathcal{M}^g$. Then we fix the isomorphism $\mathcal{M}_g \to \mathbf{R}$ so that the element $v = \psi(w) \in \mathcal{M}_g$ corresponds to $1 \in \mathbf{R}$.

With this fixed normalization, we get a function $\psi' : \mathrm{Cl}(B) \to O_g$, as above. For notational simplicity, we will write ψ instead of ψ'. Note also that this normalization implies that there exists $C \in \mathrm{Cl}(B)$ such that $\psi(C)$ is a λ-adic unit. This follows from the fact that the element $w \in \mathcal{M}$ is a linear combination, with integral coefficients, of the basis elements $[C]$, for $C \in \mathrm{Cl}(B)$. This will be useful in the sequel.

2.2 Let $\mathfrak{o}_K$ denote the maximal order of K. We select an orientation on $\mathfrak{o}_K$, and regard this choice as fixed. If $\mathfrak{o}_n \subset K$ denotes the order of conductor p^n, we get an induced orientation on $\mathfrak{o}_n$. In this framework, a Heegner point of conductor p^n is a pair

$$P = (f, R)$$

where R is an oriented Eichler order of level N^+, and $f : K \to B$ is an oriented embedding such that $f^{-1}(R) = \mathfrak{o}_n$. We identify pairs (f, R) and (f', R') if they are conjugate via the action of $B^\times$. Write X_n for the set of Heegner points of conductor p^n. The basic facts about Heegner points are as follows:

1. *Galois action*: There is an action of the group $\mathrm{Pic}(\mathfrak{o}_n)$ on the set X_n. The set X_n is a principal homogeneous space for $\mathrm{Pic}(\mathfrak{o}_n)$. Hence if e_n denotes the order of $\mathrm{Pic}(\mathfrak{o}_n)$, there are precisely e_n distinct Heegner points of conductor p^n.

2. *Tree structure*: Each Heegner point of conductor p^n has $p + 1$ neighbors, which are Heegner points of conductor p^r, for suitable r. If $n \geq 1$, then precisely p of these neighbors have level p^{n+1}, while the remaining one has level p^{n-1}. This unique Heegner point of level p^{n-1} is called the *predecessor* of P.

3. *Action of T_p*: The Hecke correspondence T_p associates to P_n the formal sum of its $p+1$ neighbors. If K_n is the kernel of the natural projection $\mathrm{Pic}(\mathfrak{o}_n) \to \mathrm{Pic}(\mathfrak{o}_{n-1})$, then we have the formal identity

$$\sum_{\sigma \in K_n} P_n^\sigma = T_p(P_{n-1}) - P_{n-2},$$

for $n \geq 2$. Here P_{n-1} is the predecessor of P_n, and P_{n-2} is the predecessor of P_{n-1}.

4. *The function ψ*: Each Heegner point $P = (f, R)$ determines a class $[P] = [R] \in \mathrm{Cl}(B)$. Thus we may view the function ψ above as being defined on the sets X_n, by putting $\psi(P) = \psi([R])$.

2.3 Gross' special value formula may now be stated as follows. Let χ denote a primitive character of $\mathrm{Pic}(O_n) \cong \mathrm{Gal}(H_n/K)$. Then there exists a period $\Omega = \Omega_{g,K}$, depending on K and g, but independent of n, such that

$$\left| \sum_{\sigma \in \mathrm{Pic}(O_n)} \chi(\sigma)\psi(P^\sigma) \right|^2 = \frac{L(g,\chi,1)}{\Omega} \cdot C_\chi \in \overline{\mathbf{Q}}. \tag{2}$$

We specify the period Ω more precisely in §2.4 below. The number C_χ is given by $C_\chi = \sqrt{D}p^n$, so that C_χ^2 is the Artin conductor of the dihedral representation $\mathrm{Ind}_{\mathbf{Q}}^K(\chi)$. Note that, by our normalization of ψ, the quantity on the right is actually *integral*.

Computation of the period

2.4 We want to relate the period appearing in the formula (2) above to the canonical integral periods in [Hid88] and [Vat99]. Let O denote a λ-adically complete discrete valuation ring, and let T be any finite, flat, reduced, O-algebra, equipped with a homomorphism $\pi : T \to O$. Let $I = \ker(\pi)$, and let η denote a generator of the ideal $\pi(\mathrm{Ann}(\ker(\pi)))$. Thus η is the so-called congruence number for π.

Let $\mathbf{T}_0$ denote the Hecke ring (over O) formed in the usual way from modular forms on $\Gamma_0(N)$, and let $\pi : \mathbf{T}_0 \to O$ denote the canonical homomorphism associated to the modular form g. Let $\mathbf{T} = \mathbf{T}_B$ denote the Hecke algebra formed by the action of Hecke operators on the module $\mathcal{M} = \mathrm{Pic}(X)$ as above, where X is the Gross curve of conductor N^+ and level N^-. This time we take for π the homomorphism ψ associated to g. Applying the construction above to $\mathbf{T}_0$ and $\mathbf{T}_B$, we obtain congruence numbers η_0 and η_B. Clearly, we have the divisibility $\eta_B | \eta_0$. Following Hida, we define a canonical period Ω_g^{can} as follows. If (g, g) denotes the Petersson inner product of g with itself, then we put $\Omega_g^{\mathrm{can}} = \frac{(g,g)}{\eta_0}$.

LEMMA 2.5 *The period Ω in the special value formula (2) is given by*

$$\Omega = \frac{(g,g)}{\eta_B}.$$

Thus we have $\Omega = \Omega_g^{can} \cdot C_{csp}$, where $C_{csp} = \eta_0/\eta_B$.

Proof. Let χ denote a primitive character of G_n, for some n. Then let $e_\chi \in \mathrm{Pic}(X) \otimes \mathbf{Q}(\chi)$ be defined by $e_\chi = \sum_{\sigma \in G_n} \chi(\sigma) P^\sigma$. Let $(\,\cdot\,,\cdot\,)$ denote the canonical intersection pairing $\mathrm{Pic}(X) \times \mathrm{Pic}(X) \to \mathbf{Q}$, extended to a complex pairing which is skew-linear in the second variable, as in [Gro87]. Then the special value formula may be equivalently stated as

$$(e_\chi, e_\chi) = \frac{L(g,\chi,1)}{(g,g)} \cdot C_\chi.$$

The lemma follows from this formula, together with the definition of the function ψ. □

REMARK 2.6 It is clear from the above that the periods Ω and Ω_g^{can} need not be equal. As we have already remarked in the introduction, this may be explained in terms of congruences. Note that the period Ω in Gross' formula actually depends on the field K.

REMARK 2.7 When dealing with questions of congruence, it is often more convenient to work with forms on $\Gamma_1(N)$ rather than $\Gamma_0(N)$. This is the approach taken in [Hid88], [Ste89], and [Vat99]. Hida's canonical integral period from [Hid88] is in fact defined as

$$\Omega_g^{\mathrm{Hida}} = \frac{(g,g)_{\Gamma_1(N)}}{\eta_1},$$

where we take the inner product and congruence divisor relative to $\Gamma_1(N)$. Furthermore, if the canonical periods $\Omega_g^{\pm}$ of [Vat99] are defined, then we will have

$$\Omega_g^{\mathrm{Hida}} = \Omega_g^{+} \cdot \Omega_g^{-}.$$

We will not concern ourselves with these alternative periods here, and mention the formulae only to emphasize the various distinctions, and to facilitate future comparisons.

Finally, we want to explain the other quantity C_{Eis} which appears in the statement of our theorems. We let ν denote the largest integer such that the function ψ is congruent to a constant modulo λ^ν, and put $C_{\mathrm{Eis}} = \tilde{\lambda}^\nu$, where $\tilde{\lambda}$ is a λ-adic uniformizer in O.

LEMMA 2.8 *Let λ denote a prime of $\overline{\mathbf{Q}}$, and let ν denote the largest positive integer such that the function $\psi : \mathrm{Cl}(B) \to O$ is constant modulo λ^ν. Then λ^ν divides the numbers $a_q - q - 1$, for primes q with $q \nmid N$.*

Proof. Suppose that ψ is congruent to a constant function modulo λ^r. Then, choosing an $x \in \mathcal{M}$ such that $\psi(x)$ is a unit, we have $\psi(T_q x) = a_q \psi(x)$. Since the Hecke correspondence T_q has degree $q+1$, we see immediately that $a_q - q - 1 \equiv 0 \pmod{\lambda^r}$. □

REMARK 2.9 Thus the number C_{Eis} measures congruences between g and a space of Eisenstein series. It is not clear to us whether λ^v is the exact gcd of the numbers $a_q - q - 1$. The truth of this statement seems tied to a multiplicity-one type theorem for $\mathrm{Pic}(X)$ in characteristic ℓ, where $\lambda | \ell$, but, as is well known, such theorems are extremely delicate. At any rate, we have not pursued this question.

3 THETA ELEMENTS

3.1 The special value formula above may be conveniently formulated in terms of theta elements in a suitable group algebra of G_n, as in [BD96]. Indeed, one might form

$$\theta = \sum_{\sigma \in G_n} \psi(P)\sigma,$$

where P is some fixed Heegner point of conductor p^n. Then, if χ is a primitive character of G_n, we will have

$$|\chi(\theta)|^2 = \frac{L(g, \chi, 1)}{\Omega} C_\chi.$$

However, the specializations of the θ element so defined to imprimitive characters χ does not admit any simple description. To get around this difficulty, we must use the notion of *regularized* Heegner points, as in [BD96].

To recall the definitions, let

$$E_p(X) = X^2 - a_p X + p = (X - \alpha)(X - \beta)$$

denote the Hecke polynomial of g at p. Given a prime λ of $\overline{\mathbf{Q}}$, we fix a choice of root, say α, of $E_p(X)$ which is a λ-adic unit. If the residue characteristic of λ is not equal to p, then $\alpha\beta = p$, so that both of α and β are λ-adic units. In this case we make the choice arbitrarily. If λ lies above p, then the unit root α exists only if a_p is a λ-adic unit, which is to say, if p is an ordinary prime for g. In this case, α is uniquely determined.

Let λ be a prime of $\overline{\mathbf{Q}}$, as above. We fix a λ-adically complete and integrally closed ring $O = O_\lambda$ which contains the Fourier coefficients of g. Given a Heegner point P_n of conductor p^n, with $n \geq 1$, we let P_{n-1} denote the predecessor of P_n. Define the regularized Heegner point $\tilde{P}_n$ by the formal expression

$$\tilde{P}_n = \frac{1}{\alpha^n} P_n - \frac{1}{\alpha^{n+1}} P_{n-1} \tag{3}$$

Note that the coefficients of $\tilde{P}_n$ lie in O, since α was assumed to be a λ-adic unit. Furthermore, it follows from the properties listed in (2.2) that, if $n \geq 2$, then we have

$$\sum_{\sigma \in K_n} (\tilde{P}_n^{\sigma}) = \tilde{P}_{n-1}. \tag{4}$$

This means that the regularized Heegner points are compatible under the norm from H_n to H_{n-1}.

3.2 Now let $\Lambda'_n = O[G_n]$, where $G_n = \mathrm{Gal}(H_n/K)$, and define $\psi(\tilde{P}_n) = \dfrac{1}{\alpha^n}\psi(P_n) - \dfrac{1}{\alpha^{n+1}}\psi(P_{n-1})$. We fix a Heegner point P_n of conductor p^n, and define the theta element $\theta(P_n) \in \Lambda'_n$ as follows:

$$\theta(P_n) = \sum_{\sigma \in G_n} \psi(\tilde{P}_n^{\sigma}) \cdot \sigma. \tag{5}$$

One checks that if χ is a character of G_n, with conductor p^r, with $1 \leq r \leq n$, then we have the specialization formula

$$\chi(\theta(P_n))\chi^{-1}(\theta(P_n)) = \frac{1}{\alpha^{2n}} \frac{L(g, \chi, 1)}{\Omega} \cdot C_{\chi}. \tag{6}$$

Note also that θ depends on the choice of the point P_n. If we choose another point, P'_n, then we will have $P'_n = P_n^{\sigma}$ for some $\sigma \in G_n$, so that $\chi(\theta(P_n))$ and $\chi(\theta(P'_n))$ differ by a root of unity. Since we are trying to calculate the λ-adic valuation of $\chi(\theta(P_n))$, we may choose the point P_n in any convenient fashion. This observation will be important later.

3.3 It is now natural to select a compatible sequence of Heegner points $P_1, P_2, \ldots, P_n, \ldots$, where each P_n is the predecessor of P_{n+1}, and form the inverse limit of the corresponding theta elements. For later use, it will be convenient to refer to the data of a Heegner point P_n, together with its predecessor P_{n-1}, as an *edge*. This terminology is motivated by the tree-like structure of the Heegner points (see [Vato1], or [BD98], [BD99b]). The regularized Heegner point $\tilde{P}_n$ introduced above may be more properly associated to the edge $\vec{e}_n$ with origin P_{n-1} and terminus P_n. In this case, we define

$$\psi(\vec{e}_n) = \psi(\tilde{P}_n) = \frac{1}{\alpha^n}\psi(P_n) - \frac{1}{\alpha^{n+1}}\psi(P_{n-1}).$$

An *end* is a sequence of oriented edges $\vec{e} = (\vec{e}_0, \vec{e}_1, \ldots, \vec{e}_n, \ldots)$, where the origin of $\vec{e}_n$ is the terminus of $\vec{e}_{n-1}$. We require that each $\vec{e}_n$ go from a Heegner point of conductor p^{n-1} to one of conductor p^n.

