Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications

Henri Darmon*

September 5, 2007

Contents

*Partly supported by CICMA and by an NSERC research grant.

Abstract

This article describes a conjectural p-adic analytic construction of global points on (modular) elliptic curves, points which are defined over the ring class fields of real quadratic fields. The resulting conjectures suggest that the classical Heegner point construction, and the theory of complex multiplication on which it is based, should extend to a variety of contexts in which the underlying field is not a CM field.

Introduction

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. It is now known (cf. [Wi], [TW], [BCDT]) that E is modular, so that $E(\mathbb{C})$ is equipped with a non-constant analytic uniformisation

$$\varphi : \mathcal{H}^*/\Gamma_0(N) \longrightarrow E(\mathbb{C}), \tag{1}$$

where $\mathcal{H}^* := \mathcal{H} \cup \mathbb{Q} \cup \{i\infty\}$ is the extended Poincaré upper half-plane, and $\Gamma_0(N) \subset \mathbf{PSL}_2(\mathbb{Z})$ is the usual Hecke congruence group, acting on $\mathcal{H}^*$ by Möbius transformations. The compact Riemann surface $\mathcal{H}^*/\Gamma_0(N)$ parametrizes pairs (A, C) where A is a (generalized) elliptic curve over $\mathbb{C}$ and $C \subset A(\mathbb{C})$ is a cyclic subgroup of order N. In this way $\mathcal{H}^*/\Gamma_0(N)$ is identified with the complex points of an algebraic curve $X_0(N)$ defined over $\mathbb{Q}$. The map φ of equation (1) is defined over $\mathbb{Q}$, in the sense that it arises, after extending scalars from $\mathbb{Q}$ to $\mathbb{C}$, from a morphism of algebraic curves defined over the rational numbers.

An important application of (1) arises from the theory of complex multiplication. More precisely, let $K \subset \mathbb{C}$ be an imaginary quadratic field and let τ be any point in $\mathcal{H} \cap K$. The set $\mathcal{O}$ of matrices in $T \in M_2(\mathbb{Z})$ which are upper-triangular modulo N and satisfy

$$T = 0 \quad \text{or} \quad T\tau = \tau \tag{2}$$

is isomorphic to an order in K (of conductor $\mathfrak{f}$, say) which can be identified with the endomorphism ring of the pair (A_τ, C_τ) attached to τ. The theory of complex multiplication asserts that this pair is defined over the ring class field H of K of conductor $\mathfrak{f}$. Hence the so-called *Heegner point* $P_\tau := \varphi(\tau) \in E(\mathbb{C})$ is defined over H as well. This remark enables the construction of a plentiful

supply of algebraic points on E, points which are defined over suitable ring class fields of imaginary quadratic fields.

The Heegner point construction is consistent with the Birch and Swinnerton-Dyer conjecture, in the following sense. The complex L-function $L(E/H, s)$ factors as a product

$$L(E/H, s) = \prod_{\chi} L(E/K, \chi, s), \tag{3}$$

where χ ranges over the complex characters $\mathrm{Gal}(H/K) \longrightarrow \mathbb{C}^\times$. The definition of $L(E/K, \chi, s)$ as an Euler product implies that

$$L(E/K, \chi, s) = L(E/K, \bar{\chi}, s). \tag{4}$$

At the same time, Rankin's method yields the analytic continuation and functional equation of the L-function $L(E/K, \chi, s)$ for each χ, relating the expressions $L(E/K, \chi, s)$ and $L(E/K, \bar{\chi}, 2-s)$. Assume for simplicity that the discriminant of K and the conductor $\mathfrak{f}$ are prime to N, which implies that all the primes dividing N are split in $K/\mathbb{Q}$. In this case the sign appearing in the functional equation is -1, so that, by parity considerations,

$$L(E/K, \chi, 1) = 0 \text{ for each } \chi : \mathrm{Gal}(H/K) \longrightarrow \mathbb{C}^\times. \tag{5}$$

It follows from (3) and (5) that

$$\mathrm{ord}_{s=1} L(E/H, s) \geq [H : K]. \tag{6}$$

The Birch and Swinnerton-Dyer conjecture leads to the expectation that

$$\mathrm{rank}(E(H)) \stackrel{?}{\geq} [H : K]. \tag{7}$$

It is believed that Heegner points account for the bulk of the growth of $\mathrm{rank}(E(H))$ as H varies over all ring class fields of K of discriminant prime to N. For example, calculations of the kind carried out by Gross and Zagier in [GZ] should prove that an equality in (6) implies that the Heegner points in $E(H)$ generate a subgroup of rank at least $[H : K]$. Under this hypothesis the work of Kolyvagin establishes an equality in (7), so that the Heegner points generate a finite index subgroup of $E(H)$.

Replacing K by a real quadratic field, one is confronted with many situations in which inequality (6) continues to hold. For example, suppose that

$N = pM$, where p is a prime which does not divide M. Let K be a real quadratic field in which p is inert and all primes ℓ dividing M are split. If H is any ring class field of K of conductor prime to N, then an argument identical to the one sketched above carries over to establish inequality (6). This is tantalising insofar as the theory of complex multiplication provides no handle on the problem of understanding inequality (7). In fact, no extension of the theory of complex multiplication to the context of real quadratic fields is known. The problem of supplying such a theory is intimately connected to Hilbert's 12th problem of constructing the class fields of real quadratic fields (or of more general number fields) by analytic means.

The main goal of this work is to formulate a conjectural (p-adic) analytic construction of global points in the Mordell-Weil groups of E over certain ring class fields of real quadratic fields, generalising the theory of complex multiplication presented above. For the convenience of the reader, the main steps in this construction, and the main theorems of this article, are summarised in the remainder of the introduction.

1. Integration on $\mathcal{H}_p \times \mathcal{H}$. Suppose now that $N = pM$, where M is a positive integer, and p is a prime not dividing M. Choose an Eichler $\mathbb{Z}[1/p]$-order R of level M in $M_2(\mathbb{Q})$. (These are all conjugate to each other.) To fix ideas, take from now on

$$R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}[1/p]) \text{ with } c \equiv 0 \pmod{M} \right\}. \tag{8}$$

Denote by $\Gamma \subset \mathbf{PSL}_2(\mathbb{Z}[1/p])$ the image of the group of elements of determinant 1 in $R^\times$. It acts by Möbius transformations both on the p-adic upper half-plane

$$\mathcal{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p) \tag{9}$$

and on the extended Poincaré upper half-plane $\mathcal{H}^*$. The induced diagonal action of Γ on $\mathcal{H}_p \times \mathcal{H}$ is discrete and discontinuous. The quotient $(\mathcal{H}_p \times \mathcal{H})/\Gamma$ is investigated in a series of works of Ihara (cf. for example [Ih1] and [Ih2]) where it is related to the special fiber of $X_0(M)$ in characteristic p. Stark [St] remarked that this quotient is formally analogous to a Hilbert modular surface.

Section 1 develops Stark's analogy by formulating a theory of integration of "differential two-forms" on the quotient $(\mathcal{H}_p \times \mathcal{H})/\Gamma$, and deriving a notion of p-adic periods associated to such forms. More precisely, it is explained

how a newform f_0 of weight 2 on $\Gamma_0(N)$ can be viewed as encoding the p-adic residues of a form ω of weight $(2,2)$ on $(\mathcal{H}_p \times \mathcal{H})/\Gamma$. If f_0 has rational Fourier coefficients (i.e., it arises from an elliptic curve E of conductor N) a so-called *double multiplicative integral* is defined, depending on a choice of a homomorphism from the Néron lattice of E to $\mathbb{Z}$:

$$\int\!\!\!\!\!\!\diagup_{\tau_1}^{\tau_2}\int_x^y \omega \in \mathbb{C}_p^\times, \quad \tau_1, \tau_2 \in \mathcal{H}_p, \quad x, y \in \mathbb{P}_1(\mathbb{Q}). \tag{10}$$

As stated in lemma 1.11 of section 1, this function of the variables τ_1, τ_2, x, y behaves formally "as if" ω were a Hilbert modular form of weight $(2,2)$ on $(\mathcal{H}_p \times \mathcal{H})/\Gamma$, even though the object ω is not defined independently of its periods.

2. Periods attached to split tori. Since E has conductor N and p divides N exactly, the curve E has multiplicative reduction at p. Let

$$\Phi_{\mathrm{Tate}} : \mathbb{C}_p^\times \longrightarrow E(\mathbb{C}_p) \tag{11}$$

be Tate's p-adic uniformisation attached to E over $\mathbb{C}_p$, and let $q \in p\mathbb{Z}_p$ denote the p-adic period attached to this uniformisation.

Let $K \simeq \mathbb{Q} \times \mathbb{Q}$ be the split quadratic algebra, and let $\Psi : K \longrightarrow M_2(\mathbb{Q})$ be a $\mathbb{Q}$-algebra embedding. Write $\bar{\Psi} : K^\times \longrightarrow \mathbf{PGL}_2(\mathbb{Q})$ for the natural homomorphism induced by Ψ. The torus $\bar{\Psi}(K^\times)$ acting on the extended upper half plane $\mathcal{H}^*$ has exactly two fixed points $x_\Psi, y_\Psi \in \mathbb{P}_1(\mathbb{Q})$. The group $\bar{\Psi}(K^\times) \cap \Gamma$ is free of rank one, generated by an element γ_Ψ. A p-adic period $I_\Psi \in \mathbb{C}_p^\times$ is associated to Ψ by choosing a point $z \in \mathcal{H}_p$ and setting

$$I_\Psi := \int\!\!\!\!\!\!\diagup_z^{\gamma_\Psi z}\int_{x_\Psi}^{y_\Psi} \omega. \tag{12}$$

It is shown in lemma 2.3 of section 2 that I_Ψ does not depend on the choice of z that was made to define it, and that it belongs to $\mathbb{Q}_p^\times$.

Let $\mathrm{ord}_p : \mathbb{C}_p^\times \longrightarrow \mathbb{Q}$ be the valuation at p normalised so that $\mathrm{ord}_p(p) = 1$, and let $\log : \mathbb{C}_p^\times \longrightarrow \mathbb{C}_p$ be any choice of p-adic logarithm. In section 2 the following identity is proved

Theorem 1

$$\log(I_\Psi) = \frac{\log(q)}{\mathrm{ord}_p(q)} \mathrm{ord}_p(I_\Psi).$$

The proof of this theorem proceeds by evaluating both expressions $\mathrm{ord}_p(I_\Psi)$ and $\log(I_\Psi)$ independently. The quantity $\mathrm{ord}_p(I_\Psi)$ is related to special values of certain partial L-functions attached to $E/\mathbb{Q}$, while $\log(I_\Psi)$ is expressed in terms of the first derivative of the corresponding p-adic L-function. Viewed in this way theorem 1 becomes a reformulation of a conjecture of Mazur, Tate and Teitelbaum [MTT] that was proved by Greenberg and Stevens [GS].

To allow for a cleaner statement of the conjectures and results, the following assumption on E is made from now on throughout the article:

Assumption 2 *The elliptic curve E is unique in its $\mathbb{Q}$-isogeny class.*

The following conjecture, a multiplicative refinement of theorem 1, relates the period I_Ψ directly to q:

Conjecture 3 *The period I_Ψ belongs to $q^{\mathbb{Z}}$.*

Remarks:

1. Theorem 1 implies that the group $I_\Psi^{\mathbb{Z}} \subset \mathbb{Q}_p^\times$ is either finite or is a lattice commensurable with $q^{\mathbb{Z}}$. More precisely, it follows from this theorem that

$$I_\Psi^{\mathrm{ord}_p(q)} = q^{\mathrm{ord}_p(I_\Psi)} \pmod{(\mathbb{Q}_p^\times)_{\mathrm{tors}}} \tag{13}$$

To prove conjecture 3 in its entirety, it remains to:

- show that $\mathrm{ord}_p(q)$ divides $\mathrm{ord}_p(I_\Psi)$, so that

$$I_\Psi = q^n \pmod{(\mathbb{Q}_p^\times)_{\mathrm{tors}}}, \quad \text{with } n = \mathrm{ord}_p(I_\Psi)/\mathrm{ord}_p(q). \tag{14}$$

  Some theoretical evidence for this divisibility is given in [BD7], using multiplicity-one results of Mazur, the level-lowering result of Ribet, and the theory of Wiles yielding an isomorphism between certain Hecke rings and deformation rings. Alternately, as explained in section 2, much of the divisibility of $\mathrm{ord}_p(I_\Psi)$ by $\mathrm{ord}_p(q)$ can be derived as a consequence of the Birch and Swinnerton-Dyer conjecture.

- remove the $(\mathbb{Q}_p^\times)_{\mathrm{tors}}$-indeterminacy in formula (14). In the case where $M = 1$, de Shalit's multiplicative refinement [DS] of the result of Greenberg and Stevens can be used to remove a large part of this indeterminacy. There is every reason to expect that the assumption $M = 1$ in [DS] is not essential, so that a full proof of conjecture 3, while not present in the literature, should lie within the scope of the methods developed in [GS] and [DS].

2. Note the analogy of conjecture 3 with the results of Oda [O] concerning periods on the Hilbert modular surface attached to a real quadratic field.

3. The Cohomology of Γ. An M-symbol with values in an abelian group C is a function $m : \mathbb{P}_1(\mathbb{Q}) \times \mathbb{P}_1(\mathbb{Q}) \longrightarrow C$, denoted $(x, y) \mapsto m\{x \to y\}$ and satisfying

$$m\{x \to y\} + m\{y \to z\} = m\{x \to z\}, \qquad m\{x \to y\} = -m\{y \to x\}, \tag{15}$$

for all $x, y, z \in \mathbb{P}_1(\mathbb{Q})$. Denote by $\mathcal{M}$ the group of $\mathbb{C}_p$-valued M-symbols, and by $\mathcal{M}(C)$ the group of C-valued M-symbols. The group $\mathbf{PSL}_2(\mathbb{Q})$ (and hence, Γ) acts on $\mathcal{M}(C)$ by the rule

$$(\gamma m)\{x \to y\} := m\{\gamma^{-1}x \to \gamma^{-1}y\}. \tag{16}$$

Choose $\tau \in \mathcal{H}_p$ and $x \in \mathbb{P}_1(\mathbb{Q})$. The double multiplicative integral of equation (10) gives rise to a one-cocycle $\tilde{c}_{f,\tau} \in Z^1(\Gamma, \mathcal{M}(\mathbb{C}_p^\times))$ by the rule

$$\tilde{c}_{f,\tau}(\gamma)\{x \to y\} = \int\!\!\!\!\!\!\diagup_{\tau}^{\gamma\tau} \int_x^y \omega. \tag{17}$$

The natural image c_f of $\tilde{c}_{f,\tau}$ in $H^1(\Gamma, \mathcal{M}(\mathbb{C}_p^\times))$ is independent of the choice of τ that was made to define it.

Basic facts about the structure of $H^1(\Gamma, \mathcal{M})$ as a module over the Hecke algebra show that the classes

$$\mathrm{ord}_p(c_f) \in H^1(\Gamma, \mathcal{M}(\mathbb{Q})) \subset H^1(\Gamma, \mathcal{M}) \tag{18}$$

and

$$\log(c_f) \in H^1(\Gamma, \mathcal{M}) \tag{19}$$

belong to the same one-dimensional $\mathbb{C}_p$-vector subspace of $H^1(\Gamma, \mathcal{M})$. Theorem 1 is used to conclude:

Theorem 4

$$\log(c_f) = \frac{\log(q)}{\mathrm{ord}_p(q)} \mathrm{ord}_p(c_f).$$

Conjecture 3 suggests the following multiplicative refinement of theorem 4.

Conjecture 5 *Let $L = \mathbb{Q}_p(\tau)$ be the field generated over $\mathbb{Q}_p$ by τ. There exists a one-cocycle $\tilde{e}_{f,\tau} \in Z^1(\Gamma, \mathcal{M}(\mathbb{Z}))$ and an M-symbol $\tilde{\eta}_{f,\tau} \in \mathcal{M}(L^\times)$ satisfying the relation*

$$\tilde{c}_{f,\tau}(\gamma)\{x \to y\} = q^{\tilde{e}_{f,\tau}(\gamma)\{x\to y\}} \times \left(\tilde{\eta}_{f,\tau}\{\gamma^{-1}x \to \gamma^{-1}y\} \div \tilde{\eta}_{f,\tau}\{x \to y\}\right), \quad (20)$$

for all $\gamma \in \Gamma$ and $x, y \in \mathbb{P}_1(\mathbb{Q})$.

Remark:
1. Note that the image e_f of $\tilde{e}_{f,\tau}$ in $H^1(\Gamma, \mathcal{M}(\mathbb{Q}))$ is determined by the property

$$\mathrm{ord}_p(c_f) = \mathrm{ord}_p(q)e_f. \quad (21)$$

2. The proofs of theorems 1 and 4 make no use of assumption 2, so these results hold without this assumption. On the other hand, computer calculations carried out by Peter Green [DG] indicate that conjecture 5 is false in general in the absence of assumption 2.

Let $\eta_{f,\tau}$ be the natural image of $\tilde{\eta}_{f,\tau}$ in $\mathcal{M}(L^\times/q^{\mathbb{Z}})$. Reducing equation (20) of conjecture 5 modulo $q^{\mathbb{Z}}$ yields

$$\oint_\tau^{\gamma\tau}\int_x^y \omega = \eta_{f,\tau}\{\gamma^{-1}x \to \gamma^{-1}y\} \div \eta_{f,\tau}\{x \to y\} \pmod{q^{\mathbb{Z}}}. \quad (22)$$

Note that this relation makes $\eta_{f,\tau}$ well-defined up to multiplication by elements in $H^0(\Gamma, \mathcal{M}(L^\times/q^{\mathbb{Z}}))$.

To avoid certain technical complications that will receive due treatment in chapter 3.3, assume for the rest of the introduction that $M = 1$; in this case the group $H^0(\Gamma, \mathcal{M}(L^\times/q^{\mathbb{Z}}))$ vanishes, so that $\eta_{f,\tau} \in \mathcal{M}(L^\times/q^{\mathbb{Z}})$ is uniquely determined by (22). Thus conjecture 5 makes it possible to define, for all $x, y \in \mathbb{P}_1(\mathbb{Q})$, the *indefinite multiplicative integral*

$$\oint_x^{\tau}\int_x^y \omega := \eta_{f,\tau}\{x \to y\} \in L^\times/q^{\mathbb{Z}}. \quad (23)$$

This indefinite integral satisfies the basic multiplicativity and Γ-equivariance properties stated in lemma 3.7 of section 3 (with $Q = q^{\mathbb{Z}}$).

The last two sections (sections 4 and 5) are devoted to studying certain p-adic periods in $\mathbb{C}_p^\times$ associated to an embedding

$$\Psi : K \longrightarrow M_2(\mathbb{Q}) \quad (24)$$

of a quadratic étale algebra K into $M_2(\mathbb{Q})$, the case $K = \mathbb{Q}\times\mathbb{Q}$ corresponding to the situation already studied in section 2. An analogous setting in which K is an imaginary quadratic field, falling somewhat outside the scope of the machinery developed above, has been explored implicitly in [BD2], using the theory of complex multiplication and some facts about the bad reduction of modular curves. Sections 4 and 5 concentrate on the case where K is a real quadratic field.

4. Periods attached to real quadratic fields. Suppose that the prime p splits in the real quadratic field K. Choose $\tau \in \mathcal{H}_p$ and $x \in \mathbb{P}_1(\mathbb{Q})$. Given $\alpha, \beta \in \bar{\Psi}(K^\times) \cap \Gamma$, the quantity

$$\langle \alpha, \beta \rangle_\Psi := \int\!\!\!\!\!\!\diagup_\tau^{\alpha^{-1}\tau} \int_x^{\beta x} \omega \div \int\!\!\!\!\!\!\diagup_\tau^{\beta^{-1}\tau} \int_x^{\alpha x} \omega \tag{25}$$

is proven in section 4 to be independent of the choice of $\tau \in \mathcal{H}_p$ and $x \in \mathbb{P}_1(\mathbb{Q})$ that is made to define it. Moreover, $\langle\ ,\ \rangle_\Psi$ defines a $\mathbb{C}_p^\times$-valued alternating bilinear pairing on $\bar{\Psi}(K^\times) \cap \Gamma$.

