Compositio Math. 141 (2005) 811–846
doi:10.1112/S0010437X0500134X

The Iwasawa theoretic Gross–Zagier theorem

Benjamin Howard

Abstract

We prove Mazur and Rubin's Λ-adic Gross–Zagier conjecture (under some restrictive hypotheses), which relates Heegner points in towers of number fields to the 2-variable p-adic L-function. The result generalizes Perrin-Riou's p-adic Gross–Zagier theorem.

Introduction

Fix forever a rational prime $p > 2$ and embeddings $\mathbb{Q}^{\mathrm{alg}} \hookrightarrow \mathbb{Q}_p^{\mathrm{alg}}$ and $\mathbb{Q}^{\mathrm{alg}} \hookrightarrow \mathbb{C}$. Fix also a normalized cuspidal newform $f \in S_2(\Gamma_0(N), \mathbb{C})$ and an imaginary quadratic field $K/\mathbb{Q}$ of discriminant D and quadratic character ϵ satisfying the Heegner hypothesis that all primes dividing N are split in K. Assume that $(p, DN) = 1$ and that f is *ordinary* at p in the sense that the Fourier coefficient $a_p(f) \in \mathbb{Q}^{\mathrm{alg}}$ has p-adic absolute value 1 at the fixed embedding $\mathbb{Q}^{\mathrm{alg}} \hookrightarrow \mathbb{Q}_p^{\mathrm{alg}}$. We let $\mathcal{B}_0$ be a number field which is large enough to contain all Fourier coefficients of f, denote by $\mathcal{A}_0$ the integer ring of $\mathcal{B}_0$, and denote by $\mathcal{A}$ and $\mathcal{B}$ the closures of $\mathcal{A}_0$ and $\mathcal{B}_0$ in $\mathbb{Q}_p^{\mathrm{alg}}$, respectively. Let H_s be the ring class field of K of conductor p^s and let H_∞ be the union over all s of H_s. We write $\Gamma = 1 + p\mathbb{Z}_p$, and let $\gamma_0 \in \Gamma$ be a topological generator. Using methods of Hida [Hid85], Perrin-Riou [PR87a, PR88] attached to f a 'two-variable' p-adic L-function

$$\mathcal{L}_f \in \mathcal{A}[[\mathrm{Gal}(H_\infty/K) \times \Gamma]] \otimes_{\mathcal{A}} \mathcal{B}$$

which interpolates the special values of twists of the complex L-function of f at $s = 1$. The p-adic L-function may be expanded as a power series in $\gamma_0 - 1$

$$\mathcal{L}_f = \mathcal{L}_{f,0} + \mathcal{L}_{f,1} \cdot (\gamma_0 - 1) + \cdots, \tag{1}$$

with each $\mathcal{L}_{f,k} \in \mathcal{A}[[\mathrm{Gal}(H_\infty/K)]] \otimes_{\mathcal{A}} \mathcal{B}$. The Heegner hypothesis forces the constant term $\mathcal{L}_{f,0}$ to vanish, and the goal of this paper is to relate the linear term $\mathcal{L}_{f,1}$ to the p-adic height pairings of Heegner points in the f-component of the Jacobian $J_0(N)$.

For every nonnegative integer s the Heegner hypothesis guarantees the existence of a Heegner point $h_s \in X_0(N)(\mathbb{C})$ of conductor p^s; that is, a cyclic N-isogeny of elliptic curves $h_s : E_s \to E'_s$ over $\mathbb{C}$ such that both E_s and E'_s have complex multiplication by *exactly* $\mathcal{O}_s = \mathbb{Z} + p^s\mathcal{O}_K$, the order of conductor p^s in K. The family $\{h_s\}$ may be chosen so that for every $s > 1$ there is a commutative diagram

$$\begin{array}{ccc} E_s & \xrightarrow{h_s} & E'_s \\ \downarrow & & \downarrow \\ E_{s-1} & \xrightarrow{h_{s-1}} & E'_{s-1} \end{array}$$

in which the vertical arrows are p-isogenies. The elliptic curve E_{s-1} (respectively E'_{s-1}) is then

Received 19 November 2003, accepted in final form 9 August 2004, published online 21 June 2005.
2000 Mathematics Subject Classification 11G05.
Keywords: Iwasawa theory, Heegner points.
This research was supported by an NSF postdoctoral fellowship.

necessarily the quotient of E_s (respectively E'_s) by its $p\mathcal{O}_{s-1}$-torsion. By the theory of complex multiplication (for example [Cor02, Proposition 1.2]) the curves E_s and E'_s, as well as the isogeny connecting them, can be defined over H_s, and so define a point $h_s \in X_0(N)(H_s)$. One then has the Euler system relations (§ 1.2)

$$T_{p^r}(h_s) = \mathrm{Norm}_{H_{s+r}/H_s}(h_{s+r}) + T_{p^{r-1}}(h_{s-1})$$

if $r, s > 0$, and

$$T_p(h_0) = \begin{cases} u \cdot \mathrm{Norm}_{H_1/H_0}(h_1) + (\sigma_p + \sigma_p^*)h_0 & \text{if } \epsilon(p) = 1 \\ u \cdot \mathrm{Norm}_{H_1/H_0}(h_1) & \text{if } \epsilon(p) = -1 \end{cases}$$

as divisors on $X_0(N)$, where T_{p^r} is the usual Hecke correspondence, $2u = |\mathcal{O}_K^\times|$, and σ_p, $\sigma_p^* \in \mathrm{Gal}(H_0/K)$ are the Frobenius automorphisms of the two primes above p in the case $\epsilon(p) = 1$. Abusing notation, we also denote by h_s the image of h_s in $J_0(N)$ under the usual embedding $X_0(N) \to J_0(N)$ taking the cusp ∞ to the origin.

Let $\mathbf{T}$ be the $\mathbb{Q}$-algebra generated by the action of the Hecke operators T_ℓ with $(\ell, N) = 1$ on $J_0(N)$. The semi-simplicity of $\mathbf{T}$ gives a decomposition of $\mathbf{T} \otimes \mathcal{B}$-modules

$$J_0(N)(H_s) \otimes_{\mathbb{Z}} \mathcal{B} \cong \bigoplus_\beta J(H_s)_\beta$$

where β ranges over $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{alg}}/\mathcal{B})$-orbits of algebra homomorphisms $\beta : \mathbf{T} \to \mathbb{Q}_p^{\mathrm{alg}}$. Each summand is stable under the action of $\mathrm{Gal}(H_s/\mathbb{Q})$, and if $\beta(\mathbf{T}) \subset \mathcal{B}$ then $\mathbf{T}$ acts on $J(H_s)_\beta$ through the character β. The fixed newform f determines one such homomorphism, and we define $h_{s,f}$ to be the projection of h_s onto the associated factor $J(H_s)_f$. Let $\alpha \in \mathcal{A}^\times$ be the unit root of $X^2 - a_p(f)X + p$. As in [BD96], define the *regularized Heegner point* $z_s \in J(H_s)_f$ for $s > 0$ by

$$z_s = \frac{1}{\alpha^s} h_{s,f} - \frac{1}{\alpha^{s+1}} h_{s-1,f}.$$

In the case $s = 0$ we define

$$z_0 = u^{-1} \cdot \begin{cases} \left(1 - \dfrac{\sigma_p}{\alpha}\right)\left(1 - \dfrac{\sigma_p^*}{\alpha}\right) h_{0,f} & \text{if } \epsilon(p) = 1 \\ \left(1 - \dfrac{1}{\alpha^2}\right) h_{0,f} & \text{if } \epsilon(p) = -1. \end{cases}$$

It follows from the Euler system relations that the points z_s are compatible under the norm (trace) maps on $J(H_s)_f$.

The case $s = 0$ of the following theorem is due to Perrin-Riou [PR87a], and has been generalized to higher weight modular forms by Nekovář [Nek95].

Theorem A. *Assume that D is odd and $\neq -3$, and that $\epsilon(p) = 1$. For any character $\eta : \mathrm{Gal}(H_s/K) \to \mathbb{Q}_p^{\mathrm{alg},\times}$*

$$\eta(\kappa_s)\log_p(\gamma_0) \cdot \mathcal{L}_{f,1}(\eta) = \sum_{\sigma \in \mathrm{Gal}(H_s/K)} \eta(\sigma)\langle z_s^\vee, z_s^\sigma \rangle$$

where $\kappa_s \in \mathrm{Gal}(H_s/K)$ is the Artin symbol of $\mathfrak{d}_s = (\sqrt{D}\mathcal{O}_K) \cap \mathcal{O}_s$,

$$\langle\ ,\ \rangle = \langle\ ,\ \rangle_{J_0(N),H_s} : J_0(N)^\vee(H_s) \times J_0(N)(H_s) \to \mathbb{Q}_p$$

is the p-adic height pairing (9) extended $\mathcal{B}$ bilinearly, and $z_s^\vee$ is the image of z_s under the canonical principal polarization of $J_0(N)$ (extended $\mathcal{B}$-linearly on Mordell–Weil groups)

$$J_0(N)(H_s) \otimes \mathcal{B} \cong J_0(N)^\vee(H_s) \otimes \mathcal{B}.$$

Both sides of the stated equality are independent of the choice of γ_0.

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

Remark 0.0.1. The p-adic height pairing $\langle\ ,\ \rangle_{J_0(N),H_s}$ referred to in the theorem is not uniquely determined (see Proposition 3.2.1 and Remark 3.2.2). We emphasize that Theorem A holds for *any* choice of p-adic height pairing $\langle\ ,\ \rangle_{J_0(N),H_s}$ as in (9).

Remark 0.0.2. Nekovář [Nek95] claims that there is a sign error in the statement of [PR87a, Théorème 1.3], but there is no small amount of confusion over Perrin-Riou's normalization of the height pairing. This is primarily due to the change of sign in Remark 3.3.1, which is our reason for maintaining the distinction between $J_0(N)$ and $J_0(N)^\vee$, and between the pairings (9) and (10). It is also possible that [PR87a] uses a different convention for the reciprocity law of class field theory; see § 3.3.

Remark 0.0.3. Theorem A should hold without the stated hypotheses on D and $\epsilon(p)$. We note that the hypothesis $D \neq -3$ is not assumed in [PR87a].

Now suppose that f has rational Fourier coefficients, $\mathcal{B}_0 = \mathbb{Q}$, and E belongs to the isogeny class of (ordinary!) elliptic curves associated to f. Fix a modular parametrization $X_0(N) \xrightarrow{\phi} E$, and let

$$\phi_* : J_0(N) \to E, \quad \phi^* : E^\vee \to J_0(N)^\vee$$

be the Albanese and Picard maps. Extending ϕ_* and ϕ^* to $\mathbb{Q}_p$-linear maps on Mordell–Weil groups, let $y_s = \phi_*(z_s) \in E(H_s) \otimes \mathbb{Z}_p$ and let $y_s^\vee$ be the unique point of $E^\vee(H_s) \otimes \mathbb{Q}_p$ with $\phi^*(y_s^\vee) = z_s^\vee$. The canonical polarization $E \cong E^\vee$ identifies y_s with $\deg(\phi) \cdot y_s^\vee$. The points y_s and $y_s^\vee$ are norm-compatible as s varies (since the z_s are). Define the Heegner L-function $\mathcal{L}_{\mathrm{Heeg}} \in \mathbb{Z}_p[[\mathrm{Gal}(H_\infty/K)]] \otimes \mathbb{Q}_p$ by

$$\mathcal{L}_{\mathrm{Heeg}} = \varprojlim \sum_{\sigma \in \mathrm{Gal}(H_s/K)} \langle y_s^\vee, y_s^\sigma \rangle_{E,H_s} \cdot \sigma$$

where the pairing is the p-adic height pairing of (9) extended $\mathbb{Q}_p$-linearly (and *not* the height pairing of (10); as E is both a curve and an abelian variety, we have reached a notational singularity). Unlike the height pairing of Theorem A, the pairing $\langle\ ,\ \rangle_{E,H_s}$ is canonical. This follows from the ordinarity of E at p and the uniqueness claims of Proposition 3.2.1. *A priori*, $\mathcal{L}_{\mathrm{Heeg}}$ lives in the larger space $\varprojlim \mathbb{Q}_p[[\mathrm{Gal}(H_s/K)]]$, but it is known that the denominators in the height pairing are bounded as s varies (this follows from the construction of [PR87a], although it is not explicitly stated there; note also Proposition 0.0.4 below).

Theorem B. *Under the hypotheses (and notation) of Theorem A,*

$$\kappa \cdot \log_p(\gamma_0) \cdot \mathcal{L}_{f,1} = \mathcal{L}_{\mathrm{Heeg}}$$

in $\mathbb{Z}_p[[\mathrm{Gal}(H_\infty/K)]] \otimes \mathbb{Q}_p$, *where* $\kappa = \varprojlim \kappa_s \in \mathrm{Gal}(H_\infty/K)$.

Theorem B is a (very slightly) strengthened form of a conjecture of Mazur and Rubin [MR02, Conjecture 9]. To make the connection between our theorem and the conjecture of Mazur and Rubin more explicit, first note that the construction of the p-adic height $\langle\ ,\ \rangle_{E,H_s}$ depends on the auxiliary choice of the idèle class character $\rho_{H_s} : \mathbf{A}_{H_s}^\times / H_s^\times \to \Gamma \xrightarrow{\log_p} \mathbb{Z}_p$ defined at the start of § 3.3. Define $\Gamma_{\mathbb{Q}_p} = \Gamma \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and extend $\log_p$ to a $\mathbb{Q}_p$-linear isomorphism $\Gamma_{\mathbb{Q}_p} \cong \mathbb{Q}_p$. Define a pairing

$$\langle\ ,\ \rangle_{E,H_s}^\Gamma : E^\vee(H_s) \times E(H_s) \to \Gamma_{\mathbb{Q}_p}$$

by $\langle\ ,\ \rangle_{E,H_s} = \log_p \circ \langle\ ,\ \rangle_{E,H_s}^\Gamma$ and set

$$\mathcal{L}_{\mathrm{Heeg}}^\Gamma = \varprojlim \sum_{\sigma \in \mathrm{Gal}(H_s/K)} \langle y_s, y_s^\sigma \rangle_{E,H_s}^\Gamma \cdot \sigma \in \mathbb{Z}_p[[\mathrm{Gal}(H_\infty/K)]] \otimes \Gamma_{\mathbb{Q}_p},$$

where we have now identified $E \cong E^\vee$ in the canonical way, so that

$$(1 \otimes \log_p)(\mathcal{L}^{\Gamma}_{\mathrm{Heeg}}) = \deg(\phi) \cdot \mathcal{L}_{\mathrm{Heeg}}.$$

Let I be the kernel of the projection

$$\mathbb{Z}_p[[\mathrm{Gal}(H_\infty/K) \times \Gamma]] \otimes \mathbb{Q}_p \;\to\; \mathbb{Z}_p[[\mathrm{Gal}(H_\infty/K)]] \otimes \mathbb{Q}_p$$

and let $w : \mathbb{Z}_p[[\mathrm{Gal}(H_\infty/K)]] \otimes \Gamma_{\mathbb{Q}_p} \;\to\; I/I^2$ be the isomorphism defined by $w(\lambda \otimes \gamma) = \lambda(\gamma - 1)$. Thus $w(\mathcal{L}^{\Gamma}_{\mathrm{Heeg}}) = \deg(\phi) \log_p(\gamma_0)^{-1} \mathcal{L}_{\mathrm{Heeg}} \cdot (\gamma_0 - 1)$. As $\mathcal{L}_{f,0} = 0$, the p-adic L-function $\mathcal{L}_f$ is contained in I, and Theorem B may be rewritten as

$$\kappa \cdot \mathcal{L}_f = \kappa \cdot \mathcal{L}_{f,1} \cdot (\gamma_0 - 1) = \frac{1}{\log_p(\gamma_0)} \mathcal{L}_{\mathrm{Heeg}} \cdot (\gamma_0 - 1) = \frac{1}{\deg(\phi)} w(\mathcal{L}^{\Gamma}_{\mathrm{Heeg}})$$

in I/I^2.

Now assume the hypotheses of Theorem A, and also that $\mathrm{Gal}(K^{\mathrm{alg}}/K)$ surjects onto the $\mathbb{Z}_p$-module automorphisms of $T_p(E)$ and that p does not divide the class number of K. Let $K_\infty \subset H_\infty$ be the anticyclotomic $\mathbb{Z}_p$-extension of K, and set $K_s = K_\infty \cap H_{s+1}$, so that $[K_s : K] = p^s$. Define $\Lambda_{\mathrm{anti}} = \mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]] \otimes \mathbb{Q}_p$, and

$$\mathcal{S}(K_s, E) = \varprojlim_k \mathrm{Sel}_{p^k}(K_s, E), \quad \mathcal{S}_\infty = (\varprojlim_s \mathcal{S}(K_s, E)) \otimes \mathbb{Q}_p$$
$$X = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(K_\infty, E), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{Q}_p.$$

Let $\tilde{y}_\infty \in \mathcal{S}_\infty$ be the inverse limit of $\tilde{y}_s = \mathrm{Norm}_{H_{s+1}/K_s}(y_{s+1}) \in \mathcal{S}(K_s, E)$, and define the *Heegner submodule* $\mathcal{H} \subset \mathcal{S}_\infty$ to be the Λ_{anti}-submodule generated by $\tilde{y}_\infty$. It follows from work of Cornut and Vatsal [Cor02, Vat02] that $\mathcal{H}$ is a free Λ_{anti}-module of rank one. It is known by work of Bertolini and the author [Ber95, How04] that X is a finitely-generated rank-one Λ_{anti}-module, $\mathcal{S}_\infty$ is free of rank one, and

$$\mathrm{char}(X_{\mathrm{tors}}) \text{ divides } \mathrm{char}(\mathcal{S}_\infty/\mathcal{H}) \cdot \mathrm{char}(\mathcal{S}_\infty/\mathcal{H})^{\iota} \tag{2}$$

where X_{tors} denotes the Λ_{anti}-torsion submodule of X, and $\lambda \mapsto \lambda^\iota$ is the involution of Λ_{anti} which is inversion on group-like elements. Perrin-Riou [PR87b, Conjecture B] has conjectured that the divisibility (2) is an equality.

Proposition 0.0.4 (Perrin-Riou [PR87b, PR91, PR92]). *There is a p-adic height pairing*

$$\mathfrak{h}_s : \mathcal{S}(K_s, E) \times \mathcal{S}(K_s, E) \;\to\; c^{-1}\mathbb{Z}_p$$

whose restriction to the image of the Kummer map $E(K_s) \otimes \mathbb{Z}_p \;\to\; \mathcal{S}(K_s, E)$ agrees with the pairing $\langle\ ,\ \rangle_{E,K_s}$ of (9) after identifying $E \cong E^\vee$ in the canonical way, where $c \in \mathbb{Z}_p$ is independent of s.

There is a Λ_{anti}-adic height pairing $\mathfrak{h}_\infty : \mathcal{S}_\infty \times \mathcal{S}_\infty \;\to\; \Lambda_{\mathrm{anti}}$ defined by

$$\mathfrak{h}_\infty(\varprojlim a_s, \varprojlim b_s) = \varprojlim \sum_{\sigma \in \mathrm{Gal}(K_s/K)} \mathfrak{h}_s(a_s, b_s^\sigma) \cdot \sigma,$$

and we define the Λ_{anti}-adic regulator $\mathcal{R}$ to be the image of this map. If

$$e : \mathbb{Z}_p[[\mathrm{Gal}(H_\infty/K)]] \otimes \mathbb{Q}_p \;\to\; \Lambda_{\mathrm{anti}}$$

is the natural projection, then the norm compatibility of the height pairing (see Remark 3.2.2; in this case the compatibility is *automatic* by the uniqueness claim of Proposition 3.2.1 and the fact that E is ordinary at p) gives

$$e(\mathcal{L}_{\mathrm{Heeg}})\Lambda_{\mathrm{anti}} = \mathfrak{h}_\infty(\tilde{y}_\infty, \tilde{y}_\infty)\Lambda_{\mathrm{anti}} = \mathrm{char}(\mathcal{S}_\infty/\mathcal{H}) \cdot \mathrm{char}(\mathcal{S}_\infty/\mathcal{H})^{\iota} \cdot \mathcal{R}.$$

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

If we assume that $\mathcal{R} \neq 0$, then Theorem B allows us to rewrite the divisibility (2) as

$$\mathrm{char}(X_{\mathrm{tors}}) \text{ divides } \frac{e(\mathcal{L}_{f,1})\Lambda_{\mathrm{anti}}}{\mathcal{R}}, \tag{3}$$

which now has the look and feel of a Λ_{anti}-adic form of the Birch and Swinnerton-Dyer conjecture and no longer makes any mention of Heegner points. It was conjectured by Mazur and Rubin [MR02, Conjecture 6] that $\mathcal{R} = \Lambda_{\mathrm{anti}}$, but those authors have since retracted that conjecture.

Note that the hypothesis on the action of Galois on the p-adic Tate module excludes the case where E has complex multiplication. Results similar to (3) in the so-called exceptional case where E has complex multiplication by K can be found in [AH03].

0.1 Plan of the proof

Enlarging $\mathcal{B}_0$ if needed, we may assume that $\mathcal{A}_0$ contains the Fourier coefficients of all normalized newforms of level dividing N, so that all algebra maps $\mathbf{T} \to \mathbb{Q}^{\mathrm{alg}}$ take values in $\mathcal{B}_0$. Fix $s > 0$ and define, for each integer $0 \leqslant i \leqslant s$, degree 0 divisors on $X_0(N)_{/H_s}$

$$c_i = (h_i) - (0), \quad d_i = (h_i) - (\infty).$$

For any pair $0 \leqslant i, j \leqslant s$ and any $\sigma \in \mathrm{Gal}(H_s/K)$ we define a p-adic modular form

$$F_\sigma^{i,j} = \sum_\beta \langle c_i, d_{j,\beta}^\sigma \rangle f_\beta \ \in S_2(\Gamma_0(N), \mathcal{B}_0) \otimes_{\mathcal{B}_0} \mathcal{B}$$

where the sum is over algebra homomorphisms $\beta : \mathbf{T} \to \mathcal{B}_0$, f_β is the associated normalized primitive (i.e. new of some level dividing N) eigenform, $\langle\ ,\ \rangle = \langle\ ,\ \rangle_{X_0(N),H_s}$ is the p-adic height pairing (10) on degree zero divisors of $X_0(N)_{/H_s}$ (viewed as a pairing on $J_0(N)(H_s)$ and extended $\mathcal{B}$-linearly; by Remark 3.3.1 this is *minus* the pairing of Theorem A) and the β subscript on d_j indicates projection to the component $J(H_s)_\beta$. Define a p-adic cusp form

$$F_\sigma = U^2 F_\sigma^{s,s} - U F_\sigma^{s,s-1} - U F_\sigma^{s-1,s} + F_\sigma^{s-1,s-1} \in S_2(\Gamma_0(Np), \mathcal{B}_0) \otimes_{\mathcal{B}_0} \mathcal{B}$$

where U is the Atkin–Lehner U_p defined by $U(\sum a_m q^m) = \sum a_{mp} q^m$. For $(m, N) = 1$, the mth Fourier coefficient of F_σ is given by the formula (see Proposition 7.0.6)

$$a_m(F_\sigma) = \langle c_s, T_{mp^2}(d_s^\sigma)\rangle - \langle c_s, T_{mp}(d_{s-1}^\sigma)\rangle - \langle c_{s-1}, T_{mp}(d_s^\sigma)\rangle + \langle c_{s-1}, T_m(d_{s-1}^\sigma)\rangle. \tag{4}$$

The pairs of divisors occurring in this expression will not be relatively prime for many values of m, but if we define divisors

$$\mathbf{h}_{s,r} = \mathrm{Norm}_{H_{s+r}/H_s}(h_{s+r}), \quad \mathbf{d}_{s,r} = \mathrm{Norm}_{H_{s+r}/H_s}(d_{s+r})$$

on $X_0(N)$ and write $m = m_0 p^r$ with $(m_0, p) = 1$, then the Euler system relation allow us to rewrite (4) as

$$a_m(F_\sigma) = \langle c_s, T_{m_0}(\mathbf{d}_{s,r+2}^\sigma)\rangle - \langle c_{s-1}, T_{m_0}(\mathbf{d}_{s,r+1}^\sigma)\rangle. \tag{5}$$

The pairs of divisors occurring here are relatively prime: the geometric points of $T_{m_0}(\mathbf{h}_{s,r})$ represent elliptic curves with complex multiplication (CM) by an order $\mathcal{O}$ for which $\mathrm{ord}_p(\mathrm{cond}(\mathcal{O})) = r + s$. Working with these divisors allows us to avoid the 'intersection theory with tangent vectors' used by Gross–Zagier to deal with divisors having common support.