Fix a choice of an end $\vec{e}$ as above. For each n, let $\theta_n = \theta(P_n) \in \Lambda'_n$, where P_n is the terminus of the edge $\vec{e}_n$. Then one checks that the elements θ_n are compatible under the natural projection $\Lambda'_{n+1} \to \Lambda'_n$, so that we may form

$$\Theta' = \Theta'(\vec{e}) = \varprojlim \theta_n \in \Lambda' = \varprojlim \Lambda'_n. \tag{7}$$

Recall that $\Lambda'_n = O[G_n]$, where $G_n = G_1 \times \Delta_n$, where Δ_n is cyclic of order $p^{n+\delta-1}$. Thus we have

$$\Lambda' = O[G_1][[\Delta_\infty]],$$

where $\Delta_\infty = \varprojlim \Delta_n$. If χ is a character of $\mathrm{Gal}(H_\infty/K)$, primitive of conductor p^n, we have the specialization formula

$$\chi(\Theta') \cdot \chi^{-1}(\Theta') = \frac{1}{\alpha^{2n}} \frac{L(g, \chi, 1)}{\Omega} \cdot C_\chi. \tag{8}$$

Note that we have said nothing about the specialization of χ to the trivial character, or to unramified characters. This is a very interesting question, but we will not discuss it here. Here we remark only that the answer is connected to certain predictable degeneracies in p-adic height pairings, and is computed by using p-adic uniformization of the Shimura curves associated to *indefinite* quaternion algebras. We refer the reader to [BD98] and [BD99b] for the details.

As in [Vato1], it will be convenient to express the character χ as $\chi = \chi_t \cdot \chi_w$, where χ_t is a tamely ramified character of G_1 and χ_w is a wild character of Δ_n, and to consider together all χ with fixed tame part χ_t. Thus, suppose χ_t is fixed. Enlarging O if necessary, we have a homomorphism $\chi_t : O[G_1] \to O$. This induces a map

$$\chi_t : \Lambda' = O[G_1][[\Delta_\infty]] \to O[[\Delta_\infty]]. \tag{9}$$

Applying the homomorphism above to the element Θ', we get a new theta element

$$\Theta = \Theta(\chi_t) \in \Lambda = O[[\Delta_\infty]].$$

Then Θ satisfies an interpolation property with respect to characters χ_w of Δ_∞. Namely, it interpolates the 'square roots' of special values $L(g, \chi_t\chi_w, 1)$, for the fixed choice of χ_t.

3.4 Now we would like to consider in more detail the case when λ is a prime of residue characteristic p. In this event, O is a finite extension of $\mathbf{Z}_p$, and $\Lambda = O[[\Delta_\infty]]$ is isomorphic to a power series ring $\mathbf{Z}_p[[T]]$. This isomorphism is realized by selecting a topological generator u of Δ_∞, and sending u to $1 + T$. In this case, the element $\Theta(\chi_t)$ may be identified with a power series $\mathbf{L}(g, \chi_t, T)$, such that if ζ is a nontrivial root of unity of p-power order, then

$$\mathbf{L}(g, \chi_t, \zeta - 1) \cdot \mathbf{L}(g, \chi_t^{-1}, \zeta^{-1} - 1) = \frac{1}{\alpha^{2n}} \frac{L(g, \chi, 1)}{\Omega} \cdot C_\chi, \tag{10}$$

where $\chi = \chi_t\chi_w$, and the character χ_w is determined by $\chi_w(u) = \zeta$.

The power series $\mathbf{L}(g, \chi_t, T)$ is a (twisted) p-adic L-function for g. By the Weierstrass preparation theorem, we have

$$\mathbf{L}(g, \chi_t, T) = p^\mu \cdot F(T) \cdot U(T),$$

where μ is a nonnegative integer, $F(T)$ is a distinguished polynomial, and $U(T)$ is an invertible power series. The integer μ is called the μ-invariant of the p-adic L-function.

Remark 3.5 It would be natural to define the p-adic L-function so as to preserve the symmetry between χ and χ^{-1}. Furthermore, we would also like to arrange that the period in the interpolation formula is the canonical period defined by Hida. Thus we define

$$L(g, \chi_t, T) = L(g, \chi_t^{-1}, T) = \mathbf{L}(g, \chi_t, T) \cdot \mathbf{L}(g, \chi_t^{-1}, (1+T)^{-1} - 1) \cdot C_{\mathrm{csp}},$$

where the constant C_{csp} is defined so that the period $\mathbf{\Omega}$ of (2) and the canonical Hida period $\mathbf{\Omega}_g^{\mathrm{can}}$ are related by $C_{\mathrm{csp}} \cdot \mathbf{\Omega}_g^{\mathrm{can}} = \mathbf{\Omega}$. However, it is more convenient in practice to work with the power series $\mathbf{L}(g, \chi_t, T)$, since the corresponding theta elements have a relatively simple form.

We would also like to remind the reader that this definition of a p-adic L-function depends on the choice of the end $\vec{e}$ that we have made above. One verifies easily that choice of a different end changes the L-function by an invertible power series. We will exploit this freedom later.

Finally, we point out that if λ has residue characteristic $\ell \neq p$, then there is no λ-adic analytic function interpolating the special values in question. However, it is still convenient to use the theta elements.

4 Preliminary reductions

Our goal is to translate our theorems about L-values into statements about the theta elements introduced above, with the idea that one can then study the theta elements in terms of distributions of Heegner points. To carry out this program, it is convenient to separate the case of $\lambda \nmid p$ and $\lambda | p$.

The case of $\lambda \nmid p$.

Let ν be the largest integer such that the function ψ is congruent to a constant modulo λ^ν, as above. Our goal is to prove the following proposition:

Proposition 4.1 *Let the tame character χ_t be given, and let Θ denote the corresponding theta element. Then, for all $n \gg 0$, there exists a primitive character χ_w of Δ_n such that $\chi(\Theta)$ satisfies*

$$\mathrm{ord}_\lambda(\chi_w(\Theta)) = \nu.$$

Assuming this proposition, and keeping in mind the definitions of the various periods, we may easily deduce Theorem 1.2 of the introduction. Indeed, it follows directly from

COROLLARY 4.2 *Suppose that the tame character χ_t has order prime to p. Suppose also that the prime λ splits completely in the field $\mathbf{Q}(\chi_t)$ obtained by adjoining to $\mathbf{Q}$ the values of χ_t, and is inert in the field $\mathbf{Q}(\mu_{p^\infty})$ obtained by adjoining all p-power roots of unity. Then*

$$\mathrm{ord}_\lambda\left(\frac{L(g,\chi,1)}{\Omega}C_\chi\right) = 2\nu$$

for all $\chi = \chi_t\chi_w$ primitive of conductor p^n, with $n \gg 0$.

Proof. By virtue of our hypothesis that λ remains inert in $\mathbf{Q}(\mu_{p^\infty})$, and splits completely in $\mathbf{Q}(\chi_t)$, we see that the characters $\chi_t\chi_w$ are all conjugate under the action of a decomposition group D_λ. Applying the proposition above, we find a character χ_w such that $\chi_w(\Theta)$ has λ-adic value equal to ν. Since all the characters $\chi_t\chi_w$ of conductor p^n are conjugate under D_λ, we see that $\chi_w(\Theta)$ has valuation ν for all χ_w, primitive of conductor p^n. Arguing similarly with χ_t^{-1}, and applying the formula

$$\frac{1}{\alpha^{2n}}\frac{L(g,\chi,1)}{\Omega}C_\chi = \chi_w(\Theta(\chi_t))\cdot\chi_w^{-1}(\Theta(\chi_t^{-1})),$$

we obtain the statement of the corollary. □

4.3 Theorem 1.3 is also a consequence of Proposition 4.1. For the field K we simply take any quadratic field in which the prime q is inert but all other primes dividing N are split. Since $\overline{\rho}$ is irreducible, we see that the number C_{Eis} is a λ-adic unit (see Lemma 2.8). Furthermore, since q divides the minimal level $\overline{N}$, and divides N to precisely the first power, we see that any modular form g' on $\Gamma_0(N)$ congruent to g modulo λ is necessarily special at q. In particular, g' occurs in the definite quaternion algebra B ramified only at q. It then follows that the number C_{csp} is also a λ-adic unit (see Lemma 2.5).

Now, consider characters of the anticyclotomic $\mathbf{Z}_p$-extension of K, where p is prime with $\ell \neq p$. Equivalently, we will take $\chi_t = 1$. (Here p is a prime with $\ell \neq p$; we will specify the choice of p below.) Then Proposition 4.1 states that we can find characters $\chi = \chi_w$ such that $\chi(\Theta)$ is a unit. Now, in view of equation (8), we want to arrange matters so that $\chi^{-1}(\Theta)$ is also a unit. This does not follow directly from the proposition, but we may instead argue as follows.

The main point is to select p in some convenient fashion. Indeed, it suffices to choose p so that the characters χ and χ^{-1} will be conjugate under the action of the decomposition group D_λ. But if χ takes values in μ_{p^r}, then the automorphism $\zeta \mapsto \zeta^{-1}$ of $\mathbf{Q}(\mu_{p^r})$ is induced by the element $-1 \in (\mathbf{Z}/p^r\mathbf{Z})^\times \cong \mathrm{Gal}(\mathbf{Q}(\mu_{p^r})/\mathbf{Q})$. Thus we need to choose an odd prime p such that the cyclic group generated by ℓ in $(\mathbf{Z}/p\mathbf{Z})^\times$ has even order $2t$, for some t. Indeed, in this case, $\ell^{p^{r-1}}$ has order $2t$ in $(\mathbf{Z}/p^r\mathbf{Z})^\times$, and we get $\ell^{tp^{r-1}} = -1$, as required. Furthermore, we want to ensure that p is relatively

prime to $ND\ell$. But it is an elementary matter to find such a p: we simply choose p so that ℓ is a quadratic nonresidue modulo p, and there are infinitely many such p by quadratic reciprocity.

Now we want to reduce the proof of Proposition 4.1 to a statement about the distribution of Heegner points.

4.4 As before, we regard the tame character χ_t and the end $\vec{e}$ as given. We want to study the λ-adic valuation of the numbers $\chi(\Theta)$, where $\chi = \chi_t\chi_w$, and χ_w varies in the set Y_n of faithful characters of Δ_n. Thus we consider the formal expression

$$S_n = \frac{1}{p^{n-2}} \sum_{\chi_w \in Y_n} \sum_{\sigma \in G_n} \chi(\sigma)\tilde{P}_n^{\sigma},$$

so that $\psi(S_n) = \frac{1}{p^{n-2}} \sum_{\chi_w} \chi(\Theta)$, where we extend ψ by linearity. Note that the factor $1/p^{n-2}$ is a λ-adic unit. It is enough to show that if $n \gg 0$, then $\mathrm{ord}_\lambda(\psi(S_n)) \leq \nu$. Indeed, it would then follow that there exists some $\chi = \chi_t\chi_w$ such that $0 \leq \mathrm{ord}_\lambda(\chi(\Theta)) \leq \nu$. On the other hand, the function ψ is congruent to a constant c modulo λ^ν, by definition of ν. Thus $\sum_{\sigma \in G_n} \chi(\sigma)\psi(P^\sigma) \equiv c\sum \chi(\sigma) \equiv 0 \pmod{\lambda^\nu}$. It follows that $\chi(\Theta) \equiv 0 \pmod{\lambda^\nu}$ for all χ, and we get $\mathrm{ord}_\lambda(\chi(\Theta)) = \nu$ for at least one χ, as required.

Thus, we must compute the λ-adic valuation of $\psi(S_n)$. We start with a formal manipulation. Applying Lemma 2.11 of [Vato1], we obtain

$$S_n = \sum_{\tau \in G_1} \chi_t(\tau) \cdot \left(\tilde{P}_n^{\tau} - p \sum_{\sigma \in K_n} \tilde{P}_n^{\tau\sigma} \right).$$

Applying the norm compatibility of the regularized Heegner points, this reduces to

$$S_n = \sum_{\tau \in G_1} \chi_t(\tau) \cdot \left(\tilde{P}_n^{\tau} - p\tilde{P}_{n-1}^{\tau} \right).$$

Finally, inserting the definition of $\tilde{P}^n$, we get

$$\begin{aligned} S_n &= \sum_{\tau \in G_1} \chi_t(\tau) \cdot \left\{ \left(\frac{1}{\alpha^n} P_n^{\tau} - \frac{1}{\alpha^{n+1}} P_{n-1}^{\tau} \right) - p \left(\frac{1}{\alpha^{n-1}} P_{n-1}^{\tau} - \frac{1}{\alpha^n} P_{n-2}^{\tau} \right) \right\} \\ &= \sum_{\tau} \chi_t(\tau) \cdot \left\{ \frac{1}{\alpha^n} P_n^{\tau} - \left(\frac{1}{\alpha^{n+1}} + \frac{p}{\alpha^{n-1}} \right) P_{n-1}^{\tau} + \frac{p}{\alpha^n} P_{n-2}^{\tau} \right\}. \quad (11) \end{aligned}$$

Now the number α is a unit. Thus, for a given end $\vec{e}$, define the formal quantity

$$\xi_n = \xi_n(\vec{e}) = \frac{1}{\alpha} P_n - \left(\frac{1}{\alpha^2} + p \right) P_{n-1} + \frac{1}{\alpha} P_{n-2}. \quad (12)$$

Then we have

$$\alpha^{n-1} S_n = \sum_{\tau \in G_1} \chi_t(\tau) \cdot \xi_n(\vec{e})^\tau.$$

Our task is to bound the absolute value of $\sum \chi_t(\tau) \cdot \psi(\xi_n^\tau)$, where we define ξ_n^τ and $\psi(\xi_n^\tau)$ in the obvious manner. Recall that we may fix the end $\vec{e}$ arbitrarily.