The group $\bar{\Psi}(K^\times) \cap \Gamma$ is a free $\mathbb{Z}$-module of rank two. Let γ_1 and $\gamma_2 \in \Gamma$ be $\mathbb{Z}$-module generators for this group. The period $I_\Psi \in \mathbb{C}_p^\times$ attached to Ψ is defined by setting

$$I_\Psi := \langle \gamma_1, \gamma_2 \rangle_\Psi. \tag{26}$$

Note that $\{I_\Psi, I_\Psi^{-1}\}$ is independent of the choice of basis (γ_1, γ_2). Theorem 6 below expresses I_Ψ in terms of the Tate period for E. More precisely, theorem 4 is shown to imply the analogue of theorem 1 for the real quadratic field K:

Theorem 6 *If I_Ψ is the period attached to Ψ as in (26), then*

$$\log(I_\Psi) = \frac{\log(q)}{\mathrm{ord}_p(q)} \mathrm{ord}_p(I_\Psi).$$

Furthermore, if conjecture 5 holds, then I_Ψ belongs to $q^{\mathbb{Z}}$.

This identity should be viewed as the counterpart of the Greenberg-Stevens formula for real quadratic fields. See [BD6], where the connection of I_Ψ with special values of L-functions attached to E/K is briefly discussed.

5. Heegner points attached to real quadratic fields. The most intriguing application of the formalism of p-adic period integrals arises when the prime p is inert in the real quadratic field K, so that the p-adic completion

K_p of K is isomorphic to the quadratic unramified extension of $\mathbb{Q}_p$. In that case certain periods $J_\Psi \in K_p^\times/q^{\mathbb{Z}}$ attached to Ψ (whose definition relies on the validity of conjecture 5) are predicted to give rise to global points on E defined over the ring class fields of K, in a manner analogous to the classical Heegner point construction when K is imaginary quadratic.

To describe J_Ψ precisely, note first that the torus $\Psi(K^\times)$ acting on $\mathcal{H}_p$ has precisely two fixed points z_Ψ and $\bar{z}_\Psi$, which belong to $\mathbb{P}_1(K_p) - \mathbb{P}_1(\mathbb{Q}_p) \subset \mathcal{H}_p$ and are interchanged by the action of $\mathrm{Gal}(K_p/\mathbb{Q}_p)$. The group $\bar{\Psi}(K^\times) \cap \Gamma$ is free of rank one, with a generator γ_Ψ of the form $\bar{\Psi}(u)$, where u is an appropriate power of the fundamental unit attached to K.

The period $J_\Psi \in K_p^\times/q^{\mathbb{Z}}$ is defined by choosing a base point $x \in \mathbb{P}_1(\mathbb{Q})$ and using the indefinite integral of (23) to set

$$J_\Psi := \not\int_x^{z_\Psi} \int_x^{\gamma_\Psi x} \omega \in K_p^\times/q^{\mathbb{Z}}. \tag{27}$$

Section 5 shows that J_Ψ does not depend on the choice of $x \in \mathbb{P}_1(\mathbb{Q})$ that was made to define it, and that it depends in fact only on the Γ-conjugacy class of Ψ.

The algebra $\Psi(K) \cap R$ is isomorphic to a $\mathbb{Z}[1/p]$-order in K. Let $\mathfrak{f}_\Psi$ be the conductor of this order, and denote by H^+ the narrow ring class field of K of conductor $\mathfrak{f}_\Psi$, defined as in section 5.2. Since p is inert in $K/\mathbb{Q}$ and does not divide $\mathfrak{f}_\Psi$, it splits completely in H^+/K. Choose an embedding of H^+ into K_p. The main conjecture of section 5 (and, indeed, of the entire paper) is

Conjecture 7 *The local point*

$$P_\Psi := \Phi_{\mathrm{Tate}}(J_\Psi) \in E(K_p)$$

is a global point in $E(H^+)$.

Conjecture 7 extends the repertoire of modular constructions of rational points on elliptic curves beyond the currently known methods, which are all based on the theory of complex multiplication. The possibility of this construction, foreshadowed in [Da2], is directly inspired by the main theorem of [BD3]. But a proof would appear to fall beyond the scope of the methods used in that article, where the theory of complex multiplication and the Cerednik-Drinfeld theory of p-adic uniformisation of Shimura curves play a central role.

Section 5 refines conjecture 7 by formulating a conjectural generalized Shimura Reciprocity Law describing the action of $\mathrm{Gal}(H^+/K)$ on P_Ψ. After a brief discussion of the expected relation between the points P_Ψ and derivatives of L-series, in the spirit of the formula of Gross and Zagier, the article concludes by presenting some numerical evidence for conjecture 7 and its refinements.

Acknowledgements. Several insights gleaned over the years in exchanges with Massimo Bertolini and Adrian Iovita have been instrumental in developing the point of view that is formulated here. It is a pleasure to acknowledge a considerable debt to these two collaborators. The author also thanks the participants of the undergraduate seminar on complex multiplication and real quadratic fields held at McGill in the summer of 2000: Derrick Chung, Jack Fearnley, Peter Green, Chiu-Fan Lee, Ivo Panyatov and Dan Segal. In particular, the implementation by Green, with the assistance of Fearnley, Lee and Panyatov, of a package of routines in Pari and C for calculating the p-adic integrals defined in section 1 has yielded a wealth of numerical evidence for conjecture 7. Some corrections and refinements of the conjectures formulated in a first draft of this article emerged in later discussions with Peter Green. While the fruit of these exchanges will be discussed more fully in [DG], some of Green's observations have found their way into the revision of this article. Finally, the author is grateful to the referee for a thorough review of the original manuscript which has led to significant improvements in the exposition.

The author's research was supported by CICMA and by grants from NSERC and FCAR. The participants of the McGill seminar on complex multiplication and real quadratic fields were supported by NSERC USR (Undergraduate Summer Research) awards.

1 Integration on $(\mathcal{H}_p \times \mathcal{H})/\Gamma$

1.1 Forms on $\mathcal{T} \times \mathcal{H}$

Let $\mathcal{T}$ be the Bruhat-Tits tree of $\mathbf{PGL}_2(\mathbb{Q}_p)$. Its set $\mathcal{V}(\mathcal{T})$ of vertices is identified with the set of $\mathbb{Q}_p^\times$-homothety classes of rank two $\mathbb{Z}_p$-modules in $\mathbb{Q}_p^2$, two vertices being joined by an edge if the corresponding homothety classes have representatives which are contained in each other with index p.

Write $\mathcal{E}(\mathcal{T})$ for the set of ordered edges of $\mathcal{T}$, and denote by $s(e)$ and $t(e)$ respectively the source and target vertex of $e \in \mathcal{E}(\mathcal{T})$.

The group $\mathbf{PGL}_2(\mathbb{Q}_p)$ acts naturally on $\mathcal{T}$ by isometries. The stabiliser of a vertex is conjugate to $\mathbf{PGL}_2(\mathbb{Z}_p)$ while the stabiliser of an edge is conjugate to the group

$$\Gamma_0(p\mathbb{Z}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{PGL}_2(\mathbb{Z}_p) \text{ such that } p|c \right\}. \tag{28}$$

Let v_* be the distinguished vertex corresponding to the homothety class of $\mathbb{Z}_p^2 \subset \mathbb{Q}_p^2$, whose stabiliser is equal to $\mathbf{PGL}_2(\mathbb{Z}_p)$. Let e_* be the edge whose source is v_* and whose stabiliser is equal to $\Gamma_0(p\mathbb{Z}_p)$. Note that the stabiliser of v_* in Γ is equal to $\Gamma_0(M)$, while the stabiliser of e_* in Γ is equal to $\Gamma_0(N)$.

Recall (cf. [GvdP]) the reduction map

$$\mathrm{red} : \mathcal{H}_p \longrightarrow \mathcal{T} \tag{29}$$

from $\mathcal{H}_p$ to the Bruhat-Tits tree $\mathcal{T}$ of $\mathbf{PGL}_2(\mathbb{Q}_p)$. The inverse image of each open edge $e \in \mathcal{E}(\mathcal{T})$ is called a *basic wide open annulus* in $\mathcal{H}_p$, while the inverse image of a vertex is an example of an affinoid subdomain of $\mathcal{H}_p$. If e is an edge of $\mathcal{T}$, the orientation on it determines an orientation of the associated annulus V_e, i.e., an "interior" B_0 and an "exterior" B_∞. (The reversed edge $\bar{e}$ obtained from e by interchanging source and target gives rise to the same annulus V_e, but the interior and exterior p-adic discs attached to e and $\bar{e}$ are exchanged.) Choose a coordinate function z_e on $\mathbb{P}_1(\mathbb{C}_p)$ which induces the identifications

$$V_e \stackrel{\simeq}{\to} \{z \in \mathcal{H}_p : 1/p < |z|_p < 1\}, \quad B_0 \stackrel{\simeq}{\to} \{z \in \mathbb{C}_p : |z|_p \leq 1/p\}. \tag{30}$$

This coordinate function is well-defined, up to multiplication by an element of $\mathcal{O}_{\mathbb{C}_p}^\times$. (For further background on $\mathcal{T}$ and its relation to $\mathcal{H}_p$, the reader is invited to consult [Kl] or [GvdP] for example.)

Digression on p-adic modular forms. For this paragraph, replace Γ temporarily by a subgroup of $\mathbf{PSL}_2(\mathbb{Q}_p)$ acting *discretely* on $\mathcal{H}_p$. (Arithmetic groups of this type can be obtained from the unit groups of $\mathbb{Z}[1/p]$ orders of *definite* quaternion algebras B which are split at p, after choosing an identification of $B \otimes \mathbb{Q}_p$ with $M_2(\mathbb{Q}_p)$; see for example [BD1] or [BDIS].)

Following [Sch], a rigid-analytic modular form of weight 2 on $\mathcal{H}_p/\Gamma$ is defined to be a rigid-analytic function f on $\mathcal{H}_p$ satisfying

$$f(\frac{az+b}{cz+d}) = (cz+d)^2 f(z), \quad \text{for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, \quad z \in \mathcal{H}_p. \tag{31}$$

The coefficient of dz_e/z_e in the Mittag-Leffler expansion of f on the affinoid B_0 is called the *residue* of f at e and is denoted $\mathrm{res}_e(f(z)dz)$. (Cf. [Sch], p. 224.)

Lemma 1.1 *The function $\kappa_f : \mathcal{E}(\mathcal{T}) \longrightarrow \mathbb{C}_p$ defined by $\kappa_f(e) = res_e(f(z)dz)$ is* harmonic*, i.e.,*

$$\kappa_f(\bar{e}) = -\kappa_f(e) \text{ for all } \ e \in \mathcal{E}(\mathcal{T}), \quad \sum_{s(e)=v} \kappa_f(e) = 0, \ \textit{for all } v \in \mathcal{V}(\mathcal{T}).$$

This lemma follows from a rigid analytic analogue of the classical residue theorem of complex analysis, and is explained in [Sch], p. 225.

Returning to the case where Γ is the subgroup of $\mathbf{SL}_2(\mathbb{Q}_p)$ of the introduction, the objects of definition (31) become trivial, since Γ acts on $\mathcal{H}_p$ with dense orbits. Motivated by an analogy with the theory of Hilbert modular forms, it seems desirable to replace rigid analytic modular forms on $\mathcal{H}_p/\Gamma$ by an appropriate notion of "form of weight $(2,2)$ on $(\mathcal{H}_p \times \mathcal{H})/\Gamma$". Such an object should be a Γ-invariant expression of the form $\omega = f(z_p, z)dz_p dz$, where z_p is a p-adic and z a complex variable. The function f would be rigid analytic in the first variable and holomorphic in the second. While it is unclear from the outset how to supply a sensible definition of ω, it is still possible to intuit a rigorous definition for its *p-adic residues*. More precisely, imagine taking the Mittag-Leffler expansion of ω on affinoid subdomains of $\mathcal{H}_p$ (leaving aside for the moment the problem that ω has not been defined!). The coefficient of dz_e/z_e in such an expansion – the residue $\mathrm{res}_e(\omega)$ – should be interpreted as a holomorphic differential form on $\mathcal{H}$. This informal discussion leads to the following precise definition, motivated by lemma 1.1 and tailored to capture the notion of the "p-adic residues of ω".

Definition 1.2 *A cusp form of weight 2 on $(\mathcal{T} \times \mathcal{H})/\Gamma$ is a function*

$$f : \mathcal{E}(\mathcal{T}) \times \mathcal{H} \longrightarrow \mathbb{C}$$

satisfying

1. *$f(\gamma e, \gamma z) = (cz+d)^2 f(e,z)$, for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.*
2. *The function f is* harmonic*, i.e., for each vertex v of $\mathcal{T}$,*

$$\sum_{s(e)=v} f(e,z) = 0,$$

and for each edge e of $\mathcal{T}$, $f(\bar{e},z) = -f(e,z)$.

3. *For each edge e of $\mathcal{T}$, the function $f_e(z) := f(e,z)$ is a cusp form of weight 2 (in the usual sense) on the group $\Gamma_e := \mathrm{Stab}_\Gamma(e)$.*

Since Γ acts transitively on the unoriented edges of $\mathcal{T}$, the group Γ_e is conjugate in Γ to $\Gamma_{e_*} = \Gamma_0(N)$, for each e. Property 1 is suggested by the desired Γ-invariance of ω, and property 2 by lemma 1.1 arising from the p-adic residue theorem. Note that an element of the space $S_2(\mathcal{T},\Gamma)$ of cusp forms of weight 2 on $(\mathcal{T}\times\mathcal{H})/\Gamma$ is completely described by a collection $\{f_e\}$ of cusp forms on Γ_e, indexed by the edges e of $\mathcal{T}$, satisfying the compatibility relation

$$f_{\gamma e}(\gamma z)d(\gamma z) = f_e(z)dz, \text{ for all } \gamma \in \Gamma, \tag{32}$$

together with the harmonicity condition 2.

In analysing the structure of $S_2(\mathcal{T},\Gamma)$ it is convenient to introduce other spaces of modular forms defined in an analogous way. Let $\tilde{\Gamma}$ be the image in $\mathbf{PGL}_2(\mathbb{Q}_p)$ of $R_+^\times$, the group of invertible matrices in R whose determinant is positive. The group Γ consists of all the elements in $\tilde{\Gamma}$ such that

$$|\gamma| := \mathrm{ord}_p(\det(\gamma)) = 0 \quad (\text{in } \mathbb{Z}/2\mathbb{Z}), \tag{33}$$

so that $\tilde{\Gamma}$ contains Γ with index 2.

Let $S_2(\mathcal{E},\tilde{\Gamma})$ denote the space of *cusp forms on* $(\mathcal{E}(\mathcal{T})\times\mathcal{H})/\tilde{\Gamma}$, defined as the functions

$$f : \mathcal{E}(\mathcal{T})\times\mathcal{H} \longrightarrow \mathbb{C}$$

satisfying the analogues of properties 1 and 3 of definition 1.2, but not necessarily property 2, and with Γ replaced by $\tilde{\Gamma}$:

1. $f(\gamma e, \gamma z) = \frac{(cz+d)^2}{\det(\gamma)} f(e,z)$, for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \tilde{\Gamma}$.
2. For each edge e of $\mathcal{T}$, the function $f_e(z) := f(e,z)$ is a cusp form of weight 2 (in the usual sense) on the group $\Gamma_e := \tilde{\Gamma} \cap \mathrm{Stab}(e)$.

Likewise, let $S_2(\mathcal{V}, \tilde{\Gamma})$ denote the space of forms on $(\mathcal{V}(\mathcal{T}) \times \mathcal{H})/\tilde{\Gamma}$, defined as the functions

$$f : \mathcal{V}(\mathcal{T}) \times \mathcal{H} \longrightarrow \mathbb{C}$$

satisfying:

1. $f(\gamma v, \gamma z) = \frac{(cz+d)^2}{\det(\gamma)} f(v, z)$, for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \tilde{\Gamma}$.
2. For each vertex v of $\mathcal{T}$, the function $f_v(z) := f(v, z)$ is a cusp form of weight 2 (in the usual sense) on the group $\Gamma_v := \tilde{\Gamma} \cap \mathrm{Stab}(v)$.

A vertex of $\mathcal{T}$ is said to be *even* if its distance from the distinguished vertex v_* is even, and is said to be *odd* otherwise. Likewise, an edge $e \in \mathcal{E}(\mathcal{T})$ is said to be even if its source vertex is even, and odd if its source vertex is odd. The group Γ preserves the parity of vertices and edges of $\mathcal{T}$, while the elements in $\tilde{\Gamma} - \Gamma$ are parity-reversing. Given $f \in S_2(\mathcal{T}, \Gamma)$, define a form $\tilde{f}$ on $\mathcal{E}(\mathcal{T}) \times \mathcal{H}$ by choosing an element $\alpha \in \tilde{\Gamma} - \Gamma$ and setting

$$\tilde{f}(e, z)dz = f(e, z)dz \quad \text{if } e \text{ is even;} \tag{34}$$

$$\tilde{f}(e, z)dz = f(\alpha e, \alpha z)d\alpha z \quad \text{if } e \text{ is odd.} \tag{35}$$

Note that

1. The definition of $\tilde{f}$ does not depend on the choice of α that was made to define it, since any two such choices differ by left multiplication by an element of Γ, and $f(e, z)dz$ is Γ-invariant.
2. The function $\tilde{f}$ belongs to $S_2(\mathcal{E}, \tilde{\Gamma})$. (To check that

   $$\tilde{f}(\gamma e, \gamma z)d\gamma z = \tilde{f}(e, z)dz \quad \text{for all} \quad \gamma \in \tilde{\Gamma},$$

   it is easiest to separate four cases, depending on the parity of e and on whether γ belongs to Γ or $\tilde{\Gamma} - \Gamma$.)
3. The assignment $i : f \mapsto \tilde{f}$ is an injective homomorphism from $S_2(\mathcal{T}, \Gamma)$ to $S_2(\mathcal{E}, \tilde{\Gamma})$. For if $\tilde{f} = 0$, the function $f(e, z)$ vanishes identically on all even edges, and hence on all edges by the harmonicity of f.

The normaliser of $\Gamma_0(N)$ in $\tilde{\Gamma}$ consists of the elements of $\tilde{\Gamma}$ that fix the unordered edge attached to e_*. Hence $\Gamma_0(N)$ has index two in this normaliser. It will be convenient for later calculations to assume that α belongs to the normaliser of $\Gamma_0(N)$ in $\tilde{\Gamma}$, so that

$$\alpha e_* = \bar{e}_*. \tag{36}$$

There are two natural degeneracy maps

$$\pi_s, \pi_t : S_2(\mathcal{E}, \tilde{\Gamma}) \longrightarrow S_2(\mathcal{V}, \tilde{\Gamma}) \tag{37}$$

defined by

$$\pi_s(f)(v,z) := \sum_{s(e)=v} f(e,z), \qquad \pi_t(f)(v,z) := \sum_{t(e)=v} f(e,z). \tag{38}$$

The exactness of the following sequence follows directly from the definitions:

$$0 \longrightarrow S_2(\mathcal{T}, \Gamma) \xrightarrow{i} S_2(\mathcal{E}, \tilde{\Gamma}) \xrightarrow{\pi_s \oplus \pi_t} S_2(\mathcal{V}, \tilde{\Gamma}) \oplus S_2(\mathcal{V}, \tilde{\Gamma}). \tag{39}$$

Let $S_2(\Gamma_0(N))$ denote the usual complex vector space of holomorphic cusp forms of weight 2 on $\mathcal{H}/\Gamma_0(N)$. Let

$$\varphi_s : X_0(N) \longrightarrow X_0(M)$$

be the natural projection arising from the inclusion $\Gamma_0(N) \subset \Gamma_0(M)$, and let $\varphi_t = \varphi_s W_p$ where W_p is the Atkin-Lehner involution at p acting on $X_0(N)$, defined by

$$W_p f_0(z) dz = f_0(\alpha z) d(\alpha z). \tag{40}$$

Making an abuse of notation, denote by the same symbols φ_s and φ_t the two *degeneracy maps* from $S_2(\Gamma_0(N))$ to $S_2(\Gamma_0(M))$ induced from φ_s and φ_t by pushforward of differential forms. More precisely, choose a system of coset representatives for $\Gamma_0(N)$ in $\Gamma_0(M)$:

$$\Gamma_0(M) = \gamma_1 \Gamma_0(N) \cup \cdots \cup \gamma_{p+1} \Gamma_0(N). \tag{41}$$

One then has

$$\varphi_s(f)(z)dz = \sum_{j=1}^{p+1} f(\gamma_j^{-1} z) d(\gamma_j^{-1} z), \quad \varphi_t(f)(z)dz = \sum_{j=1}^{p+1} f(\alpha\gamma_j^{-1} z) d(\alpha\gamma_j^{-1} z). \tag{42}$$

The kernel of

$$\varphi_s \oplus \varphi_t : S_2(\Gamma_0(N)) \longrightarrow S_2(\Gamma_0(M)) \oplus S_2(\Gamma_0(M)) \tag{43}$$

is called the subspace of *p-new* forms, denoted $S_2^{\mathrm{new-p}}(\Gamma_0(N))$. The following lemma relates the various spaces of forms on $\mathcal{T}$ to spaces of classical modular forms.

