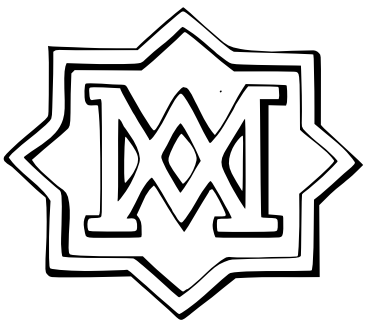
ANNALS OF MATHEMATICS

The rationality of Stark-Heegner points over genus fields of real quadratic fields

By Massimo Bertolini and Henri Darmon



SECOND SERIES, VOL. 170, NO. 1

July, 2009

ANMAAH

Annals of Mathematics, **170** (2009), 343–369

The rationality of Stark-Heegner points over genus fields of real quadratic fields

By MASSIMO BERTOLINI and HENRI DARMON

Abstract

We study the algebraicity of *Stark-Heegner points* on a modular elliptic curve E. These objects are p-adic points on E given by the values of certain p-adic integrals, but they are conjecturally defined over ring class fields of a real quadratic field K. The present article gives some evidence for this algebraicity conjecture by showing that linear combinations of Stark-Heegner points weighted by certain genus characters of K are defined over the predicted quadratic extensions of K. The non-vanishing of these combinations is also related to the appropriate twisted Hasse-Weil L-series of E over K, in the spirit of the Gross-Zagier formula for classical Heegner points.

Introduction

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, and let f be the normalised cusp form of weight 2 on $\Gamma_0(N)$ attached to E. Suppose that there is an odd prime $p\|N$ of multiplicative reduction for E, and let K be a real quadratic field satisfying the following modified Heegner hypothesis:

1. The prime p is inert in K;
2. All the primes dividing $M := N/p$ are split in K.

Fix an embedding of K and its p-adic completion K_p into $\mathbb{C}_p := \widehat{\overline{\mathbb{Q}}}_p$, and let $\mathcal{H}_p = \mathbb{C}_p - \mathbb{Q}_p$ denote the p-adic upper half plane. Note that since p is inert in K, the set $\mathcal{H}_p \cap K$ is non-empty.

The first section of this paper briefly recalls the main construction of [Dar01], which associates to the cusp form f and to any $\tau \in \mathcal{H}_p \cap K$ a so-called *Stark-Heegner point* $P_\tau \in E(K_p)$. Conjecture 5.9 of [Dar01] predicts that some integral multiple of this point is defined over a ring class field of K depending on τ, and gives an explicit description, analogous to the Shimura reciprocity law, for the action of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ on the collection of Stark-Heegner points attached to K.

The main result of the present article (Theorem 1) gives some evidence for Conjecture 5.9 of [Dar01] by showing that certain integral linear combinations of Stark-Heegner points are global points on E defined over the expected abelian extension of K. The non-vanishing of these points is also related to the first derivative at $s = 1$ of the Hasse-Weil L-series of E/K in the spirit of the Gross-Zagier formula, lending support for Conjecture 5.15 of [Dar01].

Before stating Theorem 1 precisely, some further notation is required. Let $M_2(\mathbb{Z}[1/p])$ denote the ring of 2×2 matrices with entries in $\mathbb{Z}[1/p]$, and let $R \subset M_2(\mathbb{Z}[1/p])$ denote the subring of matrices which are upper-triangular modulo M. The order associated to $\tau \in \mathcal{H}_p \cap K$ is defined to be

$$\mathcal{O}_\tau = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R \text{ such that } a\tau + b = c\tau^2 + d\tau \right\} \subset K,$$

where the inclusion on the right sends the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to the element $c\tau + d$. Via this inclusion, $\mathcal{O}_\tau$ is identified with a $\mathbb{Z}[1/p]$-order of K. Let D be the discriminant of a (not necessarily maximal) order of K, and let $\mathcal{O}_D$ denote the $\mathbb{Z}[1/p]$-order of K of that discriminant. Set

$$\mathcal{H}_p^D = \left\{ \tau \in \mathcal{H}_p \cap K \text{ such that } \mathcal{O}_\tau = \mathcal{O}_D \right\}.$$

The group

$$\Gamma := \left\{ \gamma \in R^\times \text{ such that } \det(\gamma) = 1 \right\} \tag{1}$$

acts on $\mathcal{H}_p$ by Möbius transformations, and preserves $\mathcal{H}_p^D$ for any D.