Now Proposition 4.1 is an immediate consequence of the following result, whose proof will be given in §5.

PROPOSITION 4.5 *Let the character χ_t be fixed. Then, for $n \gg 0$, there exist ends $\vec{e}$ and $\vec{d}$ such that*

$$\sum_{\tau \in G_1} \chi_t(\tau) \cdot \psi(\xi_n(\vec{e}^\tau)) \neq \sum_{\tau \in G_1} \chi_t(\tau) \cdot \psi(\xi_n(\vec{d}^\tau)) \pmod{\lambda^{\nu+1}}.$$

In particular, at least one of the numbers $\sum_{\tau \in G_1} \chi_t(\tau) \cdot \psi(\xi_n(\vec{e}^\tau))$ or $\sum_{\tau \in G_1} \chi_t(\tau) \cdot \psi(\xi_n(\vec{d}^\tau))$ has valuation less than $\upsilon + 1$.

The case of $\lambda | p$

4.6 This case is similar but easier. Let the tame character χ_t be fixed, and let Θ denote the corresponding theta element. Then it is clear from the definitions that $\chi(\Theta) \equiv 0 \pmod{\lambda^\nu}$, for any $\chi = \chi_t \chi_w$. Thus the μ-invariant of $\mathbf{L}(g, \chi_t, T)$ satisfies $\mu \geq \nu$. It suffices therefore to show that the power series $\mathbf{L}(g, \chi_t, T) = \sum c_n T^n$ has at least one coefficient c_n with valuation at most ν. Equivalently, we want to find the valuations of the coefficients of $\Theta \in O[[\Delta_\infty]]$. But now it is enough to consider the theta elements at finite level n. Thus, with the notations of (7) and (9), we write

$$\Theta_n = \chi_t(\theta_n) = \sum_{\sigma \in \Delta_n} c_n(\sigma) \sigma.$$

Then our problem to show that at least one of the numbers $c_n(\sigma)$ has valuation at most ν.

We can give an explicit formula for the $c_n(\sigma)$ as follows. Let $\vec{e}$ denote the end arising in the definition of the theta element, and write $\tilde{P}_n$ for the regularized Heegner point corresponding to the edge $\vec{e}_n$. Then we have

$$\theta_n = \sum_{\sigma \in G_n} \psi(\tilde{P}_n) \cdot \sigma,$$

which then leads to

$$c_n(\sigma) = \sum_{\tau \in G_1} \chi_t(\tau) \cdot \psi(\tilde{P}_n^{\sigma\tau}). \tag{13}$$

Thus we find that the coefficient $c_n(1)$ of the identity element in Δ_n is given explicitly by

$$c_n(1) = \sum_{\tau \in G_1} \chi_t(\tau) \cdot \psi(\tilde{P}_n^\tau).$$

Now Theorem 1.1 follows from

PROPOSITION 4.7 *There exist ends $\vec{e}$ and $\vec{d}$, with corresponding regularized Heegner points $\tilde{P}_n$ and $\tilde{Q}_n$, such that*

$$\sum_{\tau \in G_1} \chi_t(\tau)\psi(\tilde{P}_n^\tau) \neq \sum_{\tau \in G_1} \chi_t(\tau)\psi(\tilde{Q}_n^\tau) \pmod{\lambda^{\nu+1}}.$$

The proof of this proposition will be given in §5 below.

5 PROOF OF THE MAIN RESULTS

In this section, we will complete the proof of Propositions 4.5 and 4.7. Using the results and notations of [Vato1], we reduce everything to a statement about discrete subgroups in $SL_2(\mathbf{Q}_p)$.

5.1 As in [Vato1], we will write $\mathcal{T}$ for the Bruhat-Tits tree of $SL_2(\mathbf{Q}_p)$. The basic facts we will use are as follows:

1. The choice of a basepoint $P = (f, R)$ of level 1 determines an origin of $\mathcal{T}$, corresponding to the maximal order $R_p = R \otimes \mathbf{Z}_p$.

2. Write Γ^1 for the subgroup of $\Gamma' = R[1/p]^\times$ consisting of elements with reduced norm 1. Then $\Gamma^1 \subset B^\times \subset SL_2(\mathbf{Q}_p)$ is a discrete cocompact subgroup. Let $\Gamma \subset \Gamma^1$ denote a fixed torsion-free subgroup of finite index, and put $\mathcal{G} = \Gamma\backslash\mathcal{T}$. Note that the graph $\mathcal{G}$ is bipartite; this will cause us some minor inconvenience in the sequel.

3. Each vertex v of $\mathcal{T}$ determines a Heegner point $P' = P_v$ of level p^n, for some n depending on v. The point P' is represented by a pair (f, R'), where the embedding f is the same as that for the base point P, and the Eichler order R' is in normal form with respect to R, in the sense that $R'_\ell = R_\ell$ as Eichler orders in B_ℓ, for $\ell \neq p$. The class of P' in $\mathrm{Cl}(B)$ is determined as the image of v in $\Gamma'\backslash\mathcal{T}$. (Note that there are other Heegner points which are not of this kind, but those will not concern us in this paper.)

4. If $\tau \in G_1$, and P', v are as above, then there exists $\tau_p \in B_p^\times \cong GL_2(\mathbf{Q}_p)$, independent of P and v, such that the class of P'^τ is that of the vertex $v^\tau = \tau_p v$.

5. The function $\psi : \mathrm{Cl}(B) \to \mathbf{R}$ induces a function $\mathcal{G} \to \mathbf{R}$. If L^2 denotes the vector space of functions on the vertices of $\mathcal{G}$, then ψ is an eigenfunction for the operator ∇ defined by $\nabla(\phi)(v) = \sum_{w\sim v} \phi(w)$, for $\phi \in L^2$, and the sum is taken over the $p+1$ vertices w of $\mathcal{G}$ that are adjacent to v. The eigenvalue of ∇ acting on ψ is the Fourier coefficient a_p.

The genus subgroup

5.2 The proofs of Propositions 4.5 and 4.7 are based on the studying the image of the vectors $(P_n^\tau)_{\tau\in G_1}$ in the product $\prod_{\tau\in G_1}\mathcal{G}$, where $\mathcal{G}\cong \mathrm{Cl}(B)$ is the ideal class group of B. Roughly speaking, one would like to say that the vectors $(P_n^\tau)_{\tau\in G_1}$ are uniformly distributed, as $n\to\infty$. However, this turns out to be false in general, as the image of the Heegner points is constrained by the geometric action of a certain subgroup G_0 of G_1 coming from genus theory (see [Coro1], [Vato1]). We now proceed to describe this.

Let q denote a prime number such that q divides the discriminant D of K. Let $\mathfrak{q}$ denote the unique prime ideal of K lying above q. Then $\mathfrak{q}^2=(q)$, and since q is a rational integer, we see that (q) represents the trivial class in each ring class group $\mathrm{Pic}(O_n)$ (we have assumed at the outset that $(D,p)=1$, so $q\neq p$). It follows that $\mathrm{Frob}(q)$ has order 2 in each Galois group G_n, so that $\mathrm{Frob}(q)$ lies in the torsion subgroup G_1 of $\mathrm{Gal}(H_\infty/K)$. We let $G_0\subset G_1$ denote the subgroup generated by the elements $\mathrm{Frob}(q)$, as q varies over primes dividing D.

It is easy to verify (see [Vato1], Section 3.8) that the group G_0 is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^r$, where r is the number of distinct primes dividing D. The elements $\mathrm{Frob}(q)$, for primes q dividing D, form a basis for G_0 over $\mathbf{Z}/2\mathbf{Z}$. Given $\tau\in G_0$, there exists a unique subset $I_\tau\subset\{q_1,q_2,\dots,q_r\}$ such that

$$\tau=\prod_{q\in I_\tau}\mathrm{Frob}(\mathfrak{q}).$$

Conversely, any $I\subset\{q_1,q_2,\dots,q_r\}$ is of the form I_τ for a unique $\tau=\prod_{q\in I}\mathrm{Frob}(\mathfrak{q})$. For $\tau\in G_0$ we may therefore define a squarefree integer $d=d_\tau$ by saying

$$d=d_\tau=\prod_{q\in I_\tau}q.$$

The above facts are implicit in [Coro1], but do not seem to be stated explicitly there.

Now let χ_t denote any fixed tame character of G_1. We define a modified function ψ_* on Heegner points as follows:

$$\psi_*(P)=\sum_{\tau\in G_0}\chi_t(\tau)\psi(P^\tau). \tag{14}$$

Note that $\chi_t(\tau)=\pm1$ for $\tau\in G_0$, since G_0 has exponent 2. Thus ψ_* takes values in the ring generated by the values of ψ. Note also that ψ_* depends on χ_t, although we have suppressed this from the notation. Since we will be dealing throughout with a fixed character χ_t, this should not cause any problems. Furthermore, the function ψ_* takes on only finitely many values, since this is already true of ψ.

Now observe that if χ_t is given, then one has the simple identity

$$\sum_{\tau \in G_1} \chi_t(\tau)\psi(P^\tau) = \sum_{\tau \in G_1/G_0} \chi_t(\tau)\psi_*(P^\tau).$$

Let C denote a set of coset representatives for G_1/G_0. We will see below that the vectors $(P_n^\tau)_{\tau \in C}$ satisfy good independence properties. Thus we are led to reformulate everything in terms of the function ψ_*, rather than the original ψ.

The following proposition verifies that ψ_* factors through a finite quotient graph of the tree $\mathcal{T}$, in the same as manner ψ, and also satisfies the same basic properties. It is the analogue in our situation of the level raising that occurs in [Coro1]. We will also need an analogue of a lemma of Ihara, which is elementary in this context; the argument given here is drawn from Section 2 of [DT94].

We let the notation be as in §5.1.

Proposition 5.3 *The following statements hold:*

1. *There exists a finite index subgroup $\Gamma_D \subset \Gamma$ and a function ψ_D defined on $\mathcal{G}_D = \Gamma_D \backslash \mathcal{T}$, such that if the vertex v corresponds to the Heegner point P', then we we have $\psi_D([v]) = \psi_*(P')$, where $[v]$ denotes the class of v in $\mathcal{G}_D$.*

2. *The function ψ_D takes values in the ring O. It is nonzero, and if the original ψ is nonconstant modulo $\lambda^{\nu+1}$, then ψ_D is also nonconstant modulo $\lambda^{\nu+1}$.*

Proof. Let ψ denote our original function on $\mathrm{Cl}(B) \cong B^\times \backslash \hat{B}^\times / \hat{\mathbf{Q}}^\times \hat{R}^\times$, where R is the Eichler order corresponding to our fixed Heegner point $P = (f, R)$ of level 1. From this viewpoint, the relationship with Heegner points is given by $\psi(P') = \psi(x)$, where x is chosen so that $x\hat{R}x^{-1} = \hat{R}'$ as oriented Eichler orders, and $P' = (f, R')$ as usual. We want to study the modified functions $P' \mapsto \psi(P'^\tau)$, for $\tau \in G_0$, and find an adelic function ψ_D, left invariant under $B^\times$ and right invariant under an open compact subgroup, to represent ψ_*. So given $\tau \in G_0$, we let $\tilde{\tau}$ denote an idele of K whose Artin symbol is τ. We may view $\tilde{\tau}$ as an element of $\hat{B}$, via the embedding $f : K \to B$. Now define a function ψ_D on $\hat{B}^\times$ as follows:

$$\psi_D(x) = \sum_d \chi_t(\tau_d)\psi(x\tilde{\tau}_d),$$

where the sum is taken over squarefree divisors d of D, $\tau_d \in G_0$ is the corresponding element of the Galois group, and $\tilde{\tau}_d$ is the corresponding idele, as explained above. Then ψ_D is indeed left-invariant under $B^\times$ and right invariant under a suitable open compact subgroup. We proceed to clarify its relationship with ψ_*.

So let $P' = (f, R')$ be a Heegner point corresponding to the vertex v on the tree $\mathcal{T}$. From the definition of the Galois action, we have $P'^{\tau} = (f, R'^{\tau})$, where R'^{τ} is such that $\hat{R}'^{\tau} = \tilde{\tau}\hat{R}'\tilde{\tau}^{-1}$, so that $P' \mapsto \psi(P'^{\tau})$ is represented by $\psi(P'^{\tau}) = \psi(\tilde{\tau}x)$. This means, in particular, that the function ψ_D which appeared above does not represent ψ_* in any obvious manner (since $\psi(\tilde{\tau}x) \neq \psi(x\tilde{\tau})$ for general x). The key is therefore to choose the point x in some intelligent manner, and we shall accomplish this by raising the level, exactly as in [Coro1].

Given any Heegner point $P = (f, R')$, we define a new oriented Eichler order of level N^+D by requiring that $R'_D \otimes \mathbf{Z}_\ell = R' \otimes \mathbf{Z}_\ell$, if $\ell \nmid D$, and $R'_D \otimes \mathbf{Z}_q = R'(q) = R'_q \cap \tilde{\tau}_q R'_q \tilde{\tau}_q^{-1}$ for $q|D$. The embedding $f : \mathfrak{o}_n \to R'$ restricts to an embedding $\mathfrak{o}_n \to R'_D$. To fix orientations, we choose an arbitrary orientation of the maximal order $\mathfrak{o} \subset K$ at each prime $q|D$. This induces orientations on each order $\mathfrak{o}_n$, and we fix the orientations on R'_D at primes $q|D$ by requiring that the embedding $\mathfrak{o}_n \to R'_D$ be orientation-preserving.