Lemma 1.3 *1. The function which to $f(e,z)$ associates $f_0(z) := f_{e_*}(z)$ induces an isomorphism from $S_2(\mathcal{E},\tilde{\Gamma})$ to $S_2(\Gamma_0(N))$.*

2. The function which to $f(v,z)$ associates $f_0(z) := f_{v_*}(z)$ induces an isomorphism from $S_2(\mathcal{V},\tilde{\Gamma})$ to $S_2(\Gamma_0(M))$.

3. The function which to $f(e,z)$ associates $f_0(z) := f_{e_*}(z)$ induces an isomorphism from $S_2(\mathcal{T},\Gamma)$ to $S_2^{\mathrm{new-p}}(\Gamma_0(N))$.

Proof: To prove part 1, note that by definition of $S_2(\mathcal{E},\tilde{\Gamma})$, the form $f_0(z)$ is a cusp form on $\Gamma_0(N)$. The fact that $\tilde{\Gamma}$ acts transitively on $\mathcal{E}(\mathcal{T})$ implies that $f \in S_2(\mathcal{E},\tilde{\Gamma})$ is completely determined by its restriction to $\{e_*\} \times \mathcal{H}$, so that the assignment $f \mapsto f_0$ is injective. To show surjectivity, note that any f_0 in $S_2(\Gamma_0(N))$ can be extended to a form on $S_2(\mathcal{E},\tilde{\Gamma})$ by the rule

$$f_e(z)dz = f_0(\gamma z)d\gamma z \tag{44}$$

if $e = \gamma^{-1}e_*$ with $\gamma \in \tilde{\Gamma}$. Part 2 is proved in an identical way, after observing that the stabiliser of v_* in $\tilde{\Gamma}$ is equal to $\Gamma_0(M)$. Finally, to prove part 3, consider the following natural diagram in which the first row is taken from equation (39) and the vertical maps are those of lemma 1.3:

$$\begin{array}{ccccccc} 0 & \longrightarrow & S_2(\mathcal{T},\Gamma) & \stackrel{i}{\longrightarrow} & S_2(\mathcal{E},\tilde{\Gamma}) & \longrightarrow & S_2(\mathcal{V},\tilde{\Gamma}) \oplus S_2(\mathcal{V},\tilde{\Gamma}) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & S_2^{\mathrm{new-p}}(\Gamma_0(N)) & \longrightarrow & S_2(\Gamma_0(N)) & \longrightarrow & S_2(\Gamma_0(M)) \oplus S_2(\Gamma_0(M)). \end{array}$$

This diagram commutes: the commutativity of the first square follows directly from equation (34) defining i, in view of the fact that e_* is an even edge. The commutativity of the second square follows from the choice of α satisfying (36) which shows that $\gamma_1 e_*, \ldots \gamma_{p+1}e_*$ is a complete list of edges with source v_*, while $\gamma_1\alpha e_*, \ldots \gamma_{p+1}\alpha e_*$ is a complete list of edges with target v_*. Part 3 of lemma 1.3 follows from the five lemma.

The Hecke operators T_ℓ ($\ell \not| N$) act on the spaces $S_2(\mathcal{E},\tilde{\Gamma})$, $S_2(\mathcal{V},\tilde{\Gamma})$, and $S_2(\mathcal{T},\Gamma)$ via the identifications of lemma 1.3. More precisely, for each prime ℓ, write the double coset $\Gamma \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \Gamma$ as a disjoint union of left cosets:

$$\Gamma \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \Gamma = \cup_j \gamma_j \Gamma. \tag{45}$$

Then $T_\ell f$ is given by

$$(T_\ell f)(e,z)dz = \sum_j f(\gamma_j^{-1}e, \gamma_j^{-1}z)d(\gamma_j^{-1}z). \tag{46}$$

Similarly, for each prime ℓ dividing M, let W_ℓ denote the Atkin-Lehner involution at ℓ acting on $S_2^{\text{new}-\text{p}}(\Gamma_0(N))$ or on $S_2(\mathcal{T},\Gamma)$ via the identification of lemma 1.3. Writing $N = \ell^n N'$, choose integers x, y, z, t such that

$$\ell^n xt - N'yz = 1, \quad \text{and set } \alpha_\ell = \begin{pmatrix} \ell^n x & y \\ Nz & \ell^n t \end{pmatrix}. \tag{47}$$

The actions of W_ℓ are given by the rules

$$\begin{aligned} (W_\ell f_0)(z)dz &= f_0(\alpha_\ell z)d(\alpha_\ell z) && (48)\\ (W_\ell f)(e,z)dz &= f(\alpha_\ell e, \alpha_\ell z)d(\alpha_\ell z), && (49) \end{aligned}$$

for all $f_0 \in S_2(\Gamma_0(N))$ and for all $f \in S_2(\mathcal{T},\Gamma)$.

The involution W_p on $S_2(\Gamma_0(N))$ defined in (40) plays a particularly important role in our discussion.

Lemma 1.4 *Let f_0 be a form in $S_2^{\text{new}-\text{p}}(\Gamma_0(N))$ and let f be the form in $S_2(\mathcal{T},\Gamma)$ associated to it by the identification of lemma 1.3. Denote by $W_p f$ the form attached to $W_p f_0$ by this identification. Then*

$$(W_p f)(e,z)dz := -f(\alpha e, \alpha z)d(\alpha z). \tag{50}$$

(Note the minus sign appearing in this formula.)
Proof: Let e be any even edge of $\mathcal{T}$, so that $e = \gamma e_*$ for some $\gamma \in \Gamma$. A direct calculation using definition (40) of W_p and property (36) satisfied by α shows that

$$\begin{aligned} W_p f(e,z)dz &= W_p f_0(\gamma^{-1}z)d(\gamma^{-1}z) = f_0(\alpha\gamma^{-1}z)d(\alpha\gamma^{-1}z)\\ &= f(e_*, \alpha\gamma^{-1}z)d(\alpha\gamma^{-1}z) = -f(\bar{e}_*, \alpha\gamma^{-1}z)d(\alpha\gamma^{-1}z)\\ &= -f(\bar{e}, \gamma\alpha\gamma^{-1}z)d(\gamma\alpha\gamma^{-1}z)\\ &= -f(\gamma\alpha\gamma^{-1}e, \gamma\alpha\gamma^{-1}z)d(\gamma\alpha\gamma^{-1}z) = -f(\alpha e, \alpha z)d(\alpha z), \end{aligned}$$

where the last equality follows from the fact that $\gamma\alpha\gamma^{-1}$ belongs to $\tilde{\Gamma} - \Gamma$. A similar reasoning works if e is odd, and the lemma follows.

Let f_0 be a normalized newform on $\Gamma_0(N)$ having *rational* Fourier coefficients, so that it corresponds to an elliptic curve E over $\mathbb{Q}$ of conductor N by the Eichler–Shimura construction. Let f be the form in $S_2(\mathcal{T},\Gamma)$ which is related to f_0 by lemma 1.3, so that $f_{e_*} = f_0$. The form f_0 is an eigenvector for W_p acting on on $S_2(\Gamma_0(N))$. It is known that

$$W_p f_0 = -f_0 \text{ if } E \text{ has split multiplicative reduction at } p \quad (51)$$

$$W_p f_0 = f_0 \text{ if } E \text{ has non-split multiplicative reduction at } p. \quad (52)$$

Let w be the negative of the eigenvalue of W_p acting on f_0, so that $w = 1$ if E has split multiplicative reduction at p, and $w = -1$ if E has non-split multiplicative reduction at p.

Lemma 1.5 *The form f satisfies the following transformation rule under the group $\tilde{\Gamma} \supset \Gamma$:*

$$f(\gamma e, \gamma z) d(\gamma z) = w^{|\gamma|} f(e,z) dz, \quad \text{for all } \gamma \in \tilde{\Gamma}.$$

Proof: A direct consequence of the transformation property of f_0 under W_p and lemma 1.4.

1.2 Mixed period integrals

The discussion preceding definition 1.2 suggests that f should be viewed as a system of *residues* for a "form ω of weight $(2,2)$" on $(\mathcal{H}_p \times \mathcal{H})/\Gamma$, even though the ω itself is not defined. It is natural in this light to seek to attach to f periods analogous to the periods of modular forms of weight $(2,2)$ on a Hilbert modular surface.

By assumption 2, the elliptic curve E is isomorphic to the strong Weil curve in its isogeny class. Let $\varphi : \mathcal{H}^*/\Gamma_0(N) \longrightarrow E(\mathbb{C})$ be the strong Weil parametrisation attached to E. Letting ω_E denote the Néron differential of E, one has

$$\varphi^*(\omega_E) = 2\pi i c_\varphi f_0(z) dz, \quad (53)$$

where c_φ, the so-called *Manin constant*, is a rational number which is known to be equal to ± 1 in many cases (cf. [Ed]).

Choose elements x, y in the extended upper half-plane $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}_1(\mathbb{Q})$. The function $\tilde{\kappa}_f\{x \to y\} : \mathcal{E}(\mathcal{T}) \longrightarrow \mathbb{C}$ defined by

$$\tilde{\kappa}_f\{x \to y\}(e) := 2\pi i c_\varphi \int_x^y f_e(z) dz \quad (54)$$

is a complex-valued harmonic cocycle on $\mathcal{T}$, as follows immediately from the harmonicity properties of f itself. At the same time, the elements of $\mathcal{E}(\mathcal{T})$ correspond to basic compact open subsets of $\mathbb{P}_1(\mathbb{Q}_p)$ by setting

$$U(e_*) := \mathbb{Z}_p \subset \mathbb{P}_1(\mathbb{Q}_p),$$

and defining, for any edge $e = \gamma e_*$ with $\gamma \in \mathbf{GL}_2(\mathbb{Q}_p)$,

$$U(e) := \gamma U(e_*) = \gamma \mathbb{Z}_p = \{x \in \mathbb{P}_1(\mathbb{Q}_p) \text{ such that } \gamma^{-1} x \in \mathbb{Z}_p\}. \tag{55}$$

Thus $\tilde{\kappa}_f\{x \to y\}$ gives rise to a complex-valued distribution $\tilde{\mu}_f\{x \to y\}$ on the boundary $\mathbb{P}_1(\mathbb{Q}_p)$ of $\mathcal{H}_p$ by the rule

$$\tilde{\mu}_f\{x \to y\}(U(e)) = \tilde{\kappa}_f\{x \to y\}(e). \tag{56}$$

This distribution can only be integrated against locally constant complex-valued functions on $\mathbb{P}_1(\mathbb{Q}_p)$. For the purposes of p-adic integration, it is desirable that $\tilde{\kappa}_f\{x \to y\}$ take on integral, or at least p-adic integral, values. Fortunately, this can be achieved, provided that x and y belong to $\mathbb{P}_1(\mathbb{Q})$. For in this case, the values of $\tilde{\kappa}_f\{x \to y\}(e)$ can be expressed in terms of the modular symbols

$$\tilde{\lambda}_E(a, b) := 2\pi i c_\varphi \int_\infty^{-\frac{a}{b}} f_0(z) dz, \tag{57}$$

defined in [MTT], §8, where they are simply called $2\pi i c_\varphi \lambda_E(a, b)$. More precisely, choose $\gamma \in \tilde{\Gamma}$ such that $\gamma e = e_*$, and write $\gamma x = -\frac{a}{b}$, $\gamma y = -\frac{c}{d}$. Then

$$\tilde{\kappa}_f\{x \to y\}(e) = \tilde{\mu}_f\{x \to y\}(U(e)) = w^{|\gamma|}(\tilde{\lambda}_E(c, d) - \tilde{\lambda}_E(a, b)). \tag{58}$$

Let Ω denote the Néron lattice attached to the elliptic curve E. The following proposition, proved under assumption 2, plays a key role in the definition of integrals on $(\mathcal{H}_p \times \mathcal{H})/\Gamma$.

Proposition 1.6 (Drinfeld-Manin) *The $\mathbb{Z}$-module $\Lambda \subset \mathbb{C}$ generated by the modular symbols $\tilde{\lambda}_E(a, b)$ is contained in Ω.*

Proof: From equations (57) and (53),

$$\tilde{\lambda}_E(a, b) := 2\pi i c_\varphi \int_\infty^{-\frac{a}{b}} f_0(z) dz = \int_{\varphi([\infty, -\frac{a}{b}])} \omega_E, \tag{59}$$

where $\varphi([\infty, -\frac{a}{b}])$ is the image of the path joining ∞ to $-a/b$ in $\mathcal{H}^*$ under the modular parametrisation φ. By the theorem of Drinfeld and Manin, all cusps in $\mathcal{H}^*$ map to rational torsion points in E. Hence by assumption 2, $\varphi([\infty, -\frac{a}{b}])$ is a closed path on $E(\mathbb{C})$ and hence $\tilde{\lambda}_E(a,b)$ belongs to Ω.

If $E(\mathbb{R})$ has two components then Ω is generated by a positive real period Ω_+ and a purely imaginary period Ω_-. If $E(\mathbb{R})$ has one connected component, then Ω is contained with index two in the lattice spanned by Ω_+ and Ω_-, where Ω_+ (resp. Ω_-) denotes the real (resp. imaginary) half-period attached to E. In either case, thanks to proposition 1.6, one can write

$$\tilde{\lambda}_E(a,b) = \lambda_E^+(a,b) \cdot \Omega_+ + \lambda_E^-(a,b) \cdot \Omega_-, \tag{60}$$

with $\lambda_E^{\pm}(a,b) \in \mathbb{Z}$. Choose a sign $w_\infty = \pm 1$ and let $\lambda_E(a,b)$ denote $\lambda_E^+(a,b)$ (resp. $\lambda_E^-(a,b)$) if $w_\infty = 1$ (resp. $w_\infty = -1$). Write κ_f (resp. μ_f) for the $\mathbb{Z}$-valued harmonic cocycle on $\mathcal{T}$ (resp. distribution on $\mathbb{P}_1(\mathbb{Q}_p)$) attached to this modular symbol, so that, with γ, a, b, c and d as in (58),

$$\kappa_f\{x \to y\}(e) = \mu_f\{x \to y\}(U(e)) = w^{|\gamma|}(\lambda_E(c,d) - \lambda_E(a,b)). \tag{61}$$

It is worth recording the following lemma which will be used repeatedly in the sequel:

Lemma 1.7 *For all $\gamma \in \tilde{\Gamma}$, $x, y \in \mathbb{P}_1(\mathbb{Q})$, and $e \in \mathcal{E}(\mathcal{T})$,*

$$\kappa_f\{\gamma x \to \gamma y\}(\gamma e) = w^{|\gamma|}\kappa_f\{x \to y\}(e).$$

Proof: By definition,

$$\begin{aligned} \tilde{\kappa}_f\{\gamma x \to \gamma y\}(\gamma e) &= \int_{\gamma x}^{\gamma y} f_{\gamma e}(z)dz = w^{|\gamma|}\int_{\gamma x}^{\gamma y} f_e(\gamma^{-1}z)d(\gamma^{-1}z) \\ &= w^{|\gamma|}\int_x^y f_e(z)dz = w^{|\gamma|}\tilde{\kappa}_f\{x \to y\}(e). \end{aligned}$$

The same result with $\tilde{\kappa}_f$ replaced by κ_f follows at once.

The next lemma complements lemma 1.7 by describing the transformation behaviour of κ_f under the entire group $R^\times$ which contains $\tilde{\Gamma}$ with index two.

Lemma 1.8 *If $\alpha_\infty \in R^\times$ is any element of determinant -1, then*

$$\kappa_f\{\alpha_\infty x \to \alpha_\infty y\}(\alpha_\infty e) = w_\infty \kappa_f\{x \to y\}(e).$$

Proof: It is enough to show this for a single such α_∞, say the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. In this case it follows directly from the relation

$$\lambda_E(-a,b) = w_\infty \lambda_E(a,b) \tag{62}$$

satisfied by the modular symbol λ_E attached to the choice of sign w_∞. (Cf. [MTT].)

For any $\gamma \in R^\times$, set $\mathrm{sgn}(\gamma) = 0$ if $\det(\gamma) > 0$, and $\mathrm{sgn}(\gamma) = 1$ if $\det(\gamma) < 0$. Lemmas 1.7 and 1.8 can be combined into the following transformation formula satisfied by κ_f under the action of $R^\times$:

$$\kappa_f\{\gamma x \to \gamma y\}(\gamma e) = w^{|\gamma|} w_\infty^{\mathrm{sgn}(\gamma)} \kappa_f\{x \to y\}(e), \quad \text{for all } \gamma \in R^\times. \tag{63}$$

Because the values $\mu_f\{x \to y\}(U(e))$ are integral and hence p-adically bounded as $e \in \mathcal{E}(\mathcal{T})$, the distribution $\mu_f\{x \to y\}$ defines a p-adic *measure* on $\mathbb{P}_1(\mathbb{Q}_p)$. In particular, if h is any bounded locally analytic $\mathbb{C}_p$-valued function on $\mathbb{P}_1(\mathbb{Q}_p)$, the integral

$$\int_{\mathbb{P}_1(\mathbb{Q}_p)} h(t) d\mu_f\{x \to y\}(t) \in \mathbb{C}_p \tag{64}$$

can be defined in the usual way.

Digression on p-adic modular forms, continued. To motivate definition 1.9 below of the periods attached to ω, it is useful to return to the digression about p-adic modular forms and the setting where f is a rigid analytic modular form on $\mathcal{H}_p/\Gamma$, with Γ a discrete arithmetic subgroup of $\mathbf{SL}_2(\mathbb{Q}_p)$. The function $\kappa_f : \mathcal{E}(\mathcal{T}) \longrightarrow \mathbb{C}_p$ encoding the residues of f gives rise to a p-adic distribution μ_f on $\mathbb{P}_1(\mathbb{Q}_p)$ which is p-adically bounded, since $\mathcal{T}/\Gamma$ is a finite graph. In [Te], it is proved that the weight two modular form f can be recovered from its boundary distribution μ_f by the elegant Poisson inversion formula

$$f(z) = \int_{\mathbb{P}_1(\mathbb{Q}_p)} \frac{1}{z-t} d\mu_f(t). \tag{65}$$

To the modular form f and a choice of two endpoints $z_1, z_2 \in \mathcal{H}_p$ is attached the Coleman p-adic line integral $\int_{z_1}^{z_2} f(z)dz$ which depends on a choice of p-adic logarithm $\log : \mathbb{C}_p^\times \longrightarrow \mathbb{C}_p$. Taking this Coleman integral on both sides

of equation (65) and formally interchanging the order of integration on the right suggests the identity

$$\int_{z_1}^{z_2} f(z)dz = \int_{\mathbb{P}_1(\mathbb{Q}_p)} \log\left(\frac{t-z_2}{t-z_1}\right) d\mu_f(t), \tag{66}$$

which can be justified rigorously as in [BDIS] or alternately can be adopted as a *definition* of the Coleman line integral in this setting.

Returning to the original setting, but guided by formula (66), the following definition, depending similarly on a choice of log, imposes itself naturally.