In § 2 we recall some p-adic analytic results of Hida and Perrin-Riou. In particular, we recall the construction of a p-adic modular form $G_\sigma \in M_2(\Gamma_0(Np^\infty), \mathcal{A})$ (a space defined at the beginning of § 2) for each $\sigma \in \mathrm{Gal}(H_s/K)$, with the property that

$$\log_p(\gamma_0) \cdot \mathcal{L}_{f,1}(\eta) = \sum_{\sigma \in \mathrm{Gal}(H_s/K)} \eta(\sigma) L_f(G_\sigma)$$

for every character η of $\mathrm{Gal}(H_s/K)$. Here L_f is a linear functional

$$L_f : M_2(\Gamma_0(Np^\infty), \mathcal{A}) \rightarrow \mathcal{B}$$

which plays the Hida-theoretic role of taking the Petersson inner product with f.

Perrin-Riou gives an explicit formula for the Fourier coefficient $a_m(G_\sigma)$ when p divides m (Proposition 2.0.5), and in §§ 4, 5, and 6 we adapt the methods of Gross–Zagier and Perrin-Riou to compute (to the extent necessary) the Fourier coefficients of F_σ. More precisely, each Fourier coefficient has a decomposition over the finite places of H_s, $a_m(F_\sigma) = \sum_v a_m(F_\sigma)_v$, arising from the decomposition of the p-adic heights in (5) into local p-adic Néron symbols on $X_0(N)_{/H_{s,v}}$. For v lying above a rational prime $\neq p$ which splits in K, $a_m(F_\sigma)_v = 0$ (Proposition 4.0.8). For v above a nonsplit rational prime $\ell \neq p$ we derive an explicit formula (Proposition 5.4.1) for $\sum_{v|\ell} a_m(F_\sigma)_v$ similar to formulas of Gross–Zagier. For $v \mid p$ we can offer no explicit formula for $a_m(F_\sigma)_v$, instead we show that the contribution of $a_m(F_\sigma)_p$ to $a_m(F_\sigma)$ is killed by the operator L_f (Proposition 6.2.2). This is where we must impose the condition $\epsilon(p) = 1$, although Proposition 6.2.2 should also hold when $\epsilon(p) = -1$. Comparing these calculations with the Fourier coefficients of G_σ, we conclude that

$$L_f(U^{2s}(1 - U^2)G_{\sigma\kappa}) = L_f(F_\sigma),$$

and Theorems A and B follow easily (see § 7 for the details).

0.2 Notation and conventions

The data K, p, N, D, f, $\mathcal{A}_0$, and $\{h_s\}$ are fixed throughout. We continue to assume, as in § 0.1, that $\mathcal{A}_0$ contains the Fourier coefficients of all normalized primitive forms of level N. We typically do *not* assume that D is odd or $\neq -3, -4$, or that $\epsilon(p) = 1$, unless explicitly stated otherwise. The parity assumption on D is needed only for the results of Perrin-Riou cited in § 2. The condition $\epsilon(p) = 1$ and $D \neq -3, -4$ is used in the calculation of local Néron symbols above p in § 6.

If M is any $\mathbb{Z}$-module of finite type and r is a rational prime we set $M_r = M \otimes_{\mathbb{Z}} \mathbb{Z}_r$. For any integer n, any order $\mathcal{O} \subset K$, and any proper fractional $\mathcal{O}$-ideal $\mathfrak{a}$, we denote by $r_{\mathfrak{a}}(n)$ the number of proper, integral $\mathcal{O}$-ideals of norm n whose class in $\mathrm{Pic}(\mathcal{O})$ agrees with that of $\mathfrak{a}$. The order $\mathcal{O}$ will usually be clear from the context. If there is any ambiguity we will write $r_{\mathfrak{a}\mathcal{O}}(n)$. Since complex conjugation acts by inversion on $\mathrm{Pic}(\mathcal{O})$, $r_{\mathfrak{a}}(n) = r_{\mathfrak{a}^{-1}}(n)$. We define $R_{\mathfrak{a}}(n)$ to be the number of proper, integral $\mathcal{O}$-ideals of norm n in the $\mathcal{O}$-genus of $\mathfrak{a}$; that is, such that the image in $\mathrm{Pic}(\mathcal{O})/\mathrm{Pic}(\mathcal{O})^2$ agrees with the image of $\mathfrak{a}$. For any integer k we set

$$\delta(k) = 2^{\#\{\text{prime divisors of } (k,D)\}}.$$

The reciprocity map of class field theory is always normalized in the arithmetic fashion.

1. Preliminaries on elliptic curves

1.1 CM points, Heegner diagrams, and Serre's construction

Let S be an $\mathcal{O}_K$-scheme and let $\mathcal{O} = \mathcal{O}[c] \subset \mathcal{O}_K$ be the order of conductor c. Assume $(c, N) = 1$. An elliptic curve $E \rightarrow S$ is said to have CM by $\mathcal{O}$ if there is an embedding $\mathcal{O} \hookrightarrow \mathrm{End}_S(E)$. We always assume that such an embedding is normalized, in the sense that the action of $\mathcal{O}$ on the pull-back of the tangent sheaf of E by the identity section agrees with the action given by viewing the structure sheaf of S as a sheaf of $\mathcal{O}$-algebras. We say that $\mathcal{O}$ is the CM-order of E, or that E has CM by exactly $\mathcal{O}$, if this action does not extend to any larger order. A *Heegner diagram* of conductor c over S, h, is an $\mathcal{O}$-linear cyclic N-isogeny of elliptic curves $h : E \rightarrow E'$ over S, such that E and E' both have CM by exactly $\mathcal{O}$. An isogeny of Heegner diagrams means an isogeny of the underlying

$\Gamma_0(N)$-structure; i.e. a commutative diagram

$$\begin{array}{ccc} E_0 & \xrightarrow{h_0} & E_0' \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ E_1 & \xrightarrow{h_1} & E_1' \end{array}$$

in which the vertical arrows are isogenies of elliptic curves over S, and the map f takes the scheme-theoretic kernel of h_0 isomorphically to the scheme-theoretic kernel of h_1. The degree of such an isogeny is defined to be the degree of f, which is also the degree of f'. Any Heegner diagram h over S gives rise to an S-valued point of $X_0(N)_{/\mathbb{Z}}$, which we also denote by h. Since $X_0(N)$ is not a fine moduli space, Heegner diagrams which are not isomorphic over S may give rise to the same S-valued point on $X_0(N)$.

If E is an elliptic curve over S with CM by $\mathcal{O}$ and $\mathfrak{a}$ is a proper fractional $\mathcal{O}$-ideal, a theorem of Serre [Con04, Theorem 7.2] guarantees that the functor from S-schemes to $\mathcal{O}$-modules $T \mapsto E(T) \otimes_{\mathcal{O}} \mathfrak{a}$ is represented by an elliptic curve which we denote by $E \otimes_{\mathcal{O}} \mathfrak{a}$. Define $E^{\mathfrak{a}} = E \otimes_{\mathcal{O}} \mathfrak{a}^{-1}$. As in [Con04, Corollary 7.11], this construction extends to Heegner diagrams, and so to any Heegner diagram $h : E \to E'$ of conductor c over S and any $\mathfrak{a}$ as above, we obtain a new Heegner diagram

$$h^{\mathfrak{a}} : E^{\mathfrak{a}} \to E'^{\mathfrak{a}}.$$

If $S = \mathrm{Spec}(\mathbb{C})$ and E is an elliptic curve over S with CM by exactly $\mathcal{O}$, then $E(\mathbb{C}) \cong \mathbb{C}/\mathfrak{b}$ for some proper fractional $\mathcal{O}$-ideal $\mathfrak{b}$, and we have an analytic isomorphism $E^{\mathfrak{a}}(\mathbb{C}) \cong \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{b}$. By the Main Theorem of Complex Multiplication, the right-hand side is analytically isomorphic to $E^{\sigma}(\mathbb{C})$ for any $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$ whose restriction to $H[c]$ (the ring class field of conductor c) agrees with $\mathfrak{a}$ under the Artin map $\mathrm{Pic}(\mathcal{O}) \cong \mathrm{Gal}(H[c]/K)$. In particular, E has a model over $H[c]$, E^{σ} and $E^{\mathfrak{a}}$ are isomorphic over $\mathbb{C}$, and $\mathrm{Gal}(H[c]/K)$ acts transitively on the $\mathbb{C}$-isomorphism classes of elliptic curves over $H[c]$ with CM by exactly $\mathcal{O}$. Similarly all Heegner diagrams over $\mathbb{C}$ of conductor c have models over the ring class field of conductor c. If h is a Heegner diagram of conductor c defined over $H[c]$, we define the *orientation* of h to be the annihilator in $\mathcal{O}$ of the kernel of $h : E(\mathbb{C}) \to E'(\mathbb{C})$. It is an ideal $\mathcal{N}$ of $\mathcal{O}$ such that $\mathcal{O}/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Then $\mathrm{Gal}(H[c]/K)$ acts transitively on the $\mathbb{C}$-isomorphism classes of conductor c Heegner points with a given orientation.

1.2 Hecke action on CM points

Let $\mathfrak{L}$ denote the set of lattices in K, modulo multiplication by $K^{\times}$. The $K^{\times}$-class of a lattice L will be denoted $[L]$. For any $[L] \in \mathfrak{L}$ we define the conductor of $[L]$ to be the conductor of the left order of L; that is, the conductor of the order $\mathcal{O}(L) = \{\alpha \in K \mid \alpha L \subset L\}$. Every lattice of conductor c is represented uniquely (up to $K^{\times}$ action) by an element of $\mathrm{Pic}(\mathcal{O})$, where $\mathcal{O} \subset K$ is the order of conductor c.

We have the usual action of Hecke operators $\{T_m\}$ on formal sums of classes in $\mathfrak{L}$, which we wish to make explicit. The following lemma is an elementary exercise.

Lemma 1.2.1. *Suppose we are given orders $\mathcal{O}$ and $\mathcal{O}'$ of K of conductors c and d, respectively, and a proper fractional $\mathcal{O}$-ideal $\mathfrak{c}$ (respectively $\mathcal{O}'$-ideal $\mathfrak{d}$). If $c \mid d$ then the multiplicity of $[\mathfrak{c}]$ in the formal sum $T_m[\mathfrak{d}]$ is equal to $r_{\mathfrak{c}\mathfrak{d}^{-1}\mathcal{O}}(mc/d)$. If instead $d \mid c$, then the multiplicity of $[\mathfrak{c}]$ in $T_m[\mathfrak{d}]$ is given by $|\mathcal{O}'^{\times}||\mathcal{O}^{\times}|^{-1} r_{\mathfrak{c}\mathfrak{d}^{-1}\mathcal{O}'}(md/c)$.*

Lemma 1.2.2 (Euler system relations). *With notation as in the introduction and $2u = |\mathcal{O}_K^{\times}|$,*

$$T_{p^r}(h_s) = \mathrm{Norm}_{H_{s+r}/H_s}(h_{s+r}) + T_{p^{r-1}}(h_{s-1})$$

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

if $r, s > 0$, *and*

$$T_p(h_0) = \begin{cases} u \cdot \mathrm{Norm}_{H_1/H_0}(h_1) + (\sigma_p + \sigma_p^*)h_0 & \text{if } \epsilon(p) = 1 \\ u \cdot \mathrm{Norm}_{H_1/H_0}(h_1) & \text{if } \epsilon(p) = -1. \end{cases}$$

Proof. We give a brief sketch of the proof of the first relation. Let $\mathfrak{d}$ be a proper $\mathcal{O}_{s+r}$-ideal such that $\mathbb{C}/\mathfrak{d} \cong E_{s+r}(\mathbb{C})$, and for any $0 \leqslant t \leqslant s+r$, set $\mathfrak{d}_t = \mathfrak{d}\mathcal{O}_t$, so that $E_t(\mathbb{C}) \cong \mathbb{C}/\mathfrak{d}_t$. By the theory of complex multiplication, the complex elliptic curves underlying the $\Gamma_0(N)$-structures appearing in the divisor $\mathrm{Norm}_{H_{s+r}/H_s}(h_{s+r})$ are exactly the complex tori of the form $\mathbb{C}/\mathfrak{d}'$ where $\mathfrak{d}'$ is a proper $\mathcal{O}_{s+t}$-ideal satisfying $\mathfrak{d}'\mathcal{O}_s = \mathfrak{d}_s$. Using Lemma 1.2.1, such a $\mathfrak{d}'$ occurs exactly once in the formal sum $T_{p^r}[\mathfrak{d}_s]$, and does not occur in $T_{p^{r-1}}[\mathfrak{d}_{s-1}]$. As the formal sum of lattices $T_{p^r}[\mathfrak{d}_s] - T_{p^{r-1}}[\mathfrak{d}_{s-1}]$ has degree p^r, it must be exactly the formal sum of $[\mathfrak{d}']$ with $\mathfrak{d}'$ as above. □

1.3 The Serre–Tate theorem

We recall the Serre–Tate theory of deformations of elliptic curves. More detail can be found in [Con04, § 3] and [Gor02, ch. 6]. Let k be a field of nonzero characteristic ℓ and define $\mathcal{C}_k$ to be the category of local Artinian algebras $(R, \mathfrak{m}_R)$ with residue field k, together with a chosen isomorphism $R/\mathfrak{m}_R \cong k$, with morphisms given by local algebra maps inducing the identity on k. Given an elliptic curve $E \to \mathrm{Spec}(k)$, and some $R \in \mathcal{C}_k$, we define a *deformation* of E to R to be an elliptic curve $E_R \to \mathrm{Spec}(R)$ together with an isomorphism between the closed fiber of E_R and E. Similarly, we may define the notion of a deformation of the ℓ-divisible group of an elliptic curve over k. For $(R, \mathfrak{m}_R)$ an object of $\mathcal{C}_k$, let DEF_R denote the category of pairs (E, G) where E is an elliptic curve over k and G is a deformation to R of the ℓ-divisible group of E. A morphism from (E, G) to (E', G') is a pair (f, ϕ) where $f : E \to E'$ is a morphism of elliptic curves over $\mathrm{Spec}(k)$ and $\phi : G \to G'$ is a map of ℓ-divisible groups such that the base change of ϕ to the closed fiber is the map on ℓ-divisible groups over $\mathrm{Spec}(k)$ induced by f.

Theorem 1.3.1 (Serre–Tate). *For any object* $(R, \mathfrak{m}_R)$ *of* $\mathcal{C}_k$, *the functor from elliptic curves over* R *to* DEF_R *which sends* E *to the pair* $(E \times_R k, E[\ell^\infty])$ *is an equivalence of categories, where* $E[\ell^\infty]$ *denotes the* ℓ*-divisible group of* E.

Now assume that k is algebraically closed and fix an ordinary elliptic curve E over k. We have $E[\ell^\infty] \cong \mu_{\ell^\infty} \oplus \mathbb{Q}_\ell/\mathbb{Z}_\ell$ as ℓ-divisible groups over k. For any $R \in \mathcal{C}_R$ there is a distinguished deformation of the ℓ-divisible group of E to an ℓ-divisible group over R, namely the deformation $\mu_{\ell^\infty} \oplus \mathbb{Q}_\ell/\mathbb{Z}_\ell$. Applying the Serre–Tate theorem, we obtain an elliptic curve over R called the *Serre–Tate canonical lift* of E to R.

As explained in [Con04, § 3], a theorem of Grothendieck allows one to replace 'local Artinian' by 'complete local Noetherian' in the definition of $\mathcal{C}_k$, and the discussion above holds verbatim.

2. The p-adic L-function

In this section we quickly recall the essential properties of Hida's p-adic L-function $\mathcal{L}_f$ and Perrin-Riou's calculation of its linear term. We refer the reader to [Hid85, Nek95, PR87a] for more detailed treatments. Assume that D is odd. Recall that $\mathcal{A}_0 \subset \mathbb{Q}^{\mathrm{alg}}$ is the ring of integers of a number field with closure $\mathcal{A}$ in $\mathbb{Q}_p^{\mathrm{alg}}$, $\mathcal{B}$ is the fraction field of $\mathcal{A}$, and $\alpha \in \mathcal{A}^\times$ is the unit root of $X^2 - a_p(f)X + p$.

Set

$$M_2(\Gamma_0(Np^k), \mathcal{A}) = M_2(\Gamma_0(Np^k), \mathcal{A}_0) \otimes_{\mathcal{A}_0} \mathcal{A}$$

and let $M_2(\Gamma_0(Np^\infty), \mathcal{A})$ be the completion of $\bigcup_k M_2(\Gamma_0(Np^k), \mathcal{A})$ with respect to the p-adic supremum norm on Fourier coefficients. To any $s \geqslant 0$, $\sigma \in \mathrm{Gal}(H_s/K)$, and integer C prime to Dp, Perrin-Riou [PR87a, § 2.2.3] associates a measure Φ_σ^C on $\mathbb{Z}_p^\times$ with values in the space $M_2(\Gamma_0(Np^\infty), \mathcal{A})$. These are compatible as s and σ vary in the following sense: there is a measure Φ^C

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

on $\mathrm{Gal}(H_\infty/K)\times\mathbb{Z}_p^\times$ with values in $M_2(\Gamma_0(Np^\infty),\mathcal{A})$ such that for any continuous characters

$$\eta : \mathrm{Gal}(H_\infty/K) \to \mathbb{Q}_p^{\mathrm{alg},\times}, \quad \psi : \mathbb{Z}_p^\times \to \mathbb{Q}_p^{\mathrm{alg},\times}$$

such that η factors through $\mathrm{Gal}(H_s/K)$ we have the relation

$$\int_{\mathrm{Gal}(H_\infty/K)\times\mathbb{Z}_p^\times} \eta\psi\, d\Phi^C = \sum_{\sigma\in\mathrm{Gal}(H_s/K)} \eta(\sigma)\int_{\mathbb{Z}_p^\times}\psi\, d\Phi_\sigma^C$$

in $M_2(\Gamma_0(Np^\infty),\mathcal{A})\otimes_{\mathcal{A}}\mathbb{Q}_p^{\mathrm{alg}}$.

Use the notation $\tilde{T}_\ell$ to denote Hecke operators acting on modular forms of level $\Gamma_0(Np^\infty)$, to distinguish them from the operators on level $\Gamma_0(N)$. Define Hida's ordinary projector [Hid93, § 7.2]

$$e^{\mathrm{ord}} : M_2(\Gamma_0(Np^\infty),\mathcal{A}) \to M_2(\Gamma_0(Np),\mathcal{A})$$

by $e^{\mathrm{ord}}(g)=\lim_{k\to\infty}U^{k!}(g)$, where $U=\tilde{T}_p$ is given by $U(\sum a_nq^n)=\sum a_{np}q^n$ and the limit is with respect to the supremum norm on Fourier coefficients. Define modular forms of level $\Gamma_0(Np)$ by

$$f_0(z)=f(z)-\frac{p}{\alpha}f(pz), \quad f_1(z)=f(z)-\alpha f(pz).$$

These are eigenforms for *all* Hecke operators $\tilde{T}_\ell$, and satisfy $a_\ell(f_0)=a_\ell(f)=a_\ell(f_1)$ if $\ell\neq p$, and $a_p(f_0)=\alpha$, $a_p(f_1)=p/\alpha$. The $\mathcal{B}$-algebra generated by the Hecke operators $\tilde{T}_\ell$ with $(\ell,Np)=1$ acting on $M_2(\Gamma_0(Np),\mathcal{A})\otimes_{\mathcal{A}}\mathcal{B}$ is semi-simple, and so contains an idempotent e_f such that $e_f\circ\tilde{T}_\ell = a_\ell(f)e_f$. By [Hid85, § 4] there is an idempotent e_{f_0} in the algebra generated by *all* Hecke operators $\tilde{T}_\ell$, such that $e_{f_0}\circ\tilde{T}_\ell=a_\ell(f_0)e_{f_0}$ for every ℓ. As operators on modular forms, $e_{f_0}=e_{f_0}e_f$. Define a linear functional

$$l_f : M_2(\Gamma_0(Np^\infty),\mathcal{A})\otimes_{\mathcal{A}}\mathcal{B} \to \mathcal{B}$$

by $l_f(g)=a_1(e_{f_0}e^{\mathrm{ord}}g)$, and set $L_f=(1-p/\alpha^2)(1-1/\alpha^2)l_f$ (this is denoted $\tilde{L}_{f_0}$ in [PR87a]).

Lemma 2.0.2. *The linear functional $L_f : M_2(\Gamma_0(Np^\infty),\mathcal{A})\otimes_{\mathcal{A}}\mathcal{B} \to \mathcal{B}$ satisfies:*

(a) $L_f = L_f\circ e^{\mathrm{ord}}$;

(b) $L_f(f)=1-1/\alpha^2$;

(c) *if $g\in M_2(\Gamma_0(Np^\infty),\mathcal{A})$ is such that $a_m(g)=0$ for all $(m,N)=1$, then $L_f(g)=0$;*

(d) *for any positive integer m, $L_f\circ\tilde{T}_m=a_m(f_0)L_f$; in particular, $L_f\circ U=\alpha L_f$.*

Proof. The first claim is trivial, since $e^{\mathrm{ord}}\circ e^{\mathrm{ord}}=e^{\mathrm{ord}}$. The second follows from $l_f(f_0)=1$, $l_f(f_1)=0$. If g satisfies $a_m(g)=0$ for all $(m,N)=1$, then so does $e_fe^{\mathrm{ord}}g$, so we may assume that g has level $\Gamma_0(Np)$ and that $\tilde{T}_\ell g=a_\ell(f)g$ for $(\ell,Np)=1$. By Atkin–Lehner theory, g is a linear combination of f_0 and f_1. Since $a_1(g)=0$, g must be a scalar multiple of f_0-f_1. But $a_p(f_0-f_1)\neq 0$, so this scalar must be 0. The final claim follows from $e_{f_0}\circ\tilde{T}_m=a_m(f_0)e_{f_0}$. ∎

Remark 2.0.3. Contrary to the proof of [Nek95, Proposition II.5.10], the weaker hypothesis that $a_m(g)=0$ for all $(m,Np)=1$ is not sufficient to conclude that $L_f(g)=0$. The modular form $g=f_0-f_1$ provides a counterexample.

Whenever ψ is a continuous character of Γ, we extend ψ to a character of $\mathbb{Z}_p^\times$ using the usual projection $\langle\ \rangle : \mathbb{Z}_p^\times \to \Gamma$. We now define the p-adic L-function $\mathcal{L}_f$ of the introduction (compare [PR87a, Définition 2.4], but note that Perrin-Riou's $\psi(C)=\psi(\mathrm{Frob}_{C\mathcal{O}_K})$ is our $\psi(C)^2$). For any continuous character $\eta\cdot\psi$ of $\mathrm{Gal}(H_\infty/K)\times\Gamma$, set

$$\mathcal{L}_f(\eta,\psi)=\frac{1}{1-C\epsilon(C)\psi(C)^{-2}}\cdot L_f\left(\int_{\mathrm{Gal}(H_\infty/K)\times\mathbb{Z}_p^\times}\eta\cdot\psi\, d\Phi^C\right),$$

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

where C is chosen so that $(1-C\epsilon(C)\langle C\rangle^{-2}) \in \mathbb{Z}_p[[\Gamma]]^\times$. The resulting $\mathcal{L}_f \in \mathcal{A}[[\mathrm{Gal}(H_\infty/K)\times\Gamma]]\otimes_{\mathcal{A}}\mathcal{B}$ does not depend on the choice of C. Any finite-order character $\eta\cdot\psi$ of $\mathrm{Gal}(H_\infty/K)\times\Gamma$ determines a character

$$\chi(\mathfrak{b}) = \eta(\mathrm{Frob}_{\mathfrak{b}})\cdot\psi(\mathbf{N}(\mathfrak{b}))$$

on ideals of $\mathcal{O}_K$ prime to p, and there is an interpolation formula [PR87a, Théorème 1.1] relating $\mathcal{L}_f(\eta,\psi)$ to $L(f,\bar\chi,1)$, where $L(f,\bar\chi,s)$ is the Rankin product of the L-function of f and the L-function of the theta series associated to $\bar\chi$.