Now, if R_D is the Eichler order of level N^+D obtained in this way from our base point $P = (f, R)$ of level 1, then we claim that $\psi_*(P') = \psi_D(x)$, where $x \in \hat{B}^\times$ is chosen so that $x\hat{R}_D x^{-1} = \hat{R}'_D$, as oriented Eichler orders of level N^+D.

To prove this, let $\tau_d \in G_0$. Then $d = q_1 q_2 \dots q_r$ for distinct primes $q_i|D$, and $\tilde{\tau}_d = \tilde{\tau}_{q_1} \dots \tilde{\tau}_{q_r}$. The idele $\tilde{\tau}_d$ is trivial away from the primes q_i. Now let the basepoint P be fixed, as above. Let $P' = (f, R')$ be given. Then our choice of $x = (x_\ell)$ implies that $x_\ell R_\ell x_\ell^{-1} = R'_\ell$, if ℓ is any prime such that $\ell \nmid D$. If $\ell = q$ is a prime dividing D, then write T and T' for the conjugates of R_q and R'_q under $\tilde{\tau}_q$ respectively. Put $R(q) = R_q \cap T$, and $R'(q) = R'_q \cap T'$, so $R(q)$ and $R'(q)$ are local Eichler orders of level q. By definition, we have $x_q R(q) x_q^{-1} = R'(q)$. Note that this implies already that conjugation by x_q takes the pair of (local) maximal orders (R, T) to the pair (R', T'). Since we have chosen x so that it preserves the local orientations, we see that $x_q R x_q^{-1} = R'$ and $x_q T x_q^{-1} = T'$. Now an easy calculation shows that $x_q^{-1}\tau_q^{-1}x_q\tau_q$ normalizes R_q, so that $x_q^{-1}\tau_q^{-1}x_q\tau_q \in R_q$, and we have $x_q\tau_q R_q = \tau_q x_q R_q$, for each prime q. By multiplicativity we get $x\tau_d\hat{R} = \tau_d x\hat{R}$, for any $\tau_d \in G_0$, which implies that $\psi(\tilde{\tau}x) = \psi(x\tilde{\tau})$, for $\tau \in G_0$. It follows that $\psi(P'^{\tau}) = \psi(x\tilde{\tau})$ for $\tau \in G_0$. Finally, one finds that the function $P' \mapsto \psi_*(P')$ is given by $\psi_*(P') = \psi_D(x)$, where the point x is chosen as above.

We note that it follows from these considerations that the function ψ_D is right-invariant under $\hat{R}_D^\times$, and $\psi_*(P')$ depends only on the class of R'_D in the set of conjugacy classes of oriented Eichler orders of level N^+D.

We may now complete the proof of the proposition, beginning with the the first assertion. Indeed, if $P' = (f, R')$ is a Heegner point corresponding to the vertex v, then by definition R' is in normal form with respect to the base point R, and it is clear that R'_D is in normal form with respect to R_D.

Thus we may identify R'_D with the same vertex v. Applying strong approximation in $\hat{B}$, we deduce from ψ_D a function on $\mathcal{T}$, also denoted by ψ_D, such that ψ_D is invariant on the left by the group $\Gamma'_D = R_D[1/p]^\times$, which is commensurable with $\Gamma' = R[1/p]^\times$. Thus we may simply take $\Gamma_D = \Gamma'_D \cap \Gamma$ to obtain the first statement of the proposition.

As for the second, it suffices to show that the function ψ_D on $\hat{B}^\times$ is nonzero and nonconstant modulo $\lambda^{\nu+1}$. We begin with some general observations. Suppose B is a definite quaternion algebra, and $R \subset B$ any Eichler order. Suppose q is a prime number at which B is split, and such that R_q is a maximal compact subring. Fix isomorphisms $B_q \cong M_2(\mathbf{Q}_q)$ and $R_q \cong M_2(\mathbf{Z}_q)$. Let $\tilde{\tau}_q$ denote any element of R_q with reduced norm q, and let $\hat{R}(q) = \hat{R} \cap \tilde{\tau}_q \hat{R} \tilde{\tau}_q^{-1}$. If we write $S = B^\times \backslash \hat{B}^\times / \hat{\mathbf{Q}}^\times \hat{R}^\times$ and $S_q = B^\times \backslash \hat{B}^\times / \hat{\mathbf{Q}}^\times \hat{R}(q)^\times$, then there are two projections (degeneracy maps) $S_q \to S$, induced by the two inclusions of $\hat{R}(q) \to \hat{R}$, namely, the identity inclusion $\hat{R}(q) \subset \hat{R}$, and the conjugation $x \mapsto \tilde{\tau}_q^{-1} x \tilde{\tau}_q$. We write 1^* and $\tilde{\tau}_q^*$ to denote the corresponding pullback maps on k-valued functions, where k is any ring. In our application, we will have $k = O/\lambda^{\nu+1}$. Since S and S_q are defined as quotients of $\hat{B}^\times$, we may view functions on S or S_q as functions on $\hat{B}^\times$ via the natural projection maps; note that from this viewpoint we have $1^*\psi(x) = \psi(x)$, and $\tilde{\tau}_q^* \psi(x) = \psi(x\tilde{\tau}_q)$, for any function ψ on S.

Now let ψ_1 and ψ_2 denote arbitrary *nonconstant* k-valued functions on the set S. We claim that the functions $1^*\psi_1$ and $\tilde{\tau}_q^* \psi_2$ are linearly independent. This is easy to see. Indeed, suppose there is a linear dependence relation; then, by scaling the functions ψ_i we may assume that $1^*\psi_1 = \tilde{\tau}_q^* \psi_2$. But $1^*\psi_1 = \psi_1$ (viewed as a function on $\hat{B}^\times$) is right-invariant under $SL_2(\mathbf{Z}_q) \subset \hat{R}^\times$, by definition. Since ψ_2 is also right-invariant under $SL_2(\mathbf{Z}_q)$, one finds that $\tilde{\tau}_q^* \psi_2$ is invariant under $\tilde{\tau}_q SL_2(\mathbf{Z}_q) \tilde{\tau}_q^{-1}$. Since $1^*\psi_1 = \tilde{\tau}_q^* \psi_2$, it follows that $1^*\psi_1$ and $\tilde{\tau}_q^* \psi_2$ are invariant under the group generated by $SL_2(\mathbf{Z}_q)$ and $\tilde{\tau}_q SL_2(\mathbf{Z}_q) \tilde{\tau}_q^{-1}$. But it is well known that these two subgroups generate all of $SL_2(\mathbf{Q}_q)$ (this is a theorem of Ihara, see [Ser80]). Since all our functions are left-invariant under $B^\times$, and right invariant under the product of $SL_2(\mathbf{Q}_q) \cdot \prod_{\ell \neq q} R_\ell^\times \cdot \hat{\mathbf{Q}}^\times$, it follows from strong approximation in $\hat{B}^\times$ that they must be constant, which is contradictory to our hypothesis. (Note that $1^*\psi_1$ and $\tilde{\tau}_q^* \psi_2$ are constant on $\hat{B}^\times$ if and only if the original ψ_1 and ψ_2 are so on S.)

We can actually sharpen this observation as follows. It is known that the spaces of functions on S and S_q are endowed with an action of Hecke operators T_ℓ, for all but finitely many primes ℓ. With the notation above, we have $T_\ell = 1_* \tilde{\tau}_\ell^*$, where 1_* is the adjoint of 1^*. (See for [DT94], Section 2, for a detailed discussion.) So suppose further that the functions ψ_1 and ψ_2 are eigenfunctions for all but finitely many T_ℓ, corresponding to the same system of eigenvalues, so that $T_\ell \psi_i = a_\ell \psi_i$, where the eigenvalue a_ℓ is independent of i. We will also assume that $a_\ell \neq \ell + 1$, for all ℓ. Note that this already implies that the ψ_i are nonconstant, since the eigenvalue of T_ℓ acting on the constants

is $\ell + 1$. In this situation, we claim that any nontrivial linear combination $a \cdot 1^* \psi_1 + b \cdot \tilde{\tau}_q^* \psi_2$ is not only nonzero (which was proven above) but also nonconstant. But this is clear: since the Hecke operator T_ℓ commutes with $\tilde{\tau}_q^*$ if $q \neq \ell$, one finds that $a \cdot 1^* \psi_1 + b \cdot \tilde{\tau}_q^* \psi_2$ is a nonzero eigenvector for T_ℓ with eigenvalue $a_\ell \neq \ell + 1$, which implies that it is not constant.

But it is now immediate that ψ_D is nonzero and nonconstant. Indeed, if we fix a prime $q|D$, then, using multiplicativity, we can rewrite ψ_D as

$$\psi_D = 1^* \psi_{D/q} + \chi_t(\tau_q) \tilde{\tau}_q^* \psi_{D/q},$$

where

$$\psi_{D/q} = \sum_{(d,q)=1} \chi_t(\tau_d) \psi(x \tilde{\tau}_d),$$

where this time the sum is taken over squarefree divisors d of D such that d is prime to q. The preceding considerations show that ψ_D will be nonzero and nonconstant, and will be an eigenvector for T_ℓ with eigenvalue $a_\ell \neq \ell + 1$, if the same is true for $\psi_{D/q}$. But we may now argue inductively, to reduce to the case of ψ, which is known to satisfy the requisite conditions. □

Remark 5.4 In the sequel, we will work with the quotient graph $\mathcal{G}_D = \Gamma_D \backslash \mathcal{T}$ rather than $\mathcal{G}$. Thus we will use the notation $[v]$ and $[P]$ to denote the image of a vertex v, or the class of a Heegner point P', in $\mathcal{G}_D$. We shall also view the function ψ_D as being defined on the vertices of $\mathcal{G}_D$.

Note that if P and Q are Heegner points such that $[P] = [Q]$ in $\mathcal{G}_D$, then we have

$$\psi_D(P) = \sum_{\tau \in G_0} \chi_t(\tau) \psi(P^\tau) = \sum_{\tau \in G_0} \chi_t(\tau) \psi(Q^\tau) = \psi_D(Q),$$

by definition of $\mathcal{G}_D$ and ψ_D. This will be useful in the sequel.

Note also that the graph $\mathcal{G}_D$ is bipartite. However, it follows from the discussion above that ψ_D factors through a non-bipartite quotient, as was for case for ψ. Indeed, we have seen already that ψ_D factors through $\Gamma'_D \backslash \mathcal{T}$, where $\Gamma'_D = R_D[1/p]^\times$. But by Lemma 1.5 of [BD98], the latter contains an element whose determinant has odd valuation.

Proof of Propositions 4.5 and 4.7

5.5 We want to make a good choice for the end $\vec{P} = (\vec{e}_0, \vec{e}_1, \ldots, \vec{e}_n, \ldots)$ as in the definition of the theta elements and p-adic L-function. If $\tau \in G_1$, then write $\vec{e}_n^\tau$ for the conjugate of e_n under the action of τ. Let P_n be the origin of the edge $\vec{e}_n$. Then P_n is also the terminus of the preceding edge $\vec{e}_{n-1}$. Since the formula (12) involves the predecessors of P_n, we are motivated to consider the vertices P_{n-1} and P_{n-2} traversed by the end $\vec{e}$ at steps $n-1$ and $n-2$. Observe that for each n and τ, the vertices

$[P_i^\tau]$ of $\mathcal{G}_D$ corresponding to the Heegner points P_i^τ satisfy the condition that $[P_{n+1}^\tau]$ and $[P_{n-1}^\tau]$ are distinct neighbors of $[P_n^\tau]$.

With this notation, we have the following important proposition. It is the analogue in our situation of the main lemma in Ferrero-Washington [FW79]. Recall that the graph $\mathcal{G}$ is bipartite, so that the vertices of $\mathcal{G}_D$ are divided into two sets, depending on whether the distance from some given vertex is even or odd.

PROPOSITION 5.6 *Let Q_r be a given Heegner point of conductor p^r, with predecessors Q_{r-1} and Q_{r-2} of conductors p^{r-1} and p^{r-2} respectively. Let C be a fixed set of representatives of G_1/G_0. Then, for all $n \in \mathbf{Z}$ sufficiently large, with $n \equiv r \pmod 2$, we may find an end $\vec{e}$, and $\tau_0 \in C$, satisfying the following two conditions:*

1. *$[P_{n-i}^\tau] = [Q_{r-i}^\tau]$ for $\tau \in C$, $\tau \neq \tau_0$, and $0 \leq i \leq 2$;*
2. *$[P_n^{\tau_0}] = [v_n]$, $[P_{n-1}^{\tau_0}] = v_{n-1}$, and $[P_{n+1}^{\tau_0}] = v_{n+1}$, where the v_i are any given vertices of $\mathcal{G}_D$ such that v_{n-1} and v_{n+1} are distinct neighbors of v_n, subject to the constraint that $[v_n]$ and $[Q_r]$ are in the same class of the bipartition of $\mathcal{G}_D$.*

The element $\tau_0 \in G_1$ depends only the quadratic field K.

REMARK 5.7 We may view the end $\vec{d}$ as determining an infinite walk, without backtracking, on the finite graph $\mathcal{G}_D$. In concrete terms, the proposition above means that we can choose $\vec{e}$ so that, when $\tau \in C$, $\tau \neq \tau_0$, then the vertices traversed by $\vec{e}^\tau$ at stages n, $n-1$, $n-2$, are given by the original $[Q_r^\tau]$, $[Q_{r-1}^\tau]$, $[Q_{r-2}^\tau]$ respectively, while still retaining the freedom to specify the vertices traversed (at the same 3 stages) by $\vec{e}^{\tau_0}$.