Definition 1.9 *Let z_1 and z_2 be elements of $\mathcal{H}_p$, and let $x, y \in \mathbb{P}_1(\mathbb{Q})$.*

$$\int_{z_1}^{z_2}\int_x^y \omega := \int_{\mathbb{P}_1(\mathbb{Q}_p)} \log\left(\frac{t-z_2}{t-z_1}\right) d\mu_f\{x\to y\}(t) \in \mathbb{C}_p. \tag{67}$$

The following lemma shows that this definition is well-behaved:

Lemma 1.10 *The double integrals of definition 1.9 satisfy the following properties:*

$$\int_{z_1}^{z_3}\int_x^y \omega = \int_{z_1}^{z_2}\int_x^y \omega + \int_{z_2}^{z_3}\int_x^y \omega; \tag{68}$$

$$\int_{z_1}^{z_2}\int_{x_1}^{x_3} \omega = \int_{z_1}^{z_2}\int_{x_1}^{x_2} \omega + \int_{zi_1}^{z_2}\int_{x_2}^{x_3} \omega; \tag{69}$$

$$\int_{\gamma z_1}^{\gamma z_2}\int_{\gamma x}^{\gamma y} \omega = w^{|\gamma|}w_\infty^{\mathrm{sgn}(\gamma)} \int_{z_1}^{z_2}\int_x^y \omega, \quad \text{for all } \gamma \in R^\times. \tag{70}$$

Proof: The first and second identity are a direct consequence of definition 1.9, while the third follows from equation (63).

Caveat: Once again, the reader should not be misled by this notation into thinking that ω is defined by itself; only its system of p-adic residues, described by f, is defined, but this is enough to make sense of definition 1.9. Of course, the notation is meant to be suggestive, and the reader should view the left hand side of definition 1.9 as a period for a form of weight $(2,2)$ on $(\mathcal{H}_p \times \mathcal{H})/\Gamma$, with the complex period Ω_+ or Ω_- "factored out".

To obtain stronger formulae, it is preferable to avoid choosing a p-adic logarithm, exploiting the fact that $\kappa_f\{x\to y\}$ is $\mathbb{Z}$-valued to define

$$\not\int_{z_1}^{z_2}\int_x^y \omega := \not\int_{\mathbb{P}_1(\mathbb{Q}_p)} \left(\frac{t-z_2}{t-z_1}\right) d\mu_f\{x\to y\}(t) \in \mathbb{C}_p^\times. \tag{71}$$

Here $\oint\!\!\!\!\times$ denotes the multiplicative integral, in which limits of products replace the usual limits of Riemann sums. More precisely,

$$\oint\!\!\!\!\times_{\mathbb{P}_1(\mathbb{Q}_p)} g(t)d\mu(t) := \lim_{\mathcal{C}} \prod_{U_\alpha \in \mathcal{C}} g(t_\alpha)^{\mu(U_\alpha)}, \tag{72}$$

where the limit is taken over increasingly fine covers $\mathcal{C} = \{U_\alpha\}_\alpha$ of $\mathbb{P}_1(\mathbb{Q}_p)$ by disjoint compact open subsets, with $t_\alpha \in U_\alpha$. This limit exists if $\log g$ is locally analytic and g takes values in a compact subset of $\mathbb{C}_p^\times$, as is the case for the integrand appearing in (71).

The multiplicative integral has the advantage that it does not rely on a choice of p-adic logarithm. It is related to its additive counterpart by the formula

$$\int_{z_1}^{z_2}\int_x^y \omega = \log\left(\oint\!\!\!\!\times_{z_1}^{z_2}\int_x^y \omega\right). \tag{73}$$

Since any p-adic logarithm vanishes on the torsion in $\mathbb{C}_p^\times$, the multiplicative integral carries more information than the additive one. Note also that it is $\mathbb{C}_p^\times$, and not $\mathbb{C}_p$, which arises most naturally in Tate's p-adic uniformisation theory of elliptic curves with multiplicative reduction.

Properties analogous to those of lemma 1.10, with addition replaced by multiplication, hold for the multiplicative integral:

Lemma 1.11 *The double multiplicative integral of definition 1.9 satisfies the following properties:*

$$\oint\!\!\!\!\times_{z_1}^{z_3}\int_x^y \omega = \oint\!\!\!\!\times_{z_1}^{z_2}\int_x^y \omega \times \oint\!\!\!\!\times_{z_2}^{z_3}\int_x^y \omega; \tag{74}$$

$$\oint\!\!\!\!\times_{z_1}^{z_2}\int_{x_1}^{x_3} \omega = \oint\!\!\!\!\times_{z_1}^{z_2}\int_{x_1}^{x_2} \omega \times \oint\!\!\!\!\times_{z_1}^{z_2}\int_{x_2}^{x_3} \omega; \tag{75}$$

$$\oint\!\!\!\!\times_{\gamma z_1}^{\gamma z_2}\int_{\gamma x}^{\gamma y} \omega = \left(\oint\!\!\!\!\times_{z_1}^{z_2}\int_x^y \omega\right)^{w^{|\gamma|}w_\infty^{\mathrm{sgn}(\gamma)}}, \quad \text{for all } \gamma \in R^\times. \tag{76}$$

Proof: The proof is identical to that of lemma 1.10.

2 Periods attached to split tori

2.1 Preliminary calculations

Let $K = \mathbb{Q} \times \mathbb{Q}$, let $\Psi : K \longrightarrow M_2(\mathbb{Q})$ be a $\mathbb{Q}$-algebra embedding, and let c be a positve integer which is relatively prime to N. One says that Ψ is an optimal embedding of conductor c if the subring $\mathcal{O} := \Psi^{-1}(R)$ is the $\mathbb{Z}[1/p]$-order in K of conductor c, so that

$$\mathcal{O} = \{(u, v) \in \mathbb{Z}[1/p] \times \mathbb{Z}[1/p] \text{ such that } u \equiv v \pmod{c}\}. \tag{77}$$

An orientation on $\mathcal{O}$ is a ring homomorphism

$$\mathfrak{o} : \mathcal{O} \longrightarrow \mathbb{Z}/M\mathbb{Z}. \tag{78}$$

If $M = M_1 M_2$ is a factorisation of M into a product of two relatively prime integers, the homomorphism $\mathfrak{o}_{M_1,M_2}$ defined by

$$\mathfrak{o}_{M_1,M_2}((a, b)) = (a \bmod M_1, b \bmod M_2) \in \mathbb{Z}/M_1\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z} = \mathbb{Z}/M\mathbb{Z} \tag{79}$$

is an orientation, and all orientations are of this form.

An optimal embedding Ψ of conductor c gives rise to an orientation $\mathfrak{o}_\Psi$ on $\mathcal{O}$, sending $x \in \mathcal{O}$ to the residue class modulo M of the upper left hand entry of $\Psi(x)$. The embedding Ψ is said to be *oriented* if

$$\mathfrak{o}_\Psi = \mathfrak{o}_{M,1}. \tag{80}$$

Lemma 2.1 *Let $M = M_1 \ell^n M_2$ be a factorization of M into three relatively prime integers M_1, ℓ^n and M_2. If $\mathfrak{o}_\Psi = \mathfrak{o}_{M_1,\ell^n M_2}$, and α_ℓ is the matrix of (47) used to define the Atkin-Lehner involution W_ℓ, then*

$$\mathfrak{o}_{\alpha_\ell \Psi \alpha_\ell^{-1}} = \mathfrak{o}_{M_1\ell^n,M_2}.$$

Proof: This follows by a direct calculation with matrices using the definition of α_ℓ given in (47).

For each integer ν satisfying $\gcd(\nu, c) = 1$, define the embedding Ψ_ν of K into $M_2(\mathbb{Q})$ by the rule

$$\Psi_\nu(a, a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \quad \Psi_\nu(c, 0) = \begin{pmatrix} c & \nu \\ 0 & 0 \end{pmatrix}. \tag{81}$$

Note that Ψ_ν is an oriented optimal embedding of conductor c. Conversely:

Lemma 2.2 *If Ψ is any oriented optimal embedding of K of conductor c, it is Γ-conjugate to the embedding Ψ_ν for some ν with $\gcd(\nu, c) = 1$. The image of ν in $(\mathbb{Z}/c\mathbb{Z})^\times/\langle p^2\rangle$ is uniquely determined by Ψ.*

Proof: The embedding Ψ maps $(c, 0)$ to a matrix in $M_2(\mathbb{Z}[1/p])$ of determinant 0 and trace c, so that

$$\Psi(c,0) = \begin{pmatrix} r & s \\ t & u \end{pmatrix}, \quad r \equiv c \pmod{M}, \quad ru - ts = 0, \quad r + u = c.$$

Let x and y be relatively prime integers satisfying the equation $tx - ry = 0$. Note that M divides y, since M divides t and r is a unit modulo M. Hence one can choose $\gamma \in \Gamma$ of the form

$$\gamma = \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}. \tag{82}$$

A direct calculation now shows that

$$\gamma^{-1}\Psi(c,0)\gamma = \begin{pmatrix} c & \nu \\ 0 & 0 \end{pmatrix}, \tag{83}$$

where $\nu \in \mathbb{Z}[1/p]$ is relatively prime to c. Conjugating by the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix}$ shows that Ψ_ν and $\Psi_{\nu'}$ are conjugate to each other in Γ if and only if the natural images of ν and ν' in $(\mathbb{Z}/c\mathbb{Z})^\times/\langle p^2\rangle$ are the same.

Recall from the introduction that the torus $\Psi(K^\times)$ acting on $\mathcal{H}^*$ has exactly two fixed points x_Ψ and y_Ψ, and that $\bar{\Psi}(K^\times) \cap \Gamma$ is free of rank one, generated by an element $\gamma_\Psi \in \Gamma$. The period I_Ψ is then defined by choosing $z \in \mathcal{H}_p$ and setting

$$I_\Psi = \int\!\!\!\!\!\!\diagup_z^{\gamma_\Psi z} \int_{x_\Psi}^{y_\Psi} \omega. \tag{84}$$

Lemma 2.3 *The period I_Ψ does not depend on the choice of $z \in \mathcal{H}_p$ that was made to define it. Furthermore, it depends only on the Γ-conjugacy class of Ψ.*

Proof: The integral I_Ψ is independent of z, since

$$\int\!\!\!\!\!\!\diagup_{z_1}^{\gamma_\Psi z_1} \int_{x_\Psi}^{y_\Psi} \omega \div \int\!\!\!\!\!\!\diagup_{z_2}^{\gamma_\Psi z_2} \int_{x_\Psi}^{y_\Psi} \omega = \int\!\!\!\!\!\!\diagup_{z_1}^{z_2} \int_{x_\Psi}^{y_\Psi} \omega \div \int\!\!\!\!\!\!\diagup_{\gamma_\Psi z_1}^{\gamma_\Psi z_2} \int_{x_\Psi}^{y_\Psi} \omega,$$

by property (74) of the multiplicative integral stated in lemma 1.11. By property (76),

$$\oint_{z_1}^{z_2}\int_{x_\Psi}^{y_\Psi}\omega = \oint_{\gamma_\Psi z_1}^{\gamma_\Psi z_2}\int_{x_\Psi}^{y_\Psi}\omega,$$

and it follows that I_Ψ does not depend on z. Replacing Ψ by $\alpha\Psi\alpha^{-1}$ with $\alpha \in \tilde{\Gamma}$, the period attached to $\alpha\Psi\alpha^{-1}$ becomes

$$\oint_{z}^{\alpha\gamma_\Psi\alpha^{-1}z}\int_{\alpha x_\Psi}^{\alpha y_\Psi}\omega = \left(\oint_{\alpha^{-1}z}^{\gamma_\Psi\alpha^{-1}z}\int_{x_\Psi}^{y_\Psi}\omega\right)^{w^{|\alpha|}} = \left(\oint_{z}^{\gamma_\Psi z}\int_{x_\Psi}^{y_\Psi}\omega\right)^{w^{|\alpha|}}, \qquad (85)$$

where the first equality follows from property (76) of the integral, and the second equality follows from the independence of I_Ψ on z.

The goal of section 2 is to prove theorem 1 of the introduction. We begin by disposing of it in the following trivial special case.

Lemma 2.4 *Suppose that E has non-split multiplicative reduction at p and that p has odd order in $(\mathbb{Z}/c\mathbb{Z})^\times$. Then $I_\Psi = \pm 1$.*

Proof: Let t be the order of p in $(\mathbb{Z}/c\mathbb{Z})^\times$ and let $\alpha = \Psi(p^t, 1) \in \tilde{\Gamma} - \Gamma$. Then $\Psi = \alpha\Psi\alpha^{-1}$. On the other hand, by equation (85), $I_{\alpha\Psi\alpha^{-1}} = I_\Psi^{-1}$.

Because of lemma 2.4, the following assumption will be made in the rest of section 2.

Assumption 2.5 *When $w = -1$, the order of p in $(\mathbb{Z}/c\mathbb{Z})^\times$ is even.*

By interchanging x_Ψ and y_Ψ if necessary, assume that y_Ψ is an attractive fixed point for γ_Ψ and that x_Ψ is a repulsive fixed point, so that, for all $t \in \mathcal{H}_p$,

$$\gamma_\Psi^n(t) \to y_\Psi \text{ as } n \to \infty, \qquad \gamma_\Psi^n(t) \to x_\Psi \text{ as } n \to -\infty. \qquad (86)$$

Let $M_\Psi(t)$ be a Möbius transformation with coefficients in $\mathbb{Q}_p$ sending y_Ψ to 0 and x_Ψ to ∞. For example, if x_Ψ and y_Ψ are not equal to ∞, one may take

$$M_\Psi(t) = \frac{t - y_\Psi}{t - x_\Psi}.$$

Note that $M_\Psi(t)$ is well-defined up to multiplication by a scalar in $\mathbb{Q}_p^\times$.

The element γ_Ψ acts discretely on the complement $\mathbb{P}_1(\mathbb{Q}_p) - \mathrm{FP}_\Psi$ of the fixed-point set $\mathrm{FP}_\Psi := \{x_\Psi, y_\Psi\}$. In fact,

Lemma 2.6

$$M_\Psi(\gamma_\Psi t) = p^s M_\Psi(t),$$

where

$$s = 2 \times \textit{ the order of } p^2 \textit{ in } (\mathbb{Z}/c\mathbb{Z})^\times.$$

(Note that by assumption 2.5, s is equal to the order of p in $(\mathbb{Z}/c\mathbb{Z})^\times$ when $w = -1$.)

Proof: Note that the Möbius tranformations $M_\Psi(\gamma_\Psi t)$ and $M_\Psi(t)$ both send y_Ψ to 0 and x_Ψ to ∞, so they must differ by multiplication by a scalar in $\mathbb{Q}_p^\times$. A direct calculation shows that this scalar is equal to p^s, using the fact that

$$\gamma_\Psi = \bar{\Psi}\left(\begin{pmatrix} p^{s/2} & 0 \\ 0 & p^{-s/2} \end{pmatrix}\right)$$

is the image in $\mathbf{PSL}_2(\mathbb{Q}_p)$ of a matrix having eigenvalues $p^{s/2}$ and $p^{-s/2}$.

Lemma 2.6 allows the calculation of a fundamental region $\mathcal{F}_\Psi$ for the action of the element γ_Ψ on $\mathbb{P}_1(\mathbb{Q}_p) - \mathrm{FP}_\Psi$:

$$\mathcal{F}_\Psi = \{t \in \mathbb{P}_1(\mathbb{Q}_p) - \mathrm{FP}_\Psi \text{ such that } 0 \leq \mathrm{ord}_p(M_\Psi(t)) < s\}. \tag{87}$$

Points of the boundary $\mathbb{P}_1(\mathbb{Q}_p)$ of the p-adic upper half-plane $\mathcal{H}_p$ correspond to ends of $\mathcal{T}$; let $\mathrm{path}(x_\Psi, y_\Psi)$ be the infinite path on $\mathcal{T}$ joining the ends associated to x_Ψ and y_Ψ. For each vertex v on this path, let

$$U(v) \subset \mathbb{P}_1(\mathbb{Q}_p) - \mathrm{FP}_\Psi$$

be the compact open subset corresponding to all points associated to ends originating from v and not passing through any edge in $\mathrm{path}(x_\Psi, y_\Psi)$. The vertices of $\mathrm{path}(x_\Psi, y_\Psi)$ can be indexed consecutively by subscripts $j \in \mathbb{Z}$ so that

$$U(v_j) = \{t \in \mathbb{P}_1(\mathbb{Q}_p) - \mathrm{FP}_\Psi \quad \text{such that} \quad \mathrm{ord}_p(M_\Psi(t)) = j\}, \tag{88}$$

so that

$$\mathcal{F}_\Psi = U(v_0) \cup U(v_1) \cup \cdots \cup U(v_{s-1}). \tag{89}$$

Let e_j be the edge on $\mathrm{path}(x_\Psi, y_\Psi)$ joining v_{j-1} to v_j. Note that

$$\gamma_\Psi(v_j) = v_{j+s}, \qquad \gamma_\Psi(e_j) = e_{j+s}. \tag{90}$$

Set

$$m_\Psi = \kappa_f\{x_\Psi \to y_\Psi\}(e_0) = \kappa_f\{x_\Psi \to y_\Psi\}(e_s). \tag{91}$$

The remainder of section 2.1 is devoted to proving the following proposition, a first step in the evaluation of I_Ψ.

Proposition 2.7 *For all $z \in \mathcal{H}_p$,*

$$I_\Psi = \int\!\!\!\!\!\!\diagup_z^{\gamma_\Psi z} \int_{x_\Psi}^{y_\Psi} \omega = \left(\int\!\!\!\!\!\!\diagup_{\mathcal{F}_\Psi} M_\Psi(t) d\mu_f\{x_\Psi \to y_\Psi\}(t) \right) \times p^{sm_\Psi}.$$

In particular, I_Ψ belongs to $\mathbb{Q}_p^\times$.

Proof: By definition,

$$\int\!\!\!\!\!\!\diagup_z^{\gamma_\Psi z} \int_{x_\Psi}^{y_\Psi} \omega = \int\!\!\!\!\!\!\diagup_{\mathbb{P}_1(\mathbb{Q}_p)} \left(\frac{t - \gamma_\Psi z}{t - z} \right) d\mu_f\{x_\Psi \to y_\Psi\}(t). \tag{92}$$

For conciseness, write μ_f for $\mu_f\{x_\Psi \to y_\Psi\}$ and κ_f for $\kappa_f\{x_\Psi \to y_\Psi\}$ in the remainder of section 2.

Lemma 2.8 *The measure μ_f is invariant under multiplication by γ_Ψ, i.e,. $\mu_f(\gamma_\Psi U) = \mu_f(U)$ for all compact open subsets U of $\mathbb{P}_1(\mathbb{Q}_p)$.*

Proof: This follows directly from lemma 1.7.

Lemma 2.9 *If $c \in \mathbb{C}_p^\times$ is any non-zero constant, then*

$$\int\!\!\!\!\!\!\diagup_{\mathcal{F}_\Psi} c d\mu_f(t) = 1.$$

Proof: This is simply because $\mu_f(\mathcal{F}_\Psi) = \kappa_f(e_0) - \kappa_f(e_s) = 0$.