Proposition 2.0.4. *Let* $\mathbf{1}$ *denote the trivial character of* Γ. *Then* $\mathcal{L}_f(\eta,\mathbf{1})=0$ *for all continuous characters* η *of* $\mathrm{Gal}(H_\infty/K)$. *Furthermore, in the notation of (1),* $\mathcal{L}_{f,0}=0$ *and*

$$\log_p(\gamma_0)\cdot\mathcal{L}_{f,1}(\eta) = \sum_{\sigma\in\mathrm{Gal}(H_s/K)} \eta(\sigma)L_f(G_\sigma)$$

for every character η *of* $\mathrm{Gal}(H_s/K)$, *where* $G_\sigma\in M_2(\Gamma_0(Np^\infty),\mathcal{A})$ *is defined by*

$$G_\sigma = \frac{1}{1-C\epsilon(C)}\cdot\int_{\mathbb{Z}_p^\times}\log_p\ d\Phi_\sigma^C.$$

Proof. Fix an integer $s>0$. For each $\sigma\in\mathrm{Gal}(H_s/K)$ define

$$\mathcal{L}^\sigma(\psi) = \frac{1}{1-C\epsilon(C)\psi(C)^{-2}}\cdot\int_{\mathbb{Z}_p^\times}\psi\ d\Phi_\sigma^C \in M_2(\Gamma_0(Np^\infty),\mathcal{A}),$$

a function on continuous characters ψ of Γ with the property that

$$\mathcal{L}_f(\eta,\psi) = \sum_{\sigma\in\mathrm{Gal}(H_s/K)}\eta(\sigma)L_f(\mathcal{L}^\sigma(\psi))$$

for any ψ and any character η of $\mathrm{Gal}(H_s/K)$. By [PR87a, Remarque 3.19] $a_m(\mathcal{L}^\sigma(\mathbf{1}))=0$ whenever $p\mid m$, and so $U\mathcal{L}^\sigma(\mathbf{1})=0$. Lemma 2.0.2(d) now implies $L_f(\mathcal{L}^\sigma(\mathbf{1}))=0$. Since s and η were arbitrary, we deduce $\mathcal{L}_f(\eta,\mathbf{1})=0$ for all finite order η, hence for all continuous η (since $\mathcal{L}_f(\ ,\mathbf{1})\in\mathcal{A}[[\mathrm{Gal}(H_\infty/K)]]\otimes_{\mathcal{A}}\mathcal{B}$). This is equivalent to $\mathcal{L}_{f,0}=0$. Finally, recall that $\langle\ \rangle$ denotes the projection $\mathbb{Z}_p^\times\to\Gamma$ and compute

$$\begin{aligned}\lim_{t\to0}\frac{\mathcal{L}_f(\eta,\langle\ \rangle^t)}{t} &= \sum_{\sigma\in\mathrm{Gal}(H_s/K)}\frac{d}{dt}\left[\frac{\eta(\sigma)}{1-C\epsilon(C)\langle C\rangle^{-2t}}\cdot L_f\left(\int_{\mathbb{Z}_p^\times}\langle x\rangle^t\,d\Phi_\sigma^C(x)\right)\right]_{t=0}\\ &= \sum_{\sigma\in\mathrm{Gal}(H_s/K)}\frac{\eta(\sigma)}{1-C\epsilon(C)}\cdot\frac{d}{dt}\left[L_f\left(\int_{\mathbb{Z}_p^\times}\langle x\rangle^t\,d\Phi_\sigma^C(x)\right)\right]_{t=0}\end{aligned}$$

where in the second equality we have used the fact, proved above, that $L_f(\int_{\mathbb{Z}_p^\times}\mathbf{1}\,d\Phi_\sigma^C)=0$. Differentiating under the integral and using $\log_p(\gamma_0)\mathcal{L}_{f,1}(\eta)=\lim_{t\to0}(1/t)\mathcal{L}_f(\eta,\langle\ \rangle^t)$ proves the claim. □

Fix $s\geqslant 0$ and $\sigma\in\mathrm{Gal}(H_s/K)$. Choose a proper integral $\mathcal{O}_s$-ideal, $\mathfrak{a}$, such that the class of $\mathfrak{a}$ in $\mathrm{Pic}(\mathcal{O}_s)$ corresponds to σ under the Artin symbol. For any positive integer n prime to p and any positive divisor $d\mid n$, define

$$\epsilon_{\mathfrak{a}}(n,d) = \begin{cases}\left(\dfrac{D_1}{d}\right)\left(\dfrac{D_2}{-Nn/d}\right)\chi_{D_1,D_2}(\mathfrak{a}\mathcal{O}_K) & \text{if }\ \gcd(d,n/d,D)=1\\ 0 & \text{otherwise}\end{cases}$$

where $D=D_1D_2$ is the factorization into fundamental discriminants with $(d,D)=|D_2|$ and χ_{D_1,D_2} is the associated genus character. That is, the quadratic character of $\mathrm{Pic}(\mathcal{O}_K)$ associated to the extension $K(\sqrt{D_1}) = K(\sqrt{D_2})$. Set

$$\sigma'_{\mathfrak{a}}(n) = \sum_{\substack{d|n \\ d>0}} \epsilon_{\mathfrak{a}}(n,d)\log_p(n/d^2).$$

Proposition 2.0.5 (Perrin-Riou). *For any positive integer m divisible by p, the mth Fourier coefficient of G_σ is given by*

$$a_m(G_\sigma) = -\sum_{\substack{n>0 \\ (n,p)=1}} r_{\mathfrak{a}\mathfrak{d}_s}(m|D| - nN)\sigma'_{\mathfrak{a}}(n)$$

where $\mathfrak{d}_s = (\sqrt{D}\mathcal{O}_K) \cap \mathcal{O}_s$.

Proof. This is [PR87a, Proposition 3.18], where G_σ is denoted $L'_{p,\sigma,\langle\ \rangle}$. The missing minus sign in the statement of Perrin-Riou's Proposition 3.18 is a typographical error, as the proof makes clear.

In Perrin-Riou's statement $r_{\mathfrak{a}\mathfrak{d}_s}$ appears as $r_{\mathfrak{a}'}$ where $\mathfrak{a}' = \mathfrak{D}\mathfrak{a}$, and (p. 484) '$\mathfrak{D}$ est le $\mathcal{O}_s$-idéal engendré par $\sqrt{D}$'. That is, $\mathfrak{D} = \sqrt{D}\mathcal{O}_s \neq \mathfrak{d}_s$. Later, on p. 486, Perrin-Riou writes 'Lorsque $s = 0$, $\mathfrak{a}'$ et $\mathfrak{a}$ sont équivalent', although under the stated definition of $\mathfrak{D}$ they are equivalent even when $s \neq 0$, suggesting that an unannounced change of notation has occurred. The formulas of [PR87a, § 3.2.3] are correct with $\mathfrak{D}$ defined as above, while those of [PR87a, § 3.3] are correct with $\mathfrak{D}$ replaced by our $\mathfrak{d}_s$. In particular, in the proof of [PR87a, Lemme 3.17] one must interpret $\mathfrak{D}$ as our $\mathfrak{d}_s$ in order to pass from (3.7) to (3.8) ('On remplace ensuite n par $\delta_2 n\ldots$'). The key point is

$$r_{\mathfrak{D}_1^{-1}\mathfrak{a}}(m\delta_1 - nN) = r_{\mathfrak{D}_1^{-1}\mathfrak{D}_2\mathfrak{a}}(m\delta - n\delta_2 N)$$

in which $\delta = |D| = \delta_1\delta_2$ and $\mathfrak{D}_i$ is the $\mathcal{O}_s$-ideal of norm δ_i (the equality is seen by using the map on $\mathcal{O}_s$-ideals $\mathfrak{b} \mapsto \mathfrak{D}_2\mathfrak{b}$ to identify the sets of ideals being counted). Using $\mathfrak{D}_1^{-1}\mathfrak{D}_2 = \mathfrak{d}_s$ in $\mathrm{Pic}(\mathcal{O}_s)$, one obtains the correct formula. Also, the first displayed equation in the proof of [PR87a, Lemme 3.17] appears to be in error; the two p-adic modular forms in the second equality differ by shifting Fourier coefficients by δ_1 (see [PR87a, (2.4) and Lemme 3.1]). This misstatement has no effect on the proof.

Perrin-Riou's $\mathfrak{a}$ is our $\mathfrak{a}^{-1}$, but both $r_{\mathfrak{a}\mathfrak{d}_s}$ and $\sigma'_{\mathfrak{a}}$ are unchanged by $\mathfrak{a} \mapsto \mathfrak{a}^{-1}$. For $\sigma'_{\mathfrak{a}}$ this is obvious; for $r_{\mathfrak{a}\mathfrak{d}_s}$ use the fact that inversion agrees with complex conjugation in $\mathrm{Pic}(\mathcal{O}_s)$, the fact that complex conjugation preserves norms, and the fact that $\mathfrak{d}_s$ has order two in $\mathrm{Pic}(\mathcal{O}_s)$. □

Lemma 2.0.6. *Suppose that n is prime to p and that there exists a proper integral $\mathcal{O}_s$-ideal $\mathfrak{b}$ in the* $\mathrm{Pic}(\mathcal{O}_s)$*-class of $\mathfrak{a}$ with $\mathbf{N}(\mathfrak{b}) \equiv -nN \pmod{Dp}$. Then*

$$\sigma'_{\mathfrak{a}}(n) = \sum_{\ell|n} \log_p(\ell)\cdot\begin{cases} 0 & \text{if } \epsilon(\ell) = 1 \\ \mathrm{ord}_\ell(\ell n)\delta(n)R_{\mathfrak{anc}}(n/\ell) & \text{if } \epsilon(\ell) = -1 \\ \mathrm{ord}_\ell(n)\delta(n)R_{\mathfrak{anc}}(n/\ell) & \text{if } \epsilon(\ell) = 0 \end{cases}$$

where in the second and third cases $\mathfrak{n}$ is any integral $\mathcal{O}_s$-ideal of norm N and $\mathfrak{c}$ is any proper integral $\mathcal{O}_s$-ideal with $\mathbf{N}(\mathfrak{c}) \equiv -\ell \pmod{Dp}$.

Proof. By [GZ86, Proposition IV.4.6(b)], the stated equality holds with $R_{\mathfrak{anc}}(n/\ell)$ replaced by $R_{\mathfrak{anc}\mathcal{O}_K}(n/\ell)$; that is, if we count integral $\mathcal{O}_K$-ideals of norm n/ℓ in the $\mathcal{O}_K$-genus of $\mathfrak{anc}\mathcal{O}_K$. So, we only need show that $R_{\mathfrak{anc}}(n/\ell) = R_{\mathfrak{anc}\mathcal{O}_K}(n/\ell)$ under the stated hypotheses. The map $I \mapsto I\mathcal{O}_K$ takes the collection $\mathfrak{R}_{\mathfrak{anc}}(n/\ell)$ of proper $\mathcal{O}_s$-ideals of norm n/ℓ in the $\mathcal{O}_s$-genus of $\mathfrak{anc}$ injectively to the set $\mathfrak{R}_{\mathfrak{anc}\mathcal{O}_K}(n/\ell)$ of proper $\mathcal{O}_K$-ideals of norm n/ℓ in the $\mathcal{O}_K$-genus of $\mathfrak{anc}\mathcal{O}_K$. It suffices to show that this map has an inverse. More precisely, we show that the map $J \mapsto J \cap \mathcal{O}_s$ from integral $\mathcal{O}_K$-ideals of norm prime to p to integral $\mathcal{O}_s$-ideals of norm prime to p restricts to a map $\mathcal{R}_{\mathfrak{anc}\mathcal{O}_K}(n/\ell) \to \mathcal{R}_{\mathfrak{anc}}(n/\ell)$.

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

Suppose that $I = J \cap \mathcal{O}_s$ is an integral $\mathcal{O}_s$-ideal of norm n/ℓ such that $J \in \mathfrak{R}_{\mathfrak{anc}\mathcal{O}_K}(n/\ell)$. Set $p^* = (-1)^{(p-1)/2}p$. Genus theory (for example, [Cox89, § 6.A] discusses the genus theory of $\mathcal{O}_K$ at length, and that of $\mathcal{O}_s$ is similar) gives a canonical isomorphism

$$\mathrm{Pic}(\mathcal{O}_s)/\mathrm{Pic}(\mathcal{O}_s)^2 \cong \mathrm{Pic}(\mathcal{O}_K)/\mathrm{Pic}(\mathcal{O}_K)^2 \times \mathrm{Gal}(K(\sqrt{p^*})/K)$$

under which the $\mathcal{O}_s$-genus of I is sent to the $\mathcal{O}_K$-genus of $J = I\mathcal{O}_K$ in the first factor, and to its Artin symbol

$$\left(\frac{I}{K(\sqrt{p^*})/K}\right) = \left(\frac{\mathbf{N}(I)}{\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}}\right)$$

in the second factor. The same holds with I replaced by $\mathfrak{bnc}$, and since the $\mathcal{O}_K$-genera of J and $\mathfrak{bnc}\mathcal{O}_K$ agree by assumption, $I \in \mathfrak{R}_{\mathfrak{anc}}(n/\ell) = \mathfrak{R}_{\mathfrak{bnc}}(n/\ell)$ if and only if

$$\left(\frac{\mathbf{N}(I)}{\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}}\right) = \left(\frac{\mathbf{N}(\mathfrak{bnc})}{\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}}\right)$$

which occurs if and only if

$$\left(\frac{\mathbf{N}(I)}{p}\right) = \left(\frac{\mathbf{N}(\mathfrak{bnc})}{p}\right).$$

Since $\mathbf{N}(I) = n/\ell$ and $\mathbf{N}(\mathfrak{bnc}) \equiv nN^2\ell \pmod p$ we are done. □

Corollary 2.0.7. *Let $\kappa \in \mathrm{Gal}(H_s/K)$ be the Artin symbol of $\mathfrak{d}_s$. For any positive integer m divisible by p, the mth Fourier coefficient of $G_{\sigma\kappa}$ is given by the expression*

$$-\sum_{\substack{n>0\\(n,p)=1}} \sum_{\ell | n} \log_p(\ell) \cdot r_{\mathfrak{a}}(m|D| - nN) \cdot \begin{cases} 0 & \text{if } \epsilon(\ell) = 1 \\ \mathrm{ord}_\ell(\ell n)\delta(n)R_{\mathfrak{anc}}(n/\ell) & \text{if } \epsilon(\ell) = -1 \\ \mathrm{ord}_\ell(n)\delta(n)R_{\mathfrak{anc}}(n/\ell) & \text{if } \epsilon(\ell) = 0 \end{cases}$$

where in the second and third cases $\mathfrak{n}$ is any integral $\mathcal{O}_s$-ideal of norm N and $\mathfrak{c}$ is any proper integral $\mathcal{O}_s$-ideal with $\mathbf{N}(\mathfrak{c}) \equiv -\ell \pmod{Dp}$.

Proof. Combine Proposition 2.0.5 and Lemma 2.0.6, and use $\sigma'_{\mathfrak{a}} = \sigma'_{\mathfrak{a}\mathfrak{d}_s}$ (which follows from the definition of σ' and the fact that $\mathfrak{d}_s\mathcal{O}_K$ is principal) and $\kappa^2 = 1$. □

3. The p-adic height pairing

In this section we recall some known facts about p-adic Néron symbols and p-adic height pairings on abelian varieties and, when the abelian variety is the Jacobian of a curve, the connection with p-adic Néron symbols and intersection theory on the curve.

3.1 Intersection theory

Let R be a complete discrete valuation ring, $S = \mathrm{Spec}(R)$. Let $\underline{X} \to S$ be an integral, proper scheme over S with generic fiber a smooth curve X, and suppose $\underline{C}$ and $\underline{D}$ are effective Cartier divisors with no common components. Define the intersection multiplicity $i_y(\underline{C}, \underline{D})$ at a closed point y of $\underline{X}$ to be the length of the $\mathcal{O}(\underline{X})_y$-module $\mathcal{O}(\underline{X})_y/(f, g)$ where f and g are defining equations of $\underline{C}$ and $\underline{D}$ in a neighborhood of y. Define the total intersection multiplicity $i(\underline{C}, \underline{D}) = \sum_y i_y(\underline{C}, \underline{D})[k(y) : k(s)]$ where s is the closed point of S and the sum is over closed points of $\underline{X}$.

We now assume that $\underline{X}$ is regular (in particular, we do not need to distinguish between Weil divisors and Cartier divisors), and record some fundamental properties of the total intersection multiplicity. We refer the reader to [Gro85] and [La88, ch. III] for details. The total intersection multiplicity is bi-additive, and so extends to divisors with rational coefficients. We define, for C and D degree zero divisors on X with disjoint support,

$$[C, D] = i(\underline{C} + C', \underline{D}) = i(\underline{C}, \underline{D} + D')$$

where $\underline{C}$ and $\underline{D}$ are the horizontal divisors on $\underline{X}$ whose generic fibers are C and D, respectively, and C' (respectively D') is a fibral divisor with rational coefficients chosen so that the symbol $i(\underline{C}+C',\ )$ (respectively $i(\ ,\underline{D} + D')$) vanishes on all fibral divisors. Let L be the fraction field of R and let v denote the normalized valuation on L, so that $v(\varpi) = 1$ for a uniformizer π. If $C = (f)$ is a principal divisor then $[C, D] = v(f(D))$ where $D = \sum n_i(D_i)$ is a linear combination of prime divisors D_i with residue field L_i and

$$f(D) = \prod_i \mathbf{N}_{L_i/L}(f(D_i)^{n_i}). \tag{6}$$

3.2 p-adic Néron symbols, I

We now define local p-adic Néron symbols on abelian varieties. The contents of this subsection are taken from [PR87a, § 4] essentially verbatim.

Let ℓ be a rational prime and L a finite extension of $\mathbb{Q}_\ell$. Let A be an abelian variety over L and assume that either $\ell \neq p$ or that A has good reduction. Fix a nontrivial continuous additive character $\rho : L^\times \to \mathbb{Z}_p$. If $\ell = p$ we assume that ρ is ramified.

PROPOSITION 3.2.1. *There is a $\mathbb{Q}_p$-valued Néron symbol $\langle \mathfrak{C}, d\rangle = \langle \mathfrak{C}, d\rangle_{A,\rho}$ defined whenever $\mathfrak{C}$ is an algebraically trivial divisor on A, d is a zero cycle of degree zero on A rational point-by-point over L, and the supports of $\mathfrak{C}$ and d have no common points. This symbol satisfies:*

(a) *$\langle\ ,\ \rangle$ is bilinear (whenever this makes sense) and invariant under translation by elements of $A(L)$;*

(b) *if $\mathfrak{C} = (h)$ is principal then $\langle \mathfrak{C}, d\rangle = \rho(h(d))$, where $h(d) = \prod_i f(d_i)$ is defined as in (6);*

(c) *for any endomorphism $\phi : A \to A$, $\langle \phi^*\mathfrak{C}, d\rangle = \langle \mathfrak{C}, \phi_* d\rangle$;*

(d) *for any $x_0 \in A(L)$ and any $\mathfrak{C}$ as above, the function $x \mapsto \langle \mathfrak{C}, (x) - (x_0)\rangle$ is continuous for the ℓ-adic topology on $A(L)$;*

(e) *if $\ell = p$, L' is a finite extension of L contained in the $\mathbb{Z}_p$-extension of L cut out by ρ, and $\mathfrak{C}$ is a degree zero divisor on $A_{/L'}$, then*

$$\langle \mathbf{N}_{L'/L}\mathfrak{C}, d\rangle \subset c^{-1}\rho(\mathbf{N}_{L'/L}(L'))$$

whenever this is defined, for some constant $c \in \mathbb{Z}_p$ independent of L', $\mathfrak{C}$, and d.

Furthermore, if $\ell \neq p$, or if $\ell = p$ and A has ordinary reduction, then such a symbol is unique.

Proof. In the case $\ell \neq p$, or $\ell = p$ but A has ordinary reduction, see the references after [PR87a, Théorème 4.2] for existence. In the case $\ell = p$ with nonordinary reduction, the existence is [PR87a, Théorème 4.7]. The translation invariance is not stated explicitly by Perrin-Riou, but follows from the construction as in [Blo80, Lemma 2.14]. We sketch the proof of the uniqueness. If $\langle\ ,\ \rangle'$ is another such symbol then we may define

$$G(\mathfrak{C}, x) = \langle \mathfrak{C}, (x) - (0)\rangle - \langle \mathfrak{C}, (x) - (0)\rangle'.$$

This defines a function $A^\vee(L) \times A(L) \to \mathbb{Q}_p$ which is linear in the first variable and continuous in the second. Using translation invariance and the theorem of the square [Mil86, Theorem 6.7], one can show that G is also linear in the second variable. Hence for fixed $\mathfrak{C}$, $G(\mathfrak{C},\ )$ defines a continuous linear map $A(L) \to \mathbb{Q}_p$. If $\ell \neq p$ this map must be trivial for topological reasons. If $\ell = p$ and A has ordinary reduction, then $A^\vee$ also has ordinary reduction, and [Maz72, Proposition 4.39] implies that the universal norms from the (ramified) $\mathbb{Z}_p$-extension cut out by ρ have finite index in $A^\vee(L)$. From this and the boundedness property (e), we see that G is identically zero. □

When $\ell \neq p$ the Néron symbol is compatible with base extension in the following sense. If L'/L is a finite extension, $A' = A \times_L L'$, and $\rho' = \rho \circ \mathbf{N}_{L'/L}$, then

$$\langle \mathfrak{C}, d \rangle_{A',\rho'} = \langle \mathbf{N}_{L'/L} \mathfrak{C}, d \rangle_{A,\rho} \tag{7}$$

for $\mathfrak{C}$ an algebraically trivial divisor on A' and d a point-by-point rational zero cycle of degree zero on A. This allows us to remove the hypothesis in Proposition 3.2.1 that d is rational point-by-point, by choosing an extension L'/L over which d becomes pointwise rational and defining

$$\langle \mathfrak{C}, d \rangle_{A,\rho} = [L' : L]^{-1} \langle \mathfrak{C}, d \rangle_{A',\rho'}.$$

This is independent of the choice of L' by (7). Proposition 3.2.1(b) continues to hold for this slight extension of the Néron symbol, provided that one extends the definition of $h(d)$ as in (6).

When $\ell = p$ the Néron symbol on A may not uniquely determined by the properties above, but one can choose a compatible family (in the sense that (7) holds) of Néron symbols $\langle\ ,\ \rangle_{A',\rho'}$ as L' varies over the finite extensions of L. Again, this allows one to remove the hypothesis that d is defined point-by-point. Perrin-Riou only states the existence of compatible families for subfields of the extension of L cut out by ρ, but the same argument holds for all finite extensions.

Remark 3.2.2. Although the choice of a Néron symbol on A in residue characteristic p is (sometimes) not unique, our results do not depend on the choice. Hence we fix, once and for all, a choice of Néron symbol on $J_0(N)_{H_s,v}$ for every s and every prime v of H_s above p, with the understanding that these choices are compatible as s varies in the sense of (7).

Now suppose that A is the Jacobian of a smooth, proper, geometrically connected curve X over L, and that X has an L-rational point ∞. Let $\alpha : X \to A$ be the canonical embedding $x \mapsto (x) - (\infty)$. Suppose we are given degree zero divisors C and D on X with disjoint support. Pullback by α restricts to an isomorphism $\alpha^* : \mathrm{Pic}^0(A) \to \mathrm{Pic}^0(X)$, and so there is an algebraically trivial divisor $\mathfrak{C}$ whose associated line bundle pulls back to the line bundle associated to C. Thus $C = \alpha^*\mathfrak{C} + (f)$ for some rational function f on X. The pair $(\mathfrak{C}, f)$ may be chosen so that (f) is disjoint from D and then it follows that $\mathfrak{C}$ has no points in common with $\alpha_* D$. We now define

$$\langle C, D \rangle_{X,\rho} = \langle \mathfrak{C}, \alpha_* D \rangle_{A,\rho} + \rho(f(D)), \tag{8}$$

where $f(D)$ is defined by (6). This is independent of the choice of $\mathfrak{C}$ (by Proposition 3.2.1(b)) and the choice of f (which is determined up to $L^\times$ once $\mathfrak{C}$ is chosen).