To complement this proposition, we need to know that we can make good choices for the vertices traversed by $\vec{e}^{\tau_0}$. That such choices exist is the content of

LEMMA 5.8 *There exists a vertex x of $\mathcal{G}_D$, together with distinct neighbors y and z, such that $\psi_D(y)$ and $\psi_D(z)$ are not congruent modulo $\lambda^{\nu+1}$. We may choose the vertex x to lie in either class of the bipartition of $\mathcal{G}$.*

Proof. We have seen in Proposition 5.3 that the function ψ_D on $\mathcal{G}_D$ is not congruent to a constant function modulo $\lambda^{\nu+1}$. So ψ_D takes on at least two distinct values modulo $\lambda^{\nu+1}$. Suppose that, for every vertex x of $\mathcal{G}_D$, the function ψ_D is constant modulo $\lambda^{\nu+1}$ on the neighbours y of x. Since this is true for *every* x, it would follow that ψ_D takes on precisely two values modulo $\lambda^{\nu+1}$, say a and b. Dividing the vertices of $\mathcal{G}_D$ into corresponding sets A and B, it follows that every edge of $\mathcal{G}_D$ goes

from A to B. Then $\mathcal{G}_D$ must be a bipartite graph, and the function ψ_D must respect the bipartition. But ψ_D factors through the quotient $\Gamma'_D \backslash \mathcal{G}_D$ of $\mathcal{G}_D$, and we have remarked above that Γ'_D contains an element which interchanges the two halves of the bipartition. This implies that ψ_D is constant modulo $\lambda^{\nu+1}$, a contradiction. Thus we obtain at least one vertex x satisfying our requirements. The fact that we may choose x to lie in either class of the bipartition also follows from the fact that Γ'_D contains an element that interchanges the vertices in the bipartition. □

5.9 Before embarking upon the proof of Proposition 5.6, we want to show how it implies Propositions 4.5 and 4.7. Let x, y, z denote the vertices of $\mathcal{G}_D$ provided by Lemma 5.8. Note that the vertex x may be chosen from either half of the bipartition; we will have to keep track of this choice in the sequel. Now select a vertex w such that w is adjacent to x, but such that w is distinct from both y and z. Such a w exists because $\mathcal{G}_D$ is regular of degree $p+1 \geq 4$. Since w and y are adjacent to x, it is clear from the considerations of [Vato1] that there exists a Heegner point Z_r of level p^r, with predecessors Z_{r-1} and Z_{r-2}, such that $[Z_{r-1}] = x$, while $[Z_{r+1}] = y$, and $[Z_{r-2}] = w$. Observe that the choice of x determines the parity of r.

Now Proposition 5.6 states that, for all $n \gg 0$, of suitable parity, there exists an end $\vec{e}$ (perhaps depending on n), with corresponding Heegner points P_j, such that $[P^\tau_{n-i}] = [Z^\tau_{r-i}]$, for each i, and $\tau \in C$. In particular, the vertices $[P^{\tau_0}_j]$ traversed by $\vec{e}^{\tau_0}$ at stages $n-2$, $n-1$, n, are w, x, y respectively. Applying Proposition 5.6 again, we now find another end $\vec{d}$, with corresponding Heegner points Q_j, such that $[Q^\tau_{n-i}] = [Z^\tau_{r-i}]$, for $i = 0, 1, 2$, and $\tau \in C$, $\tau \neq \tau_0$. At $\tau = \tau_0$, we require that $[Q^{\tau_0}_{n-2}]$, $[Q^{\tau_0}_{n-1}]$, $[Q^{\tau_0}_n]$ are w, x, z, respectively.

Now we compare the associated theta elements. We begin by considering the situation of Proposition 4.5. Fixing some end of $\mathcal{T}$, and letting ξ_n denote the quantity defined in (12), our job is to compute the absolute value of the expression

$$\sum_{\tau \in G_1} \chi_t(\tau)\psi(\xi^\tau_n) = \sum_{\tau \in C} \chi_t(\tau)\psi_D(\xi^\tau_n),$$

where $\psi_D(\xi^\tau_n) = \sum_{\tau \in G_0} \chi_t(\tau)\psi(\xi^\tau_n)$. But since the function ψ_D factors through the finite graph $\mathcal{G}_D$, we find that $\psi_D(\xi_n(\vec{e})^\tau) = \psi_D(\xi_n(\vec{d})^\tau)$, for $\tau \in C$, $\tau \neq \tau_0$. On the other hand, we have $[P^{\tau_0}_{n-1}] = [Q^{\tau_0}_{n-1}] = x$ and $[P^{\tau_0}_{n-2}] = [Q^{\tau_0}_{n-2}] = w$, while $[P^{\tau_0}_n] = y$ and $[Q^{\tau_0}_{n-1}] = z$. By choice of the vertices y and z, and the formula (12), we find that

$$\psi_D(\xi_n(\vec{e})^{\tau_0}) - \psi_D(\xi_n(\vec{d})^{\tau_0}) = \frac{1}{\alpha^2}\left(\psi_D(z) - \psi_D(y)\right) \neq 0 \pmod{\lambda^{\nu+1}}.$$

This gives the statement of Proposition 4.5, for all $n \gg 0$ of suitable parity. To complete the proof, one simply repeats the argument, upon choosing x appropriately. Finally, one obtains Proposition 4.7 in precisely the same fashion.

We now proceed to the proof of Proposition 5.6.

5.10 Let P denote a Heegner point, corresponding to the vertex $v \in \mathcal{T}$. We want to control the classes in $\mathcal{G}_D$ of the various P^τ, for $\tau \in C$, and then say something about the various predecessors. Then it is natural to introduce the vector $(\tau_p v)_{\tau \in C}$, and study its distribution in the product $\mathcal{G}_D \times \ldots \mathcal{G}_D$, where the product is indexed by the elements of C. Note also that $\mathcal{G}_D = \Gamma_D \backslash \mathcal{T}$. If we put $\Gamma_D^\tau = \tau_p \Gamma_D \tau_p^{-1}$, and $\mathcal{G}_D^\tau = \Gamma_D^\tau \backslash \mathcal{G}$, then there is an isomorphism $\mathcal{G}_D \cong \mathcal{G}_D^\tau$ induced by $v \mapsto \tau_p v$. It will be convenient in the sequel to reformulate the problem so that we consider the distribution of the diagonal vector $(v, \ldots, v)$ in $\prod_{\tau \in C} \mathcal{G}_D^\tau$. Letting $\tilde{K}$ denote a maximal compact subgroup of $\tilde{G} = PGL_2(\mathbf{Q}_p)$, we have $\mathcal{T} = \tilde{G}/\tilde{K}$, and

$$\prod_{\tau \in C} \mathcal{G}_D^\tau = \prod_{\tau \in C} \Gamma_D^\tau \backslash \tilde{G} / \tilde{K}.$$

We are therefore led to consider $\Gamma_C \backslash \tilde{G}_C$, where $\Gamma_C = \prod_{\tau \in C} \Gamma_D^\tau$, and $\tilde{G}_C = \prod_{\tau \in C} \tilde{G}$. In order to do this, we need some simple preliminary results. Note that $PSL_2(\mathbf{Q}_p) \subset PGL_2(\mathbf{Q}_p)$ is a subgroup of index two; it will actually be essential to work with the smaller group, as it is a simple group, and generated by unipotent elements.

Lemma 5.11 *Let G denote the group $PSL_2(\mathbf{Q}_p) = SL_2(\mathbf{Q}_p)/\pm 1$. Then G admits no nontrivial automorphism commuting with all inner automorphisms.*

Proof. Let ϕ denote any automorphism of G which commutes with all conjugations. Let x and g be arbitrary elements of G; then we have

$$g\phi(x)g^{-1} = \phi(gxg^{-1}) \iff g\phi(x)g^{-1} = \phi(g)\phi(x)\phi(g)^{-1}$$

since ϕ commutes with the conjugation by g. This implies that $g^{-1}\phi(g)$ commutes with $\phi(x)$, for any x and g. Letting x vary, we find that $g^{-1}\phi(g)$ is in the center of G, so that $g^{-1}\phi(g) = 1$. □

Lemma 5.12 *Let $r \geq 2$ denote an integer, and let $G_* = \prod_{i=1}^r G$, where $G = PSL_2(\mathbf{Q}_p)$. Let $\Delta \subset G_*$ denote the diagonal subgroup consisting of the elements $\Delta(x) = (x, \ldots, x)$, for $x \in G$. Let $H \subset G_*$ denote any nontrivial subgroup which is normalized by Δ. Then one of two possibilities occurs: either*

1. *$H = \Delta$, or*
2. *there is a proper subset $S \subset \{1, 2, \ldots, r\}$ such that H has nonempty intersection with $G_*^S = \prod_{i \in S} G$. In this case, $H \cap G_*^S$ is normalized by the diagonal subgroup $\Delta^S \subset G^S$. Here Δ^S consists of the elements $\Delta^S(x)$, for $x \in G$, where $\Delta^S(x) = (x_1, \ldots, x_r)$ has component $x_i = x$ for $i \in S$, and $x_i = 1$ if not.*

Proof. We note at the outset that $H \cap G_*^S$ is normalized by Δ^S, because H is normalized by Δ. Now since H is nontrivial, we may assume, by relabeling if necessary, that the projection of H to the first factor is nontrivial. Then, since H is normalized by Δ, and $G = PSL_2(\mathbf{Q}_p)$ is a simple group, we find that the projection of H onto the first factor is surjective. Thus, for any $x \in G$, we may select some $\phi(x) = (\phi_1(x) \ldots, \phi_r(x)) \in H$ such that $\phi_1(x) = x$. Suppose that there exists some $x \in G$ such that $\phi(x)$ is not unique. In this case, there exist distinct elements $\phi(x)$, $\phi'(x)$ in H such that each of $\phi(x)$ and $\phi'(x)$ have first component x. Considering $\phi(x)\phi'(x)^{-1}$, we find that H has nontrivial intersection with the subgroup G_*^S, where $S = \{2, 3, \ldots, r\}$. Thus case 2 of the lemma holds.

We may therefore assume that, for each $x \in G$, there is a unique $\phi(x)$ with first component x. Letting x, $y \in G$, we find that

$$\phi(x)\phi(y) = (x, \ldots, \phi_r(x)) \cdot (y, \ldots, \phi_r(y) = (xy, \ldots, \phi_r(x)\phi_r(y)).$$

Thus $\phi(x)\phi(y)$ is an element of H with first component xy. By uniqueness, we find that $\phi(x)\phi(x) = \phi(xy)$ by definition of $\phi(xy)$. It follows from the formula above that $\phi_i(x)\phi_i(y) = \phi_i(xy)$, for every x, y, so that each ϕ_i is a homomorphism. If $\phi_i(x) = 1$ for some x and i, we see that $H \cap G_*^S$ is nonempty for $S = \{1, 2, \ldots, i-1, i+1 \ldots, r\}$ and we are in case 2. Thus we may assume that each ϕ_i is injective. Using the fact that H is normalized by the diagonal, together with the uniqueness, we see in fact that each $\phi_i : G \to G$ is surjective, and commutes with all conjugations. But now the lemma above implies that each ϕ_i is the identity map, so that H is the diagonal subgroup, as stated in case 1.

LEMMA 5.13 *Let G_* be as in the lemma above. For each $i = 1, \ldots, r$, let Γ_i denote a discrete and cocompact subgroup of G, and let $\Gamma_* = \prod_{i=1}^r \Gamma_i \subset G_*$. Let X denote the closure of of the product $\Gamma_* \cdot \Delta$, where Δ is the diagonal, as above. Suppose that, for $i \neq j$, the groups Γ_i and Γ_j are not commensurable. Then X contains a subgroup of the form $1 \times \ldots G \times 1$, concentrated on the i-th factor, for some i with $1 \leq i \leq r$.*

Proof. As in [Vato1], the main ingredient is Ratner's theorem (see [Rat95], Theorem 2, and [Vato1], Theorem 4.7) on closures of unipotent orbits. Indeed, Ratner's theorem implies that the set X is of the form $\Gamma_* \cdot H$, where H is a closed subgroup of G_* containing Δ, such that $\Gamma_* \cdot H$ is closed in G_*. Note that H must strictly contain the diagonal, since the groups Γ_i and Γ_j are not commensurable for $i \neq j$ (this follows from the case $r = 2$, which was already proven in Corollary 4.8 of [Vato1]). Also, since $\Delta \subset H$, it is trivial that H is normalized by Δ. Choose some $(x_1, x_2, \ldots, x_r) \in H$ with, say, $x_1 \neq x_2$. Since $(x_1, x_1, \ldots, x_1) \in H$, we see that $H^S = H \cap G_*^S$ is nontrivial, where $S = \{2, 3, \ldots, r\}$. Furthermore, H^S is normalized by Δ^S. It follows from the lemma above that H^S

is either diagonal, or has nonempty intersection with some $G_*^{S'}$, where $S' \subsetneq S$. If H^S is diagonal, then we are done by induction on r. If not, we repeat the argument with S' instead of S. If $H^{S'}$ is diagonal, then we are done, otherwise we can shrink S'. Repeating this argument, we reduce to the case when S' has just one element, and $H^S = H \cap G_*^{S'}$ is nontrivial and concentrated on the i-th factor. Since H^S is normalized by the diagonal, and $PSL_2(\mathbf{Q}_p)$ is simple, we find that H contains the i-th factor, as required.