Proof of proposition 2.7:
To evaluate the integral appearing in the right hand side of equation (92), break up the region of integration $\mathbb{P}_1(\mathbb{Q}_p)$ as follows:

$$\mathbb{P}_1(\mathbb{Q}_p) = U_-(n) \cup U_+(n) \cup \bigcup_{j=-n}^{n} \gamma_\Psi^j \mathcal{F}_\Psi, \tag{93}$$

where

$$\begin{aligned} U_-(n) &= \{t \in \mathbb{P}_1(\mathbb{Q}_p) - \mathrm{FP}_\Psi \text{ s.t. } \mathrm{ord}_p(M_\Psi(t)) < -ns\} \cup \{x_\Psi\}, \\ U_+(n) &= \{t \in \mathbb{P}_1(\mathbb{Q}_p) - \mathrm{FP}_\Psi \text{ s.t. } \mathrm{ord}_p(M_\Psi(t)) \geq (n+1)s\} \cup \{y_\Psi\}. \end{aligned}$$

Invoking lemma 2.8, define

$$I(n) := \prod_{j=-n}^{n} \oint_{\gamma_\Psi^j \mathcal{F}_\Psi} \left(\frac{t-\gamma_\Psi z}{t-z} \right) d\mu_f(t) = \prod_{j=-n}^{n} \oint_{\mathcal{F}_\Psi} \left(\frac{\gamma_\Psi^j t-\gamma_\Psi z}{\gamma_\Psi^j t-z} \right) d\mu_f(t). \quad (94)$$

Observe that

$$\mu_f(U_-(n)) = -\kappa_f(e_0) = -m_\Psi, \quad \mu_f(U_+(n)) = \kappa_f(e_s) = m_\Psi. \quad (95)$$

Hence by definition of the multiplicative integral,

$$\oint_{\mathbb{P}_1(\mathbb{Q}_p)} \left(\frac{t-\gamma_\Psi z}{t-z} \right) d\mu_f(t) = \left(\frac{x_\Psi-\gamma_\Psi z}{x_\Psi-z} \right)^{-m_\Psi} \left(\frac{y_\Psi-\gamma_\Psi z}{y_\Psi-z} \right)^{m_\Psi} \lim_{n\to\infty} I(n)$$

$$= \left(\frac{M_\Psi(\gamma_\Psi z)}{M_\Psi(z)} \right)^{m_\Psi} \lim_{n\longrightarrow\infty} I(n) = p^{sm_\Psi} \lim_{n\to\infty} I(n), \quad \text{by lemma 2.6.} \quad (96)$$

Note that the integrand $\frac{\gamma_\Psi^j t-\gamma_\Psi z}{\gamma_\Psi^j t-z}$ appearing in the definition of $I(n)$ and the function $\frac{t-\gamma_\Psi^{-j+1} z}{t-\gamma_\Psi^{-j} z}$ differ by a non-zero scalar multiple (depending on z but not on t), so that by lemma 2.9

$$\oint_{\mathcal{F}_\Psi} \left(\frac{\gamma_\Psi^j t-\gamma_\Psi z}{\gamma_\Psi^j t-z} \right) d\mu_f(t) = \oint_{\mathcal{F}_\Psi} \left(\frac{t-\gamma_\Psi^{-j+1} z}{t-\gamma_\Psi^{-j} z} \right) d\mu_f(t). \quad (97)$$

Interchanging the order of summation and integration in the definition (94) of $I(n)$,

$$\begin{aligned} I(n) &= \oint_{\mathcal{F}_\Psi} \left(\prod_{j=-n}^{n} \frac{t-\gamma_\Psi^{-j+1} z}{t-\gamma_\Psi^{-j} z} \right) d\mu_f(t) && (98) \\ &= \oint_{\mathcal{F}_\Psi} \frac{(t-\gamma_\Psi^{n+1} z)}{(t-\gamma_\Psi^{-n} z)} d\mu_f(t) && (99) \\ &= \oint_{\mathcal{F}_\Psi} M(\gamma_\Psi^{n+1} z; \gamma_\Psi^{-n} z; t) d\mu_f(t), && (100) \end{aligned}$$

where for $a, b \in \mathcal{H}$, $M(a; b; t)$ is any Möbius transformation sending a to 0 and b to ∞.

By (86), there exists a sequence of scalars $\lambda_n \in \mathbb{C}_p^\times$ such that the $\mathbb{C}_p^\times$-valued functions $\lambda_n M(\gamma_\Psi^{n+1} z; \gamma_\Psi^{-n} z; t)$ converge to $M_\Psi(t)$ uniformly on compact subsets of $\mathbb{P}_1(\mathbb{Q}_p) - \{x_\Psi, y_\Psi\}$ as $n \to \infty$, so that

$$\lim_{n\to\infty} I(n) = \int\!\!\!\!\!\!\diagup_{\mathcal{F}_\Psi} M_\Psi(t) d\!\!\!\!\diagup\mu_f(t). \tag{101}$$

Combining this with equations (92) and (96),

$$\int\!\!\!\!\!\!\diagup_z^{\gamma_\Psi z} \int_{x_\Psi}^{y_\Psi} \omega = \left(\int\!\!\!\!\!\!\diagup_{\mathcal{F}_\Psi} M_\Psi(t) d\!\!\!\!\diagup\mu_f\{x_\Psi \to y_\Psi\}(t) \right) \times p^{sm_\Psi}, \tag{102}$$

as was to be shown.

2.2 Evaluation of $\mathbf{ord}_p(I_\Psi)$

Define the so-called *Winding element* attached to Ψ by choosing a vertex of $\mathcal{T}$ and setting

$$W_\Psi = \sum_{v \to \gamma_\Psi v} \kappa_f\{x_\Psi \to y_\Psi\}(e),$$

the sum being taken over all edges in the path joining v to $\gamma_\Psi v$.

Lemma 2.10 *The winding element W_Ψ does not depend on the choice of $v \in \mathcal{V}(\mathcal{T})$ that was made to define it, and it depends only on the Γ-conjugacy class of Ψ.*

Replacing v by v' changes W_Ψ by the quantity

$$\begin{aligned} &\sum_{v' \to \gamma_\Psi v'} \kappa_f\{x_\Psi \to y_\Psi\}(e) - \sum_{v \to \gamma_\Psi v} \kappa_f\{x_\Psi \to y_\Psi\}(e) \\ &\quad = \sum_{v' \to v} \kappa_f\{x_\Psi \to y_\Psi\}(e) - \sum_{\gamma_\Psi v' \to \gamma_\Psi v} \kappa_f\{x_\Psi \to y_\Psi\}(e) = 0, \end{aligned}$$

where the first equality follows from the harmonicity of $\kappa_f\{x_\Psi \to y_\Psi\}$ and the fact that $\mathcal{T}$ is simply connected, while the second equality follows from the Γ-invariance of κ_f (lemma 1.7).

Proposition 2.11

$$\mathrm{ord}_p(I_\Psi) = W_\Psi.$$

Proof: By proposition 2.7,

$$\mathrm{ord}_p\left(\int\!\!\!\!\!\!\times_z^{\gamma_\Psi z}\int_{x_\Psi}^{y_\Psi}\omega\right) = \mathrm{ord}_p\left(\int\!\!\!\!\!\!\times_{\mathcal{F}_\Psi} M_\Psi(t)d\mu_f(t)\times p^{sm_\Psi}\right) \quad (103)$$

$$= \left(\int_{\mathcal{F}_\Psi}\mathrm{ord}_p(M_\Psi(t))d\mu_f(t)\right) + sm_\Psi. \quad (104)$$

But the function $g(t) := \mathrm{ord}_p(M_\Psi(t))$ is locally constant on $\mathcal{F}_\Psi$, and satisfies

$$g(t) = i, \text{ for all } t \in U(v_i). \quad (105)$$

Hence

$$\mathrm{ord}_p\left(\int\!\!\!\!\!\!\times_z^{\gamma_\Psi z}\int_{x_\Psi}^{y_\Psi}\omega\right) = \left(\sum_{i=0}^{s-1} i(\kappa_f(e_i)-\kappa_f(e_{i+1}))\right) + s\kappa_f(e_s) \quad (106)$$

$$= \sum_{i=1}^{s}\kappa_f(e_i) = \sum_{v_0\to\gamma_\Psi v_0}\kappa_f(e) = W_\Psi, \quad (107)$$

and the result follows.

Lemma 2.1 implies that any embedding Ψ of conductor c is conjugate, under the action of the group generated by the matrices α_ℓ, to an oriented optimal embedding of conductor c. In particular, since the newform f_0 is an eigenvector for all the Atkin-Lehner involutions, one has

Lemma 2.12 *Given any embedding $\Psi : K \longrightarrow M_2(\mathbb{Q})$ of conductor c, there exists an oriented embedding Ψ' of conductor c for which*

$$I_{\Psi'} = I_\Psi^{\pm 1}.$$

Hence, to show conjecture 3 or theorem 1 it is enough to show it for all oriented optimal embeddings. Lemma 2.2 allows us to focus exclusively on the embeddings of the special form described in (81). When $\Psi = \Psi_\nu$, the following proposition evaluates the winding number W_Ψ in terms of the modular symbols $\lambda_E(a,b)$ attached to E in equation (57) of section 1.

Proposition 2.13 *Let J be the coset of $(\mathbb{Z}/c\mathbb{Z})^\times$ consisting of a such that $a/\nu \equiv p^j \pmod{c}$ for some $j = j(a)$. Then*

$$\mathrm{ord}_p(I_{\Psi_\nu}) = W_{\Psi_\nu} = \sum_{a\in J} w^{j(a)}\lambda_E(a,c). \quad (108)$$

Proof: Keeping the notations of the discussion preceding the statement of proposition 2.7, note that

$$W_\Psi = \kappa_f\{x_\Psi \to y_\Psi\}(e_0) + \cdots + \kappa_f\{x_\Psi \to y_\Psi\}(e_{s-1}). \tag{109}$$

A direct calculation reveals that the two fixed points for the action of $\Psi(K^\times)$ on $\mathbb{P}_1(\mathbb{Q})$ are

$$x_\Psi = \infty \quad \text{and} \quad y_\Psi = -\frac{\nu}{c}, \tag{110}$$

and that a fundamental region for the action of γ_Ψ on $\mathbb{P}_1(\mathbb{Q}_p) - \{x_\Psi, y_\Psi\}$ is therefore given by

$$\mathcal{F}_\Psi = \left\{ t \in \mathbb{P}_1(\mathbb{Q}_p) \text{ such that } 0 \leq \mathrm{ord}_p\left(t + \frac{\nu}{c}\right) < s \right\}, \tag{111}$$

where s is twice the order of p^2 in $(\mathbb{Z}/c\mathbb{Z})^\times$. By proposition 2.7, and since $M_\Psi(t)$ can be chosen to be equal to $t + \frac{\nu}{c}$,

$$\begin{aligned} U(e_j) &= \left\{ t \in \mathbb{P}_1(\mathbb{Q}_p) \text{ such that } \mathrm{ord}_p\left(t + \frac{\nu}{c}\right) \geq j \right\}, & (112) \\ &= \left\{ t \in \mathbb{P}_1(\mathbb{Q}_p) \text{ such that } p^{-j}\left(t + \frac{\nu}{c}\right) \in \mathbb{Z}_p \right\}. & (113) \end{aligned}$$

Hence $U(e_j) = U(\gamma^{-1} e_*)$, where $\gamma = \begin{pmatrix} 1 & -\nu' \\ 0 & p^j \end{pmatrix}$. Noting that

$$\gamma x_\Psi = \infty, \quad \gamma(y_\Psi) = \frac{(-\nu - c\nu')/p^j}{c}, \quad |\gamma| = j, \tag{114}$$

we find

$$\mu_f(U(e_j)) = \kappa_f\{x_\Psi \to y_\Psi\}(e_j) = w^j \lambda_E(a, c), \tag{115}$$

where a is an integer which is defined modulo c by the congruence $a \equiv \nu p^{-j}$. The result follows.

Let χ be a Dirichlet character of conductor c prime to N.

Lemma 2.14 *If $\chi(p) = w$, then*

$$\sum_{\nu \in (\mathbb{Z}/c\mathbb{Z})^\times} \chi(\nu) W_{\Psi_\nu} = s \sum_{a \in (\mathbb{Z}/c\mathbb{Z})^\times} \chi(a) \lambda_E(a, c).$$

Proof: This follows from proposition 2.13 by a direct calculation.

Recall the choice of sign w_∞ that was made in defining the modular symbol $\lambda_E(a,c)$.

Lemma 2.15 *If $\chi(p) = w$ and $\chi(-1) = -w_\infty$, then*

$$\sum_{\nu \in (\mathbb{Z}/c\mathbb{Z})^\times} \chi(\nu) W_{\Psi_\nu} = 0.$$

Proof: This follows directly from lemma 2.14 and from the relation

$$\lambda_E(-a,b) = w_\infty \lambda_E(a,b) \tag{116}$$

satisfied by the modular symbols attached to the choice of sign w_∞.

Let

$$L(f_0,\chi,s) = L(E/\mathbb{Q},\chi,s) = \sum_{n=1}^{\infty} a_n \chi(n) n^{-s} \tag{117}$$

be the L-series of $E/\mathbb{Q}$ twisted by χ. Write

$$\tau(\chi) := \sum_{\nu \in (\mathbb{Z}/c\mathbb{Z})^\times} \chi(\nu) e^{2\pi i \nu/c} \tag{118}$$

for the Gauss sum attached to χ.

Proposition 2.16 *If $\chi(p) = w$ and $\chi(-1) = w_\infty$, then*

$$\sum_{\nu \in (\mathbb{Z}/c\mathbb{Z})^\times} \chi(\nu) W_{\Psi_\nu} = \frac{sc}{\tau(\chi)} \frac{L(E/\mathbb{Q},\chi,1)}{c_\varphi \Omega_{w_\infty}}.$$

Proof: This follows by combining lemma 2.14 with equation (8.6) of §I.8 of [MTT]. (The discrepancy involving the factors of $2\pi i$ and c_φ are accounted for by the different normalisations used in the definition of $\lambda_E(a,c)$ in [MTT] and in this article.)

Lemma 2.17 *There exist infinitely many Dirichlet characters χ of conductor prime to N satisfying*

$$\chi(p) = w, \quad \chi(-1) = w_\infty, \qquad \sum_{\nu \in (\mathbb{Z}/c\mathbb{Z})^\times} \chi(\nu) W_{\Psi_\nu} \neq 0.$$

Proof: In view of proposition 2.16, it is enough to show that there exist infinitely many Dirichlet characters of conductor prime to N satisfying

$$\chi(p) = w, \quad \chi(-1) = w_\infty, \quad L(E/\mathbb{Q}, \chi, 1) \neq 0. \tag{119}$$

This can be proved by considering averages of $L(E/\mathbb{Q}, \chi, 1)$ as χ ranges over characters of conductor c satisfying $\chi(p) = w$ and $\chi(-1) = w_\infty$, and showing that such averages are non-zero as c becomes large. In fact, when $M \neq 1$ or $w_\infty \neq -1$, it is enough to consider averages over quadratic characters χ. In the exceptional situation where $N = p$ and $ww_\infty = -1$, the sign in the functional equation of $L(E/\mathbb{Q}, \chi, s)$ is always -1. It then becomes necessary to allow χ to be a non-quadratic character, so that this sign does not force the vanishing of $L(E/\mathbb{Q}, \chi, s)$ at $s = 1$. See for example [MM] where non-vanishing results for twists of L-series, and the averaging techniques used to obtain them, are explained in detail.

Remarks:
1. The non-vanishing of the expression $\sum_a \chi(a)\lambda_E(a, c)$, for some Dirichlet character χ, is an elementary consequence of the fact that the paths between elements of $\mathbb{P}_1(\mathbb{Q})$ generate the rational homology of the curve $\mathcal{H}^*/\Gamma_0(N)$ so that the modular symbols $\lambda_E(a, c)$ cannot vanish identically. It seems more difficult to exploit this property of the modular symbols to establish the corresponding non-vanishing as χ ranges over the smaller subset of characters satisfying $\chi(p) = w$ and $\chi(-1) = w_\infty$, without exploiting the connection between modular symbols and special values of twisted L-series and invoking analytic arguments to establish non-vanishing theorems for such twists.

2. The fact that E has split (resp. non-split) multiplicative reduction at p when $w = 1$ (resp. when $w = -1$) combined with the fact that $\chi(p) = w$ implies that the factor $\mathrm{ord}_p(q)$ appears as one of the fudge factors (attached to the prime p) in the algebraic part of the special value $L(E/\mathbb{Q}, \chi, 1)$ predicted by the Birch and Swinnerton-Dyer conjecture. Hence for all such χ, one expects that

$$\mathrm{ord}_p(q) \text{ divides } \frac{L(E/\mathbb{Q}, \chi, 1)}{\Omega_{w_\infty}}. \tag{120}$$

This can be used to deduce the corresponding divisibility of $\mathrm{ord}_p(I_\Psi)$ by $\mathrm{ord}_p(q)$, at least away from the primes dividing s, c and c_φ, and lends some support for conjecture 3. (Cf the remarks immediately following the statement of theorem 1 in the introduction.)

The divisibility of $\mathrm{ord}_p(I_\Psi)$ by $\mathrm{ord}_p(q)$ will be established in many cases, independently of any conjectures, in [BD7].

2.3 Evaluation of $\log(I_\Psi)$

Set $\Psi = \Psi_\nu$ as before. The following proposition evaluates $\log(I_\Psi)$ explicitly in terms of modular symbols.

Proposition 2.18 *Let J_n be the coset in $(\mathbb{Z}/p^n c\mathbb{Z})^\times$ consisting of a such that $a/\nu \equiv p^j \pmod{c}$ for some $j = j(a)$. Then*

$$\log(I_\Psi) = \int_z^{\gamma_\Psi z} \int_{x_\Psi}^{y_\Psi} \omega = \lim_{n\to\infty} w^n \sum_{a\in J_n} w^{j(a)} \log(a) \lambda_E(a, p^n c).$$

Note that the expression $w^{j(a)}$ which appears in the right-hand limit is well defined, since assumption 2.5 makes the parity of j well-defined in the case where $w = -1$.

Proof of proposition 2.18: By proposition 2.7, and since $M_\Psi(t)$ can be chosen to be equal to $t + \frac{\nu}{c}$,

$$\int_z^{\gamma_\Psi z} \int_{x_\Psi}^{y_\Psi} \omega = \log(I_\Psi) = \int_{\mathcal{F}_\Psi} \log\left(t + \frac{\nu}{c}\right) d\mu_f\{x_\Psi \to y_\Psi\}(t). \tag{121}$$

As in the discussion preceding the proof of proposition 2.7, write

$$\mathcal{F}_\Psi = U(v_0) \cup \cdots \cup U(v_{s-1}), \tag{122}$$

where

$$U(v_j) = \left\{ t \in \mathbb{P}_1(\mathbb{Q}_p) \text{ such that } \mathrm{ord}_p\left(t + \frac{\nu}{c}\right) = j \right\}. \tag{123}$$

For each positive integer n, the compact open subset $U(v_j)$ can be further decomposed as

$$U(v_j) = \cup_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} U_{j,a}, \tag{124}$$

where

$$U_{j,a} = \left\{ t \in U(v_j) \text{ such that } p^{-j}\left(t + \frac{\nu}{c}\right) \equiv a \pmod{p^n} \right\}. \tag{125}$$

Choose an integer ν' such that

$$\nu' \equiv -\frac{\nu}{c} \pmod{p^{n+s}}, \tag{126}$$

and observe that

$$U_{j,a} = U(\gamma^{-1}e_*), \text{ where } \gamma = \begin{pmatrix} 1 & -\nu' - p^j a \\ 0 & p^{n+j} \end{pmatrix} \in R^\times. \tag{127}$$

Noting that

$$\gamma x_\Psi = \infty, \quad \gamma(y_\Psi) = \frac{(-\nu - c\nu')/p^j - ac}{cp^n}, \quad |\gamma| = n + j, \tag{128}$$

we find by equation (61) of section 1 that

$$\mu_f\{x_\Psi \to y_\Psi\}(U_{j,a}) = w^{n+j}\lambda_E(a_j, cp^n), \tag{129}$$

where a_j is an integer which is defined modulo cp^n by the congruences

$$a_j \equiv ac \pmod{p^n}, \quad a_j \equiv \nu p^{-j} \pmod{c}. \tag{130}$$

It follows that

$$\int_{\mathcal{F}_\Psi} \log\left(t + \frac{\nu}{c}\right) d\mu_f\{x_\Psi \to y_\Psi\}(t) = \lim_{n\to\infty} w^n \sum_a w^{j(a)} \log(a)\lambda_E(a, p^n c), \tag{131}$$

where the sum ranges over $a \in J_n$. The proposition follows.

We now turn to the proof of theorem 1 of the introduction.