3.3 p-adic Néron symbols, II

Identifying Γ with the Galois group of the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$ via the cyclotomic character, the reciprocity map of class field theory and the p-adic logarithm define an idèle class character

$$\rho_{\mathbb{Q}} : \mathbf{A}_{\mathbb{Q}}^\times / \mathbb{Q}^\times \to \Gamma \xrightarrow{\log_p} \mathbb{Z}_p.$$

Fix a finite extension $L/\mathbb{Q}$, let ρ_L be the idèle class character of L defined by $\rho_L = \rho_{\mathbb{Q}} \circ \mathbf{N}_{L/\mathbb{Q}}$. For each finite place v of L, let π_v be a uniformizer of L_v and let $\mathbf{N}(v)$ denote the absolute residue degree of v. We may decompose $\rho_L = \sum_v \rho_{L_v}$ as a sum of local characters, and then $\rho_{L_v}(\pi_v) = \log_p(\mathbf{N}(v))$ for any prime v not above p. We note that this does not agree with [PR87a, p. 501], which seems to be in error (note also the remarks of [Nek95, § II.6.4]), although perhaps this is attributable to a different normalization of class field theory. We remind the reader that we always use the *arithmetic* conventions.

Let A be an abelian variety over L with good reduction above p. Summing the local Néron symbols $\langle\ ,\ \rangle_v = \langle\ ,\ \rangle_{A_v,\rho_{L_v}}$ on the completions $A_v = A \times_L L_v$ defines a bilinear pairing on Mordell–Weil groups

$$\langle\ ,\ \rangle_{A,L} : A^\vee(L) \times A(L) \to \mathbb{Q}_p. \tag{9}$$

Indeed, given $a \in A^\vee(L)$ and $b \in A(L)$, let $\mathfrak{C}$ be an algebraically trivial divisor on A which represents a and let $d = \sum n_i(d_i)$ be a zero cycle of degree zero on A with $\sum n_i d_i = b$. These can be chosen so that $\mathfrak{C}$ and d have no points in common and we then define

$$\langle a, b\rangle_{A,L} = \sum_v \langle \mathfrak{C}, d\rangle_v$$

where the sum is over the finite places of L. A different choice of $\mathfrak{C}$ changes the pairing by

$$\sum_v \langle (h), d\rangle_v = \sum_v \rho_{L,v}(h(d)) = \rho_L(h(d)) = 0$$

for some rational function h on A. Now fix $\mathfrak{C}$ and consider the expression $\sum_v \langle \mathfrak{C}, d\rangle_v$. We have just seen that this depends only on the linear equivalence class of $\mathfrak{C}$ (which is translation invariant), and thus the translation invariance of each $\langle\ ,\ \rangle_v$ shows that $\sum_v \langle \mathfrak{C}, d\rangle_v$ is translation invariant in the second variable (with $\mathfrak{C}$ held fixed). From this one may deduce

$$\sum_v \langle \mathfrak{C}, d\rangle_v = \sum_v \langle \mathfrak{C}, (b) - (0)\rangle_v,$$

and so the left-hand side depends only on b and not on the choice of d.

Now suppose X is a proper, smooth, geometrically connected curve over L with an L-rational point, and that A is the Jacobian of X. Let $\alpha : X \to A$ be the associated canonical embedding. For each place v of L we have from § 3.2 a $\mathbb{Q}_p$-valued symbol $\langle\ ,\ \rangle_{X_v,\rho_{L_v}}$ on disjoint divisors on $X_v = X \times_L L_v$. By summing over all places, we obtain a symbol

$$\langle\ ,\ \rangle_{X,L} = \sum_v \langle\ ,\ \rangle_{X_v,\rho_{L_v}} \tag{10}$$

defined on degree zero divisors of X with disjoint support. This pairing descends to a (symmetric) pairing on linear equivalence classes (this follows from Proposition 3.3.2(a,b) below and the fact that $\rho = \sum_v \rho_{L_v}$ vanishes on $L^\times$). In particular, $\langle\ ,\ \rangle_{X,L}$ extends bilinearly to all pairs of degree zero divisors, without the assumption of disjoint support.

Remark 3.3.1. As $\langle\ ,\ \rangle_{X,L}$ is defined on linear equivalence classes, it descends to a bilinear pairing

$$\langle\ ,\ \rangle_{X,L} : A(L) \times A(L) \to \mathbb{Q}_p.$$

which agrees with the pairing $-\langle\ ,\ \rangle_{A,L}$ when one identifies $A \cong A^\vee$ via the canonical principal polarization [PR87a, § 4.3].

Proposition 3.3.2. *Let v be a prime of L above a rational prime ℓ. The local Néron symbol $\langle C, D\rangle_v = \langle C, D\rangle_{X_v,\rho_{L_v}}$, defined on degree zero divisors on X_v with disjoint support, satisfies:*

(a) *$\langle\ ,\ \rangle_v$ is symmetric and bilinear;*

(b) *if $C = (f)$ is a principal divisor, then $\langle C, D\rangle_v = \rho_{L_v}(f(D))$;*

(c) *if T is a correspondence from X to itself and T^ι is the dual correspondence, then*

$$\langle TC, D\rangle_v = \langle C, T^\iota D\rangle_v;$$

(d) *for $d_0 \in X_v(L_v) - \mathrm{supp}(C)$, the function on $X_v(L_v) - \mathrm{supp}(C)$*

$$d \mapsto \langle C, (d) - (d_0)\rangle_v$$

is continuous for the v-adic topology;

(e) *if $\ell = p$, L' is a finite extension of L_v contained in the cyclotomic $\mathbb{Z}_p$-extension of L_v, and C and D are degree zero divisors on $X_v \times_{L_v} L'$ and X_v, respectively, then*

$$\langle \mathbf{N}_{L'/L_v} C, D\rangle_v \subset c^{-1}\rho_{\mathbb{Q}_p}(\mathbf{N}_{L'/\mathbb{Q}_p}(L'))$$

whenever this is defined, for some constant $c \in \mathbb{Z}_p$ independent of C, D, and L'.

Furthermore $\langle\ ,\ \rangle_v$ takes values in a compact subset of $\mathbb{Q}_p$.

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

Proof. Properties (a)–(e) are direct consequences of the analogous properties of the Néron symbol on A in Proposition 3.2.1, except for the symmetry (which is stated without proof in [PR87a], but can be deduced from the construction of the pairing of Proposition 3.2.1). For the final claim one uses the finite generation of the p-primary part $A(L_v)$ as a $\mathbb{Z}_p$-module and the specified behavior on principal divisors. □

Proposition 3.3.3. *For any prime v of L with residue characteristic $\neq p$ and any degree zero divisors C and D on X_v with disjoint support,*

$$\langle C, D\rangle_v = \log_p(\mathbf{N}(v))\ [C, D]$$

where $[C, D]$ is the pairing of § 3.1 for any regular, integral, proper scheme $\underline{X}$ over the integer ring of L_v whose generic fiber is X_v.

Proof. Using the discussion of § 3.1, one can show that the right-hand side satisfies properties (a)–(d) of Proposition 3.3.2, and so it suffices to show that these determine $\langle\ ,\ \rangle_v$ uniquely. This is similar to the uniqueness argument of Proposition 3.2.1; the difference of two such symbols would define a continuous bilinear function $A(L_v) \times A(L_v) \to \mathbb{Q}_p$, which must be trivial for topological reasons. □

4. Intersections on modular curves

Fix $s > 0$ and $\sigma \in \mathrm{Gal}(H_s/K)$. Let ℓ be a rational prime, v a place of H_s above ℓ, F the completion of the maximal unramified extension of $H_{s,v}$, W the integer ring of F, and $\mathfrak{m}$ the maximal ideal of W. Set $W_n = W/\mathfrak{m}^{n+1}$. We denote by $X = X_0(N)_{/\mathbb{Z}}$ the canonical integral model of [KM85], and set $\underline{X} = X \times_{\mathbb{Z}} W$.

Definition 4.0.4. Given elliptic curves with $\Gamma_0(N)$-structure $\underline{x}$ and $\underline{y}$ over $\mathrm{Spec}(W)$, we define $\mathrm{Hom}_{W_n}(\underline{y}, \underline{x})_{\deg(m)}$ to be the set of degree m isogenies (of elliptic curves with $\Gamma_0(N)$-structure, in the sense of § 1.1)

$$\underline{y} \times_W W_n \ \to\ \underline{x} \times_W W_n.$$

Proposition 4.0.5. *Let $\underline{x}, \underline{y} \in \underline{X}(W)$ represent elliptic curves with $\Gamma_0(N)$-structure over W, and assume that these sections intersect properly and reduce to regular, noncuspidal points in the special fiber. Then*

$$i(\underline{x}, \underline{y}) = \frac{1}{2} \sum_{n \geqslant 0} |\mathrm{Hom}_{W_n}(\underline{y}, \underline{x})_{\deg(1)}|.$$

Proof. This is [GZ86, Proposition III.6.1], or [Con04, Theorem 4.1]. □

Now assume $\ell \neq p$ and fix an integer $m = m_0 p^r$ with $r > 0$ and $(m_0, Np) = 1$. Choose an embedding $H_\infty \hookrightarrow F$ extending $H_s \hookrightarrow F$. Recall the notation

$$\mathbf{h}_{s,r} = \mathrm{Norm}_{H_{s+r}/H_s}(h_{s+r}), \quad \mathbf{d}_{s,r} = \mathrm{Norm}_{H_{s+r}/H_s}(d_{s+r})$$

of the introduction. For any $t \geqslant 0$, let $\underline{h}_t$ be the Zariski closure (with the reduced subscheme structure) of $h_t \in X(F)$ in $\underline{X}$ and let $T_{m_0}(\underline{\mathbf{h}}^\sigma_{s,r})$ be the horizontal Weil divisor on $\underline{X}$ with generic fiber $T_{m_0}(\mathbf{h}^\sigma_{s,r})$. By the valuative criterion of properness, the closed subscheme $\underline{h}_{s+r}$ has the form $\mathrm{Spec}(W) \to \underline{X}$. Moreover, the section $\underline{h}_{s+r}$ arises from a Heegner diagram defined over W. Indeed, by [Cor02, Proposition 1.2] or [SeTa69, Theorems 8,9] the point $h_{s+r} \in X(H_{s+r})$ arises from a Heegner diagram over H_{s+r} with good reduction above ℓ, and so the section $\underline{h}_{s+r}$ represents the Néron model over W of this Heegner diagram. Taking the quotient of $\underline{h}_{s+r}$ by its $p\mathcal{O}_{s+r-1}$-torsion, we obtain a Heegner diagram represented by the section $\underline{h}_{s+r-1} \in \underline{X}(W)$, and so on through all lower conductors. In particular, we now have a p-isogeny of Heegner diagrams defined over W.

$$\begin{array}{ccc} \underline{E}_s & \xrightarrow{\underline{h}_s} & \underline{E}'_s \\ \phi \downarrow & & \downarrow \phi' \\ \underline{E}_{s-1} & \xrightarrow{\underline{h}_{s-1}} & \underline{E}'_{s-1} \end{array} \tag{11}$$

Although the expression for the local Néron symbol at $\ell \neq p$ in terms of intersection theory requires working on a regular model (which $\underline{X}$ is not when $\ell \mid N$) and modifying the divisors in questions by a fibral divisor, in our situation these details can be ignored.

PROPOSITION 4.0.6. *Suppose that $\ell \neq p$ and $0 \leqslant t \leqslant s$. Then*

$$\langle c_t, T_{m_0}(\mathbf{d}^{\sigma}_{s,r})\rangle_v = \log_p(\mathbf{N}(v)) \cdot i(\underline{h}_t, T_{m_0}(\underline{\mathbf{h}}^{\sigma}_{s,r})),$$

where the pairing on the left is the local Néron symbol on $X_{/H_{s,v}}$ of Proposition 3.3.2 and i is the intersection multiplicity on $\underline{X}$ of § 3.1.

The proof is as in [GZ86, Proposition III.3.3], together with Proposition 3.3.3.

Remark 4.0.7. In order to make sense of $i(\underline{h}_t, T_{m_0}(\underline{\mathbf{h}}^{\sigma}_{s,r}))$ when $\ell \mid N$ we need to justify why the prime Weil divisors occurring in $T_{m_0}(\underline{\mathbf{h}}^{\sigma}_{s,r})$ are locally principal, so that $T_{m_0}(\underline{\mathbf{h}}^{\sigma}_{s,r})$ may be viewed as a Cartier divisor. The geometric points of $T_{m_0}(\mathbf{h}^{\sigma}_{s,r})$ all occur in the support of $T_m(h^{\sigma}_s)$. If $\ell \mid N$ then these points represent Heegner diagrams which are prime-to-ℓ isogenous to h^{σ}_s, and so are all defined over F. Arguing as in [Con04, Corollary 2.7] (Conrad's p is our ℓ), the Zariski closures of these points on $\underline{X}$ are sections to the structure map $\underline{X} \to \mathrm{Spec}(W)$ and lie in the smooth locus. In particular, the associated ideal sheaves are locally free of rank one.

PROPOSITION 4.0.8. *Suppose $\ell \neq p$ and $\epsilon(\ell) = 1$. Then for all $0 \leqslant t \leqslant s$, $\langle c_t, T_{m_0}(\mathbf{d}^{\sigma}_{s,r})\rangle_v = 0$, where the pairing $\langle\ ,\ \rangle_v$ is as in Proposition 4.0.6.*

Proof. By Proposition 4.0.6 we must show that $i(\underline{h}_t, T_{m_0}(\underline{\mathbf{h}}^{\sigma}_{s,r})) = 0$. The claim is unchanged if we replace W by the integer ring of a finite extension of F. Doing so, we assume that the divisor $T_{m_0}(\mathbf{h}^{\sigma}_{s,r})$ is defined point-by-point over F and that the horizontal divisor $T_{m_0}(\mathbf{d}^{\sigma}_{s,r})$ on $\underline{X}$ is a sum of sections to the structure map, each of which represents a Heegner diagram over W whose conductor divides mp^s and has exact valuation $s + r > t$ at p. Let $\underline{x}$ be one such Heegner diagram, and let $\mathcal{O}$ and $\mathcal{O}'$ be the endomorphism rings of $\underline{x}$ and its closed fiber, respectively. These are orders in K, as $\underline{x}$ has ordinary reduction, and $\mathcal{O} \subset \mathcal{O}'$. By the Serre–Tate theorem, $\mathcal{O}$ is the intersection (in $K \otimes \mathbb{Q}_\ell$) of $\mathcal{O}'$ and $\mathcal{O} \otimes \mathbb{Z}_\ell$, therefore

$$\mathrm{ord}_p(\mathrm{cond}(\mathcal{O}')) = \mathrm{ord}_p(\mathrm{cond}(\mathcal{O})) = s + r > t.$$

The same argument shows that the valuation at p of the conductor of the CM order of the special fiber of $\underline{h}_t$ is t, and so the Heegner diagram $\underline{h}_t$ is distinct in the special fiber from all Heegner diagrams appearing in $T_{m_0}(\underline{\mathbf{h}}^{\sigma}_{s,r})$. By Proposition 4.0.5, $i(\underline{h}_t, T_{m_0}(\underline{\mathbf{h}}^{\sigma}_{s,r})) = 0$. □

5. Nonsplit primes away from p

In this section we examine the local Néron pairings between Heegner points at places lying above rational primes $\neq p$ which are nonsplit in K. The methods are based on those of Chapter III of [GZ86], and this portion of Gross and Zagier's work has been reworked and rewritten by Conrad [Con04] with the addition of considerably more detail.

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

Keep the notation of § 4, and assume $\ell \neq p$ is nonsplit in K. In particular $\ell \nmid N$. Fix a prime v of H_s (with $s > 0$, as always) above ℓ and an integral $\mathcal{O}_s$-ideal $\mathfrak{a}$ of norm prime to $D\ell p$ whose class in $\mathrm{Pic}(\mathcal{O}_s)$ represents σ under the Artin map. We denote by $\mathfrak{l}$ the unique prime of $\mathcal{O}_s$ above ℓ (we sometimes let $\mathfrak{l}$ denote the $\mathcal{O}_K$-ideal $\mathfrak{l}\mathcal{O}_K$; a mild abuse of notation). If $\epsilon(\ell) = -1$ then $\mathfrak{l} = \ell\mathcal{O}_s$ is trivial in $\mathrm{Pic}(\mathcal{O}_s)$, $\mathfrak{l}$ splits completely in H_s, and v has absolute residue degree 2. If $\epsilon(\ell) = 0$ then $\mathfrak{l}^2 = \ell\mathcal{O}_s$ and $\mathfrak{l}$ is not a principal ideal of $\mathcal{O}_s$ (if D is not prime then $\mathfrak{l}\mathcal{O}_K$ is not principal, if $D = -\ell$ is prime then $\mathfrak{l} = (\sqrt{D} \cap \mathcal{O}_s)$ is not principal since $s > 0$). Thus, when $\epsilon(\ell) = 0$, $\mathfrak{l}$ has order 2 in $\mathrm{Pic}(\mathcal{O}_s)$ and again v has residue degree 2.

5.1 Intersection via Hom sets

Proposition 5.1.1. *For any integer $m = m_0 p^r$ with $(m_0, Np) = 1$,*

$$\langle c_s, T_{m_0}(\mathbf{d}^\sigma_{s,r+2})\rangle_v = \log_p(\ell) \sum_{n \geqslant 0} (|\mathrm{Hom}_{W_n}(\underline{h}^{\mathfrak{a}}_s, \underline{h}_s)_{\deg(mp^2)}| - |\mathrm{Hom}_{W_n}(\underline{h}^{\mathfrak{a}}_{s-1}, \underline{h}_s)_{\deg(mp)}|)$$

$$\langle c_{s-1}, T_{m_0}(\mathbf{d}^\sigma_{s,r+1})\rangle_v = \log_p(\ell) \sum_{n \geqslant 0} (|\mathrm{Hom}_{W_n}(\underline{h}^{\mathfrak{a}}_s, \underline{h}_{s-1})_{\deg(mp)}| - |\mathrm{Hom}_{W_n}(\underline{h}^{\mathfrak{a}}_{s-1}, \underline{h}_{s-1})_{\deg(m)}|)$$

where $\langle\ ,\ \rangle_v$ is the local Néron symbol on $X_{/H_{s,v}}$ of Proposition 3.3.2, and the Hom *sets are those of Definition 4.0.4.*

Proof. We prove the first equality. The proof of the second involves only a change of subscripts.

First consider the easy case where $(\ell, m_0) = 1$. Then the divisor $T_{m_0}(\mathbf{h}^\sigma_{s,r+2})$ on $\underline{X}_{/F}$ (recall that F is the completion of the maximal unramified extension of $H_{s,v}$, W is its integer ring, and $\underline{X} = X_0(N)_{/W}$) is a sum of sections to the structure map. Hence, the same is true of the horizontal divisor $T_{m_0}(\underline{\mathbf{h}}^\sigma_{s,r+2})$ on $\underline{X}$, and each section represents a Heegner diagram over $\mathrm{Spec}(W)$. Namely, if we fix an extension of σ to $\mathrm{Gal}(H_{s+r+2}/K)$ and an ideal $\mathfrak{a}$ of $\mathcal{O}_{s+r+2}$ representing this extension, then

$$T_{m_0}(\underline{\mathbf{h}}^\sigma_{s,r+2}) = \sum_{\mathfrak{b}} \sum_{C} \underline{h}^{\mathfrak{ab}}_{s+r+2/C} \tag{12}$$

where $\mathfrak{b}$ runs over classes in $\mathrm{Pic}(\mathcal{O}_{s+r+2})$ which are trivial in $\mathrm{Pic}(\mathcal{O}_s)$, C runs over the order m_0-subgroup schemes of the Heegner diagram $\underline{h}^{\mathfrak{ab}}_{s+r+2}$ over $\mathrm{Spec}(W)$ and the subscript $/C$ means the quotient by C (which makes sense since $(m_0, N) = 1$). Since ℓ does not divide m_0, each C is étale (in fact, constant), determined uniquely by its reduction to W_n for any n, and the decomposition (12) holds over W_n. By Proposition 4.0.5

$$\begin{aligned} i(\underline{h}_s, T_{m_0}(\underline{\mathbf{h}}^\sigma_{s,r+2})) &= \sum_{\mathfrak{b}} \sum_{C} i(\underline{h}_s, \underline{h}^{\mathfrak{ab}}_{s+r+2/C}) \\ &= \frac{1}{2} \sum_n \sum_{\mathfrak{b}} \sum_C |\mathrm{Hom}_{W_n}(\underline{h}^{\mathfrak{ab}}_{s+r+2/C}, \underline{h}_s)_{\deg(1)}| \\ &= \frac{1}{2} \sum_n \sum_{\mathfrak{b}} |\mathrm{Hom}_{W_n}(\underline{h}^{\mathfrak{ab}}_{s+r+2}, \underline{h}_s)_{\deg(m_0)}|, \end{aligned}$$

and by Proposition 4.0.6 the first equality of Proposition 5.1.1 follows once we show

$$|\mathrm{Hom}_{W_n}(\underline{h}^{\mathfrak{a}}_s, \underline{h}_s)_{\deg(mp^2)}| = |\mathrm{Hom}_{W_n}(\underline{h}^{\mathfrak{a}}_{s-1}, \underline{h}_s)_{\deg(mp)}| + \sum_{\mathfrak{b}} |\mathrm{Hom}_{W_n}(\underline{h}^{\mathfrak{ab}}_{s+r+2}, \underline{h}_s)_{\deg(m_0)}|. \tag{13}$$

The p^{r+2}-torsion on $\underline{h}^{\mathfrak{a}}_s$ is constant as a group scheme, and so the kernel of any degree mp^2 isogeny $f : \underline{h}^{\mathfrak{a}}_s \to \underline{h}_s$ over W_n determines an order p^{r+2}-subgroup of $\underline{h}^{\mathfrak{a}}_s(W)$. By the Euler system relations of § 1.2, every such subgroup is either the kernel of a map which factors through $\phi^{\mathfrak{a}} : \underline{h}^{\mathfrak{a}}_s \to \underline{h}^{\mathfrak{a}}_{s-1}$, or is the kernel of the dual isogeny to $\phi^{\mathfrak{ab}} \circ \cdots \circ \phi^{\mathfrak{ab}} : \underline{h}^{\mathfrak{ab}}_{s+r+2} \to \underline{h}^{\mathfrak{a}}_s$ for some choice of $\mathfrak{b}$, and the

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

two cases are mutually exclusive. Thus f has one of the two forms

$$\underline{h}_s^{\mathfrak{a}} \xrightarrow{\phi^{\mathfrak{a}}} \underline{h}_{s-1}^{\mathfrak{a}} \xrightarrow{\psi} \underline{h}_s, \quad \underline{h}_s^{\mathfrak{a}} \xrightarrow{(\phi^{\mathfrak{ab}}\circ\cdots\circ\phi^{\mathfrak{ab}})^\vee} \underline{h}_{s+r+2}^{\mathfrak{ab}} \xrightarrow{\psi} \underline{h}_s$$

where ψ has degree either mp or m_0 (respectively). The equality (13) follows.