5.14 We may now prove Proposition 5.6. We are interested in triples $\mathbf{v} = (v_{n-1}, v_n, v_{n+1})$, where each v_i is a vertex of $\mathcal{T}$, and there are oriented edges leading from v_{n-1} to v_n, and then from v_n to v_{n+1}. Equivalently, the vertices v_{n-1} and v_{n+1} are distinct neighbours of v_n. Given such a triple $\mathbf{v}$, and an element $\tau \in G_1$, we may define the conjugate $\mathbf{v}^\tau$ in the obvious manner.

Now let X denote the set of such triples $\mathbf{v}' = (v'_{n-1}, v'_n, v'_{n+1})$, where this time the v'_i are vertices of the finite graph $\mathcal{G}_D$, subject to the same adjacency conditions. Then X is a finite set, and we are interested in studying the image of $(\mathbf{v}^\tau)_{\tau \in C}$ inside $\prod_\tau X$. So write $\tilde{X}$ for the set of triples $\mathbf{v} = (v_{n-1}, v_n, v_{n+1})$ as above, but this time with the $v_i \in \mathcal{T}$. Then there is an action of $\tilde{G} = PGL_2(\mathbf{Q}_p)$ on $\tilde{X}$, by left translation, and, using the description of vertices of $\mathcal{T}$ in terms of homethety classes of lattices [Ser80], one checks easily that this action is transitive. Furthermore, the stabilizer of any given $\mathbf{v}$ is an open compact subgroup N (a subgroup of 'level' p^2). One deduces from this that $X = \Gamma_D \backslash \tilde{G}/N$, and that the image of $\mathbf{v}$ in X is computed simply as the image of $\mathbf{v}$ in the quotient. Furthermore, the class of $\mathbf{v}^\tau$ is simply computed as the image of $\tau_p \mathbf{v}$. Equivalently, the class of $\mathbf{v}^\tau$ is determined by the image of $\mathbf{v}$ in $X_\tau = \Gamma_D^\tau \backslash G/N$.

We apply the foregoing results, taking as the Γ_i the groups Γ_D^τ. Note that $\prod \Gamma_D^\tau \subset \prod SL_2(\mathbf{Q}_p)$, by definition of the groups Γ_D^τ. Now, the points Q_i of Proposition 5.6 determines a triple $\mathbf{v}$, and we let $x \in \tilde{G}$ represent the corresponding point in $\tilde{G}/N$. In view of Lemma 5.13 above, there exist $\tau_0 \in C$, and $y \in G = SL_2(\mathbf{Q}_p)$, together with elements $\gamma_\tau \in \Gamma_D^\tau$, for $\tau \in C$ such that $\gamma_\tau y$ is very close to 1 in PSL_2 for all $\tau \neq \tau_0$, and $\gamma_{\tau_0} y$ may be specified to lie in an arbitrary open set (again in PSL_2). Taking the element $yx \in G$, we find that yx determines the same class as x in X_τ for $\tau \neq \tau_0$, while the image of $yx \in \mathcal{G}_D^{\tau_0}$ may be specified arbitrarily, subject to the stated parity condition. Note also that the element τ_0 depends only on the quadratic field K. This proves that the desired patterns occur for Heegner points of some large conductor; that the patterns occur for points of conductor p^n for all $n \gg 0$, with $n \equiv r \pmod 2$, follows from Ratner's theorem on uniform distribution (see [Vat01], Theorem 4.11, or [Rat95], Theorem 4). □

We want to point out a simple consequence of Lemma 5.13.

PROPOSITION 5.15 *Let $\tau \mapsto C_\tau$ be any function from C to $\mathrm{Cl}(B)$. Then there exists a Heegner point P*

of conductor p^n, for all $n \gg 0$, such that $[P^\tau] = C_\tau$, for each $\tau \in C$.

Proof. It follows from Lemma 5.13 and induction on r that $\Gamma_D \cdot \Delta$ is dense in G_*. □

6 Jochnowitz Congruences

In this section we will show how the foregoing results may be used to study the nontriviality of classical Heegner points on modular curves. Thus let g denote a modular form of level N, and let K denote a quadratic field in which all primes dividing N are split, so that $L(g, K, s)$ has functional equation with sign -1. (This is the classical Heegner hypothesis.) Let E denote the abelian variety attached by Shimura to g. Then we are interested in studying $E(H_\infty)$, where $H_\infty = \cup H_n$ is the compositum of all ring class fields of conductor p^n, and the goal is to find points of infinite order. As for the torsion points, the following lemma is well-known (see [BD96], Lemma 6.3):

Lemma 6.1 *We have $E(H_n) = F_n \oplus E_n$, where E_n is $\mathbf{Z}$-free and F_n is finite of order bounded independent of n. Thus the torsion subgroup F_∞ of $E(H_\infty)$ is finite, and $F_n = F_m = F_\infty$, for n and m sufficiently large.*

The basic mechanism for producing points is that of complex multiplication. As in the introduction, we let $Q \in X_0(N)$ be the CM point defined by a pair $(A, \mathfrak{n})$, where A is an elliptic curve with complex multiplications by the order O_c of conductor c, and $\mathfrak{n}$ is a fractional ideal of O_c with norm N. Then the point Q is defined over $K(c)$. By abuse of notation, we shall continue to write Q for the point $(Q - \infty) \in J_0(N)$, where ∞ denotes the cusp at infinity on $X_0(N)$.

Let $\tilde{Q}$ denote the image of Q in $E(K(c))$. We want some criterion for determining whether or not the point $\tilde{Q}$ and its various twists are of infinite order. This is provided by the following simple observation, at least when $c = p^n$.

Lemma 6.2 *Let $c = p^n$, and let the groups E_n and F_n be as in the preceding lemma. Let ℓ denote a prime number such that the order of $F_\infty = \cup F_n$ is prime to ℓ. Let $\tilde{Q}$ be any point in $E(H_n)$. Then $\tilde{Q}$ has infinite order if and only if it is nonzero in $E_n \otimes \mathbf{F}_\ell$.*

More generally, let χ be a character of $\mathrm{Gal}(H_n/K)$, and let $\lambda|\ell$ denote a prime of $\mathbf{Z}[\chi]$ above ℓ. Write k for the residue field of $\mathbf{Z}[\chi]$ at λ. Then $\tilde{Q}_\chi = \sum \chi(\sigma)\tilde{Q}^\sigma$ has nonzero height if and only if $\tilde{Q}_\chi$ is nonzero in $E(H_n) \otimes k$.

Proof. Clear, because $F_n \otimes \mathbf{F}_\ell = 0$ by our choice of ℓ. Note also that the height pairing is nondegenerate on the free part of $E(H_n)$, and isotropic on the torsion part F_n. □

Preliminary choices

We will prove our main result (Theorem 1.4) by relating the nonvanishing of $\tilde{Q}_\chi$ in $E(H_n) \otimes k$ to the nonvanishing modulo λ of the special value $L(h, \chi, 1)$, where h is a suitably chosen form of level Nq, congruent modulo λ to the original g, and applying our previous results to show that the latter is a unit for almost all χ.

We begin by specifying more precisely the choices of ℓ and q which intervene in this program. It will be convenient in the sequel to write $\chi = \chi_t \chi_w$, and to group together all characters with a fixed tame part χ_t. To make the choices below, we assume that the tame character χ_t is fixed.

6.3 Let the modular form $g = \sum a_n(g) q^n$ be as above. Then, for any prime λ of $\overline{\mathbf{Q}}$, of residue characteristic ℓ, there exists a Galois representation $\rho = \rho_\lambda : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(O)$, where O is a λ-adically complete DVR such that $\mathrm{Tr}(\mathrm{Frob}(q)) = a_q(g) \in O$, for $q \nmid N\ell$. If k denotes the residue field O/λ, then there is a unique semisimple residual representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(k)$ satisfying $\mathrm{Tr}(\mathrm{Frob}(q)) = \overline{a}_q(g) \in k$.

We will choose the primes λ (and ℓ) such that the following conditions are met. To make sense of condition 5 below, we assume that the fields $\mathbf{Q}(\chi_t)$ and $\mathbf{Q}(\mu_{p^\infty})$ are linearly disjoint. This will always be the case if the class number of K is prime to p.

1. The prime number ℓ is relatively prime to $2NDp$.
2. ℓ does not divide the order of the Shimura subgroup, which is by definition the kernel of the natural map $J_0(N) \to J_1(N)$.
3. ℓ does not divide the order of F_∞, where F_∞ is as above.
4. The representation $\overline{\rho}$ is irreducible, and
5. ℓ splits completely in $\mathbf{Q}(\chi_t)$, while remaining inert in $\mathbf{Q}(\mu_{p^\infty})$.

There are clearly infinitely many $\lambda | \ell$ satisfying these conditions.

6.4 Now we want to choose an auxiliary prime q, for the purpose of raising the level. We will select q such that

1. $q \nmid 2NDp\ell$,
2. q is inert in K, and
3. $\overline{\rho}(\mathrm{Frob}(q)) = \overline{\rho}(c)$, where c denotes a complex conjugation.

Note that the third condition implies that $X^2 - a_q X + q \equiv X^2 - 1 \pmod{\lambda}$. In particular, we have $q \equiv -1 \pmod{\ell}$.

Under the above hypotheses, the following theorem of Ribet [Rib84] is fundamental.

THEOREM 6.5 *There exists a modular form $h = \sum b_n(h) q^n$ on $\Gamma_0(Nq)$ such that $a_n \equiv b_n \pmod{\lambda}$, for all $(n, q) = 1$, and such that $b_q \equiv \pm 1 \pmod{\lambda}$.*

Observe that h is of level $M = Nq$, and so $L(h, \chi, s)$ has functional equation with sign $+1$. Thus the results developed in the first part of this paper are applicable. As we have already remarked, our goal is to relate the nonvanishing of $L(h, \chi, 1)$ modulo λ to the indivisibility of classical Heegner points for g. The next section collects the necessary facts about Heegner points on modular curves.

CM points on modular curves

We note at the outset of this discussion that if A is an elliptic curve with complex multiplication by the quadratic field K, then we identify $\mathrm{End}_{\overline{\mathbf{Q}}}(A) \otimes \mathbf{Q}$ with K by fixing an embedding $K \hookrightarrow \overline{\mathbf{Q}}$, and an isomorphism $\mathrm{Lie}(A)_{\overline{\mathbf{Q}}} \cong \overline{\mathbf{Q}}$. Then the natural action of $\mathrm{End}_{\overline{\mathbf{Q}}}(A) \otimes \mathbf{Q}$ on $\mathrm{Lie}_{\overline{\mathbf{Q}}}(A)$ gives a map $\mathrm{End}_{\overline{\mathbf{Q}}}(A) \otimes \mathbf{Q} \to \overline{\mathbf{Q}}$ which identifies $\mathrm{End}_{\overline{\mathbf{Q}}}(A) \otimes \mathbf{Q}$ with K.

6.6 **Enhanced elliptic curves**. Recall that an *enhanced* elliptic curve over a field k is a pair (A, b) where A is an elliptic curve over k and $b \subset A$ is a k-rational subgroup of order N whose points over an algebraic closure of k form a cyclic group. (This terminology is due to Ribet, [Rib90].) There is an evident notion of isomorphism classes of such enhanced elliptic curves. Each enhanced elliptic curve over k is by definition a k-rational point of the modular curve $X_0(N)$.

Now recall the usual Heegner points on $X_0(N)$. Over $\mathbf{C}$, these are pairs $Q = (A, b)$, where A is an elliptic curve with complex multiplication by an order $\mathfrak{o}_c$ of conductor c in K, enhanced with a cyclic subgroup b of order N which is stable under the action of endomorphisms in $\mathfrak{o}_c$. We shall assume throughout that N is prime to c.

Let $\mathfrak{n} \subset \mathfrak{o}_c$ denote the annihilator of b in $\mathfrak{o}_c$. Then b determines and is determined by $\mathfrak{n}$, since $b = A[\mathfrak{n}] \subset A$ is the set of elements killed by $\mathfrak{n}$. Note also that $\mathfrak{o}_c/\mathfrak{n} \cong \mathbf{Z}/N\mathbf{Z}$. We will sometimes write $(A, \mathfrak{n})$ instead of (A, b), and say that the subgroup b is associated to the ideal $\mathfrak{n}$.

In this situation, the theory of complex multiplication states that the point (A, b) on $X_0(N)$ may be defined over the ring class field $K(c)$. There are e_c such Heegner points Q on $X_0(N)$, where e_c is the order of the group $\mathrm{Pic}(\mathfrak{o}_c)$, and the group $\mathrm{Gal}(K(c)/K) \cong \mathrm{Pic}(\mathfrak{o}_c)$ acts simply and transitively on the set of Heegner points.

Let $\mathfrak{Q}$ be a prime of $\overline{\mathbf{Q}}$ whose residue characteristic q is prime to NDc, where D is the discriminant

of K, and such that $\mathfrak{q} = \mathfrak{Q} \cap K$ is inert in K. The curve A admits a model over $K(c)$ with good reduction at $\mathfrak{Q}$, and the reduction $\overline{A}$ of A at $\mathfrak{Q}$ is a supersingular elliptic curve in characteristic q.