Proof of theorem 1.
By combining propositions 2.18 and 2.13, one is reduced to showing that for each ν in $(\mathbb{Z}/c\mathbb{Z})^\times/\langle p^2\rangle$,

$$\lim_{n\to\infty} w^n \sum_{a\in J_n} w^{j(a)} \log(a)\lambda_E(a, p^n c) = \frac{\log(q)}{\mathrm{ord}_p(q)} \sum_{a\in J} w^{j(a)}\lambda_E(a, c). \tag{132}$$

Let $\chi : (\mathbb{Z}/c\mathbb{Z})^\times \longrightarrow \mathbb{C}_p^\times$ be a Dirichlet character with the property that $\chi(p) = w$, so that in particular χ factors through $(\mathbb{Z}/c\mathbb{Z})^\times/\langle p^2\rangle$. Recall the sign w_∞ that was used to define $\lambda_E(a, b)$. If $\chi(-1) = -w_\infty$, then a direct calculation using the relation $\lambda_E(-a, b) = w_\infty\lambda_E(a, b)$ shows that

$$\lim_{n\to\infty} w^n \sum_{a\in(\mathbb{Z}/p^n c\mathbb{Z})^\times} \chi(a)\log(a)\lambda_E(a, p^n c) = \sum_{a\in(\mathbb{Z}/c\mathbb{Z})^\times} \chi(a)\lambda_E(a, c) = 0. \tag{133}$$

If $\chi(-1) = w_\infty$, then the exceptional zero conjecture of Mazur, Tate and Teitelbaum ([MTT], §13, conjecture 1) proved by Greenberg and Stevens [GS] states that for all such χ,

$$\lim_{n\to\infty} w^n \sum_{a\in(\mathbb{Z}/p^nc\mathbb{Z})^\times} \chi(a)\log(a)\lambda_E(a,p^nc) = \frac{\log(q)}{\mathrm{ord}_p(q)} \sum_{a\in(\mathbb{Z}/c\mathbb{Z})^\times} \chi(a)\lambda_E(a,c), \tag{134}$$

where the sums now are taken over all congruence classes a in $(\mathbb{Z}/p^nc\mathbb{Z})^\times$ and $(\mathbb{Z}/c\mathbb{Z})^\times$ respectively. Hence relation (134) holds for all Dirichlet characters χ such that $\chi(p) = w$. But the relation expressed in equation (132) can be written as a $\mathbb{C}_p$-linear combination of the relations expressed in equation (134). Theorem 1 follows.

3 The cohomology of Γ

3.1 The cohomology of M-symbols

Recall from the introduction that an M-symbol with values in an abelian group C is a function

$$m\{\ \to\ \} : \mathbb{P}_1(\mathbb{Q}) \times \mathbb{P}_1(\mathbb{Q}) \longrightarrow C \tag{135}$$

satisfying

$$m\{x\to y\} + m\{y\to z\} = m\{x\to z\}, \qquad m\{x\to y\} = -m\{y\to x\}, \tag{136}$$

for all $x, y, z \in \mathbb{P}_1(\mathbb{Q})$. The group of $\mathbb{C}_p$-valued M-symbols is denoted $\mathcal{M}$, and more generally the group of C-valued M-symbols is denoted by $\mathcal{M}(C)$. Recall also that Γ acts on $\mathcal{M}(C)$ by the rule

$$(\gamma m)\{x\to y\} := m\{\gamma^{-1}x\to\gamma^{-1}y\}. \tag{137}$$

The cohomology groups $H^i(\Gamma, \mathcal{M})$ play the crucial role in this section. Recall that Γ acts on $\mathcal{T}$ with e_* as fundamental region. The stabiliser of e_* in Γ is equal to $\Gamma_0(N)$ and the stabiliser of $s(e_*)$ (resp of $t(e_*)$) is equal to $\Gamma_0(M)$ (resp $\Gamma_0'(M) := \alpha_p\Gamma_0(M)\alpha_p^{-1}$). Proposition 13 of sec. II.2.8 of [Se1], applied to the case $M = \mathcal{M}$ and $G = \Gamma$ acting on $\mathcal{T}$, yields a natural exact sequence of $\mathbb{C}_p$-vector spaces

$$\begin{aligned} \mathcal{M}^{\Gamma_0(M)} \oplus \mathcal{M}^{\Gamma_0'(M)} \longrightarrow \mathcal{M}^{\Gamma_0(N)} \xrightarrow{\theta} H^1(\Gamma, \mathcal{M}) \\ \longrightarrow H^1(\Gamma_0(M), \mathcal{M}) \oplus H^1(\Gamma_0'(M), \mathcal{M}). \end{aligned} \tag{138}$$

To describe the map θ explicitly, note that a $\Gamma_0(N)$-invariant M-symbol $m\{x\to y\}$ gives rise to a unique system of M-symbols m_e indexed by the edges of $\mathcal{T}$, satisfying $m_{e_*}\{x\to y\} = m\{x\to y\}$ as well as

$$m_{\gamma e}\{\gamma x\to\gamma y\} = m_e\{x\to y\}, \quad m_{\bar{e}}\{x\to y\} = -m_e\{x\to y\}, \tag{139}$$

for all $x, y \in \mathbb{P}_1(\mathbb{Q})$ and $\gamma \in \Gamma$. One can then write

$$(\theta m)(\gamma)\{x\to y\} = \sum_{v_*\to\gamma v_*} m_e\{x\to y\}. \tag{140}$$

All the cohomology groups appearing in the exact sequence (138) are endowed with a natural action of the Hecke operators T_ℓ with $\ell \not| N$, defined as in [Sh], §8.3. Furthermore these groups are equipped with the "Atkin-Lehner involution W_∞ at ∞", defined using the matrix $\alpha_\infty = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ of determinant -1 which belongs to the normalisers of the groups $\Gamma_0(N)$, $\Gamma_0(M)$, $\Gamma_0'(M)$, and Γ in $R^\times$. On M-symbols W_∞ is defined by the rule

$$(W_\infty m)\{x\to y\} = m\{\alpha_\infty x\to\alpha_\infty y\} = m\{-x\to -y\}, \tag{141}$$

and on $H^1(\Gamma, \mathcal{M})$ by the rule

$$(W_\infty c)(\gamma)\{x\to y\} = c(\gamma^{\alpha_\infty})\{-x\to -y\}. \tag{142}$$

A direct calculation exploiting the explicit description of θ given by (140) shows that the maps arising in (138) are compatible with the action of the Hecke operators T_ℓ as well as with the involution W_∞. For example, to check this last compatibility note that

$$\theta(W_\infty m)(\gamma)\{x\to y\} = \sum_{v_*\to\gamma v_*} (W_\infty m)_e\{x\to y\} = \sum_{v_*\to\gamma v_*} m_{\alpha_\infty e}\{-x\to -y\}. \tag{143}$$

As e ranges over the edges in the path joining v to γv, the edges $\alpha_\infty e$ range over the edges in the path joining $\alpha_\infty v_* = v_*$ to $\alpha_\infty\gamma v_* = \gamma^{\alpha_\infty} v_*$. Hence the right hand side of (143) is equal to

$$\sum_{v_*\to\gamma^{\alpha_\infty} v_*} m_e\{-x\to -y\} = W_\infty(\theta(m))(\gamma)\{x\to y\}. \tag{144}$$

Given the newform in $S_2(\mathcal{T},\Gamma)$ satisfying

$$T_\ell(f) = a_\ell(f) f \tag{145}$$

for all $\ell \not| N$, and a $\mathbb{C}_p$-vector space H equipped with the commuting actions of the Hecke operators T_ℓ and the involution W_∞, denote by H^f the f-isotypic component of H, defined as the set of classes $c \in H$ for which

$$T_\ell(c) = a_\ell(f) c \text{ for all } \ell \not| N. \tag{146}$$

Denote also by H^{w_∞} the space on which the involution W_∞ acts with the eigenvalue w_∞, and by H^{f,w_∞} the intersection of H^f and H^{w_∞}.

Proposition 3.1 *The space $(\mathcal{M}^{\Gamma_0(N)})^{f,w_\infty}$ is a one-dimensional $\mathbb{C}_p$-vector space.*

Proof: Let $\mathcal{F}$ be the space of $\mathbb{C}_p$-valued functions on $\mathbb{P}_1(\mathbb{Q})$, endowed with the natural action of Γ. The assignment $d : \mathcal{F} \longrightarrow \mathcal{M}$ defined by

$$(df)\{x \to y\} := f(y) - f(x) \tag{147}$$

defines a surjective homomorphism of Γ-modules, with kernel the space of constant functions, identified with $\mathbb{C}_p$. Taking the $\Gamma_0(N)$-cohomology of the exact sequence

$$0 \longrightarrow \mathbb{C}_p \longrightarrow \mathcal{F} \xrightarrow{d} \mathcal{M} \longrightarrow 0 \tag{148}$$

yields the exact sequence of cohomology groups

$$\mathcal{F}^{\Gamma_0(N)} \longrightarrow \mathcal{M}^{\Gamma_0(N)} \longrightarrow H^1(\Gamma_0(N), \mathbb{C}_p) \longrightarrow H^1(\Gamma_0(N), \mathcal{F}) \tag{149}$$

which is compatible under the natural action of the Hecke operators and the involution W_∞. On the other hand, the space $\mathcal{F}^{\Gamma_0(N)}$ is *Eisenstein*, i.e.,

$$\text{If } x \in \mathcal{F}^{\Gamma_0(N)}, \text{ then } T_\ell x = (\ell+1)x \text{ for all } \ell \not| N. \tag{150}$$

The same is true of $H^1(\Gamma_0(N), \mathcal{F})$, since $\mathcal{F}$ can be written as a direct sum of induced modules:

$$\mathcal{F} = \oplus_x \mathrm{Ind}_{\Gamma_x}^{\Gamma_0(N)} \mathbb{C}_p, \tag{151}$$

where the direct sum is taken over a system of representatives for the $\Gamma_0(N)$-orbits in $\mathbb{P}_1(\mathbb{Q})$, and Γ_x denotes the stabiliser of x in $\Gamma_0(N)$. By Shapiro's lemma,

$$H^1(\Gamma_0(N), \mathcal{F}) = \oplus_x H^1(\Gamma_x, \mathbb{C}_p), \tag{152}$$

and the action of the Hecke algebra on this module is Eisenstein. It follows that $(\mathcal{F}^{\Gamma_0(N)})^f = 0$ and that $H^1(\Gamma_0(N), \mathcal{F})^f = 0$. By the Eichler-Shimura period isomorphism (cf. [Sh]. §8.2), the space $H^1(\Gamma_0(N), \mathbb{C}_p)^f$ is a two-dimensional $\mathbb{C}_p$-vector space, on which the involution W_∞ acts with eigenvalues 1 and -1. Proposition 3.1 therefore follows from the exact sequence (149).

Proposition 3.2 *The map θ induces an isomorphism from $(\mathcal{M}^{\Gamma_0(N)})^{f,w_\infty}$ to $H^1(\Gamma, \mathcal{M})^{f,w_\infty}$.*

Proof: The arguments used in the proof of proposition 3.1 show that the action of the Hecke operators on $H^0(\Gamma_0(M), \mathcal{M})$ factors through the natural image of the algebra of Hecke operators in the endomorphism ring of the space of modular forms of weight 2 on $\Gamma_0(M)$. Since the Hecke eigenvalues attached to f are those of a newform of level N, it follows that

$$H^0(\Gamma_0(M), \mathcal{M})^f = 0. \tag{153}$$

Pursuing the long exact sequence in cohomology attached to the $\Gamma_0(M)$-cohomology of the sequence (148) yields the sequence

$$H^1(\Gamma_0(M), \mathcal{F}) \longrightarrow H^1(\Gamma_0(M), \mathcal{M}) \longrightarrow H^2(\Gamma_0(M), \mathbb{C}_p). \tag{154}$$

The same argument as in the proof of proposition 3.1 (with N replaced by M) shows that $H^1(\Gamma_0(M), \mathcal{F})$ is Eisenstein and hence that $H^1(\Gamma_0(M), \mathcal{F})^f = 0$. Furthermore it is well-known that $H^2(\Gamma_0(M), \mathbb{C}_p) = 0$. (For example, if $\Gamma_0(M)$ acts on $\mathcal{H}$ without fixed points, then it is a free group.) Hence it follows that

$$H^1(\Gamma_0(M), \mathcal{M})^f = 0. \tag{155}$$

The result now follows from (153) and (155) (and the corresponding statements with $\Gamma_0(M)$ replaced by the conjugate subgroup $\Gamma_0'(M)$) combined with the exact sequence (138).

Corollary 3.3 *The vector space $H^1(\Gamma, \mathcal{M})^{f,w_\infty}$ is one-dimensional over $\mathbb{C}_p$.*

Proof: This follows from propositions 3.1 and 3.2.

3.2 Proof of theorem 4

Given $\tau \in \mathcal{H}_p$, a 1-cocycle $\tilde{c}_{f,\tau} \in Z^1(\Gamma, \mathcal{M}(\mathbb{C}_p^\times))$ is defined by setting

$$\tilde{c}_{f,\tau}(\gamma)\{x \to y\} = \not\int_{\tau}^{\gamma\tau} \int_x^y \omega. \tag{156}$$

The image of $\tilde{c}_{f,\tau}$ in $H^1(\Gamma, \mathcal{M}(\mathbb{C}_p^\times))$, denoted c_f, does not depend on τ. Let $\mathrm{ord}_p(c_f) \in H^1(\Gamma, \mathcal{M})$ be the cohomology class obtained by applying the function $\mathrm{ord}_p : \mathbb{C}_p^\times \longrightarrow \mathbb{Q} \subset \mathbb{C}_p$ to c_f, and let $\log(c_f)$ be the image of c_f in $H^1(\Gamma, \mathcal{M})$ under the logarithm map.

Lemma 3.4 *The class* $\mathrm{ord}_p(c_f)$ *is non-zero. (And hence generates the one-dimensional* $\mathbb{C}_p$*-vector space* $H^1(\Gamma, \mathcal{M})^{f,w_\infty}$*.)*

Proof: Suppose that $\mathrm{ord}_p(c_f) = 0$. Then the one-cocycle $\mathrm{ord}_p(\tilde{c}_{f,\tau})$ is the coboundary of an M-symbol $\eta \in \mathcal{M}$:

$$\mathrm{ord}_p(\tilde{c}_{f,\tau})(\gamma)\{x \to y\} = \eta\{\gamma^{-1}x \to \gamma^{-1}y\} - \eta\{x \to y\}. \tag{157}$$

Let Ψ be an oriented embedding of $\mathbb{Q}\times\mathbb{Q}$ of conductor c prime to M in $M_2(\mathbb{Q})$. Letting $\gamma = \gamma_\Psi$ and $(x, y) = (x_\Psi, y_\Psi)$, the right-hand term of equation (157) disappears and one finds

$$W_\Psi = 0 \quad \text{for all such } \Psi. \tag{158}$$

This contradicts lemma 2.17.

We are now ready to prove theorem 4 of the introduction:

Proof of theorem 4: Since $\mathrm{ord}_p(c_f)$ and $\log(c_f)$ each belong to the one-dimensional vector space $H^1(\Gamma, \mathcal{M})^{f,w_\infty}$, and since $\mathrm{ord}_p(c_f) \neq 0$, there exists a constant $\mathcal{L}_f \in \mathbb{C}_p$ such that $\log(c_f) = \mathcal{L}_f \mathrm{ord}_p(c_f)$. Hence there is an M-symbol $\eta \in \mathcal{M}$ such that

$$\log(\tilde{c}_{f,\tau}(\gamma)\{x \to y\}) = \mathcal{L}_f \mathrm{ord}_p(\tilde{c}_{f,\tau}(\gamma)\{x \to y\}) + (\eta\{\gamma^{-1}x \to \gamma^{-1}y\} - \eta\{x \to y\}),$$

for all $\gamma \in \Gamma$ and $x, y \in \mathbb{P}_1(\mathbb{Q})$. Choosing an embedding Ψ of conductor prime to N and letting $(x, y) = (x_\Psi, y_\Psi)$ and $\gamma = \gamma_\Psi$ as in the proof of lemma 3.4 shows that

$$\log(I_\Psi) = \mathcal{L}_f \mathrm{ord}_p(I_\Psi). \tag{159}$$

By proposition 2.17 it is possible to choose a Ψ for which $\mathrm{ord}_p(I_\Psi) = W_\Psi$ is non-zero. It now follows from theorem 1 that

$$\mathcal{L}_f = \frac{\log(q)}{\mathrm{ord}_p(q)}, \tag{160}$$

as was to be shown.

Remark: While the evaluation of the constants $\mathcal{L}_f$ requires the full strength of the Greenberg-Stevens theorem, the equality $\log(c_f) = \mathcal{L}_f \mathrm{ord}_p(c_f)$ for *some* $\mathcal{L}_f \in \mathbb{C}_p$ is sufficient to imply that $\log(I_\Psi) = \mathcal{L}_f \mathrm{ord}_p(I_\Psi)$ for all Ψ, with $\mathcal{L}_f$ not depending on Ψ. This in turn implies that the extra zero occurring in the exceptional zero conjecture of Mazur, Tate and Teitelbaum is of "local type" in the sense of [MTT], ch I, §19. In other words, the factor $\mathcal{L}_f$, which describes the discrepancy between the first derivative of the p-adic L-function attached to E in [MTT] and the special value of the classical L-function attached to E, is invariant under twists by Dirichlet characters χ for which $\chi(p) = 1$. Note that our proof of this fact is based on little more than purely formal arguments involving the cohomology of Γ.

3.3 Indefinite integrals

Theorem 4 justifies the slightly stronger multiplicative refinement of it that is formulated in conjecture 5 of the introduction. Assume this conjecture. Let τ be an element of $\mathcal{H}_p$ and let L be the field generated by τ over $\mathbb{Q}_p$. The conjecture guarantees the existence of an M-symbol $\eta_{f,\tau} \in \mathcal{M}(L^\times/q^{\mathbb{Z}})$ satisfying

$$\not\int_\tau^{\gamma\tau} \int_x^y \omega = \eta_{f,\tau}\{\gamma^{-1}x \to \gamma^{-1}y\} \div \eta_{f,\tau}\{x \to y\} \pmod{q^{\mathbb{Z}}} \tag{161}$$

for all $\gamma \in \Gamma$ and $x, y \in \mathbb{P}_1(\mathbb{Q})$. The M-symbol $\eta_{f,\tau}$ is defined uniquely by this property modulo elements of $H^0(\Gamma, \mathcal{M}(L^\times/q^{\mathbb{Z}}))$.

Let $\Gamma' \subset \Gamma$ denote the smallest normal subgroup of Γ generated by the commutators and the rational elements in Γ. (An element of Γ is said to be *rational* if its fixed points belong to $\mathbb{P}_1(\mathbb{Q})$.)

Lemma 3.5 *The group Γ' is of finite index in Γ. It is equal to Γ if $M = 1$.*

Proof: The first part of this lemma follows for example from theorem 2 of [Me] (see also Théorème 3 of [Se2]). The second part follows from a direct calculation, using the fact that $\mathbf{SL}_2(\mathbb{Z})$ is equal to its commutator subgroup.

Remark: The main result of [Me], stating that the group Γ has the congruence subgroup property, makes it possible to calculate Γ', and bound its index, in any specific situation. See [BD7] for a more complete discussion.

Let e_Γ denote the exponent of the finite abelian group Γ/Γ'.

Proposition 3.6 *Let C be an abelian group (with trivial Γ-action) and let t be the exponent of the e_Γ-torsion module $C[e_\Gamma]$. If x and y are in the same Γ-orbit in $\mathbb{P}_1(\mathbb{Q})$, and m belongs to $\mathcal{M}(C)^\Gamma$, then*

$$t \cdot m\{x \to y\} = 0.$$

Proof: It follows directly from the Γ-invariance of m that the function which to γ associates $m\{x \to \gamma x\}$ is a homomorphism from Γ to C. Hence its kernel contains the commutator subgroup of Γ. It also contains the rational elements, since if $\gamma y = y$ for some $y \in \mathbb{P}_1(\mathbb{Q})$,

$$m\{x \to \gamma x\} = m\{x \to y\} + m\{y \to \gamma x\} = m\{x \to y\} + m\{y \to x\} = 0.$$

Proposition 3.6 follows.

Let $Q_0 = (L^\times/q^{\mathbb{Z}})[e_\Gamma]$ be the e_Γ-torsion subgroup of $L^\times/q^{\mathbb{Z}}$, and let $Q \subset L^\times$ denote the preimage of Q_0 under the natural projection. It follows from proposition 3.6 that the image of $\eta_{f,\tau}\{x \to y\}$ in $L^\times/Q$ does not depend on the choice of M-symbol $\eta_{f,\tau}$ satisfying (161), if x and y belong to the same Γ-orbit in $\mathbb{P}_1(\mathbb{Q})$. This makes it possible to define the indefinite integral attached to τ by the rule

$$\not\int_x^y \omega := \text{ the natural image of } \eta_{f,\tau}\{x \to y\} \text{ in } L^\times/Q, \tag{162}$$

for all such x, y. Note that when $M = 1$, lemma 3.5 implies that $Q = q^{\mathbb{Z}}$.