Now consider the case where ℓ divides m_0. This is considerably more involved, but nearly all of what we need is covered by the generality of [Con04, § 6] (which is based on [GZ86, III § 4–6]), to which we refer the reader for the proof of (14) below. Write $m_0 = m_1\ell^t$ with $(\ell, m_1) = 1$. As above, the divisor $T_{m_1}(\underline{\mathbf{h}}_{s,r+2}^{\sigma})$ on $\underline{X}$ is a sum of sections, each of which represents a Heegner diagram over $\mathrm{Spec}(W)$, and we denote by Z the set of such sections

$$Z = \{\underline{h}_{s+r+2/C}^{\mathfrak{ab}} \mid \mathfrak{b} \in \mathrm{Ker}(\mathrm{Pic}(\mathcal{O}_{s+r+2}) \to \mathrm{Pic}(\mathcal{O}_s))\}$$

where C runs over the order m_1 subgroup schemes of $\underline{h}_{s+r+2}^{\mathfrak{ab}}$. For each $\underline{z} \in Z$, one has the expected (but much more subtle) equality

$$\begin{aligned} i(\underline{h}_s, T_{m_0}(\underline{h}_{s+r+2}^{\mathfrak{a}})) &= \sum_{\underline{z}\in Z} i(\underline{h}_s, T_{\ell^t}(\underline{z})) \\ &= \frac{1}{2}\sum_{\underline{z}\in Z}\sum_{n\geqslant 0} |\mathrm{Hom}_{W_n}(\underline{z}, \underline{h}_s)_{\deg(\ell^t)}| \\ &= \frac{1}{2}\sum_{n}\sum_{\mathfrak{b}} |\mathrm{Hom}_{W_n}(\underline{h}_{s+r+2}^{\mathfrak{ab}}, \underline{h}_s)_{\deg(m_0)}|. \end{aligned} \tag{14}$$

With this in hand, the remainder of the proof is exactly as in the case $(\ell, m_0) = 1$. □

5.2 Inclusion-exclusion

Our goal is, for any positive integer m with $(m, N) = 1$, to express the sum over n of

$$\begin{aligned} &|\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)_{\deg(mp^2)}| - |\mathrm{Hom}_{W_n}(\underline{h}_{s-1}^{\mathfrak{a}}, \underline{h}_s)_{\deg(mp)}| \\ &\quad - |\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_{s-1})_{\deg(mp)}| + |\mathrm{Hom}_{W_n}(\underline{h}_{s-1}^{\mathfrak{a}}, \underline{h}_{s-1})_{\deg(m)}| \end{aligned} \tag{15}$$

as a sum over elements in the quaternion algebra $B = \mathrm{End}_{W_0}(\underline{h}_s) \otimes_{\mathbb{Z}} \mathbb{Q}$.

LEMMA 5.2.1. *Base change to the fiber induces a degree preserving injection*

$$\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s) \to \mathrm{Hom}_{W_0}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s),$$

and similarly for the other Hom *sets occurring in (15).*

Proof. This is [Con04, Lemma 2.1(2)] or [Gor02, Proposition VI.2.4(2)]. □

The isogeny ϕ induces injections

$$\mathrm{Hom}_{W_n}(\underline{h}_{s-1}^{\mathfrak{a}}, \underline{h}_s) \xrightarrow{\circ\phi^{\mathfrak{a}}} \mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s) \to \mathrm{Hom}_{W_0}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)$$

$$\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_{s-1}) \xrightarrow{\phi^\vee\circ} \mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s) \to \mathrm{Hom}_{W_0}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)$$

whose images we denote by L_n and $L_n^\vee$, respectively. We also define M_n to be the image of the injective composition

$$\mathrm{Hom}_{W_n}(\underline{h}_{s-1}^{\mathfrak{a}}, \underline{h}_{s-1}) \to \mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s) \to \mathrm{Hom}_{W_0}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)$$

where the first arrow is given by $f \mapsto \phi^\vee \circ f \circ \phi^{\mathfrak{a}}$. Clearly $M_n \subset L_n \cap L_n^\vee$. The scheme-theoretic kernels

$$\ker(\phi : \underline{E}_s \to \underline{E}_{s-1}), \quad \ker(\phi^{\mathfrak{a}} : \underline{E}_s^{\mathfrak{a}} \to \underline{E}_{s-1}^{\mathfrak{a}})$$

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

are constant group schemes of order p over W. We define

$$C = (\ker\ \phi)(W_0), \quad C^{\mathfrak{a}} = (\ker\ \phi^{\mathfrak{a}})(W_0).$$

Definition 5.2.2. We say that $f \in \mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)$ is *stable* if the restriction of f to the fiber $f_0 : \underline{E}_s^{\mathfrak{a}}(W_0) \to \underline{E}_s(W_0)$ takes $C^{\mathfrak{a}}$ into C. We say that f is *unstable* otherwise, and make similar definitions for maps from $\underline{h}_s$ to itself. If $Z \subset \mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)$ is any subset, we write Z^{stable} and Z^{unstable} for the subsets of stable and unstable elements of Z.

Lemma 5.2.3. *Suppose that m is any positive integer with $(m, N) = 1$. Base change to the fiber identifies the stable elements of degree mp^2 in $\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)$ with the degree mp^2 elements of $L_n \cup L_n^{\vee}$.*

Proof. Fix $f \in \mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)$ of degree divisible by p and prime to N. Letting f_0 denote the restriction of f to geometric points as above, f is stable if and only if either $f_0(C^{\mathfrak{a}}) = 0$ or $f_0(C^{\mathfrak{a}}) = C$. The first condition is equivalent to $f_0 = g_0 \circ \phi^{\mathfrak{a}}$ for some $g_0 \in \mathrm{Hom}_{W_0}(\underline{E}_{s-1}^{\mathfrak{a}}, \underline{E}_s)$. Since $\phi^{\mathfrak{a}}$ has degree p it induces an isomorphism on ℓ-divisible groups over W_n, and so the map on ℓ-divisible groups induced by g_0 lifts to W_n. By the Serre–Tate theorem g_0 itself lifts to a morphism over W_n, and so $f \in L_n$. Now suppose $f_0(C^{\mathfrak{a}}) = C$. Since the degree of f is divisible by p we must have $f_0(\underline{E}_s^{\mathfrak{a}}(W_0)[p]) = C$, and so $f_0^{\vee}(C) = (f_0^{\vee} \circ f_0)(\underline{E}_s^{\mathfrak{a}}(W_0)[p]) = 0$. Hence, $f_0^{\vee} = g_0 \circ \phi$ for some $g_0 \in \mathrm{Hom}_{W_0}(\underline{E}_{s-1}, \underline{E}_s^{\mathfrak{a}})$, and so $f_0 \in L_n^{\vee}$ as above.

Conversely, if $f_0 \in L_n \cup L_n^{\vee}$ then either $f_0(C^{\mathfrak{a}}) = 0$ or $f_0^{\vee}(C) = 0$. In the second case we compute the Weil e_p-pairing

$$e_p(f_0(\underline{E}_s^{\mathfrak{a}}(W_0)[p]), C) = e_p(\underline{E}_s^{\mathfrak{a}}(W_0)[p], f_0^{\vee}(C)) = 0.$$

This implies $f_0(\underline{E}_s^{\mathfrak{a}}(W_0)[p]) \subset C$, and so, in either case, $f_0(C^{\mathfrak{a}}) \subset C$ and f is stable. □

Lemma 5.2.4. *For any positive integer m with $(m, N) = 1$, the composition*

$$\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s) \to \mathrm{Hom}_{W_0}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s) \xrightarrow{p} \mathrm{Hom}_{W_0}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)$$

taking $f \mapsto pf_0$ identifies the unstable elements of $\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)_{\deg(m)}$ with the complement of $(M_n)_{\deg(mp^2)}$ in $(L_n \cap L_n^{\vee})_{\deg(mp^2)}$ (the degree mp^2 elements of M_n and $L_n \cap L_n^{\vee}$, respectively).

Proof. First suppose that we are given some $f \in \mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)$; the claim is that $pf_0 \in M_n$ if and only if f is stable. By definition $pf_0 \in M_n$ if and only if there is some $f' \in \mathrm{Hom}_{W_n}(\underline{E}_{s-1}^{\mathfrak{a}}, \underline{E}_{s-1})$ such that $pf = \phi^{\vee} \circ f' \circ \phi^{\mathfrak{a}}$, or equivalently, such that $\phi \circ f = f' \circ \phi^{\mathfrak{a}}$. Furthermore, this is equivalent to finding $f_0' \in \mathrm{Hom}_{W_0}(\underline{E}_{s-1}^{\mathfrak{a}}, \underline{E}_{s-1})$ such that $\phi \circ f_0 = f_0' \circ \phi^{\mathfrak{a}}$ holds in the fiber (since ϕ and $\phi^{\mathfrak{a}}$ induce isomorphisms on ℓ-divisible groups over W_n, the map on ℓ-divisible groups induced by f_0' lifts to W_n, and so the Serre–Tate theorem implies that f_0' itself lifts). Such an f_0' exists if and only if $(\phi \circ f_0)(C^{\mathfrak{a}}) = 0$, which is equivalent to f being stable.

Now suppose we are given a homomorphism $g_0 \in L_n \cap L_n^{\vee}$ of degree divisible by p^2, with $g_0 \notin M_n$. There is some $y \in \mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_{s-1})$ such that g_0 is the restriction of $g = \phi^{\vee} \circ y$ to the fiber. Let y_0 denote the restriction of y to the fiber. If $y_0(C^{\mathfrak{a}}) = 0$ we could write $y_0 = y_0' \circ \phi^{\mathfrak{a}}$ for some $y_0' \in \mathrm{Hom}_{W_0}(\underline{E}_{s-1}^{\mathfrak{a}}, \underline{E}_{s-1})$. As above, the map on ℓ-divisible groups induced by such a y_0' would lift to W_n, and so by the Serre–Tate theorem y_0' itself would lift to some $y' \in \mathrm{Hom}_{W_n}(\underline{E}_{s-1}^{\mathfrak{a}}, \underline{E}_{s-1})$ with g_0 equal to the restriction of $\phi^{\vee} \circ y' \circ \phi^{\mathfrak{a}}$ to the fiber. This contradicts $g_0 \notin M_n$, so $y_0(C^{\mathfrak{a}}) \neq 0$. Since p divides the degree of y_0 we must have $y_0(\underline{E}_s^{\mathfrak{a}}(W_0)[p]) = y_0(C^{\mathfrak{a}})$. Now $g_0 \in L_n$ implies

$$0 = g_0(C^{\mathfrak{a}}) = (\phi_0^{\vee} \circ y_0)(C^{\mathfrak{a}}) = g_0(\underline{E}_s^{\mathfrak{a}}(W_0)[p]),$$

so $g_0 = pf_0$ for some $f_0 \in \mathrm{Hom}_{W_0}(\underline{E}_s^{\mathfrak{a}}, \underline{E}_s)$. As above, the Serre–Tate theorem guarantees that f_0 lifts to a morphism f over W_n. □

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

COROLLARY 5.2.5. *The expression (15) is equal to*

$$|\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)^{\mathrm{unstable}}_{\deg(mp^2)}| - |\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)^{\mathrm{unstable}}_{\deg(m)}|.$$

Proof. By the definitions of M_n, L_n and $L_n^\vee$,

$$|\mathrm{Hom}_{W_n}(\underline{h}_{s-1}^{\mathfrak{a}}, \underline{h}_{s-1})_{\deg(m)}| = |(M_n)_{\deg(mp^2)}|$$
$$|\mathrm{Hom}_{W_n}(\underline{h}_{s-1}^{\mathfrak{a}}, \underline{h}_{s})_{\deg(mp)}| = |(L_n)_{\deg(mp^2)}|$$
$$|\mathrm{Hom}_{W_n}(\underline{h}_{s}^{\mathfrak{a}}, \underline{h}_{s-1})_{\deg(mp)}| = |(L_n^\vee)_{\deg(mp^2)}|.$$

Consequently, the expression (15) is equal to

$$|\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)^{\mathrm{unstable}}_{\deg(mp^2)}| + |\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)^{\mathrm{stable}}_{\deg(mp^2)}| - |(L_n)_{\deg(mp^2)}| - |(L_n^\vee)_{\deg(mp^2)}| + |(M_n)_{\deg(mp^2)}|.$$

By Lemma 5.2.3 this is

$$|\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)^{\mathrm{unstable}}_{\deg(mp^2)}| + |(L_n \cup L_n^\vee)_{\deg(mp^2)}| - |(L_n)_{\deg(mp^2)}| - |(L_n^\vee)_{\deg(mp^2)}| + |(M_n)_{\deg(mp^2)}|$$

which we write as

$$|\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)^{\mathrm{unstable}}_{\deg(mp^2)}| - |(L_n \cap L_n^\vee)_{\deg(mp^2)}| + |(M_n)_{\deg(mp^2)}|$$
$$= |\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)^{\mathrm{unstable}}_{\deg(mp^2)}| - |\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)^{\mathrm{unstable}}_{\deg(m)}|$$

using Lemma 5.2.4. □

Set $R = \mathrm{Hom}_{W_0}(\underline{h}_s, \underline{h}_s)$ and $B = R \otimes_{\mathbb{Z}} \mathbb{Q}$. Thus, B is a rational quaternion algebra ramified exactly at ℓ and ∞, and $R \subset B$ is a level-N Eichler order [Con04, Lemma 7.1]. The reduction map

$$\mathrm{Hom}_W(\underline{h}_s, \underline{h}_s) \;\to\; \mathrm{Hom}_{W_0}(\underline{h}_s, \underline{h}_s)$$

induces an embedding $\iota : K \;\to\; B$ which, by the Serre–Tate theorem, is *optimal* for the pair $(\mathcal{O}_s, R)$ in the sense that $\iota(K) \cap R = \iota(\mathcal{O}_s)$. We henceforth regard K as a subfield of B, suppressing ι from the notation. There is a canonical decomposition

$$B = B^+ \oplus B^- = K \oplus Kj$$

where $j \in B$ is a trace zero element with the property $jxj^{-1} = \bar{x}$ for all $x \in K$. This characterizes j up to multiplication by $\mathbb{Q}^\times$. The reduced norm is additive with respect to this decomposition, i.e. $\mathbf{N}(b^+ + b^-) = \mathbf{N}(b^+) + \mathbf{N}(b^-)$. We wish to determine which $b \in R = \mathrm{Hom}_{W_0}(\underline{h}_s, \underline{h}_s)$ are unstable.

LEMMA 5.2.6. *An endomorphism $b \in R$ is unstable if and only if*

$$\mathrm{ord}_p \mathbf{N}(b^+) = \mathrm{ord}_p \mathbf{N}(b^-) = -2s,$$

where $b^\pm$ is the projection of b to the summand $B^\pm$.

Proof. We are free to assume that j is chosen in R. Let T denote the p-adic Tate module of $\underline{E}_s(W_0)[p^\infty]$ and set $V = T \otimes \mathbb{Q}_p$. The split quaternion algebra $B_p = B \otimes \mathbb{Q}_p$ acts on V, and the stabilizer of $T \subset V$ is exactly $R_p = R \otimes \mathbb{Z}_p$ (since the order R is locally maximal away from N). Under the identification of V/T with $\underline{E}_s(W_0)[p^\infty]$, the subgroup $\mathcal{O}_{s-1,p}T/T$ is identified with C, and so the unstable elements of R are exactly those which do not stabilize the lattice $T' = \mathcal{O}_{s-1,p}T \supset T$. As an $\mathcal{O}_{s,p}$-module, T is free of rank one (proof: T is isomorphic as an $\mathcal{O}_{s,p}$-module to some fractional $\mathcal{O}_{s,p}$-ideal; by the optimality of $K \;\to\; B$ with respect to $(\mathcal{O}_s, R)$, this ideal is proper, and all proper ideals of $\mathcal{O}_{s,p}$ are principal). Fix a generator $t \in T$, and let $X \in \mathcal{O}_{s,p}$ be such that $jt = Xt$. This implies, in particular, that $\mathbf{N}(X) = \mathbf{N}(j)$. As a $\mathbb{Z}_p$-module, T is generated by t and $p^s\sqrt{D}t$, and so $\alpha + \beta j \in B$ (with α, $\beta \in K$) stabilizes T if and only if the elements

$$(\alpha + \beta j)t = (\alpha + \beta X)t, \quad (\alpha + \beta j)p^s\sqrt{D}t = (\alpha - \beta X)p^s\sqrt{D}t$$

are in T. From this we deduce that

$$R_p = \{\alpha + \beta j \in B_p \mid \alpha, \beta X \in (p^s\sqrt{D})^{-1}\mathcal{O}_{s,p}, \alpha + \beta X \in \mathcal{O}_{s,p}\}.$$

Applying similar reasoning to the lattice T', we find that the order of B_p leaving both T and T' stable is

$$R_p^{\text{stable}} = \{\alpha + \beta j \in B_p \mid \alpha, \beta X \in (p^{s-1}\sqrt{D})^{-1}\mathcal{O}_{s-1,p}, \alpha + \beta X \in \mathcal{O}_{s,p}\}.$$

Given $b = \alpha + \beta j \in R_p$, set $\alpha' = p^s\sqrt{D}\alpha$ and $\beta' = p^s\sqrt{D}\beta$. It is easily seen that the set of elements of $\mathcal{O}_{s,p}$ of norm divisible by p is equal to the unique maximal ideal $p\mathcal{O}_{s-1,p} \subset \mathcal{O}_{s,p}$. Since $\alpha' \equiv -\beta' X \pmod{p^s\sqrt{D}\mathcal{O}_{s,p}}$, α' is a unit if and only if $\beta' X$ is a unit. Both elements are units if and only if $\mathrm{ord}_p\mathbf{N}(\alpha) = \mathrm{ord}_p\mathbf{N}(\beta X) = -2s$, and both are nonunits if and only if $\alpha + \beta j \in R_p^{\text{stable}}$. □

Proposition 5.2.7. *For any nonnegative integers m, n with $(m, N) = 1$, there is a bijection between $\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)^{\text{unstable}}_{\deg(m)}$ and the set of all $b \in R \cdot \mathfrak{a}$ such that:*

(a) $\mathbf{N}(b) = m\mathbf{N}(\mathfrak{a})$;

(b) $\mathrm{ord}_p\mathbf{N}(b^+) = \mathrm{ord}_p\mathbf{N}(b^-) = -2s$;

(c) *and*

$$\mathrm{ord}_\ell(D\mathbf{N}(b^-)) \geqslant \begin{cases} 2n+1 & \text{if } \epsilon(\ell) = -1 \\ n+1 & \text{if } \epsilon(\ell) = 0. \end{cases}$$

Proof. By [GZ86, Proposition III.7.3] or [Con04, Theorem 7.12 and (7-3)] there is an isomorphism of left $\mathcal{O}_s$-modules

$$\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s) \cong \mathrm{Hom}_{W_n}(\underline{h}_s, \underline{h}_s) \otimes_{\mathcal{O}_s} \mathfrak{a}$$

whose image (viewed as a lattice in $R\mathfrak{a}$) is exactly those elements satisfying property (c), under which the degree m isogenies correspond to those satisfying property (a). We must show that this bijection takes the stable elements onto those $b = b^+ + b^-$ for which property (b) fails. The isomorphism in question is defined as follows. The map

$$\mathrm{End}_{W_n}(\underline{E}_s) \otimes_{\mathcal{O}_s} \mathfrak{a} \xrightarrow{\xi_n} \mathrm{Hom}_{W_n}(\mathrm{Hom}_{\mathcal{O}_s}(\mathfrak{a}, \underline{E}_s), \underline{E}_s) \cong \mathrm{Hom}_{W_n}(\underline{E}_s^{\mathfrak{a}}, \underline{E}_s)$$

defined by $\xi_n(f \otimes x)(\phi) = f(\phi(x))$ is an isomorphism of $\mathcal{O}_s$-modules by Lemma 7.13 of [Con04], and taking level N structure into account we obtain an injection of left $\mathcal{O}_s$-modules

$$\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s) \cong \mathrm{Hom}_{W_n}(\underline{h}_s, \underline{h}_s) \otimes_{\mathcal{O}_s} \mathfrak{a} \hookrightarrow R\mathfrak{a}.$$

This injection identifies

$$\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)^{\text{stable}} \cong \mathrm{Hom}_{W_n}(\underline{h}_s, \underline{h}_s)^{\text{stable}} \otimes_{\mathcal{O}_s} \mathfrak{a}$$

inside of $R\mathfrak{a}$ (this is easily checked everywhere locally using the fact that $\mathfrak{a}$ is proper, hence locally principal). Localizing at p and using $(\mathbf{N}(\mathfrak{a}), p) = 1$, the claim follows from Lemma 5.2.6. □

For any order S of B, define

$$D_s^{\mathfrak{a}}(S, m) = \left\{ b \in S \cdot \mathfrak{a} \;\middle|\; \begin{matrix} \mathbf{N}(b) = m\mathbf{N}(\mathfrak{a}) \\ \mathrm{ord}_p\mathbf{N}(b^+) = \mathrm{ord}_p\mathbf{N}(b^-) = -2s \end{matrix} \right\}$$
$$\Delta_s^{\mathfrak{a}}(S, m) = \sum_{b \in D_s^{\mathfrak{a}}(S,m)} \begin{cases} \frac{1}{2}(1 + \mathrm{ord}_\ell\mathbf{N}(b^-)) & \text{if } \epsilon(\ell) = -1 \\ \mathrm{ord}_\ell(D\mathbf{N}(b^-)) & \text{if } \epsilon(\ell) = 0. \end{cases} \tag{16}$$

Corollary 5.2.8. *For $(m, N) = 1$,*

$$\sum_{n \geqslant 0} |\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}}, \underline{h}_s)^{\text{unstable}}_{\deg(m)}| = \Delta_s^{\mathfrak{a}}(R, m).$$

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

Proof. When $\epsilon(\ell) = 0$ this is immediate from the proposition above. When $\epsilon(\ell) = -1$ it is similarly clear, provided one knows that $\mathrm{ord}_\ell \mathbf{N}(b^-)$ is always odd; but (as we see in the next section) we are free to choose j in such a way that $\mathrm{ord}_\ell \mathbf{N}(j) = 1$, so writing $b^- = \beta j$ with $\beta \in K$, $\mathrm{ord}_\ell(\mathbf{N}(b^-)) = 1 + \mathrm{ord}_\ell \mathbf{N}(\beta)$ is odd. □

5.3 Quaternionic sums

We continue to let B be the rational quaternion algebra of discriminant ℓ and assume we have a fixed embedding $K \hookrightarrow B$. As noted before, this embedding induces a splitting $B = B^+ + B^- = K \oplus Kj$. Let $\mathcal{S}$ denote the (finite) set of $K^\times$-conjugacy classes of $\mathcal{O}_s$-optimal, level N Eichler orders in B; that is, level N Eichler orders S such that $S \cap K = \mathcal{O}_s$, modulo the conjugation action of $K^\times$. For such an S, the value of $\Delta_s^{\mathfrak{a}}(S, m)$ (defined in (16)) depends only on the class of S in $\mathcal{S}$. Define

$$\Delta_s^{\mathfrak{a}}(m) = \sum_{S \in \mathcal{S}} \Delta_s^{\mathfrak{a}}(S, m).$$

The remainder of this subsection is devoted to the proof of the following proposition. The statement holds without parity restrictions on D, but *we will assume throughout that D is odd*, referring the reader to [Man04] for a description of the needed changes to the proof in the case where D is even. The method of proof follows the calculations performed in [GZ86, § III.9] (and described in great detail in [Man04]). The main difference (apart from working in higher conductor) is that we have 'removed the Euler factor at p' by adding the condition $\mathrm{ord}_p \mathbf{N}(b^+) = \mathrm{ord}_p \mathbf{N}(b^-) = -2s$ to the set $D_s^{\mathfrak{a}}(S, m)$ over which the summation $\Delta_s^{\mathfrak{a}}(S, m)$ occurs.

Proposition 5.3.1. *There is a proper integral $\mathcal{O}_s$-ideal $\mathfrak{q}$ such that for every positive integer m*

$$\Delta_s^{\mathfrak{a}}(m) = \sum_{\substack{n>0 \\ \ell \mid n, (n,p)=1}} \delta(n) r_{\mathfrak{a}}(mp^{2s}|D| - nN) \cdot \begin{cases} \mathrm{ord}_\ell(\ell n) R_{\mathfrak{a}\mathfrak{q}\mathfrak{n}}(n/\ell) & \text{if } \epsilon(\ell) = -1 \\ \mathrm{ord}_\ell(n) R_{\mathfrak{a}\mathfrak{q}\mathfrak{n}\mathfrak{l}}(n/\ell) & \text{if } \epsilon(\ell) = 0 \end{cases}$$

where $\mathfrak{n}$ is any integral $\mathcal{O}_s$-ideal with $\mathcal{O}_s/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$. When $\epsilon(\ell) = -1$, we may take $\mathbf{N}(\mathfrak{q}) \equiv -\ell \pmod{Dp}$, and when $\epsilon(\ell) = 0$ we may take $\mathbf{N}(\mathfrak{q}\mathfrak{l}) \equiv -\ell \pmod{Dp}$.