According to classical results of Deuring, the supersingular elliptic curves in characteristic q correspond bijectively (via the endomorphism rings) to the set of conjugacy classes of maximal orders in the definite quaternion algebra B ramified only at q and ∞. Thus $\overline{A}$ determines a class $[A]$ (depending on $\mathfrak{Q}$) of maximal orders in B. On the other hand, the reduction $\overline{b}$ of b is a cyclic subgroup of order N in $\overline{A}$. Thus the pair $\overline{Q} = (\overline{A}, \overline{b}) \in X_0(N)(\mathbf{F}_{q^2})$ is an enhanced supersingular elliptic curve in characteristic q.

The following proposition generalizes the classical results of Deuring.

PROPOSITION 6.7 *The enhanced supersingular elliptic curves in characteristic q are in 1-1 correspondence with the right ideal classes of any fixed Eichler order R of level N in B. Equivalently, the enhanced supersingular curves correspond to conjugacy classes of oriented Eichler orders of level N.*

Proof. This is Proposition 3.3 of [Rib90]. The construction of the correspondence will be recalled below. □

6.8 **Ribet's construction**. In this section we will recall how reduction mod $\mathfrak{Q}$ of CM points on $X_0(N)$ produces Heegner points on quaternion algebras, in the sense previously considered in this paper. In other words, if we are given a pair (A, b) where A in an elliptic curve with complex multiplications by $\mathfrak{o}_c$, and b is a cyclic subgroup of order N, we want to construct an oriented Eichler order R of level N, together with an oriented embedding $f : O_c \to R$. Our discussion will follow pp 439-441 of [Rib90]; for an alternative viewpoint, the reader may consult [Cor01].

From now on, we shall assume that the conductor c is a power of p, for a fixed prime p. This will be adequate for our purposes in the rest of this paper. We shall also fix an ideal $\mathfrak{n}$ of norm N in $\mathfrak{o}_K$. Then $\mathfrak{n} \cap \mathfrak{o}_n$ is an ideal of index N in $\mathfrak{o}_n$. If A is a given elliptic curve with complex multiplications by $\mathfrak{o}_n$, for $n \geq 0$, we may view A as being enhanced with the cyclic subgroup $b = A[\mathfrak{n}]$.

So let (A, b) be as above. The reduction (at $\mathfrak{Q}$) of endomorphisms gives an embedding

$$f : \mathfrak{o}_n \to R,$$

where $R \subset \mathrm{End}(\overline{A})$ is the Eichler order of level N given as follows. If we let $t : \overline{A} \to \overline{A}/\overline{b}$ denote the canonical quotient map, then there is a natural inclusion of $\mathrm{End}(\overline{A}/\overline{b})$ into $\mathrm{End}(\overline{A}) \otimes \mathbf{Q} \cong B$ given by $\phi \mapsto t \circ \phi \circ t^{-1}$. Then R is presented as the intersection $\mathrm{End}(\overline{A}) \cap \mathrm{End}(\overline{A}/\overline{b})$. One checks readily that $\mathfrak{o}_n \to \mathrm{End}(\overline{A})$ induces an embedding $\mathfrak{o}_n \to R$.

Note that this prescription allows us to associate to any enhanced supersingular curve $(\overline{A}, \overline{b})$ an Eichler order R of level N. This is the correspondence of Proposition 6.7, but we need to fix the

orientations. In the present situation, this is easy. The fixed ideal $\mathfrak{n}$ chosen at the outset gives a homomorphism $\mathfrak{o}_K \to \mathbf{Z}/N\mathbf{Z}$, which defines local orientations on $\mathfrak{o}_K$ at each (split) prime dividing N. This induces local orientations on each order $\mathfrak{o}_n$. Similarly, an arbitrary choice of local orientation at q on $\mathfrak{o}_K$ leads to an orientation at q on each $\mathfrak{o}_n$. We therefore orient the Eichler order R that we have constructed by requiring that the embedding $\mathfrak{o}_n \to R$ be an oriented embedding.

Note however that the Eichler order R so constructed arises as a subring of the quaternion algebra $\mathrm{End}(E) \otimes \mathbf{Q}$, and that there is no canonical way to compare the Eichler orders associated to different elliptic curves. Thus we fix an enhanced elliptic curve $(A, \mathfrak{n})$ of conductor 1. For any elliptic curve A_0 with CM by $\mathfrak{o}_n$, we choose a a nonzero isogeny $\gamma : A \to A_0$. Then $t \mapsto \gamma^{-1} \circ t \circ \gamma$ induces $\mathrm{End}(A)_0 \to \mathrm{End}A$, and an isomorphism $\mathrm{End}(A)_0 \otimes \mathbf{Q} \to \mathrm{End}(A) \otimes \mathbf{Q}$. If R_0 is the Eichler order associated to A_0 (or $\overline{A}_0$), then this procedure identifies R_0 with an oriented Eichler order of level N inside the quaternion algebra $B = \mathrm{End}(\overline{A}) \otimes \mathbf{Q}$. Owing to the indeterminacy in the choice of γ, the order R_0 is only determined up to conjugacy in $B^\times$.

In summary, given an enhanced elliptic curve $(A, \mathfrak{n})$ where A has complex multiplication by $\mathfrak{o}_n$ and b is associated to a fixed ideal $\mathfrak{n}$ of norm N in $\mathfrak{o}_K$, we have constructed a pair (f, R), where R is an oriented Eichler order in a fixed realization B of the quaternion algebra of discriminant q, and $f : \mathfrak{o}_n \to R$ is an oriented embedding. The pair (f, R) is a Heegner point on B as defined in the first part of this paper.

For completeness, we shall review the construction of Ribet which leads to the proof of Proposition 6.7 above. As explained above, any enhanced elliptic curve $(\overline{A}, \overline{b})$ in characteristic q gives rise to an Eichler order R of level N inside the quaternion algebra $B = \mathrm{End}(\overline{A}) \otimes \mathbf{Q}$. We fix an enhanced elliptic curve $(\overline{A}, \overline{b})$ in characteristic q, together with the associated Eichler order R. Then the set of oriented Eichler orders of level N in $B = \mathrm{End}(\overline{A}) \otimes \mathbf{Q}$ coincides with the double coset space $B^\times \backslash \hat{B} / \hat{\mathbf{Q}}^\times \hat{R}^\times$. As we have already remarked, $B^\times \backslash \hat{B} / \hat{\mathbf{Q}}^\times \hat{R}^\times = B^\times \backslash \hat{B} / \hat{R}^\times$ is isomorphic to the set of right ideal classes of R.

Now let $(\overline{A}_0, \overline{b}_0)$ denote any other enhanced supersingular curve in characteristic q. Write $\mathrm{Hom}_N(\overline{A}, \overline{A}_0)$ for the subset of $\mathrm{Hom}(\overline{A}, \overline{A}_0)$ consisting of homomorphisms that carry $\overline{b}$ to $\overline{b}_0$. Then $\mathrm{Hom}_N(\overline{A}, \overline{A}_0)$ is a locally free right-R module, under composition with endomorphisms of $\overline{A}$. Thus we can associate to the pair $(\overline{A}_o, \overline{b}_0)$ the class in $B^\times \backslash \hat{B} / \hat{R}^\times$ of the locally free right-R-module $\mathrm{Hom}_N(\overline{A}, \overline{A}_0)$. In terms of Eichler orders, we may associate to $(\overline{A}_0, \overline{b}_0)$ the left order of the right ideal $\mathrm{Hom}_N(\overline{A}, \overline{A}_0)$. One checks without difficulty that if $(A, \mathfrak{n})$ is a CM point of conductor p^n on $X_0(N)$ (with a fixed choice of $\mathfrak{n}$), and $P = (f, R)$ is the point on B constructed above, then the class of R in $\mathrm{Cl}(B)$ coincides with the class associated to the enhanced supersingular curve $(\overline{A}, \overline{b})$ by Ribet's construction.

6.9 **Action of the Picard group**. Let A denote an elliptic curve with complex multiplication by $\mathfrak{o}_n$,

enhanced with a cyclic subgroup b, and let $Q = (A, b)$ be the corresponding a CM point on $X_0(N)$. Then we have seen that reduction at $\mathfrak{Q}$ gives rise to a pair $P = (f, R)$, where R is an oriented Eichler order of level N in the quaternion algebra B ramified at q and infinity. Thus P is a Heegner point on B, as in the first part of this paper.

The next lemma verifies that the association $Q \mapsto P$ is compatible with the action of $\mathrm{Pic}(\mathfrak{o}_n)$, but before stating the result, we would also like to fix some notation. Given a point $Q = (A, b)$, we have two distinct notations of reduction, namely we have the geometric point $x = x(Q) = (\overline{A}, \overline{b}) \in X_0(N)(\mathbf{F}_{q^2})$, and the point $P = (f, R)$ on the definite quaternion algebra arising from the supersingular point x. It will be convenient in the sequel to write $\overline{Q}$ to denote the point P, since it will be the point P that is of primary interest, and it will be important to keep track of the dependence of $P = \overline{Q}$ on Q.

Lemma 6.10 *Let $Q = (A, b)$ denote a CM point on $X_0(N)$ as above. Let $P = \overline{Q}$ denote the corresponding point on the definite quaternion algebra B. Then, if $\sigma \in \mathrm{Pic}(O_n)$, we have*

$$\overline{Q^\sigma} = \overline{Q}^\sigma,$$

where σ acts on the left via the Artin map $\mathrm{Pic}(O_n) \to \mathrm{Gal}(K(p^n)/K)$, followed by the Galois action on geometric points, and the action on the right is the one from section 2.2.

Proof. This is [BD97], Lemma 4.2. □

Raising the level

Theorem 6.5 states that there exists a form $h = \sum b_n(h) q^n$ of level Nq, new at q, such that $a_n(g) \equiv b_n(h) \pmod{\lambda}$ (for $(n, q) = 1$, and $b_q(h) = \epsilon = \pm 1$. The precise value of ϵ will not be relevant to our discussion. We let ψ denote the function considered in the first part of this paper, attached to the modular form g. We may now state the theorem that is our target in this section:

Theorem 6.11 *Let χ denote any anticyclotomic character of conductor p^n, with $n \geq 1$. Let Q_n denote a Heegner point on $X_0(N)$ of conductor p^n, and let $\tilde{Q}_n$ denote its image under the quotient map $J_0(N) \to E$. Let P_n denote its reduction modulo $\mathfrak{Q}$, as above. If the number $\sum_\sigma \chi(\sigma)\psi(P_n^\sigma)$ is a λ-adic unit, then the point $\sum_\sigma \chi(\sigma)\tilde{Q}_n^\sigma$ is nonzero in $E(H_n) \otimes k$, and so in $E(H_n) \otimes \mathbf{Q}(\chi)$*

As described in the introduction, the proof of this theorem amounts to finding two different ways of describing the function $\psi : \mathrm{Cl}(B) \to O/\lambda$, one in terms of the modular curve $X_0(N)$, and the other in terms of the Gross curve X of level $M = Nq$. Furthermore, it is clear that this theorem, together with Theorem 1.2, implies Theorem 1.4 of the introduction.

Construction of an unramified cover

6.12 We want to define the Galois cover of $X_0(N)$ which is necessary for our construction. Let $\pi : J_0(N) \to E$ denote the modular parametrization of E. We may assume that the kernel of π is connected, and stable under the Hecke operators, so that there is an induced action of the Hecke algebra on E. We let $\mathfrak{m}$ denote the maximal ideal of $\mathbf{T}$ cut out by the form g modulo λ; it it follows from the fact that $\overline{\rho}$ is irreducible that $E[\mathfrak{m}]$ has dimension two over $k = \mathbf{T}/\mathfrak{m}$. Furthermore, the action of $\mathrm{Frob}(q)$ on $E[\mathfrak{m}]$ is given up to conjugation by the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. We let $V = E[\mathfrak{m}]$, and let $V_\pm$ denote the $\pm$ eigenspace for $\mathrm{Frob}(q)$. Then $V_\pm$ is a finite flat group scheme over $\mathbf{F}_q$, which becomes constant over $\mathbf{F}_{q^2}$.

Now let $E_\pm = E/V_\pm$. Then $E_\pm$ is defined over $\mathbf{F}_q$, since the finite subgroup $V_\pm$ is $\mathbf{F}_q$-stable. Let $E_\pm \to E$ denote the dual isogeny, so that the kernel $W_\pm$ of $E_\pm \to E$ is Cartier dual to $V_\pm$. Note that under our hypotheses, we have $q \equiv -1 \pmod{\ell}$, so that μ_ℓ becomes constant over $\mathbf{F}_{q^2}$; this implies that we have $W_\pm \cong V_\pm$ over $\mathbf{F}_{q^2}$, and that in fact all these group schemes are constant. In particular, the covering map $E_\pm \to E$ is a Galois cover over $\mathbf{F}_{q^2}$, with Galois group $W_\pm \cong k$. *A priori*, this is an isomorphism of additive groups, but, note also that $V_\pm$ is stable under the action of the Hecke algebra, and that the module $W_\pm$ being dual to $V_\pm$, it inherits the structure of a k-module as well.

Now consider the composite $X_0(N) \to J_0(N) \to E$. Pullback of the cover $E_\pm \to E$ gives a cover $X_\pm \to X_0(N)$, which has structural group $W_\pm$, and so is Galois over $\mathbf{F}_{q^2}$.