Lemma 3.7 *The indefinite multiplicative integral of (23) satisfies the following properties:*

$$\not\int_{\tau_1}^{\tau_2}\int_x^y \omega = \not\int_x^{\tau_2}\int_x^y \omega \div \not\int_x^{\tau_1}\int_x^y \omega, \pmod{Q} \tag{163}$$

$$\not\int_{x_1}^{\tau}\int_{x_1}^{x_3} \omega = \not\int_{x_1}^{\tau}\int_{x_1}^{x_2} \omega \times \not\int_{x_2}^{\tau}\int_{x_2}^{x_3} \omega, \pmod{Q} \tag{164}$$

$$\not\int_{\gamma x}^{\gamma\tau}\int_{\gamma x}^{\gamma y} \omega = \left(\not\int_x^{\tau}\int_x^{y} \omega\right)^{w^{|\gamma|}w_\infty^{\mathrm{sgn}(\gamma)}}, \pmod{Q} \tag{165}$$

for all $\gamma \in R^\times$.

Proof: The first identity is proved by showing that the coboundary of the M-symbol $\eta_{f,\tau_2} \div \eta_{f,\tau_1}$ (viewed as a 0-cochain with values in $\mathcal{M}(L^\times/q^{\mathbb{Z}})$) agrees with the coboundary of the M-symbol

$$m_{\tau_1,\tau_2}\{x \to y\} := \not\int_{\tau_1}^{\tau_2}\int_x^y \omega.$$

The second relation follows directly from the definitions. The third is proved by showing that the $L^\times/q^{\mathbb{Z}}$-valued M-symbol $\gamma\eta_\tau$ satisfies the defining property of the M-symbol $w^{|\gamma|}w_\infty^{\mathrm{sgn}(\gamma)}\eta_{\gamma\tau}$, so that these two M-symbols are equal up to elements in $\mathcal{M}(L^\times/q^{\mathbb{Z}})^\Gamma$.

4 Periods attached to real quadratic fields

Suppose in this section that the prime p splits in the real quadratic field K, and let Ψ denote an algebra embedding of K into $M_2(\mathbb{Q})$.

Choose a base point $\tau \in \mathcal{H}_p$ and $x \in \mathbb{P}_1(\mathbb{Q})$, and define a $\mathbb{C}_p^\times$-valued function on $\Gamma \times \Gamma$ by the rule

$$\langle \alpha, \beta \rangle_\Psi := \not\int_{\tau}^{\alpha^{-1}\tau}\int_x^{\beta x} \omega \div \not\int_{\tau}^{\beta^{-1}\tau}\int_x^{\alpha x} \omega \tag{166}$$

Lemma 4.1 *If* α *and* β *commute, the expression* $\langle \alpha, \beta \rangle_\Psi$ *does not depend on the choices of* $\tau \in \mathcal{H}_p$ *and* $x \in \mathbb{P}_1(\mathbb{Q})$ *that were made to define it.*

Proof: The element $\langle \alpha, \beta \rangle_\Psi$ can be expressed in terms of the $\mathbb{C}_p^\times$-valued 2-cocycle $\tilde{d}_{\tau,x} \in Z^2(\Gamma, \mathbb{C}_p^\times)$ defined by setting

$$\tilde{d}_{\tau,x}(\alpha, \beta) := \tilde{c}_{f,\tau}(\alpha^{-1})\{x \to \beta x\} = \oint_\tau^{\alpha^{-1}\tau} \int_x^{\beta x} \omega. \tag{167}$$

More precisely, one has

$$\langle \alpha, \beta \rangle_\Psi = \tilde{d}_{\tau,x}(\alpha, \beta) \div \tilde{d}_{\tau,x}(\beta, \alpha). \tag{168}$$

A direct calculation shows that the natural image d of $\tilde{d}_{\tau,x}$ in $H^2(\Gamma, \mathbb{C}_p^\times)$ does not depend on the choices of τ and x, so that a different choice would have the effect of multiplying d by a coboundary of the form $h(\alpha, \beta) = g(\alpha) \times g(\beta) \div g(\alpha\beta)$. The corresponding change in $\langle \alpha, \beta \rangle_\Psi$ is then given by $h(\alpha, \beta) \div h(\beta, \alpha)$. Since α and β commute, this ratio of coboundaries is equal to 1 and the result follows.

The Dirichlet S-unit theorem implies that the group $\mathcal{O}_1^\times$ is free of rank two, so that $\bar{\Psi}(K) \cap \Gamma = \bar{\Psi}(\mathcal{O}_1^\times)$ is free of rank two as well.

Lemma 4.2 *The restriction of* $\langle\ ,\ \rangle_\Psi$ *to* $\bar{\Psi}(\mathcal{O}_1^\times)$ *is a bilinear alternating* $\mathbb{C}_p^\times$*-valued pairing.*

Proof: Note that the restriction of $\langle\ ,\ \rangle_\Psi$ to $\bar{\Psi}(\mathcal{O}_1^\times)$ does not depend on the choice of τ and x, by lemma 4.1. A direct calculation based on the definitions shows that $\langle\ ,\ \rangle_\Psi$ is bilinear and alternating.

Let γ_1 and $\gamma_2 \in \Gamma$ be $\mathbb{Z}$-module generators for $\Psi(K) \cap \Gamma$. The period $I_\Psi \in \mathbb{C}_p^\times$ attached to Ψ is defined by setting

$$I_\Psi := \langle \gamma_1, \gamma_2 \rangle_\Psi. \tag{169}$$

Note that $\{I_\Psi, I_\Psi^{-1}\}$ is independent of the choice of basis (γ_1, γ_2).

Proof of theorem 6: Let $\mathrm{ord}_p(d_f)$ and $\log(d_f)$ be the classes in $H^2(\Gamma, \mathbb{C}_p)$ obtained from d_f by applying ord_p and log respectively. Theorem 4 implies that

$$\log(d_f) = \frac{\log(q)}{\mathrm{ord}_p(q)} \mathrm{ord}_p(d_f). \tag{170}$$

The first part of theorem 6 follows immediately from (168) and (170). It also follows from these arguments that the period I_Ψ belongs to $q^{\mathbb{Z}}$ assuming conjecture 5.

Remark:

1. Choose a prime $\mathfrak{p}$ of K above p, and let $\bar{\mathcal{O}}^\times$ be the p-adic closure of the group $\mathcal{O}^\times$ in $K_{\mathfrak{p}}^\times = \mathbb{Q}_p^\times$. In [BD6], it is explained how the period I_Ψ, taken modulo this finite index subgroup, can be interpreted as the leading term in a θ-element which interpolates the special values of $L(E/K, 1)$ twisted by certain finite order characters of $\mathrm{Gal}(\bar{K}/K)$. On the other hand, $\mathrm{ord}_p(I_\Psi)$ can be expressed in terms of algebraic parts of classical special values of certain partial L-functions attached to E/K. Thus, theorem 6 can be viewed as giving an exceptional zero result for the leading terms of the theta-elements attached to elliptic curves over a real quadratic K, expressing his leading term in terms of Tate's period attached to E.

2. Note that the identities of conjectures 3 and theorem 6 provide a *natural lifting* of the exceptional zero conjectures (which are formulated as identities in compact quotients of $K_p^\times$ admitting a Galois-theoretic interpretation) to the group $K_p^\times$ itself; this suggests that the exceptional zero conjectures might arise as *consequences* of more basic identities involving double integrals of ω, identities which can be expressed without appealing to the notion of p-adic L-functions or θ-elements. It is this point of view that provided some of the inspiration for the conjectures of the next section.

5 Heegner points attached to real quadratic fields

5.1 The main conjecture

Assume now that the prime p is inert in the real quadratic field K. For $x \in K$, let $\bar{x}$ denote the Galois conjugate of x. Fix embeddings of K into $\mathbb{R}$ and $\mathbb{C}_p$, so that K can be viewed simultaneously as a subfield of these two fields.
As before, let

$$\Psi : K \longrightarrow M_2(\mathbb{Q}) \tag{171}$$

be an algebra embedding. As in section 2, the *conductor* of Ψ is defined to be the conductor of the $\mathbb{Z}[1/p]$-order $\mathcal{O} = \Psi^{-1}(R)$ of K. Let c denote this conductor, and make the following simplifying assumption from now on:

Assumption 5.1 *The discriminant $c^2\mathrm{Disc}(K)$ of $\mathcal{O}$ is relatively prime to N.*

The torus $\bar{\Psi}(K^\times)$ acting on $\mathcal{H}_p$ by Möbius transformations has two fixed points in $\mathbb{P}_1(K_p) - \mathbb{P}_1(\mathbb{Q}_p) \subset \mathcal{H}_p$ which are interchanged by $\mathrm{Gal}(K_p/\mathbb{Q}_p)$. Let z_Ψ be the unique fixed point with the property that $\Psi(\lambda)$ acts on the tangent space of $\mathcal{H}_p$ at z_Ψ by multiplication by $\lambda/\bar{\lambda}$ (i.e., such that the column vector $(z_\Psi, 1)$ is an eigenvector for $\Psi(\lambda)$ with eigenvalue λ), and let $\bar{z}_\Psi$ be the other fixed point. The group $\bar{\Psi}(K^\times) \cap \Gamma$ is free of rank one, generated by the element $\gamma_\Psi := \bar{\Psi}(u)$ where u is a generator for the group of units of norm one in $\mathcal{O}^\times$. Normalise γ_Ψ by the requirement that u be greater than 1 (relative to the chosen real embedding of K).

A period $I_\Psi \in \mathbb{C}_p^\times$ is naturally attached to Ψ by choosing a base point $x \in \mathbb{P}_1(\mathbb{Q})$ and setting

$$I_\Psi := \int\!\!\!\!\!\!\diagup_{\bar{z}_\Psi}^{z_\Psi} \int_x^{\gamma_\Psi x} \omega \in K_p^\times. \tag{172}$$

Lemma 5.2 *The period I_Ψ does not depend on the choice of $x \in \mathbb{P}_1(\mathbb{Q})$ that was made to define it. Furthermore, it depends only on the Γ-conjugacy class of Ψ.*

The proof is identical to the proof of lemma 2.3. (But observe how the roles of the places p and ∞ are interchanged in these two proofs.)

Let H^+ denote the narrow ring class field of K of conductor c. (The definition of this class field is recalled in section 5.2.) The Galois groups $\mathrm{Gal}(H^+/\mathbb{Q})$ is a generalized dihedral group, in which any element mapping to a generator of $\mathrm{Gal}(K/\mathbb{Q})$ is necessarily of order two. Hence, since the prime p is inert in $K/\mathbb{Q}$, it splits completely in H^+/K. Fix an embedding of H^+ into $\mathbb{C}_p$. (This is tantamount to choosing a prime ideal of H^+ above p.)

Conjecture 5.3 *The local point*

$$P_\Psi^- := \Phi_{\mathrm{Tate}}(I_\Psi) \in E(K_p)$$

is a global point in $E(H^+)$.

Conjecture 5.3 makes it clear that the period I_Ψ is a more subtle arithmetic invariant than in the previous situations that were treated. Indeed, one disposes of no modular construction of global points on E over ring class

fields of real quadratic fields, such as is provided by the theory of complex multiplication when K is a quadratic imaginary field.

As will be seen in section 5.2, the points P_Ψ^- are not the "right" generalisation of Heegner points in this setting, because they fail to obey an analogue of the classical Shimura reciprocity law (cf. the discussion following the statement of corollary 5.12).

To obtain the appropriate generalisation, choose a Γ-orbit in $\mathbb{P}_1(\mathbb{Q})$, say $\Gamma\infty$ to fix ideas. Select any x in this orbit and use the indefinite multiplicative integral of (162) to define

$$J_\Psi := \not\int_x^{z_\Psi} \int_x^{\gamma_\Psi x} \omega \in K_p^\times / Q.$$

Lemma 5.4 *The period J_Ψ does not depend on the choice of $x \in \Gamma\infty$. Furthermore, it depends only on the Γ-conjugacy class of Ψ.*

Proof: This follows directly from the properties of the indefinite multiplicative integral given in lemma 3.7, by manipulations identical to those presented in the proof of lemma 2.3.

Thus, J_Ψ is a canonical element in $K_p^\times/Q$ attached to Ψ. It is related to the period I_Ψ as follows:

Lemma 5.5 *For all embeddings Ψ of K into $M_2(\mathbb{Q})$,*

$$J_\Psi / \bar{J}_\Psi = \not\int_{\bar{z}_\Psi}^{z_\Psi} \int_x^{\gamma_\Psi x} \omega = I_\Psi \pmod{Q}.$$

Proof: This follows directly from property (163) of lemma 3.7 of the indefinite multiplicative integral.

Let t denote the exponent of the group Q_0 introduced before, so that

$$t \text{ divides } \gcd(e_\Gamma, (p^2-1)\mathrm{ord}_p(q)). \tag{173}$$

Since raising to the power t maps Q to $q^{\mathbb{Z}}$, the element J_Ψ^t is well-defined element in $K_p^\times/q^{\mathbb{Z}}$. In view of lemma 5.5, the following modification of conjecture 5.3 is natural:

Conjecture 5.6 *The local point*

$$P_\Psi := \Phi_{\mathrm{Tate}}(J_\Psi^t) \in E(K_p)$$

is a global point in $E(H^+)$.

Assuming this conjecture, one can (and will) view P_Ψ as global points in $E(H^+)$.

5.2 A Shimura Reciprocity Law

The goal of the Shimura Reciprocity Law is to give an explicit (conjectural) description of the action of $\mathrm{Gal}(H^+/K)$ on the global points P_Ψ. An indispensable ingredient in formulating such a law is the concrete description of $\mathrm{Gal}(H^+/K)$ provided by class field theory.

Let $I \subset K$ be a free $\mathbb{Z}[1/p]$-submodule of rank two. The order associated to I is the set of $\lambda \in K$ satisfying $\lambda I \subset I$. A fractional $\mathcal{O}$-ideal of K is a free $\mathbb{Z}[1/p]$-module of rank two in K whose associated order is equal to $\mathcal{O}$. Two such fractional $\mathcal{O}$-ideals I_1 and I_2 are said to be *equivalent* if there exists $\alpha \in K^\times$ such that $I_1 = \alpha I_2$, and are said to be *strictly equivalent* if α can be chosen to be of positive norm. Let $\mathrm{Pic}(\mathcal{O})$ (resp. $\mathrm{Pic}^+(\mathcal{O})$) denote the group of equivalence (resp. strict equivalence) classes of fractional $\mathcal{O}$-ideals in K, where the group operation is the usual multiplication of fractional ideals. Let h and h^+ denote the cardinalities of $\mathrm{Pic}(\mathcal{O})$ and $\mathrm{Pic}^+(\mathcal{O})$ respectively. Note that if $\mathcal{O}^\times$ contains an element of negative norm, then strict equivalence is no stronger than equivalence and $h^+ = h$. Otherwise, we have $h^+ = 2h$.

The reciprocity law of class field theory identifies $\mathrm{Pic}^+(\mathcal{O})$ and $\mathrm{Pic}(\mathcal{O})$ with the Galois groups of certain abelian extensions of K, denoted H^+ and H respectively. The field H^+ is the strict ring class field of K of conductor c introduced in section 5.1, and H is simply called the ring class field of K of conductor c. The extension H is the maximal totally real subfield of H^+. Denote by rec the isomorphism given by the reciprocity law of class field theory:

$$\mathrm{rec} : \mathrm{Pic}(\mathcal{O}) \xrightarrow{\simeq} \mathrm{Gal}(H/K), \quad \mathrm{rec} : \mathrm{Pic}^+(\mathcal{O}) \xrightarrow{\simeq} \mathrm{Gal}(H^+/K). \tag{174}$$

Lemma 5.7 *An embedding Ψ of conductor c exists if and only if there is a ring homomorphism $\mathfrak{o}$ from $\mathcal{O} = \Psi^{-1}(R)$ to $\mathbb{Z}/M\mathbb{Z}$.*

Proof: If such a Ψ exists, the algebra homomorphism $\mathfrak{o}_\Psi : \mathcal{O} \longrightarrow \mathbb{Z}/M\mathbb{Z}$ which to $x \in \mathcal{O}$ associates the upper left-hand entry of the matrix $\Psi(x) \pmod M$ is the desired homomorphism. Conversely, given such an $\mathfrak{o}$, choose a $\mathbb{Z}[1/p]$-module basis (e_1, e_2) for $\mathcal{O}$ with the property that the image of e_1 in $\mathcal{O}/M\mathcal{O}$ is annihilated by $\ker \mathfrak{o}$. The action of $\alpha \in \mathcal{O}$ on this basis is expressed by a matrix $m_\alpha \in R$ and the assignment $\alpha \mapsto M_\alpha$ gives the desired Ψ.

The homomorphism $\mathfrak{o}_\Psi$ is called the *orientation at M* attached to the embedding Ψ. Conjugation by Γ (in fact, by $R^\times$) preserves the orientation of Ψ, so

that $\mathfrak{o}_\Psi$ is an invariant of the Γ-conjugacy class of Ψ. For the definition that follows, it is worth recalling that the compact group $\Psi(K_p^\times/\mathbb{Q}_p^\times)$ acts on $\mathcal{T}$ leaving exactly one vertex fixed, and permuting transitively all the vertices (or edges) which are at a common distance from this fixed vertex.

Fix an orientation $\mathfrak{o} : \mathcal{O} \longrightarrow (\mathbb{Z}/M\mathbb{Z})$. Let $\mathrm{Emb}(\mathcal{O}, R)$ denote the set of optimal embeddings $\Psi : K \longrightarrow M_2(\mathbb{Q})$ of conductor c satisfying:

1. $\mathfrak{o}_\Psi = \mathfrak{o}$;
2. The vertex of $\mathcal{T}$ fixed by $\Psi(K^\times)$ is an even vertex.

Since conjugation by the Atkin-Lehner matrices α_ℓ transitively permutes the possible orientations of Ψ, and conjugation by $\alpha_p \in \tilde{\Gamma} - \Gamma$ interchanges the odd and even vertices of $\mathcal{T}$, it follows that $\mathrm{Emb}(\mathcal{O}, R)$ is non-empty if and only if an embedding of conductor c exists. Let $\mathrm{Emb}(\mathcal{O}, R)/\Gamma$ denote the set of orbits of $\mathrm{Emb}(\mathcal{O}, R)$ under conjugation by Γ.

Proposition 5.8 *The sets $Emb(\mathcal{O}, R)/\Gamma$ and $Pic^+(\mathcal{O})$ are in natural bijection with each other. In particular, $Emb(\mathcal{O}, R)$ is finite of cardinality h^+.*

Proof: A basis (e_1, e_2) for K over $\mathbb{Q}$ is said to be *positive* if

$$\det \begin{pmatrix} e_1 & \bar{e}_1 \\ e_2 & \bar{e}_2 \end{pmatrix} > 0, \quad \text{and} \quad \mathrm{ord}_p \det \begin{pmatrix} e_1 & \bar{e}_1 \\ e_2 & \bar{e}_2 \end{pmatrix} = 0 \pmod 2.$$

Choose an element λ^- of $K^\times$ of negative norm.
Given an embedding $\Psi \in \mathrm{Emb}(\mathcal{O}, R)$, recall the distinguished fixed point z_Ψ of $\bar{\Psi}(K^\times)$ associated to it in section 5.1 and let $\mathfrak{a}_\Psi$ denote the fractional $\mathcal{O}$-ideal defined by

$$\mathfrak{a}_\Psi = \begin{cases} \mathcal{O}z_\Psi + \mathcal{O} & \text{if } (z_\Psi, 1) \text{ is a positive basis of } K \text{ over } \mathbb{Q} \\ \lambda^-(\mathcal{O}z_\Psi + \mathcal{O}) & \text{if } (z_\Psi, 1) \text{ is a negative basis of } K \text{ over } \mathbb{Q}. \end{cases} \tag{175}$$

Conjugating Ψ by an element $\alpha \in \Gamma$ has the effect of replacing $\mathfrak{a}_\Psi$ by an ideal which is equivalent to it, in the strict sense. This is because if $\alpha = \begin{pmatrix} r & s \\ t & u \end{pmatrix}$, then the bases $(z_\Psi, 1)$ and $(\alpha z_\Psi, 1)$ have the same sign of orientation if the element $(tz_\Psi + u)$ is of positive norm, and have opposite orientation otherwise. Hence the function which to Ψ associates the narrow ideal class $\mathfrak{c}_\Psi$ of $\mathfrak{a}_\Psi$ gives a well-defined map

$$\eta_1 : \mathrm{Emb}(\mathcal{O}, R)/\Gamma \longrightarrow \mathrm{Pic}^+(\mathcal{O}).$$

In the opposite direction, given an ideal class $\mathfrak{c}$ in $\mathrm{Pic}^+(\mathcal{O})$, choose a representative ideal $\mathfrak{a}$, and let (e_1, e_2) be a $\mathbb{Z}[1/p]$-module basis for $\mathfrak{a}$ chosen so that:

1. The image of e_1 in $\mathfrak{a}/M\mathfrak{a}$ is annihilated by $\ker \mathfrak{o}$.
2. The pair (e_1, e_2) is a positive basis for $K/\mathbb{Q}$.