If $\hat{K}^\times$ denotes the group of finite idèles of K and $\hat{\mathcal{O}}_s^\times \subset \hat{K}^\times$ is the group of units in the profinite completion of $\mathcal{O}_s$, then there is an action of the ring class group $\hat{K}^\times / K^\times \hat{\mathcal{O}}_s^\times \cong \mathrm{Pic}(\mathcal{O}_s)$ on $\mathcal{S}$: if $x = (x_r) \in \hat{K}^\times$ and $S \in \mathcal{S}$ then S^x is defined by the relation $(S^x)_r = x_r S_r x_r^{-1} \subset B_r$ for every rational prime r. In terms of $\mathcal{O}_s$-ideals the action is again by conjugation: $S^{\mathfrak{b}} = \mathfrak{b} S \mathfrak{b}^{-1}$.

Lemma 5.3.2. *The action of $\mathrm{Pic}(\mathcal{O}_s)$ on $\mathcal{S}$ is transitive, and the stabilizer of any element is the subgroup generated by the class of $\mathfrak{l}$ (so has order 1 if $\epsilon(\ell) = -1$ and order 2 if $\epsilon(\ell) = 0$).*

Proof. Let S and S' be $\mathcal{O}_s$-optimal level N Eichler orders. To prove the transitivity of the action of $\mathrm{Pic}(\mathcal{O}_s)$ on $\mathcal{S}$, we must show that S_r and S'_r are conjugate by elements of $K_r^\times$ for every prime r. The proof of [Man04, Theorem A.15] shows that this is the case if either $\mathcal{O}_{s,r}$ is maximal (which occurs for all $r \neq p$) or if S_r and S'_r are maximal (which occurs for all $(r, N) = 1$). To compute the kernel of the action, fix $S \in \mathcal{S}$ and let $x = (x_r)$ be a finite idèle of K. If $S = S^x$ in $\mathcal{S}$ then there is some $y \in K^\times$ such that $x_r y_r^{-1}$ is contained in $N(S_r)$, the normalizer of S_r in $B_r^\times$, for every prime r.

If $(r, N\ell) = 1$ then $N(S_r) = \mathbb{Q}_r^\times S_r^\times$, and so

$$x_r y_r^{-1} \in (\mathbb{Q}_r^\times S_r^\times) \cap K_r^\times = \mathbb{Q}_r^\times \mathcal{O}_{s,r}^\times.$$

If $r \mid N$ then $\mathbb{Q}_r^\times S_r^\times$ has index 2 in $N(S_r)$. Fix an isomorphism $\psi : B_r \cong M_2(\mathbb{Q}_r)$ in such a way that $\psi(K_r) \cong \mathbb{Q}_r \oplus \mathbb{Q}_r$ is the quadratic subalgebra of diagonal matrices, and let $S'_r \subset M_2(\mathbb{Q}_r)$ be the usual Eichler order of integral matrices whose lower left entry is divisible by $N_r = r^{\mathrm{ord}_r(N)}$. As S_r and $\psi^{-1}(S'_r)$ are both $\mathcal{O}_{s,r}$-optimal, by the discussion above there is a $z \in K_r^\times$ such

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

that $zS_rz^{-1} = \psi^{-1}(S'_r)$. Thus, replacing ψ by a $\psi(K^\times)$-conjugate we may also assume that $\psi(S_r) = S'_r$. Having made such a choice, we now suppress ψ from the notation. The nontrival coset of $\mathbb{Q}_r^\times S_r^\times$ in $N(S_r)$ is represented by the matrix

$$\alpha = \begin{pmatrix} 0 & 1 \\ N_r & 0 \end{pmatrix},$$

and one now checks directly that

$$x_r y_r^{-1} \in N(S_r) \cap K_r^\times = (\mathbb{Q}_r^\times S_r^\times \sqcup \alpha \mathbb{Q}_r^\times S_r^\times) \cap K_r^\times = \mathbb{Q}_r^\times \mathcal{O}_{s,r}^\times.$$

When $r = \ell$, B_ℓ has a unique maximal order, hence $N(S_\ell) \cap K_\ell^\times = K_\ell^\times$. We have shown that a finite idèle (x_r) acts trivially on $\mathcal{S}$ if and only if $(x_r) \in \hat{\mathbb{Q}}^\times \hat{\mathcal{O}}_s^\times K_\ell^\times K^\times = \hat{\mathcal{O}}_s^\times K_\ell^\times K^\times$. □

Let $\mathcal{W}_0$ denote the set of prime divisors of Dp if $\epsilon(\ell) = -1$, and the set of prime divisors $\neq \ell$ of Dp if $\epsilon(\ell) = 0$. Let $\mathcal{W}$ be the free abelian group (written multiplicatively) of exponent 2 on the elements of $\mathcal{W}_0$, and define a homomorphism

$$\mathcal{W} \to \mathrm{Pic}(\mathcal{O}_s)[2]$$

by sending $w \mapsto (\sqrt{D})_w$, the finite idèle of K which is 1 away from w and equal to the image of $\sqrt{D}$ under $K^\times \to K_r^\times$ at each $r \mid w$. This map allows us to view $\mathcal{S}$ as a $\mathcal{W}$-module. By genus theory, the map $\mathcal{W} \to \mathrm{Pic}(\mathcal{O}_s)[2]$ is surjective. The kernel has order 2 if $\epsilon(\ell) = -1$, and has order 1 if $\epsilon(\ell) = 0$.

As in [GZ86, pp. 265–266], we now choose a particular model for the quaternion algebra B. Detailed proofs of the following assertions can be found in [Man04]. If $\epsilon(\ell) = -1$ then choose a prime q such that $\left(\frac{-\ell q}{r}\right) = 1$ for all primes $r \mid D$. For such a q the quaternion algebra B is isomorphic to the quaternion algebra $\left(\frac{D, -\ell q}{\mathbb{Q}}\right)$ (meaning the quaternion algebra $B = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}ij$ with $i^2 = D$, $j^2 = -\ell q$, $ij = -ji$) and q is split in K. We may, and do, further impose the condition $q \equiv -\ell \pmod{Dp}$. If $\epsilon(\ell) = 0$ then choose a prime $q \neq \ell$ such that $\left(\frac{-q}{r}\right) = 1$ for all primes $r \mid (D/\ell)$, and with $\left(\frac{-q}{\ell}\right) = -1$. For such a q the quaternion algebra B is isomorphic to the quaternion algebra $\left(\frac{D, -q}{\mathbb{Q}}\right)$, and again such a q is split in K. We further impose the condition $\ell q \equiv -\ell \pmod{Dp}$. We henceforth fix a q as above and identify

$$B \cong \begin{cases} \left(\dfrac{D, -\ell q}{\mathbb{Q}}\right) & \text{if } \epsilon(\ell) = -1 \\ \left(\dfrac{D, -q}{\mathbb{Q}}\right) & \text{if } \epsilon(\ell) = 0. \end{cases}$$

In either case we regard K as a subfield of B via $\sqrt{D} \mapsto i$, so that conjugation by j acts as complex conjugation on K. Let $\mathfrak{D}_s = p^s\sqrt{D}\mathcal{O}_s$ denote the different of the order $\mathcal{O}_s$. Fix an integral $\mathcal{O}_s$-ideal $\mathfrak{n}$ such that $\mathcal{O}_s/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$, and let $\mathfrak{q}$ be an integral $\mathcal{O}_s$-ideal of norm q.

Lemma 5.3.3. *If $\epsilon(\ell) = -1$ there is a collection $\{X_r \in \mathbb{Z}_r^\times \mid r \in \mathcal{W}_0\}$ such that*

$$R = \{\alpha + \beta j \mid \alpha \in \mathfrak{D}_s^{-1},\ \beta \in \mathfrak{D}_s^{-1}\mathfrak{n}\mathfrak{q}^{-1},\ \alpha - X_r\beta \in \mathcal{O}_{s,r}\ \forall r \in \mathcal{W}_0\}$$

is an $\mathcal{O}_s$-optimal level N Eichler order, and such that $X_r^2 = -\ell q$. If $\epsilon(\ell) = 0$ there is a collection $\{X_r \in \mathbb{Z}_r^\times \mid r \in \mathcal{W}_0\}$ such that

$$R = \{\alpha + \beta j \mid \alpha \in \mathfrak{D}_s^{-1}\mathfrak{l},\ \beta \in \mathfrak{D}_s^{-1}\mathfrak{l}\mathfrak{n}\mathfrak{q}^{-1},\ \alpha - X_r\beta \in \mathcal{O}_{s,r}\ \forall r \in \mathcal{W}_0\}$$

has the above property, and $X_r^2 = -q$.

Proof. Suppose $\epsilon(\ell) = -1$. The order $S = \mathcal{O}_s + \mathfrak{q}^{-1}j \subset B$ has reduced discriminant $p^{2s}D\ell$, and for a prime r not dividing pND, $R_r = S_r$. Thus, the lattice R_r is a maximal order at such primes.

If $r \mid N$ then $R_r = \mathcal{O}_{s,r} + \mathfrak{n}_r j$ is an Eichler order of level $r^{\mathrm{ord}_r N}$, so it remains to consider R_r for $r \mid Dp$. We have assumed $q \equiv -\ell \pmod{Dp}$, so that by Hensel's lemma $j^2 = -\ell q$ has a square root $X_r \in \mathbb{Z}_r^\times$ for each $r \mid Dp$. If we set $t_r = X_r - j$ then one readily computes $jt_r = -X_r t_r$, so that $B_r \cdot t_r = K_r \cdot t_r$ is a two-dimensional $\mathbb{Q}_r$-vector space on which B_r acts by left multiplication. Exactly as in the proof of Lemma 5.2.6, the (necessarily maximal) order leaving $\mathcal{O}_{s,r} \cdot t_r$ stable is

$$R_r = \{\alpha + \beta j \in B_r \mid \alpha, \beta X_r \in \mathfrak{D}_{s,r}^{-1}, \alpha - \beta X_r \in \mathcal{O}_{s,r}\}.$$

This shows that R is a level N Eichler order, and the $\mathcal{O}_s$-optimality is immediate from the explicit description. The case $\epsilon(\ell) = 0$ is entirely similar. □

Fix a family $\{X_r\}$ and an order R as in the lemma. It is verified by direct calculation that for any $w \in \mathcal{W}$, R^w has the same explicit form as R, but with X_r replaced by

$$X_r^w = \begin{cases} -X_r & \text{if } r \mid w \\ X_r & \text{otherwise.} \end{cases}$$

LEMMA 5.3.4. *If $\mathfrak{g}$ is any integral $\mathcal{O}_s$-ideal of norm prime to Dp then*

$$\sum_{w\in\mathcal{W}} \sum_{b\in D_s^{\mathfrak{a}}(R^{w\mathfrak{g}},m)} (1+\mathrm{ord}_\ell \mathbf{N}(b^-))$$
$$= \sum_{\substack{n>0 \\ \ell\mid n,(n,p)=1}} \delta(n) r_{\mathfrak{a}}(mp^{2s}|D| - nN) \cdot \begin{cases} 4\cdot r_{\mathfrak{a}\mathfrak{q}\bar{\mathfrak{n}}\bar{\mathfrak{g}}^2}(n/\ell)\ \mathrm{ord}_\ell(\ell n) & \text{if } \epsilon(\ell) = -1 \\ 2\cdot r_{\mathfrak{a}\mathfrak{q}\bar{\mathfrak{n}}\bar{\mathfrak{g}}^2\mathfrak{l}}(n/\ell)\ \mathrm{ord}_\ell(n) & \text{if } \epsilon(\ell) = 0. \end{cases} \tag{17}$$

Proof. Suppose that $\epsilon(\ell) = -1$. The lattice $R^{w\mathfrak{g}}\mathfrak{a}$ is given explicitly by

$$R^{w\mathfrak{g}}\mathfrak{a} = \{\alpha + \beta j \mid \alpha \in \mathfrak{D}_s^{-1}\mathfrak{a},\ \beta \in \mathfrak{D}_s^{-1}\mathfrak{n}\mathfrak{q}^{-1}\mathfrak{g}\bar{\mathfrak{g}}^{-1}\bar{\mathfrak{a}},\ \alpha - X_r^w\beta \in \mathcal{O}_{s,r} \forall r \mid Dp\}.$$

Denote by $\mathfrak{C}$ the set of all pairs $(\mathfrak{c}^+, \mathfrak{c}^-)$ of proper, integral $\mathcal{O}_s$-ideals such that:

(a) $\mathbf{N}(\mathfrak{c}^+) + \ell N \mathbf{N}(\mathfrak{c}^-) = mp^{2s}|D|$;

(b) $\mathfrak{c}^+$ and $\mathfrak{c}^-$ are prime to p;

(c) $\mathfrak{c}^+$ lies in the $\mathrm{Pic}(\mathcal{O}_s)$-class of $\bar{\mathfrak{a}}$;

(d) $\mathfrak{c}^-$ lies in the $\mathrm{Pic}(\mathcal{O}_s)$-class of $\mathfrak{a}\bar{\mathfrak{n}}\mathfrak{q}\bar{\mathfrak{g}}^2$;

and for each $w \in \mathcal{W}$ let $F^w : D_s^{\mathfrak{a}}(R^{w\mathfrak{g}}, m) \to \mathfrak{C}$ be the function defined by sending $b = \alpha + \beta j$ to the pair

$$\mathfrak{c}^+ = \alpha\mathfrak{D}_s\mathfrak{a}^{-1}, \quad \mathfrak{c}^- = \beta\mathfrak{D}_s\mathfrak{q}\mathfrak{n}^{-1}\mathfrak{g}^{-1}\bar{\mathfrak{g}}\bar{\mathfrak{a}}^{-1}. \tag{18}$$

If $D_s^{\mathfrak{a}}(R^{w\mathfrak{g}}, m)$ contained both $b = \alpha + \beta j$ and $\alpha - \beta j$ then we would have $b^+ = \alpha \in \mathcal{O}_{s,p}$, contradicting $\mathrm{ord}_p \mathbf{N}(b^+) = -2s$. This implies that F^w is two-to-one.

The claim is that every element of $\mathfrak{C}$ is in the image of F^w for exactly $2\delta(\mathbf{N}(\mathfrak{c}^-))$ choices of w, so that

$$\sum_{w\in\mathcal{W}} \sum_{b\in D_s^{\mathfrak{a}}(R^{w\mathfrak{g}},m)} (1+\mathrm{ord}_\ell \mathbf{N}(b^-)) = 4 \sum_{(\mathfrak{c}^+,\mathfrak{c}^-)\in\mathfrak{C}} (2+\mathrm{ord}_\ell \mathbf{N}(\mathfrak{c}^-)) \cdot \delta(\mathbf{N}(\mathfrak{c}^-)). \tag{19}$$

To verify this, fix $(\mathfrak{c}^+, \mathfrak{c}^-) \in \mathfrak{C}$ and choose generators

$$\alpha\mathcal{O}_s = \mathfrak{c}^+\mathfrak{D}_s^{-1}\mathfrak{a}, \quad \beta\mathcal{O}_s = \mathfrak{c}^-\mathfrak{D}_s^{-1}\mathfrak{q}^{-1}\mathfrak{n}\mathfrak{g}\bar{\mathfrak{g}}^{-1}\bar{\mathfrak{a}}.$$

Then $b = \alpha + \beta j$ lies in $D_s^{\mathfrak{a}}(R^{w\mathfrak{g}}, m)$ if and only if $\alpha - X_r^w\beta \in \mathcal{O}_{s,r}$ for every prime divisor r of Dp, or equivalently, if $\alpha' \equiv X_r^w\beta' \pmod{\mathfrak{D}_{s,r}}$ for every r, where $\alpha' = p^s\sqrt{D}\,\alpha$, $\beta' = p^s\sqrt{D}\,\beta \in \mathcal{O}_s$. The action of complex conjugation on $\mathcal{O}_s/\mathfrak{D}_s$ is trivial and so we have

$$\alpha'^2 \equiv \mathbf{N}(\alpha') = \mathbf{N}(\mathfrak{a})\mathbf{N}(\mathfrak{c}^+) \equiv -\ell N \mathbf{N}(\mathfrak{c}^-)\mathbf{N}(\mathfrak{a}) = -\ell q \mathbf{N}(\beta') \equiv X_r^2\beta'^2$$

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

modulo $\mathfrak{D}_{s,r}$. When $r \neq p$, $\mathcal{O}_{s,r}/\mathfrak{D}_{s,r}$ is a field, and so $\alpha' \equiv \pm X_r\beta'$. The congruence holds for both signs if and only if $\alpha' \equiv 0$, which holds if and only if $r \mid \mathbf{N}(\mathfrak{c}^-)$. When $r = p$, $\alpha' \in \mathcal{O}_{s,r}^\times$ and the unit group of the ring $\mathbb{Z}/p^{2s}\mathbb{Z} \cong \mathcal{O}_{s,r}/\mathfrak{D}_{s,r}$ has no 2-torsion apart from ± 1. Hence, $\alpha' \equiv \pm X_r\beta'$ for a unique choice of sign. We have shown that $\alpha + \beta j$ is contained in $D_s^{\mathfrak{a}}(R^{w\mathfrak{g}}, m)$ for exactly $\delta(\mathbf{N}(\mathfrak{c}^-))$ choices of w. The element $\alpha - \beta j$ lies in $D_s^{\mathfrak{a}}(R^{w\mathfrak{g}}, m)$ for another $\delta(\mathbf{N}(\mathfrak{c}^-))$ choices of w, all distinct from the first set of choices. This proves (19). The right-hand side of (19) agrees with the right-hand sum in the statement of the lemma by setting $n = \ell\mathbf{N}(\mathfrak{c}^-)$.

The case where $\epsilon(\ell) = 0$ is very similar: the set $\mathfrak{C}$ is instead taken to be the collection of pairs of proper, integral $\mathcal{O}_s$-ideals $(\mathfrak{c}^+, \mathfrak{c}^-)$ such that:

(a) $\mathbf{N}(\mathfrak{c}^+) + N\mathbf{N}(\mathfrak{c}^-) = mp^{2s}|D|$;

(b) $\mathfrak{c}^+$ and $\mathfrak{c}^-$ are prime to p and divisible by $\mathfrak{l}$;

(c) $\mathfrak{c}^+$ lies in the $\mathrm{Pic}(\mathcal{O}_s)$-class of $\bar{\mathfrak{a}}$;

(d) $\mathfrak{c}^-$ lies in the $\mathrm{Pic}(\mathcal{O}_s)$-class of $\mathfrak{a}\bar{\mathfrak{n}}\mathfrak{q}\bar{\mathfrak{g}}^2$.

The function from $D_s^w(R^{w\mathfrak{g}}, m)$ to $\mathfrak{C}$ is then exactly as in (18), and the expression on the left-hand side of (17) is equal to

$$4 \sum_{(\mathfrak{c}^+,\mathfrak{c}^-)\in\mathfrak{C}} \mathrm{ord}_\ell \mathbf{N}(\mathfrak{c}^-) \cdot 2^{\#\{r\in\mathcal{W}_0 \mid r \text{ divides } \mathbf{N}(\mathfrak{c}^-)\}} = 2 \sum_{\substack{n>0\\ \ell\mid n,(n,p)=1}} r_{\mathfrak{a}}(mp^{2s}|D| - nN) r_{\mathfrak{a}\mathfrak{q}\bar{\mathfrak{n}}\bar{\mathfrak{g}}^2}(n)\delta(n)\mathrm{ord}_\ell(n)$$

by taking $n = \mathbf{N}(\mathfrak{c}^-)$. This is equivalent to the stated equality. □

Proof of Proposition 5.3.1. Fix a set $\mathfrak{G} = \{\mathfrak{g}\}$ of proper integral $\mathcal{O}_s$-ideals of norm prime to Dp such that $\{\mathfrak{g}^2 \mid \mathfrak{g} \in \mathfrak{G}\}$ represents $\mathrm{Pic}(\mathcal{O}_s)^2$. As $\mathfrak{g}$ varies over $\mathfrak{G}$ and w varies over $\mathcal{W}$, $w\mathfrak{g}$ varies over $\mathrm{Pic}(\mathcal{O}_s)$ hitting each ideal class once if $\epsilon(\ell) = 0$ and twice if $\epsilon(\ell) = -1$. By Lemmas 5.3.2 and 5.3.4 (recall also that we are assuming D odd) we have

$$\begin{aligned}
\Delta_s^{\mathfrak{a}}(m) &= \frac{1}{2}\sum_{w\in\mathcal{W}}\sum_{\mathfrak{g}\in\mathfrak{G}} \Delta_s^{\mathfrak{a}}(R^{w\mathfrak{g}}, m)\\
&= \frac{1}{2(1-\epsilon(\ell))}\sum_{\mathfrak{g}\in\mathfrak{G}}\sum_{w\in\mathcal{W}}\sum_{b\in D_s^{\mathfrak{a}}(R^{w\mathfrak{g}},m)} \big(1 + \mathrm{ord}_\ell \mathbf{N}(b^-)\big)\\
&= \sum_{\substack{n>0\\ \ell\mid n,(n,p)=1}} \delta(n) r_{\mathfrak{a}}(mp^{2s}|D| - nN) \cdot \begin{cases} \mathrm{ord}_\ell(\ell n) R_{\mathfrak{a}\mathfrak{q}\mathfrak{n}}(n/\ell) & \text{if } \epsilon(\ell) = -1\\ \mathrm{ord}_\ell(n) R_{\mathfrak{a}\mathfrak{q}\mathfrak{n}\mathfrak{l}}(n/\ell) & \text{if } \epsilon(\ell) = 0. \end{cases}
\end{aligned}$$
□

5.4 The ℓ-contribution to the height

Fix $m = m_0p^r$ with $(m_0, Np) = 1$. Let $\mathfrak{b}$ be a proper integral $\mathcal{O}_s$-ideal, and denote by $\tau \in \mathrm{Gal}(H_s/K)$ the Artin symbol of $\mathfrak{b}$. We consider the quantity

$$\langle c_s^\tau, T_{m_0}(\mathbf{d}_{s,r+2}^{\sigma\tau})\rangle_v - \langle c_{s-1}^\tau, T_{m_0}(\mathbf{d}_{s,r+1}^{\sigma\tau})\rangle_v$$

where the pairing is the local Néron symbol on $X_{/H_{s,v}}$ of Proposition 3.3.2. By replacing h_i with h_i^τ in Proposition 5.1.1, this is equal to

$$\log_p(\ell)\sum_{n\geqslant 0}(|\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}\mathfrak{b}}, \underline{h}_s^{\mathfrak{b}})_{\deg(mp^2)}| - |\mathrm{Hom}_{W_n}(\underline{h}_{s-1}^{\mathfrak{a}\mathfrak{b}}, \underline{h}_s^{\mathfrak{b}})_{\deg(mp)}|$$
$$- |\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{a}\mathfrak{b}}, \underline{h}_{s-1}^{\mathfrak{b}})_{\deg(mp)}| + |\mathrm{Hom}_{W_n}(\underline{h}_{s-1}^{\mathfrak{a}\mathfrak{b}}, \underline{h}_{s-1}^{\mathfrak{b}})_{\deg(m)}|),$$

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

which is equal, by Corollary 5.2.5, to

$$\log_p(\ell)\sum_{n\geqslant 0}(|\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{ab}},\underline{h}_s^{\mathfrak{b}})^{\mathrm{unstable}}_{\deg(mp^2)}| - |\mathrm{Hom}_{W_n}(\underline{h}_s^{\mathfrak{ab}},\underline{h}_s^{\mathfrak{b}})^{\mathrm{unstable}}_{\deg(m)}|).$$

By Corollary 5.2.8, this last expression is equal to

$$\log_p(\ell)(\Delta_s^{\mathfrak{a}}(R^{\mathfrak{b}^{-1}}, mp^2) - \Delta_s^{\mathfrak{a}}(R^{\mathfrak{b}^{-1}}, m)),$$

where we have used [Con04, (7-8)] to identify $\mathrm{End}_{W_0}(\underline{h}_s^{\mathfrak{b}})$ with $\mathfrak{b}^{-1}\cdot\mathrm{End}_{W_0}(\underline{h}_s)\cdot\mathfrak{b}$ inside of $B = \mathrm{Hom}_{W_0}(\underline{h}_s,\underline{h}_s)\otimes\mathbb{Q}$.

PROPOSITION 5.4.1. *For any positive integer $m = m_0p^r$ with $(m_0, Np) = 1$ and any ℓ nonsplit in K,*

$$\sum_w(\langle c_s, T_{m_0}(\mathbf{d}^{\sigma}_{s,r+2})\rangle_w - \langle c_{s-1}, T_{m_0}(\mathbf{d}^{\sigma}_{s,r+1})\rangle_w) = \log_p(\ell)(\Delta_s^{\mathfrak{a}}(mp^2) - \Delta_s^{\mathfrak{a}}(m))$$

where the sum is over all primes w of H_s above ℓ and $\Delta_s^{\mathfrak{a}}(m)$ is the quantity defined in § 5.3 (and computed explicitly in Proposition 5.3.1), and the pairing is the local Néron symbol on $X_{/H_{s,w}}$ of Proposition 3.3.2.