Let $x \in X_0(N)(\mathbf{F}_{q^2})$. Then the mechanism of the Frobenius substitution (see [Ser59], Ch. VI, §22), gives an element $F(x) \in \mathrm{Gal}(X_\pm / X) \cong W_\pm$. Thus we deduce a map

$$F_\pm : X_0(N)(\mathbf{F}_{q^2}) \to W_\pm.$$

This applies in particular when x is a supersingular point, since, as is well-known, all supersingular points are rational over $\mathbf{F}_{q^2}$. Note that the cover $X_\pm$, being the pullback of an isogeny, depends on the embedding $X_0(N) \to J_0(N)$. We shall follow the standard procedure and take this embedding to be given by $x \mapsto (x - \infty)$. It should be pointed out that the cusp infinity is rational over $\mathbf{F}_q$, and that the fiber over infinity, being the group scheme $W_\pm$, becomes constant over $\mathbf{F}_{q^2}$. It follows from this that the map $F_\pm$ is well-defined on $X_0(N)(\mathbf{F}_{q^2})$.

Fixing an isomorphism $W_\pm \cong k$, writing Σ for the set of supersingular points on $X_0(N)$, and extending $F_\pm$ by linearity, we obtain a morphism

$$F_\pm : \mathbf{Z}[\Sigma] \to k, \tag{15}$$

LEMMA 6.13 *The following statements hold:*

1. *The map $F_\pm$ defined in (15) is nonzero and surjective.*

2. *If $x \in X_0(N)(\mathbf{F}_{q^2})$ is any point, and T_r is a Hecke operator with $q \neq r$, then we have $F_\pm(T_r x) = t_r F_\pm(x)$, where t_r is the image of T_r in $\mathbf{T}/\mathfrak{m}$.*

3. *If ϕ denotes the Frobenius element in $\mathrm{Gal}(\mathbf{F}_{q^2}/\mathbf{F}_q)$, and $x \in X_0(N(\mathbf{F}_{q^2}))$ is any point, then we have $F_\pm(\phi(x)) = \phi(F_\pm(x))$, where $\phi(q)$ acts on $F_\pm(x) \in W_\pm$ via the usual Galois module structure.*

Proof. The first statement follows from a theorem of Ihara. Indeed, Theorem 1 of [Iha75], shows that if $X(N)$ denotes the modular curve corresponding to the full congruence subgroup of level N, then the fundamental group of $X(N)(\mathbf{F}_{q^2})$ is generated by the Frobenius elements of the supersingular points. Thus, if $X' \to X(N)$ is any connected unramified Galois cover over $\mathbf{F}_{q^2}$, then the reciprocity map $\mathbf{Z}[\Sigma(N)] \to \mathrm{Gal}(X'/X(N))$ is nonzero and surjective, where $\Sigma(N)$ denotes the set of supersingular points on $X(N)$. Note that the supersingular points on $X(N)$ are all rational over $\mathbf{F}(q^2)$ and that the natural projection $X(N) \to X_0(N)$ takes $\Sigma(N)$ to Σ.

We let $X' = X'_\pm$ be the pullback to $X(N)$ of $X_\pm \to X_0(N)$, where the cover $X_\pm$ of $X_0(N)$ is as above, and the pullback is taken under the natural projection of $X(N)$ to $X_0(N)$. Then we claim that $X'_\pm$ is connected. Indeed, if this were not the case, then the kernel of $J_0(N) \to J(N)$ would have an element of order ℓ, since $X_\pm$ is a degree ℓ cover of $X_0(N)$. But $J_0(N) \to J(N)$ factors as $J_0(N) \to J_1(N) \to J(N)$, and the latter map is injective since the cusp ∞ is totally ramified in $X(N) \to X_1(N)$. Thus $\ker\{J_0(N) \to J(N)\} = \ker\{J_0(N) \to J_1(N)\}$ is the Shimura subgroup, and we have assumed that ℓ is relatively prime to the order of this subgroup.

Thus $X'_\pm$ is connected, and $\mathbf{Z}[\Sigma(N)] \to \mathrm{Gal}(X'/X(N))$ is nonzero and surjective. But now it also follows from the fact that ℓ is prime to the order of the Shimura subgroup that the cover $X_\pm \to X_0(N)$ is linearly disjoint from $X(N) \to X_0(N)$. Thus $\mathrm{Gal}(X'_\pm/X(N))$ is canonically isomorphic to $\mathrm{Gal}(X_\pm/X_0(N))$. Since $\Sigma(N)$ projects to Σ, and all these points are rational over $\mathbf{F}_{q^2}$, the first statement now follows from the functorial properties of the reciprocity map.

As for the second, select $y \in J_0(N)(\overline{\mathbf{F}}_q)$ such that $\ell y = x$. Then, if $\pi_\pm : E \to E_\pm = E/V_\pm$ is the quotient map, and $\pi_\pm^*$ is the dual, we have $\pi_\pm^* \circ \pi_\pm(y) = \ell y = x$, so that if $z = \pi_\pm(y)$, then $\pi_\pm^*(z) = x$. If $\phi' = \phi^q$ denotes the Frobenius element in $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_{q^2})$, then $z' = \phi'(z)$ also satisfies $\pi_\pm^*(z') = x$, since x is fixed by ϕ'. Thus $z' - z \in \ker(\pi_\pm^*)$, and one checks without difficulty that $F_\pm(x) = z' - z \in W_\pm$. See also [Ser59], Ch. 6, §23.

On the other hand, we also have $\ell T_r y = T_r x$. Since T_r is defined over $\mathbf{F}_q$, we find that

$$\phi'(T_r y) - T_r y = T_r(\phi'(y) - y) \in J_0(N)[\ell].$$

The required statement follows upon applying $\pi_\pm$. Care has to be taken with one point, namely, that the action of $\mathbf{T}$ on $W_\pm$, viewed as a quotient of $J_0(N)[\ell]$, coincides with the one induced by duality from $V_\pm$. But this follows from autoduality of $J_0(N)[\ell]$ under the twisted Weil pairing. (Note that the Atkin-Lehner involution acts as ± 1 on $J_0(N)[\mathfrak{m}]$.)

The final statement may be proved in a similar fashion. Choosing $z \in E_\pm$ such that $\pi_\pm^*(z) = x$, we have $\pi_\pm(\phi(z)) = \phi(x)$, so that

$$\phi(F_\pm(x)) = \phi(\phi'(z) - z) = \phi'(\phi(z)) - \phi(z).$$

□

6.14 Now let $Q = (A, b) \in X_0(N)(H_n)$ denote a Heegner point, as above. Recall our convention that x denotes the geometric point $(\overline{A}, \overline{b}) \in X_0(N)(\mathbf{F}_{q^2})$, and that $\overline{Q}$ denotes the point deduced from x on the quaternion algebra B.

Applying $F_\pm$ to the point x, we obtain $F_\pm(x) = F_\pm(Q) \in W_\pm$. It is clear that if $F_\pm(Q) \neq 0$, then the image of x in $E(\mathbf{F}_{q^2})$ is nonzero in $E(\mathbf{F}_{q^2}) \otimes k$. In view of our choice of ℓ, we find that $\tilde{Q}$ has infinite order in $E(H_n)$. Indeed, the following slightly stronger lemma is obvious:

LEMMA 6.15 *Let $Q = (A, b)$ be as above, and let χ denote any character of $\mathrm{Gal}(H_n/K)$. Then, if $\sum_\sigma \chi(\sigma) F_\pm(Q^\sigma)$ is nonzero in $W_\pm \otimes k(\chi)$, the point $\sum_\sigma \chi(\sigma)\tilde{Q}^\sigma$ is nonzero in $E(H_n) \otimes \mathbf{Q}(\chi)$.*

6.16 To complete the proof of Theorem 6.11, we relate the functions $F_\pm$ to certain functions ψ coming from definite quaternion algebras. Let h be a form of level $M = Nq$, congruent to g, as above. Let X denote the Gross curve of level N, associated to the quaternion algebra B ramified at infinity and q. Let $\mathcal{M}$ denote the group $\mathrm{Pic}(X)$. It follows from Proposition 6.7 that M may be identified with the free $\mathbf{Z}$-module on the set Σ of supersingular points on the modular curve $X_0(N)$. Furthermore, if $\mathbf{T}(M)$ denotes the Hecke algebra of level $M = Nq$ acting on $\mathcal{M} = \mathbf{Z}[\Sigma]$, then one can relate the action of the Hecke operators in $\mathbf{T}(M)$ to those in $\mathbf{T} = \mathbf{T}(N)$ as follows. For clarity, we will write T_r^M or T_r^N to denote the r-th Hecke operator at levels M and N respectively. With these notations, it is known that, if r is prime to q, then the action of T_r^M on $\mathcal{M} \cong \mathbf{Z}[\Sigma]$ is induced from the action of T_r^N acting on $\Sigma(N)$. For a discussion of this, we refer the reader to [Rib90], pp 444-445. On the other hand, one knows ([Rib90], Proposition 3.8) that $T_q(M)$ acts on $\mathbf{Z}[\Sigma(N)]^0$ via the Frobenius automorphism $x \mapsto \phi(x)$ of $\Sigma(N)$, where the superscript 0 denotes the subgroup of divisors of degree zero.

Let $\psi = \psi_h : \mathcal{M} \to O$ denote the homomorphism associated to h, as in §1. If $x \in \mathbf{Z}[\Sigma]^0$, we may view x as an element of $\mathcal{M}$. Then we have $\psi(T_r(x)) = b_r(h)\psi(x)$, for the eigenvalue $b_r(h)$ of $T_r = T_r(M)$ acting on h. Furthermore, we have $\psi(T_q(x)) = \epsilon\psi(x)$, where $b_q(x) = \epsilon = \pm 1$. It

follows from a multiplicity-one theorem of Mazur [Rib90], Theorem 6.4, that, up to unit multiples, there is a *unique* such nonzero homomorphism $\mathcal{M}^0 \to \overline{\mathbf{F}}_\ell$. Choosing the sign $\alpha = \pm$ judiciously, and scaling by a unit if needed, we find, from Lemma 6.13, that the function F_α satisfies the same properties of Hecke invariance, so that we get $F_\alpha = \text{unit} \cdot \psi \pmod{\lambda}$. Theorem 6.11 is now immediate consequence.

References

[BD90] M. Bertolini and H. Darmon, *Kolyvagin's descent and Mordell-Weil groups over ring class fields*, J. Reine Angew. Math. **412** (1990), 63–74.

[BD96] M. Bertolini and H. Darmon, *Heegner points on Mumford-Tate curves*, Invent. Math. **126** (1996), no. 3, 413–456.

[BD97] M. Bertolini and H. Darmon, *A rigid analytic Gross-Zagier formula and arithmetic applications*, Ann. of Math. (2) **146** (1997), no. 1, 111–147, With an appendix by Bas Edixhoven.

[BD98] M. Bertolini and H. Darmon, *Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization*, Invent. Math. **131** (1998), no. 3, 453–491.

[BD99a] M. Bertolini and H. Darmon, *Euler systems and Jochnowitz congruences*, Amer. J. Math. **121** (1999), no. 2, 259–281.

[BD99b] M. Bertolini and H. Darmon, *p-adic periods, p-adic L-functions, and the p-adic uniformization of Shimura curves*, Duke Math. J. **98** (1999), no. 2, 305–334.

[Cor01] C. Cornut, *Mazur's conjecture for Heegner points*, to appear in Inv. Math, 2001.

[DT94] F. Diamond and R. Taylor, *Non-optimal levels of mod ℓ modular representations*, Invent. Math **115** (1994), 435–462.

[FW79] B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), no. 2, 377–395.

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

[Gro87] B. Gross, *Heights and the special values of L-series*, Number Theory (H. Kisilevsky and J. Labute, eds.), CMS Conference Proceedings, vol. 7, Amer. Math. Soc., 1987, pp. 115–189.

[Hid88] H. Hida, *Modules of congruence of Hecke algebras and L-functions associated with cusp forms*, Amer. J. Math. **110** (1988), no. 2, 323–382.

[Hid01] H. Hida, *The mu-invariant of p-adic Hecke l-functions*, available from http://wwww.math.ucla.edu/ hida, 2001.

[Iha75] Y. Ihara, *On modular curves over finite fields*, Discrete subgroups of Lie groups and applications to moduli, Oxford University Press, 1975.

[Joc94] N. Jochnowitz, *A p-adic conjecture about derivatives of L-series*, p-adic monodromy and the Birch-Swinnerton Dyer conjecture (B. Mazur and G. Stevens, eds.), Amer. Math. Soc, 1994.

[Maz84] B. Mazur, *Modular curves and arithmetic*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983), PWN, 1984, pp. 185–211.

[PR88] B. Perrin-Riou, *Fonctions L p-adiques associées à une forme modulaire et à un corps quadratique imaginaire*, J. London Math. Soc. (2) **38** (1988), no. 1, 1–32.

[Rat95] M. Ratner, *Raghunathan's conjectures for Cartesian products of real and p-adic Lie groups*, Duke Math. J. **77** (1995), no. 2, 275–382.

[Rib84] K. A. Ribet, *Congruence relations between modular forms*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983) (Warsaw), PWN, 1984, pp. 503–514.

[Rib90] K. A. Ribet, *On modular representations of* $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.

[Ser59] J.-P. Serre, *Groupes algébriques et corps de classes*, Hermann, 1959.

[Ser80] J.-P. Serre, *Trees*, Springer Verlag, 1980.

[Ste89] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Invent. Math. **98** (1989), 75–106.

[Vat99] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. **98** (1999), no. 2, 397–419.

[Vat01] V. Vatsal, *Uniform distribution of Heegner points*, to appear in Invent. Math., 2001.

[Was78] L. Washington, *The non-p-part of the class number in a cyclotomic* $\mathbf{Z}_p$*-extension*, Invent. Math. **49** (1978), no. 1, 87–97.

[Zha01] S. Zhang, *Gross-Zagier formula for GL_2*, preprint, 2001.