Given $\lambda \in \mathcal{O}$, the matrix m_λ expressing the action of multiplication by λ on $\mathfrak{a}$, relative to the basis (e_1, e_2), is an element of R, and the assignment $\lambda \mapsto m_\lambda$ is an algebra embedding of $\mathcal{O}$ into R which gives rise to an optimal embedding $\Psi_{\mathfrak{c}}$ of conductor c. The class of $\Psi_{\mathfrak{c}}$ in $\mathrm{Emb}(\mathcal{O}, R)/\Gamma$ does not depend on the choice of basis (e_1, e_2) satisfying properties 1 and 2 above, and is unaffected by replacing the ideal $\mathfrak{a}$ by $\lambda\mathfrak{a}$ for any element λ of K of positive norm. Hence it give rise to a well-defined function

$$\eta_2 : \mathrm{Pic}^+(\mathcal{O}) \longrightarrow \mathrm{Emb}(\mathcal{O}, R)/\Gamma.$$

The reader will check that η_1 and η_2 are inverse to each other and hence define bijections between the two sets.

Thanks to proposition 5.8, the set $\mathrm{Emb}(\mathcal{O}, R)/\Gamma$ is equipped with a natural simply transitive action by $\mathrm{Pic}^+(\mathcal{O})$, denoted

$$(\mathfrak{c}, \Psi) \mapsto \mathfrak{c} * \Psi.$$

The following conjecture is an analogue of the classical Shimura Reciprocity Law.

Conjecture 5.9 *The global points $P_\Psi \in E(H^+)$ attached to the embeddings Ψ via conjecture 5.6 satisfy*

$$P_{\mathfrak{c}*\Psi} = \mathrm{rec}(\mathfrak{c})^{-1}(P_\Psi), \quad \textit{for all } \mathfrak{c} \in \mathrm{Pic}^+(\mathcal{O}).$$

We now proceed to deduce properties of the points P_Ψ under the assumption that they satisfy conjecture 5.9.

The Action of $\mathbf{Gal}(K_p/\mathbb{Q}_p)$.
Let τ_p denote the generator of $\mathrm{Gal}(K_p/\mathbb{Q}_p) = \mathrm{Gal}(K/\mathbb{Q})$, so that $\tau_p(z) = \bar{z}$. Thanks to the chosen embedding of H^+ into K_p, the involution τ_p can be viewed as an element of $\mathrm{Gal}(H^+/K)$. Recall the Atkin-Lehner involution W_N acting on $S_2(\Gamma_0(N))$ and let w_N denote the eigenvalue of W_N attached to the eigenform f_0.

Proposition 5.10 *Assume the Shimura reciprocity law of conjecture 5.9. Then there exists $\sigma \in Gal(H^+/K)$ (depending on P_Ψ and on the chosen embedding of H^+ into K_p) such that*

$$\bar{P}_\Psi := \tau_p(P_\Psi) = w_N \sigma P_\Psi.$$

Proof: First note that

$$\tau_p J_\Psi = \oint_x^{\bar{z}_\Psi} \int_x^{\gamma_\Psi x} \omega = J_{\Psi'}^{-1}, \tag{176}$$

where $\Psi' = \Psi \circ \tau_p$ is the embedding obtained from Ψ by composing with τ_p. Note that Ψ' is an optimal embedding of conductor c, and that $\Psi'(K^\times)$ fixes an even vertex of $\mathcal{T}$, since Ψ' has the same image as Ψ. But Ψ' does not have the same orientation as Ψ; more precisely, $\mathfrak{o}_{\Psi'} = \mathfrak{o}_\Psi \circ \tau_p$. By the analogue of lemma 2.1 for real quadratic embeddings, $\alpha_M \Psi' \alpha_M^{-1}$ is an oriented optimal embedding. Therefore, by proposition 5.8 there exists $\mathfrak{c} \in \mathrm{Pic}^+(\mathcal{O})$ such that

$$\Psi' = \alpha_M(\mathfrak{c} * \Psi)\alpha_M^{-1} \tag{177}$$

in $\mathrm{Emb}(\mathcal{O}, R)/\Gamma$. It follows from (176) and (177) and the fact that f_0 is an eigenform for W_M with eigenvalue w_M that

$$\tau_p J_\Psi = J_{\mathfrak{c}*\Psi}^{-w_M}. \tag{178}$$

Raise both sides of this equality to the t-th power, and apply Φ_{Tate}, remembering that

$$\Phi_{\mathrm{Tate}} \circ \tau_p = w\tau_p \circ \Phi_{\mathrm{Tate}}. \tag{179}$$

One thus finds, after setting $\sigma = \mathrm{rec}(\mathfrak{c})^{-1}$ and invoking conjecture 5.9:

$$w\tau_p P_\Psi = -w_M P_{\mathfrak{c}*\Psi} = -w_M \sigma P_\Psi. \tag{180}$$

Proposition 5.10 now follows from the fact that w is the negative of the Atkin-Lehner involution at p acting on f_0, so that $-w_M/w = w_N$.

Remark: The Heegner points arising in the classical theory of complex multiplication satisfy a relation similar to the one of proposition 5.10, but with τ_p replaced by complex conjugation. This is hardly surprising, since the prime p plays much the same role in our theory as the infinite place in the classical theory.

Corollary 5.11 *Assume conjecture 5.9. If $h^+ = 1$ then P_Ψ belongs to $E(K)^{w_N}$, the w_N-eigenspace for the action of τ_p on $E(K)$.*

Corollary 5.12 *Assume conjecture 5.9. There exists $\sigma \in Gal(H^+/K)$, depending on the embedding Ψ and on the chosen embedding of H^+ into $\mathbb{C}_p$, such that*

$$tP_\Psi^- = P_\Psi - w\bar{P}_\Psi = P_\Psi + w_M \sigma P_\Psi.$$

Remark: It follows from this corollary that if $w_M = 1$ and $h^+ = 1$, then $tP_\Psi^- = 2P_\Psi$. This remark is sometimes useful because it is somewhat easier to compute P_Ψ^- than P_Ψ. Note however that the points P_Ψ^- are *not* permuted by the action of $\mathrm{Gal}(H^+/K)$, since τ_p does not commute with the elements of this Galois group. Hence, it is essential to work with the better-behaved points P_Ψ if one wishes to calculate Mordell-Weil groups of E over larger ring class fields of K.

The action of complex conjugation.

Let τ_∞ be a complex conjugation in $\mathrm{Gal}(H^+/\mathbb{Q})$. Note that since $K/\mathbb{Q}$ is real and complex conjugation is of order 2, it belongs to the center of $\mathrm{Gal}(H^+/K)$; in particular, it does not depend on the choice of complex embedding of H^+ used to define τ_∞.

Proposition 5.13 *Assume conjecture 5.9. Then*

$$\tau_\infty P_\Psi = w_\infty P_\Psi.$$

Proof: By the Shimura reciprocity law,

$$\tau_\infty P_\Psi = P_{\alpha_\infty \Psi \alpha_\infty^{-1}},$$

where $\alpha_\infty \in R^\times$ is a matrix of determinant -1. On the other hand, by lemma 3.7,

$$J_{\alpha_\infty \Psi \alpha_\infty^{-1}} = J_\Psi^{w_\infty}.$$

The result now follows by raising both sides to the power t and applying Φ_{Tate}.

Corollary 5.14 *Assume conjecture 5.9. If $w_\infty = 1$ then P_Ψ belongs to $E(H)$.*

Remark: It follows from the above corollary that if $w_\infty = 1$, and the order $\mathcal{O}$ has class number 1, then the point P_Ψ belongs to $E(K)$. If furthermore $w_N = 1$ then P_Ψ belongs to $E(\mathbb{Q})$.

5.3 A Gross-Zagier conjecture

Choose a complex character

$$\chi : \mathrm{Pic}^+(\mathcal{O}) \longrightarrow \mathbb{C}^\times \quad \text{such that } \chi(\tau_\infty) = w_\infty. \tag{181}$$

Conjecture 5.9 predicts that the $\mathbb{C}$-linear combination of points

$$P_\chi = \sum_{\mathfrak{c} \in \mathrm{Pic}^+(\mathcal{O})} \bar{\chi}(\mathfrak{c}) P_{\mathfrak{c}*\Psi} \tag{182}$$

belongs to $(E(H^+) \otimes \mathbb{C})^\chi$, the χ-eigenspace for the action of $\mathrm{Gal}(H^+/K)$ on $E(H^+) \otimes \mathbb{C}$. In particular, when χ is the trivial character, the point $P_K := P_\chi$ is a global point in $E(K)$.

Inspired by the formula of Gross and Zagier, one could surmise that there is a simple formula expressing the height of P_χ (after extending this height to a Hermitian pairing on $E(H^+) \otimes \mathbb{C})$) as a multiple of $L'(E/K, \chi, 1)$ by an explicit non-zero fudge factor.

Conjecture 5.15 *The vector P_χ is non-zero if and only if*

$$L'(E/K, \chi, 1) \neq 0.$$

In particular, the point P_K is of infinite order if and only if $L'(E/K, 1) \neq 0$.

A proof of conjecture 5.15 is hard to conceive of in the absence of some machinery for tackling conjectures 7 and 5.9. A precise conjectural Gross-Zagier formula relating the height of P_K to $L'(E/K, 1)$, and some numerical evidence for it, is given in [DG] for elliptic curves of prime conductor.

5.4 Numerical evidence

1. Let E be the elliptic curve $X_0(11)$ with minimal Weierstrass equation

$$y^2 + y = x^3 - x^2 - 10x - 20.$$

It has split multiplicative reduction at 11 so that $w = 1$ and $w_{11} = -1$. The real quadratic field of smallest discriminant in which 11 is inert is $K = \mathbb{Q}(\sqrt{2})$. The sign in the functional equation for $L(E/K, s)$ is -1, and, as

predicted by the Birch and Swinnerton-Dyer conjecture, $E(K)$ contains a point of infinite order

$$P = \left(9/2, \frac{-2+7\sqrt{2}}{4}\right),$$

which in fact generates $E(K)$ up to torsion. Since the field K has narrow class number one, there is a unique oriented optimal embedding Ψ of K of conductor 1, up to conjugation in Γ. We have checked, to an 11-adic accuracy of 11^{-8}, that

$$P_\Psi = \Phi_{\mathrm{Tate}}(J_\Psi) = P.$$

It is instructive to compare this calculation with the significantly more cumbersome ones that were already carried out in [Da2], section 5.1.
Note that the curve E is not unique in its $\mathbb{Q}$-isogeny class. The above calculation indicates that assumption 2 is unduly restrictive and ought to be relaxed, perhaps at the cost of some minor extra complications. This question will be discussed more fully in [DG].

2. Let E be the elliptic curve of conductor 43 with minimal Weierstrass equation given by

$$E : y^2 + y = x^3 + x^2.$$

The quadratic field $K = \mathbb{Q}(\sqrt{37})$ has narrow class number 1, and the order in K of conductor 2 has narrow class number 3. Let Ψ_j $(j = 1, 2, 3)$ denote representatives of the three distinct $\mathbf{SL}_2(\mathbb{Z}[1/43])$-conjugacy classes of oriented optimal embeddings of K into $M_2(\mathbb{Q})$ of conductor 2. Let τ_j be the fixed point for $\Psi_j(K^\times)$ acting on $\mathcal{H}_{43}$, chosen as in section 5.2. A direct calculation shows that one may take τ_1, τ_2 and τ_3 to be

$$\frac{-3+\sqrt{37}}{4}, \quad \frac{-3+\sqrt{37}}{7}, \quad \text{and} \quad -6+\sqrt{37}. \tag{183}$$

Choose $w_\infty = 1$ and set

$$P_j = P_{\Psi_j} = \Phi_{\mathrm{Tate}}(\not\int_{x}^{\tau_j} \int_{x}^{\gamma_{\Psi_j} x} \omega).$$

After computing $P_j = (x_j, y_j)$ numerically to 4 significant 43-adic digits (i.e., modulo 43^4) one finds:

$$\begin{aligned}
P_1 &= (1953822 + 3156001\sqrt{37}, 1647778 + 1133177\sqrt{37}) \pmod{43^4} \\
P_2 &= (1953822 + 262800\sqrt{37}, 1647778 + 2285624\sqrt{37}) \pmod{43^4} \\
P_3 &= (2929963, 123259). \pmod{43^4}
\end{aligned}$$

Further calculation reveals that:

$$\prod_j (t - x_j) = t^3 - 5t^2 - 5t - 1 \pmod{43^4}, \tag{184}$$

$$\prod_j (t - y_j) = t^3 + 17t^2 + 17t - 1 \pmod{43^4}. \tag{185}$$

Let $f_x(t)$ and $f_y(t)$ denote the polynomials in $\mathbb{Q}[t]$ appearing on the right hand sides of (184) and (185) respectively. It is natural to guess (although the author is far from being able to prove this!) that the 43-adic numbers x_j and y_j are roots of these polynomials, a guess which is buttressed by the fact that

1. The splitting field over $\mathbb{Q}$ of both $f_x(t)$ and $f_y(t)$ is the ring class field H of $\mathbb{Q}(\sqrt{37})$ of conductor 2;
2. If x is a root of $f_x(t)$ and y is the (unique) root of $f_y(t)$ defined over $\mathbb{Q}(x)$, the pair (x, y) is a point on $E(H)$.

Such a 43-adic calculation, leading to the discovery of global points on E defined over a cyclic cubic extension of a real quadratic field, can be viewed as providing strong evidence for conjectures 7 and 5.9.

The author is indebted to Peter Green for producing this example. More extensive numerical evidence for conjectures 7, 5.9 and 5.15 will be presented in [DG].

References

[BCDT] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, to appear.

[BD1] M. Bertolini and H. Darmon, *Heegner points on Mumford-Tate curves*. Invent. Math **126** 413–456 (1996).

[BD2] M. Bertolini and H. Darmon, *A rigid-analytic Gross-Zagier formula and arithmetic applications*. Annals of Math **146** (1997) 111-147.

[BD3] M. Bertolini and H. Darmon, *Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformisation*. Invent. Math, **131** (1998), no. 3, 453–491.

[BD4] M. Bertolini and H. Darmon, *p-adic periods, p-adic L-functions and the p-adic uniformisation of Shimura curves*, Duke Math. J. **98** (1999), no. 2, 305–334.

[BD5] M. Bertolini and H. Darmon, *Iwasawa's main conjecture for elliptic curves in the anticyclotomic setting*, submitted.

[BD6] M. Bertolini, H. Darmon. *The p-adic L-functions of modular elliptic curves*. To appear in *2001 and Beyond: Springer's special volume for WMY 2000*, Springer-Verlag, 2001.

[BD7] M. Bertolini, H. Darmon. *Euler systems attached to elliptic curves over ring class fields of real quadratic fields*, in progress.

[BDIS] M. Bertolini, H. Darmon, A. Iovita, M. Spiess, *Teitelbaum's conjecture in the anticyclotomic setting*, American Journal of Mathematics, to appear.

[BFG] D. Blasius, J. Franke, and F. Grunewald, *Cohomology of S-arithmetic subgroups in the number field case*. Invent. Math. **116** (1994), no. 1-3, 75–93.

[Da1] H. Darmon, *Heegner points, Heegner cycles, and congruences*, in "Elliptic curves and related topics", CRM proceedings and lecture notes vol. **4**, H. Kisilevsky and M. Ram Murty eds. (1992) pp. 45-60.

[Da2] H. Darmon. *Stark-Heegner points over real quadratic fields*. Number theory (Tiruchirapalli, 1996), 41–69, Contemp. Math., **210**, Amer. Math. Soc., Providence, RI, 1998.

[DG] H. Darmon, P. Green, *Elliptic curves and class fields of real quadratic fields: algorithms and evidence*, Journal of experimental mathematics, submitted.

[DS] E. de Shalit, *p-adic periods and modular symbols of elliptic curves of prime conductor*. Invent. Math. **121** (1995), no. 2, 225–255.

[Ed] B. Edixhoven, *On the Manin constants of modular elliptic curves*. Arithmetic algebraic geometry (Texel, 1989), 25–39, Progr. Math., **89**, Birkhäuser Boston, Boston, MA, 1991.

[GvdP] L. Gerritzen; M. van der Put,*Schottky groups and Mumford curves*. Lecture Notes in Mathematics, **817**. Springer, Berlin, 1980.

[GS] R. Greenberg, G. Stevens, *p-adic L-functions and p-adic periods of modular forms*. Invent. Math. **111** (1993), no. 2, 407–447.

[Gr] B.H. Gross, *Heights and the special values of L-series*. Number theory (Montreal, Que., 1985), 115–187, CMS Conf. Proc., **7**, Amer. Math. Soc., Providence, RI, 1987.

[GZ] B.H. Gross, D.B. Zagier. *Heegner points and derivatives of L-series*. Invent. Math. **84** (1986), no. 2, 225–320.

[Ih1] Y. Ihara, *On congruence monodromy problems*. Vol. 1. Lecture Notes, No. 1 Department of Mathematics, University of Tokyo, Tokyo 1968.

[Ih2] Y. Ihara, *Congruence relations and Shimūra curves*. Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 291–311, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979.

[Kl] C. Klingenberg, *On p-adic L-functions of Mumford curves. p*-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), 277–315, Contemp. Math., **165**, Amer. Math. Soc., Providence, RI, 1994.

[Me] J. Mennicke, *On Ihara's modular group*. Invent. Math. **4** (1967) 202–228.

[MM] M.R. Murty; V.K. Murty. *Non-vanishing of L-functions and applications*. Progress in Mathematics, **157**. Birkhuser Verlag, Basel, 1997.

[MTT] B. Mazur, J. Tate, J. Teitelbaum. *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*. Invent. Math. **84** (1986), no. 1, 1–48.

[MT] B. Mazur, J. Tate. *Refined conjectures of the "Birch and Swinnerton-Dyer type"*. Duke Math. J. **54** (1987), no. 2, 711–750.

[O] T. Oda, *Periods of Hilbert modular surfaces*. Progress in Mathematics, **19**. Birkhäuser, Boston, Mass., 1982.

[Sch] P. Schneider, *Rigid-analytic L-transforms*. Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), 216–230, Lecture Notes in Math., **1068**, Springer, Berlin-New York, 1984.

[Se1] J-P. Serre. Trees. Translated from the French by John Stillwell. Springer-Verlag, Berlin-New York, 1980.

[Se2] J.-P. Serre, *Le problème des groupes de congruence pour* $\mathbf{SL}_2$. Ann. of Math. (2) **92** (1970) 489–527.

[Sh] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Reprint of the 1971 original. Publications of the Mathematical Society of Japan, 11. Kanô Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994.

[St] H.M. Stark, *Modular forms and related objects.* Number theory (Montreal, Que., 1985), 421–455, CMS Conf. Proc., 7, Amer. Math. Soc., Providence, R.I., 1987.

[Te] J.T. Teitelbaum. *Values of p-adic L-functions and a p-adic Poisson kernel*. Invent. Math. **101** (1990), no. 2, 395–410.

[TW] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*. Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*. Ann. of Math. (2) **141** (1995), no. 3, 443–551.