Proof. Let $\mathrm{Pic}^{\ell}(\mathcal{O}_s)$ denote the quotient of $\mathrm{Pic}(\mathcal{O}_s)$ by the subgroup generated by the class of the unique prime of K above ℓ. Then $\mathrm{Pic}^{\ell}(\mathcal{O}_s)$ acts simply transitively on the set $\mathcal{S}$ by Lemma 5.3.2, and also acts simply transitively on the primes of H_s above ℓ. If we let $\mathfrak{b}$ vary over a set of representatives of $\mathrm{Pic}^{\ell}(\mathcal{O}_s)$ and use the relation $\langle x^{\tau}, y^{\tau}\rangle_v = \langle x, y\rangle_{\tau^{-1}(v)}$ for $\tau\in\mathrm{Gal}(H_s/K)$, then the claim follows from the discussion above. □

6. Néron symbols above p

In this section we use the methods of Perrin-Riou [PR87a, § 5.3] to analyze the p-adic Néron symbol on $X_0(N)$ at primes above p.

Fix $s > 0$, $\sigma\in\mathrm{Gal}(H_s/K)$, and assume that $\epsilon(p) = 1$ and $D \neq -3, -4$. As always, we let $\mathfrak{a}\subset\mathcal{O}_s$ be a proper ideal whose Artin symbol is σ. For any positive integer m, we let T_m be the usual Hecke correspondence on $X_0(N)$ (taking the Atkin–Lehner U_ℓ at primes dividing N). For any correspondence T from a curve to itself, we let T^{ι} denote the transpose correspondence. Thus $T_m = T_m^{\iota}$ for $(m, N) = 1$. If $\mathfrak{p}$ is one of the two primes of K above p, we let δ be the order of $\mathfrak{p}$ in the ideal class group of K.

6.1 Some modular forms

Fix a place v of H_s above p.

LEMMA 6.1.1. *Let R be the integer ring of $H_{s,v}$ and let $\underline{\mathbf{h}}^{\sigma}_{s,r}$ be the horizontal divisor of $X_0(N)_{/R}$ with generic fiber $\mathbf{h}^{\sigma}_{s,r}$. For any divisor $\underline{C}$ on $X_0(N)_{/R}$, there is a constant $c = c(\underline{C})$ such that the intersection multiplicity $i(\underline{C}, \underline{\mathbf{h}}^{\sigma}_{s,r})$ of § 3.1 depends only on $r \pmod{\delta}$ when $r > c$.*

Proof. It suffices to prove this when $\underline{C}$ is effective. The extension H_∞/H_0 is totally ramified at v, and we let w denote the unique place of H_∞ above v. Let $F(r)$ be the completion of the maximal unramified extension of $H_{s+r,w}$ with integer ring $W(r)$, and let $W(r)_k$ be the quotient of $W(r)$ by the $(k+1)$th power of the maximal ideal. Let $\hat{\mathbb{Q}}_p^{\mathrm{unr}}$ denote the completion of the maximal unramified extension of $\mathbb{Q}_p$. The extension $H_{s+r,w}/H_{0,w}$ is totally ramified of degree $p^{r+s-1}(p-1)$, and $H_{0,w}\subset\hat{\mathbb{Q}}_p^{\mathrm{unr}}$. From this one easily deduces that $F(r)$ is the compositum of $\hat{\mathbb{Q}}_p^{\mathrm{unr}}$ and $H_{s+r,w}$ (so is abelian over $\mathbb{Q}_p$), and that $F(r)/\hat{\mathbb{Q}}_p^{\mathrm{unr}}$ is totally ramified of degree $p^{r+s-1}(p-1)$. By class field theory $F(r) = \hat{\mathbb{Q}}_p^{\mathrm{unr}}(\mu_{p^{s+r}})$. Decompose $\underline{C} = \sum_{k=0}^{e_r}\underline{y}(k)$ as a sum of prime divisors on $X_0(N)_{/W(r)}$.

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

For r greater than or equal to some r_0 the sequence e_r is constant and $\underline{h}^\sigma_{s,r}$ has no components in common with $\underline{C}$. Abbreviate $e = e_{r_0}$ and take $c = r_0 + \delta$.

Fix $r_1 > c$, $r = r_1 + i\delta$ with $i \geqslant 0$, and an extension of σ to $\mathrm{Gal}(H_\infty/K)$. By [Con04, Lemma 2.4] or [SeTa69, Theorems 8, 9(1)] the point $h^\sigma_{s+r} \in X_0(N)(F(r))$ represents a Heegner diagram over $F(r)$ having good reduction, and so its Zariski closure $\underline{h}^\sigma_{s+r}$ in $X_0(N)_{/W(r)}$ is a section to the structure map representing a Heegner diagram over $W(r)$. As in § 4, the choice of Heegner diagram $\underline{h}^\sigma_{s+r}$ determines a family of isogenous Heegner diagrams over $W(r)$,

$$\underline{h}^\sigma_{s+r} \to \underline{h}^\sigma_{s+r-1} \to \cdots .$$

The generic geometric kernel of the map $\underline{h}^\sigma_{s+r} \to \underline{h}^\sigma_{s+r-1}$ is stable under the action of the absolute Galois group of $F(r)$, and the Euler system relations of § 1.2 tell us that no other order p subgroup of $\underline{h}^\sigma_{s+r}(F(r)^{\mathrm{alg}})$ has this property. Indeed, the remaining p quotients by order p subgroups are permuted simply transitively by $\mathrm{Gal}(F(r+1)/F(r))$. It follows that this kernel must be the kernel in $\underline{h}^\sigma_{s+r}[p]$ of reduction to $W(r)_0$ (recall $\epsilon(p) = 1$, so $\underline{h}^\sigma_{s+r}$ has ordinary reduction) and the map $\underline{h}^\sigma_{s+r} \to \underline{h}^\sigma_{s+r-1}$ reduces to the absolute Frobenius in the closed fiber. The action of $\mathcal{O}_{s+r}$ on the closed fiber of $\underline{h}^\sigma_{s+r}$ extends to an action of the maximal order (we have just shown that the closed fiber of $\underline{h}^\sigma_{s+r}$ is isomorphic to a Galois conjugate of the closed fiber of $\underline{h}^\sigma_0$), and if $\mathfrak{p}$ denotes the prime of K below v, then the action of any generator of the principal ideal $\mathfrak{p}^\delta$ is a degree p^δ purely inseparable endomorphism, whose kernel must therefore be the kernel of the δ^{th}-iterate of Frobenius. This shows that the Heegner diagrams $\underline{h}^\sigma_{s+r}$ and $\underline{h}^\sigma_{s+r-\delta}$ are isomorphic over $\mathrm{Spec}(W(r)_0)$, and that the closed fiber of $\underline{h}^\sigma_{s+r}$ is the base change to $W(r)$ of the closed fiber of the Zariski closure of $h^\sigma_{s+r_1}$ on $X_0(N)_{/W(r_1)}$.

We claim that the Heegner diagram $\underline{h}^\sigma_{s+r-\delta}$ is distinct from $\underline{h}^\sigma_{s+r}$ over $W(r)_1$, so that Proposition 4.0.5 gives the intersection formula

$$i(\underline{h}^\sigma_{s+r}, \underline{h}^\sigma_{s+r-\delta}) = \tfrac{1}{2}|\mathcal{O}_K^\times| = 1 \tag{20}$$

on $X_0(N)_{/W(r)}$. Indeed, if these Heegner diagrams are isomorphic over $W(r)_1$, then the reduction of such an isomorphism to $W(r)_0$ allows us to view $\underline{h}^\sigma_{s+r-\delta}$ and $\underline{h}^\sigma_{s+r}$ over $W(r)_1$ as isomorphic *deformations* of the common closed fiber, which we denote by g. Let $T = \varprojlim g(W(r)_0)[p^k] \cong \mathbb{Z}_p$. The theory of Serre–Tate coordinates (for example [Gor02, ch. 3, Theorem 4.2]) associates to these Heegner diagrams over $W(r)$ (viewed as deformations of g) two bilinear maps

$$q_{s+r-\delta}, q_{s+r} : T \otimes T \to 1 + \mathfrak{m}_{W(r)}.$$

The first surjects onto $\mu_{p^{s+r-\delta}}$, and the second onto $\mu_{p^{s+r}}$. Since we assume the Heegner diagrams over $W(r)_1$ are isomorphic as deformations of g, the bilinear maps $q_{s+r-\delta}, q_{s+r}$ are congruent modulo $1 + \mathfrak{m}^2_{W(r)}$. This is a contradiction, as $\mu_{p^{s+r-\delta}}$ is contained in $1 + \mathfrak{m}^2_{W(r)}$ while $\mu_{p^{s+r}}$ is not (use the fact, noted above, that $F(r) = \hat{\mathbb{Q}}_p^{\mathrm{unr}}(\mu_{p^{r+s}})$ to replace $\mathfrak{m}_{W(r)}$ with the maximal ideal of $\mathbb{Z}_p[\mu_{p^{r+s}}]$).

Each prime divisor $\underline{y}(k)$ occurring in the support of $\underline{C}$ either does not meet the common closed point of $\underline{h}^\sigma_{s+r-\delta}$, $\underline{h}^\sigma_{s+r}$, in which case $i(\underline{y}(k), \underline{h}^\sigma_{s+r}) = 0$, or it does, in which case $\underline{y}(k)$ intersects both $\underline{h}^\sigma_{s+r-\delta}$ and $\underline{h}^\sigma_{s+r}$. Assume we are in the latter case. The divisors $\underline{y}(k)$ and $\underline{h}^\sigma_{s+r-\delta}$ on $X_0(N)_{/W(r)}$ both arise as the base change of divisors defined over $W(r-\delta)$. Since base change through a finite extension multiplies intersections by the ramification degree, $i(\underline{y}(k), \underline{h}^\sigma_{s+r-\delta}) > 1$. If also $i(\underline{y}(k), \underline{h}^\sigma_{s+r}) > 1$, then $i(\underline{h}^\sigma_{s+r}, \underline{h}^\sigma_{s+r-\delta}) > 1$, contradicting (20). Thus $i(\underline{y}(k), \underline{h}^\sigma_{s+r}) = 1$. We have shown that

$$i(\underline{C}, \underline{\mathbf{h}}^\sigma_{s,r})_R = i(\underline{C}, \underline{h}^\sigma_{s+r})_{W(r)} = \sum_{k=0}^{e} i(\underline{y}(k), \underline{h}^\sigma_{s+r})_{W(r)}$$

(the subscripts denoting the bases over which the intersections are computed) is equal to the number of $\underline{y}(k)$, $0 \leqslant k \leqslant e$, which contain the closed point of $\underline{h}^\sigma_{s+r}$. By the discussion earlier this is equal to the number of $\underline{y}(k)$ on $X_0(N)_{/W(r_1)}$ which contain the closed point of the Zariski closure of $h^\sigma_{s+r_1}$ on $X_0(N)_{/W(r_1)}$, which is equal to $i(\underline{C}, \underline{\mathbf{h}}^\sigma_{s,r_1})_R$ by taking $r = r_1$ in the preceding argument. □

Let us say that a divisor C on $X_0(N)_{/H_{s,v}}$ has *good support* if its support contains no cusps except possibly for the cusp 0. Note that the set of such divisors is stable under the action of T^i_m for any m. This follows easily from the fact that the main Atkin–Lehner involution w on $X_0(N)$ satisfies $wT_m w = T^\iota_m$ and $w \cdot \infty = 0$, and that $T_m \cdot \infty$ is supported at ∞. For C of degree zero with good support we define a formal q-expansion

$$\phi(C)_v = \sum_{m=m_0p^r} \langle C, T_{m_0}\mathbf{d}^\sigma_{s,r}\rangle_v q^m \tag{21}$$

where $\langle\ ,\ \rangle_v$ is the p-adic Néron symbol on $X_0(N)_{/H_{s,v}}$ of Proposition 3.3.2, and where for any integer $m > 0$ we write $m = m_0p^r$ with $(m_0, p) = 1$. Let U denote the shift operator on formal q-expansions $U(\sum a_m q^m) = \sum a_{mp} q^m$. The q-expansion $\phi(C)_v$ is only defined if C has support prime to $T_{m_0}(\mathbf{d}^\sigma_{s,r})$ for every $m = m_0p^r$, but for any C with good support and degree 0 the q-expansion $U^k\phi(C)_v$ is defined for $k \gg 0$. Indeed, the geometric points in the support of $T_{m_0}(\mathbf{d}^\sigma_{s,r+k})$ each represent either the cusp ∞ or a CM elliptic curve such that the valuation at p of the conductor of the CM order is exactly $s + r + k$.

We can use the Lemma 6.1.1 to compute p-adic Néron symbols at v in the only case where they are known to be related to intersection pairings: the case where one divisor is principal.

Corollary 6.1.2. *Suppose C is the divisor of a rational function on $X_0(N)_{/H_{s,v}}$, and that C has good support. Then for each integer $m > 0$*

$$\lim_{k\to\infty} a_m(U^k(U^\delta - 1)\phi(C)_v) = 0.$$

Proof. Write $m = m_0p^r$ with $(m_0, p) = 1$. The divisor $T^\iota_{m_0}(C)$ is again principal with good support, and we fix a rational function f with $(f) = T^\iota_{m_0}(C)$. Writing v for the normalized valuation on $H_{s,v}$, the intersection theory of § 3.1 gives

$$v(f(\mathbf{d}^\sigma_{s,r+k+\delta})) = [(f), \mathbf{d}^\sigma_{s,r+k+\delta}] = i(\underline{(f)}, \underline{\mathbf{h}}^\sigma_{s,r+k+\delta})) - p^{r+k+\delta} \cdot i(\underline{(f)}, \underline{\infty}))$$

where the underlining of divisors indicates passing to horizontal divisors on $X_0(N)_{/R}$, R the integer ring of $H_{s,v}$. Similarly

$$v(f(\mathbf{d}^\sigma_{s,r+k})) = [(f), \mathbf{d}^\sigma_{s,r+k}] = i(\underline{(f)}, \underline{\mathbf{h}}^\sigma_{s,r+k})) - p^{r+k} \cdot i(\underline{(f)}, \underline{\infty})).$$

From this and Lemma 6.1.1 we deduce

$$\begin{aligned} v\left(\frac{f(\mathbf{h}^\sigma_{s,r+k+\delta})}{f(\mathbf{h}^\sigma_{s,r+k})}\right) &= v\left(\frac{f(\mathbf{d}^\sigma_{s,r+k+\delta})}{f(\mathbf{d}^\sigma_{s,r+k})}\right) + (p^\delta - 1)p^{r+k} \cdot v(f(\infty)) \\ &= (p^\delta - 1)p^{r+k} \cdot [v(f(\infty)) - i(\underline{(f)}, \underline{\infty})] \end{aligned}$$

for k large. Multiplying f by an element of $H^\times_{s,v}$ does not change (f), and so we may assume that $v(f(\infty)) = i(\underline{(f)}, \underline{\infty})$. Then $f(\mathbf{h}^\sigma_{s,r+k+\delta})/f(\mathbf{h}^\sigma_{s,r+k})$ is a unit in $H_{s,v}$ for k large. It is also the norm of some $u_k \in H_{s+r+k,v}$, the completion of H_{s+r+k} at the unique prime above v. Using Proposition 3.3.2(b)

$$\begin{aligned} a_m(U^k(U^\delta - 1)\phi(C)_v) &= \langle C, T_{m_0}\mathbf{d}^\sigma_{s,r+k+\delta}\rangle_v - \langle C, T_{m_0}\mathbf{d}^\sigma_{s,r+k}\rangle_v \\ &= \rho_{H_{s,v}}(f(\mathbf{d}^\sigma_{s,r+k+\delta})) - \rho_{H_{s,v}}(f(\mathbf{d}^\sigma_{s,r+k})) \\ &= \rho_{H_{s,v}}\left(\frac{f(\mathbf{h}^\sigma_{s,r+k+\delta})}{f(\mathbf{h}^\sigma_{s,r+k})}\right) - (p^\delta - 1)p^{r+k}\rho_{H_{s,v}}(f(\infty)) \\ &= \rho_{\mathbb{Q}_p}(\mathrm{Norm}_{H_{s+r+k,v}/\mathbb{Q}_p}(u_k)) - (p^\delta - 1)p^{r+k}\rho_{H_{s,v}}(f(\infty)). \end{aligned}$$

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

Since p is split, the field $H_{s+r+k,v}$ is abelian over $\mathbb{Q}_p$, the unit norms from $H_{s+r+k,v}$ to $\mathbb{Q}_p$ converge to 1 as $k\to\infty$, and so the final expression converges to 0. □

Given any point $P\in J_0(N)(H_{s,v})$ we may choose a degree zero divisor C on $X_0(N)_{/H_{s,v}}$ having good support which represents P. Corollary 6.1.2 implies that for any sequence of integers $b=(b_k)$ with $b_k\to\infty$, the q-expansion with $\mathbb{Q}_p$-coefficients

$$\Phi_b(P)_v \stackrel{\mathrm{def}}{=} \lim_{k\to\infty} U^{b_k}(U^\delta-1)\phi(C)_v,$$

if the limit exists (in the sense of coefficient-by-coefficient convergence; there is no assumption of uniformity) depends only on P and not on the choice of C.

Definition 6.1.3. A sequence of integers $b=(b_k)$ is *admissible* if $b_k\to\infty$ and if the limit (coefficient-by-coefficient) defining $\Phi_b(P)_v$ exists for every $P\in J_0(N)(H_{s,v})$.

Lemma 6.1.4. *Any sequence of integers tending to ∞ admits an admissible subsequence.*

Proof. Fix a sequence $b=(b_k)$ of integers tending to ∞. Let C be a degree zero divisor on $X_0(N)_{H_{s,v}}$ with good support, and consider the first Fourier coefficient

$$a_1(U^{b_k}(U^\delta-1)\phi(C)_v)=\langle C,\mathbf{d}^\sigma_{s,b_k+\delta}-\mathbf{d}^\sigma_{s,b_k}\rangle_v.$$

By the final claim of Proposition 3.3.2 the sequence on the right-hand side takes values in a compact subset of $\mathbb{Q}_p$, and so we may choose a convergent subsequence. By Corollary 6.1.2 and the finite dimensionality of $J_0(N)(H_{s,v})\otimes\mathbb{Q}_p$, we may repeat this process, eventually replacing b by a subsequence (still denoted b, abusively) such that

$$\lim_{k\to\infty} a_1(U^{b_k}(U^\delta-1)\phi(C)_v)$$

exists for every degree zero divisor with good support. By the same argument we may assume that the limit $\lim_{k\to\infty} a_p(U^{b_k}(U^\delta-1)\phi(C)_v)$ also exists for all such divisors. Now fix $m=m_0p^r$ with $(m_0,p)=1$. From the definition of ϕ we have

$$a_m(U^{b_k}(U^\delta-1)\phi(C)_v)=a_{p^r}(U^{b_k}(U^\delta-1)\phi(T^\iota_{m_0}C)_v) \tag{22}$$

(for k large enough that both sides are defined). If $r=0$ or 1, then the limit as $k\to\infty$ exists by the above choice of b. For $r>1$ we use the Euler system relations of § 1.2 to see that

$$\begin{aligned}\mathbf{d}^\sigma_{s,r+b_k}&=\mathrm{Norm}_{H_{s+b_k+1}/H_s}\mathbf{d}^\sigma_{s+b_k+1,r-1}\\&=\mathrm{Norm}_{H_{s+b_k+1}/H_s}(T_{p^{r-1}}d^\sigma_{s+b_k+1}-T_{p^{r-2}}d^\sigma_{s+b_k})\\&=T_{p^{r-1}}\mathbf{d}^\sigma_{s,b_k+1}-pT_{p^{r-2}}\mathbf{d}^\sigma_{s,b_k}\end{aligned}$$

which, together with the same formula with b_k replaced by $b_k+\delta$, implies that the right-hand side of (22) equals (for $k\gg 0$)

$$a_p(U^{b_k}(U^\delta-1)\phi(T^\iota_{m_0p^{r-1}}C)_v)-p\cdot a_1(U^{b_k}(U^\delta-1)\phi(T^\iota_{m_0p^{r-2}}C)_v),$$

and this limit exists as $k\to\infty$. □

Fix an admissible sequence b. Note that the above proof shows that

$$a_{mp}(\Phi_b(P)_v)=\begin{cases}a_p(\Phi_b(T^\iota_mP)_v) & \text{if } (m,p)=1\\ a_p(\Phi_b(T^\iota_mP)_v)-pa_1(\Phi_b(T^\iota_{m/p}P)_v) & \text{otherwise.}\end{cases} \tag{23}$$

Let $\mathbf{T}^{\mathrm{full}}$ denote the $\mathbb{Q}_p$-algebra generated by the Hecke operators T_m for all $m>0$ acting on $J_0(N)$. For any $P\in J_0(N)(H_{s,v})$ and any $i>0$, the linear functional on $\mathbf{T}^{\mathrm{full}}$ defined by $T\mapsto a_i(\Phi_b(T^\iota P)_v)$

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

determines a p-adic modular form

$$h_i(P) = \sum a_i(\Phi_b(T_m^\iota P)_v) \cdot q^m \in S_2(\Gamma_0(N), \mathbb{Q}) \otimes \mathbb{Q}_p$$

of level $\Gamma_0(N)$ (as does any linear functional on $\mathbf{T}^{\mathrm{full}}$; this follows from [Hid93, § 5.3 Theorem 1] and the identification of $\mathbf{T}^{\mathrm{full}}$ with the Hecke algebra acting on weight two cusp forms). The relation (23) can be written as

$$U \cdot \Phi_b(P)_v = h_p(P) - pV \cdot h_1(P)$$

where $V(\sum a_n q^n) = \sum a_n q^{pn}$. As V takes modular forms of level $\Gamma_0(N)$ to modular forms of level $\Gamma_0(Np)$, we may define

$$\Psi_b(P)_v = U \cdot \Phi_b(P)_v \in M_2(\Gamma_0(Np), \mathcal{A}) \otimes_{\mathcal{A}} \mathcal{B}$$

for any $P \in J_0(N)(H_{s,v})$.

6.2 Annihilation of E_σ

Recall Hida's ordinary projector $e^{\mathrm{ord}} = \lim_{k\to\infty} U^{k!}$ from § 2. Fix an admissible (in the sense of Definition 6.1.3, and for all primes above p simultaneously) subsequence $b = (b_k)$ of $k!$ and define, for any $P \in J_0(N)(H_s)$, a p-adic modular form $\Psi_b(P) = \sum_{v|p} \Psi_b(P)_v$ where the sum is over primes v of H_s above p. Similarly, define $\phi(C) = \sum_v \phi(C)_v$ (whenever $\phi(C)_v$ is defined for all v above p).

In the next section, we shall see that there is a modular form

$$E_\sigma \in M_2(\Gamma_0(Np^\infty), \mathcal{A}) \otimes \mathcal{B}$$

with the following property: if $\langle\ ,\ \rangle_p$ denotes the sum of the local p-adic Néron symbols on $X_0(N)_{/H_{s,v}}$ at the primes of H_s above p, then for any $m = m_0 p^r$ with $(m_0, Np) = 1$ the mth Fourier coefficient of E_σ is given by the expression

$$\begin{aligned} a_m(E_\sigma) &= \langle c_s, T_{m_0}(\mathbf{d}^\sigma_{s,r+2})\rangle_p - \langle c_{s-1}, T_{m_0}(\mathbf{d}^\sigma_{s,r+1})\rangle_p \\ &= a_{mp^2}(\phi(c_s)) - a_{mp}(\phi(c_{s-1})), \end{aligned}$$

where, as in § 0.1, $c_i = (h_i) - (0)$. From this we immediately deduce the following.

Lemma 6.2.1. *There is a modular form $g \in M_2(\Gamma_0(Np), \mathcal{A}) \otimes \mathcal{B}$ such that $a_m(g) = 0$ whenever $(m, N) = 1$, and*

$$(U^\delta - 1)e^{\mathrm{ord}} E_\sigma = U\Psi_b(c_s) - \Psi_b(c_{s-1}) + g.$$

Proof. Compare both sides coefficient by coefficient. □

The significance of Lemma 6.2.1 is the following: while E_σ depends *a priori* on the divisors c_s and c_{s-1}, the p-adic modular forms $\Psi_b(c_s)$ and $\Psi_b(c_{s-1})$ depend only on the images in $J_0(N)(H_s)$. This plays a crucial role in the proof of the following proposition.

Proposition 6.2.2. *Let f be the modular form fixed in the introduction. The p-adic modular form E_σ is annihilated by the linear functional L_f of Lemma 2.0.2.*

Proof. By Lemmas 2.0.2(c) and (d) and 6.2.1

$$(\alpha^\delta - 1)L_f(E_\sigma) = L_f((U^\delta - 1)e^{\mathrm{ord}} E_\sigma) = \alpha L_f(\Psi_b(c_s)) - L_f(\Psi_b(c_{s-1})),$$

and so it suffices to show that $L_f(\Psi_b(P)_v) = 0$ for every $P \in J_0(N)(H_s)$ and every prime v of H_s above p. Fix one such prime and let $\mathbf{T}$ be the $\mathbb{Q}$-algebra generated by all T_ℓ with $(\ell, N) = 1$ acting on $J_0(N)$. Recall from the introduction the decomposition

$$J_0(N)(H_s) \otimes \mathcal{B} \cong \bigoplus_\beta J(H_s)_\beta$$

where the sum is over all algebra homomorphisms $\beta : \mathbf{T} \to \mathbb{Q}_p^{\mathrm{alg}}$ (and recall that all such maps take values in $\mathcal{B}$ by hypothesis) and $\mathbf{T}$ acts on $J(H_s)_\beta$ through the character β. Let β_f be the homomorphism associated to the fixed newform f.

Suppose that $P \in J(H_s)_\beta$ for some character β, and extend $\Psi_b(\ )_v$ $\mathcal{B}$-linearly to $J_0(N)(H_s) \otimes \mathcal{B}$. We treat the cases $\beta \neq \beta_f$ and $\beta = \beta_f$ separately.

Lemma 6.2.3. *If $\beta \neq \beta_f$, then $L_f(\Psi_b(P)_v) = 0$.*

Proof. Use the notation $\tilde{T}_m$ for Hecke operators in level $\Gamma_0(Np)$. For any m prime to Np we have

$$a_m(f) L_f(\Psi_b(P)_v) = L_f(\tilde{T}_m \Psi_b(P)_v) = L_f(\Psi_b(T_m P)_v) = \beta(T_m) L_f(\Psi_b(P)_v)$$

(the first equality is by Lemma 2.0.2, the second is a straightforward calculation, and the third is obvious). Thus, if $L_f(\Psi_b(P)_v) \neq 0$, then $\beta_f(T_m) = \beta(T_m)$ for all $(m, Np) = 1$. The Atkin–Lehner strong multiplicity one theorem [AL70, Lemma 24] thus implies that $\beta_f = \beta$, a contradiction. □

Lemma 6.2.4. *If $\beta = \beta_f$, then $L_f(\Psi_b(P)_v) = 0$.*

Proof. We follow the lead of [PR87a, Example 4.12]. Let R be the integer ring of $H_{s,v}$, $\mathfrak{m}$ the maximal ideal of R, and $\mathbf{F} = R/\mathfrak{m}$. Let G_n be the p^n-torsion of the Néron model of $J_0(N)$ over R, a finite group scheme over R. Let G_n^0 and G_n^{et} be the connected component and maximal étale quotient of G_n, respectively, and let $G_n^{0,\mathrm{et}}$ (respectively $G_n^{0,0}$) be the maximal subgroup scheme of G_n^0 with étale dual (respectively quotient with connected dual).

By the theory of Dieudonné modules the Frobenius and Verschiebung morphisms on $(G_n^{0,0})_{/\mathbf{F}}$ are nilpotent, and so by the Eichler–Shimura congruence the same is true of the Hecke operator T_p. This is equivalent to $T_p^i(I) \subset \mathfrak{m}I$ for some i, where A is the Hopf algebra over R associated to the affine group scheme $G_n^{0,0}$, I is the kernel of the augmentation map $A \to R$, and T_p is now viewed as an R-algebra map $A \to A$. For any Artinian quotient $R/\mathfrak{m}^k R$ of R and any R-algebra map $\tau : A \to R/\mathfrak{m}^k R$,

$$(\tau \circ T_p^{ik})(I) \subset \tau(\mathfrak{m}^k I) = 0.$$

Back in the world of group schemes, this says that T_p acts as a nilpotent operator on $G_n^{0,0}(R/\mathfrak{m}^k)$ for any k and any n. From this it follows easily that T_p acts as a topologically nilpotent operator on R-valued points of the formal group scheme $\hat{G}^{0,0}$ associated to the p-divisible group $\varinjlim G_n^{0,0}$.

Let $\hat{G}^0$ and $\hat{G}^{0,\mathrm{et}}$ be the formal group schemes associated to G_n^0 and $G_n^{0,\mathrm{et}}$, respectively. As $\hat{G}^0(R) \subset J_0(N)(H_{s,v})$ with finite index, we may identify

$$\hat{G}^0(R) \otimes \mathcal{B} \cong J_0(N)(H_{s,v}) \otimes \mathcal{B}.$$

As $\beta_f(T_p) = a_p(f) \in \mathcal{A}^\times$ is a unit, any element of $\hat{G}^0(R) \otimes \mathcal{B}$ on which $\mathbf{T}$ acts through β_f must come from the subspace $\hat{G}^{0,\mathrm{et}}(R) \otimes_{\mathbb{Z}_p} \mathcal{B}$. We are thus reduced to the case $P \in \hat{G}^{0,\mathrm{et}}(R)$. By [Sch87, Theorem 1(i)] (together with the proof of [Sch87, Theorem 2]), the universal norms in $\hat{G}^{0,\mathrm{et}}(R)$ from any ramified $\mathbb{Z}_p$-extension of $H_{s,v}$ have finite index. We are thus further reduced to the case where $P \in J_0(N)(H_{s,v})$ is a universal norm from L_∞, the cyclotomic $\mathbb{Z}_p$-extension of $H_{s,v}$. Let $L_n \subset L_\infty$ be the extension of $H_{s,v}$ with $[L_n : H_{s,v}] = p^n$, and write $P = \mathbf{N}_{L_n/L_0} Q_n$ for some $Q_n \in J_0(N)(L_n)$. Lift Q_n to a degree zero divisor on $X_0(N)_{/L_n}$ with support prime to the cusps. Then for $m = m_0 p^r$ with $(m_0, p) = 1$,

$$\begin{aligned} a_m(\Psi_b(P)_v) &= \lim_{k \to \infty} a_m(U^{b_k+1}(U^\delta - 1)\phi(\mathbf{N}_{L_n/L_0} Q_n)_v) \\ &= \lim_{k \to \infty} \langle \mathbf{N}_{L_n/L_0} Q_n, T_{m_0} \mathbf{d}^\sigma_{s, b_k+1+\delta+r} - T_{m_0} \mathbf{d}^\sigma_{s, b_k+1+r} \rangle_{X_0(N), H_{s,v}}. \end{aligned}$$

Using Proposition 3.3.2(e), we at last deduce $\Psi_b(P)_v = 0$. □

This completes the proof of Proposition 6.2.2. □

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

Remark 6.2.5. The reader is invited to reconsider the case $\beta = \beta_f$ under the additional hypothesis that f is ordinary at *every* place of $\mathbb{Q}^{\mathrm{alg}}$ above p. Then the abelian variety (up to isogeny) A_f attached to f by Eichler–Shimura theory is ordinary at p, and a theorem of Mazur [Maz72, Proposition 4.39] tells us that the universal norm subgroup of $A_f(H_{s,v})$ from a ramified $\mathbb{Z}_p$-extension has finite index.

7. Completion of the proofs

Assume that D is odd and $\neq -3$, and that $\epsilon(p) = 1$. Fix $s > 0$ and $\sigma \in \mathrm{Gal}(H_s/K)$. Let $\mathfrak{a}$ be a proper integral $\mathcal{O}_s$-ideal of norm prime to p whose class in $\mathrm{Pic}(\mathcal{O}_s)$ represents σ. Recall from § 0.1 the p-adic modular form F_σ defined by

$$F_\sigma = U^2 F_\sigma^{s,s} - U F_\sigma^{s,s-1} - U F_\sigma^{s-1,s} + F_\sigma^{s-1,s-1} \in M_2(\Gamma_0(Np), \mathcal{A}) \otimes_{\mathcal{A}} \mathcal{B}.$$

Proposition 7.0.6. *For every $m = m_0 p^r$ with $(m_0, Np) = 1$,*

$$\begin{aligned} a_m(F_\sigma) &= \langle c_s, T_{mp^2}(d_s^\sigma)\rangle - \langle c_s, T_{mp}(d_{s-1}^\sigma)\rangle + \langle c_{s-1}, T_m(d_{s-1}^\sigma)\rangle - \langle c_{s-1}, T_{mp}(d_s^\sigma)\rangle \\ &= \langle c_s, T_{m_0}(\mathbf{d}_{s,r+2}^\sigma)\rangle - \langle c_{s-1}, T_{m_0}(\mathbf{d}_{s,r+1}^\sigma)\rangle. \end{aligned} \tag{24}$$

where $\langle\ ,\ \rangle = \langle\ ,\ \rangle_{X_0(N),H_s}$ is the global pairing of (10) viewed as a pairing on $J_0(N)(H_s)$, and c_s, d_s, $\mathbf{c}_{s,r}$, and $\mathbf{d}_{s,r}$ are as in § 0.1. Furthermore, extending the height pairing $\mathcal{B}$-bilinearly to $J_0(N)(H_s) \otimes \mathcal{B}$,

$$L_f(F_\sigma) = (\alpha^2 - 1)\alpha^{2s}\langle z_s, z_s^\sigma\rangle$$

where L_f is the linear functional on $M_2(\Gamma_0(Np^\infty), \mathcal{A})$ of Lemma 2.0.2 and z_s is the regularized Heegner point appearing in Theorem A.

Proof. Recall, for $i, j \leqslant s$ and any m, that

$$a_m(F_\sigma^{i,j}) = \sum_\beta \langle c_i, d_{j,\beta}^\sigma\rangle a_m(f_\beta)$$

where the sum is over algebra homomorphisms $\beta : \mathbf{T} \to \mathbb{Q}^{\mathrm{alg}}$, f_β is the associated primitive eigenform, and $d_{j,\beta}^\sigma$ is the projection of $d_j^\sigma \in J_0(N)(H_s)$ to $J(H_s)_\beta$. Thus, if $(m, N) = 1$,

$$a_m(F_\sigma^{i,j}) = \sum_\beta \langle c_i, \beta(T_m) d_{j,\beta}^\sigma\rangle = \sum_\beta \langle c_i, T_m d_{j,\beta}^\sigma\rangle = \langle c_i, T_m d_j^\sigma\rangle.$$

The first claim follows easily from this and the Euler system relations of § 1.2.

For the second claim,

$$L_f(F_\sigma) = \alpha^2 L_f(F_\sigma^{s,s}) - \alpha L_f(F_\sigma^{s,s-1}) - \alpha L_f(F_\sigma^{s-1,s}) + L_f(F_\sigma^{s-1,s-1})$$

by the final claim of Lemma 2.0.2. It follows from the same lemma that $L_f(f_\beta) = 0$ unless $f_\beta = f$ (as in the proof of Lemma 6.2.3), while $L_f(f) = 1 - \alpha^{-2}$. Therefore,

$$L_f(F_\sigma^{i,j}) = (1 - \alpha^{-2})\langle c_i, d_{j,f}^\sigma\rangle = (1 - \alpha^{-2})\langle d_{i,f}, d_{j,f}^\sigma\rangle$$

where the subscript f indicates projection to the component $J(H_s)_{\beta_f}$ of the algebra homomorphism $\beta_f : \mathbf{T} \to \mathbb{Q}^{\mathrm{alg}}$ associated to f, and the second equality uses the fact that $c_i - d_i = (\infty) - (0)$ is torsion in $J_0(N)(H_s)$ and that summands $J(H_s)_\beta$ are orthogonal for distinct β (an easy consequence of Proposition 3.3.2(c)). This gives

$$\begin{aligned} L_f(F_\sigma) &= (1 - \alpha^{-2})[\alpha^2\langle d_{s,f}, d_{s,f}^\sigma\rangle - \alpha\langle d_{s,f}, d_{s-1,f}^\sigma\rangle - \alpha\langle d_{s-1,f}, d_{s,f}^\sigma\rangle + \langle d_{s-1,f}, d_{s-1,f}^\sigma\rangle] \\ &= (1 - \alpha^{-2})\langle \alpha d_{s,f} - d_{s-1,f}, \alpha d_{s,f}^\sigma - d_{s-1,f}^\sigma\rangle \\ &= (\alpha^2 - 1)\langle \alpha^s z_s, \alpha^s z_s^\sigma\rangle \end{aligned}$$

as z_s was defined to be $\alpha^{-s}(d_{s,f} - \alpha^{-1} d_{s-1,f})$ (in the introduction we abusively confused h_i with $d_i = (h_i) - (\infty)$). □

As explained in § 0.1, in each of the pairings of (24) the divisors have disjoint supports, and so we may decompose $a_m(F_\sigma) = \sum_v a_m(F_\sigma)_v$ as a sum of local Néron symbols on $X_v = X_0(N) \times_{\mathbb{Q}} H_{s,v}$ by defining

$$a_m(F_\sigma)_v = \langle c_s, T_{m_0}(\mathbf{d}^\sigma_{s,r+2})\rangle_v - \langle c_{s-1}, T_{m_0}(\mathbf{d}^\sigma_{s,r+1})\rangle_v$$

where for each prime v of H_s, $\langle\ ,\ \rangle_v = \langle\ ,\ \rangle_{X_v, \rho_{H_{s,v}}}$ is the local Néron symbol of Proposition 3.3.2. We also define, for a rational prime ℓ, $a_m(F_\sigma)_\ell = \sum_{v|\ell} a_m(F_\sigma)_v$.

Proposition 7.0.7. *Suppose $(m, N) = 1$. Then*

$$\sum_{\ell \neq p} a_m(F_\sigma)_\ell = a_{mp^{2s}}(G_{\sigma\kappa}) - a_{mp^{2s+2}}(G_{\sigma\kappa}),$$

where G_σ is the p-adic modular form of Proposition 2.0.4.

Proof. For any $\ell \neq p$, Proposition 4.0.8 shows that $a_m(F_\sigma)_\ell = 0$ when $\epsilon(\ell) = 1$, while Propositions 5.3.1 and 5.4.1 give an explicit formula for $a_m(F_\sigma)_\ell$ when $\epsilon(\ell) \neq 1$. Corollary 2.0.7 gives an explicit formula for the right-hand side. □

Proof of Theorem A. If we define a p-adic modular form $E_\sigma \in M_2(\Gamma_0(Np^\infty), \mathcal{A}) \otimes_{\mathcal{A}} \mathcal{B}$ by

$$E_\sigma = F_\sigma - U^{2s}(1 - U^2) G_{\sigma\kappa},$$

then for every $m = m_0 p^r$ with $(m_0, Np) = 1$ Proposition 7.0.7 implies

$$a_m(E_\sigma) = \langle c_s, T_{m_0}(\mathbf{d}^\sigma_{s,r+2})\rangle_p - \langle c_{s-1}, T_{m_0}(\mathbf{d}^\sigma_{s,r+1})\rangle_p.$$

Proposition 6.2.2 now implies $L_f(E_\sigma) = 0$, and so

$$L_f(F_\sigma) = L_f(U^{2s}(1 - U^2) G_{\sigma\kappa}).$$

Applying Lemma 2.0.2(d) and Proposition 7.0.6

$$(\alpha^2 - 1)\alpha^{2s} \langle z_s, z_s^\sigma\rangle_{X_0(N), H_s} = \alpha^{2s}(1 - \alpha^2) L_f(G_{\sigma\kappa}).$$

Summing over σ and applying Proposition 2.0.4,

$$\sum_\sigma \eta(\sigma)\langle z_s, z_s^\sigma\rangle_{X_0(N), H_s} = -\sum_\sigma \eta(\sigma) L_f(G_{\sigma\kappa}) = -\log_p(\gamma_0)\eta(\kappa) \cdot \mathcal{L}_{f,1}(\eta)$$

for any character η of $\mathrm{Gal}(H_s/K)$. We now view z_s as an element of $J_0(N)(H_s) \otimes \mathcal{B}$, let $z_s^\vee$ be the image of z_s in $J_0(N)(H_s)^\vee \otimes \mathcal{B}$ under the canonical polarization, and switch to the height pairing $\langle\ ,\ \rangle_{J_0(N), H_s}$ of (9). Recalling Remark 3.3.1,

$$\sum_\sigma \eta(\sigma)\langle z_s^\vee, z_s^\sigma\rangle_{J_0(N), H_s} = \log_p(\gamma_0)\eta(\kappa) \cdot \mathcal{L}_{f,1}(\eta).$$

This completes the proof of Theorem A when $s > 0$. If η is a character of $\mathrm{Gal}(H_0/K)$, then we may view η as a character of $\mathrm{Gal}(H_s/K)$ for some $s > 0$, and this does not change the value of $\mathcal{L}_{f,1}(\eta)$. As the z_s and $z_s^\vee$ are norm compatible

$$\begin{aligned}\sum_{\sigma \in \mathrm{Gal}(H_s/K)} \eta(\sigma)\langle z_s^\vee, z_s^\sigma\rangle_{J_0(N), H_s} &= \sum_{\sigma \in \mathrm{Gal}(H_0/K)} \eta(\sigma)\langle z_s^\vee, z_0^\sigma\rangle_{J_0(N), H_s} \\ &= \sum_{\sigma \in \mathrm{Gal}(H_0/K)} \eta(\sigma)\langle z_0^\vee, z_0^\sigma\rangle_{J_0(N), H_0},\end{aligned}$$

so Theorem A also holds when $s = 0$. □

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press

Proof of Theorem B. If we show that

$$\langle y_s^\vee, y_s^\sigma \rangle_{E,H_s} = \langle z_s, z_s^\sigma \rangle_{J_0(N),H_s} \tag{25}$$

for any s then we are done, as Theorem A shows that the two sides of the equality of Theorem B agree on all finite-order characters. Implicit in this statement is that (25) holds for any choice of height pairing $\langle\ ,\ \rangle_{J_0(N),H_s}$ as in (9) (recall that the definition of (9) depends on the possibly noncanonical choice of the local symbol $\langle\ ,\ \rangle_{J_0(N)_v,\rho_{H_{s,v}}}$ of Proposition 3.2.1 for each place v above p, and that there is a unique choice of local symbol $\langle\ ,\ \rangle_{E_v,\rho_{H_{s,v}}}$ at every place v). Fix a prime v of H_s and define a $\mathbb{Q}_p$-valued symbol $\langle c, d\rangle$ on pairs of degree zero divisors on $E_v = E \times_{\mathbb{Q}} H_{s,v}$ with disjoint support (and d rational over $H_{s,v}$ point-by-point) by

$$\langle c, d\rangle = \frac{1}{n}\langle \phi^* c, \delta\rangle_{J_0(N)_v,\rho_{H_{s,v}}}$$

where δ is a zero cycle on $J_0(N)_v$ such that $n \cdot d = \phi_*\delta$ for some n (using the fact that $\phi_* : J_0(N)(H_{s,v}) \rightarrow E(H_{s,v})$ has finite cokernel). It can be shown that the symbol $\langle\ ,\ \rangle$ satisfies the properties of Proposition 3.2.1, and so must be the *unique* symbol $\langle\ ,\ \rangle_{E_v,\rho_{H_{s,v}}}$. From this one easily deduces the compatibility of the global symbols (9)

$$\langle c, \phi_* d\rangle_{E,H_s} = \langle \phi^* c, d\rangle_{J_0(N),H_s}$$

for $c \in E(H_s)$ and $d \in J_0(N)(H_s)$. The equality (25) is then obvious from the definition of y_s and $y_s^\vee$. □

ACKNOWLEDGEMENTS

The author thanks Dick Gross for several helpful conversations, Brian Conrad for helpful correspondence, and the anonymous referee for suggesting many improvements to an earlier draft of this article.

REFERENCES

AH03 A. Agboola and B. Howard, *Anticyclotomic Iwasawa theory of CM elliptic curves*, Preprint (2003).

AL70 A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(N)$, Math. Ann. **185** (1970), 134–160.

Ber95 M. Bertolini, *Selmer groups and Heegner points in anticyclotomic* $\mathbb{Z}_p$*-extensions*, Compositio Math. **99** (1995), 153–182.

BD96 M. Bertolini and H. Darmon, *Heegner points on Mumford–Tate curves*, Invent. Math. **126** (1996), 413–456.

Blo80 S. Bloch, *A note on height pairings, Tamagawa numbers, and the Birch and Swinnerton-Dyer conjecture*, Invent. Math. **58** (1980), 65–76.

Con04 B. Conrad, *Gross–Zagier revisited*, with an appendix by W. R. Mann, in *Heegner points and Rankin L-series*, eds H. Darmon and S.-W. Zhang, Math. Sci. Res. Inst. Publ., vol. 49 (Cambridge University Press, 2004), 67–163.

Cor02 C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), 495–523.

Cox89 D. Cox, *Primes of the form* $x^2 + ny^2$ (John Wiley & Sons, New York, 1989).

Gor02 E. Goren, *Lectures on Hilbert modular varieties and modular forms* (American Mathematical Society, New York, 2002).

Gro85 B. Gross, *Local heights on curves*, in *Arithmetic Geometry*, eds G. Cornell and J. Silverman (Springer, New York, 1985), 327–339.

GZ86 B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.

Hid85 H. Hida, *A p-adic measure attached to the zeta function associated with two elliptic modular forms I*, Invent. Math. **79** (1985), 159–195.

Hid93 H. Hida, *Elementary Theory of L-functions and Eisenstein Series*, London Mathematical Society Student Texts, vol. 26 (Cambridge University Press, 1993).

How04 B. Howard, *The Heegner point Kolyvagin system*, Compositio Math. **140** (2004), 1439–1472.

KM85 N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves* (Princeton University Press, Princeton, NJ, 1985).

La88 S. Lang, *Introduction to Arakelov theory* (Springer, Berlin, 1988).

Man04 W. R. Mann, *Elimination of quaternionic sums*, in *Heegner points and Rankin L-series*, eds H. Darmon and S.-W. Zhang, Math. Sci. Res. Inst. Publ., vol. 49 (Cambridge University Press, 2004), 139–163.

Maz72 B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

MR02 B. Mazur and K. Rubin, *Elliptic curves and class field theory*, in *Proc. International Congress of Mathematicians*, Beijing, 2002, vol. 2 (Higher Ed. Press, Beijing, 2002), 185–196.

Mil86 J. S. Milne, *Abelian varieties*, in *Arithmetic Geometry*, eds G. Cornell and J. Silverman (Springer, New York, 1985), 103–150.

Nek95 J. Nekovář, *On the p-adic height of Heegner cycles*, Math. Ann. **302** (1995), 609–686.

PR87a B. Perrin-Riou, *Points de Heegner et dérivées de fonctions L p-adiques*, Invent. Math. **89** (1987), 455–510.

PR87b B. Perrin-Riou, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), 399–456.

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), 1–32.

PR91 B. Perrin-Riou, *Théorie d'Iwasawa et hauteurs p-adiques (cas des variétés abéliennes)*, unpublished manuscript (1991).

PR92 B. Perrin-Riou, *Théorie d'Iwasawa et hauteurs p-adiques*, Invent. Math. **109** (1992), 137–185.

Sch87 P. Schneider, *Arithmetic of formal groups and applications I: Universal norm subgroups*, Invent. Math. **87** (1987), 587–602.

SeTa69 J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.

Vat02 V. Vatsal, *Uniform distribution of Heegner points*, Invent. Math. **148** (2002), 1–46.

Benjamin Howard howard@math.harvard.edu
Department of Mathematics, Harvard University, Cambridge, MA 02138, USA
Current address: Department of Mathematics, University of Chicago, Chicago, IL 60637, USA

https://doi.org/10.1112/S0010437X0500134X Published online by Cambridge University Press