Let $G_D := \mathrm{Pic}^+(\mathcal{O}_D)$ denote the Picard group of oriented $\mathcal{O}_D$-modules, or equivalently, the group of $\mathbf{SL}_2(\mathbb{Z})$-equivalence classes of primitive integral binary quadratic forms of discriminant D equipped with the group law given by Gaussian composition. Class field theory defines an isomorphism

$$\mathrm{rec} : G_D \longrightarrow \mathrm{Gal}(H_D/K),$$

where H_D is the so-called *narrow ring class field* attached to $\mathcal{O}_D$. The fact that p is inert in K implies that the prime ideal $p\mathcal{O}_K$ splits completely in H_D/K. Choose a prime of H_D above p. This choice determines an extension to H_D of the chosen embedding $K \longrightarrow \mathbb{C}_p$.

The quotient $\Gamma\backslash\mathcal{H}_p^D$ is equipped with a natural action of G_D whose definition is recalled in Section 1.4, and which is written $(g, \tau) \mapsto \tau^g$, for $g \in G_D$ and $\tau \in \Gamma\backslash\mathcal{H}_p^D$.

Conjecture 5.9 of [Dar01] predicts that some fixed multiple of P_τ is a global point in $E(H_D)$, so that P_τ belongs to $E(H_D) \otimes \mathbb{Q}$, and

$$P_{\tau^g} = \mathrm{rec}(g)^{-1}(P_\tau) \quad \text{for all } g \in G_D. \tag{2}$$

(Note that this compatibility does not depend on the choice of embedding of H_D into $\mathbb{C}_p$ that was made.)

Suppose now that D is the discriminant of K. A *genus character* of K is a quadratic unramified character of $\mathrm{Gal}(\bar{K}/K)$. Such a genus character χ cuts out a biquadratic (or quadratic, in the special case where χ is the trivial character) extension of $\mathbb{Q}$, denoted H_χ:

$$H_\chi = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2}), \quad \text{where } D = D_1 D_2.$$

Let χ_1, χ_2, and ϵ_K be the Dirichlet characters associated to the quadratic fields $\mathbb{Q}(\sqrt{D_1})$, $\mathbb{Q}(\sqrt{D_2})$, and K respectively. Note that $\chi_1\chi_2 = \epsilon_K$. The genus characters are in bijection with the factorisations of D into a product of two relatively prime fundamental discriminants, or, equivalently, with the unordered pairs of primitive quadratic Dirichlet characters (χ_1, χ_2) of coprime conductors satisfying $\chi_1\chi_2 = \epsilon_K$. (The trivial character χ corresponds to the factorisation $D = 1 \cdot D$.) Let $E(H_\chi)^\chi$ denote the submodule of the Mordell-Weil group $E(H_\chi)$ on which $\mathrm{Gal}(H_D/K)$ acts via the character χ.

Define the point

$$P_\chi = \sum_{g \in G_D} \chi(g) P_{\tau^g} \in E(K_p).$$

Equation (2) implies that an integral multiple of P_χ belongs to $E(H_\chi)^\chi$, and Conjecture 5.15 of [Dar01] predicts that this point is of infinite order if and only if $L'(E/K,\chi,1)\neq 0$.

Let $q\in p\mathbb{Z}_p$ be the Tate period attached to E, and write

$$\Phi_{\mathrm{Tate}}: K_p^\times/q^{\mathbb{Z}}\longrightarrow E(K_p)$$

for the Tate uniformisation (which is defined since p is inert in K and E therefore acquires split multiplicative reduction over K_p). Let $\log_q: K_p^\times\longrightarrow K_p$ denote the branch of the p-adic logarithm satisfying $\log_q(q)=0$, and define a homomorphism

$$\log_E: E(K_p)\longrightarrow K_p$$

by the rule

$$\log_E(P):=\log_q(\Phi_{\mathrm{Tate}}^{-1}(P)).$$

For each $m|N$ with $\gcd(m,N/m)=1$, let w_m denote the sign of the Fricke involution at m acting on f. Note that the modified Heegner hypothesis implies that $\epsilon_K(-M)=1$, and therefore $\chi_1(-M)=\chi_2(-M)$. The main result of this article is

THEOREM 1. *Let χ be the genus character attached to the pair of Dirichlet characters χ_1 and χ_2. Suppose that E has at least two primes of multiplicative reduction, and that $\chi_1(-M)=-w_M$.*

1. *There is a global point $\mathbf{P}_\chi\in E(H_\chi)^\chi$ and $t\in\mathbb{Q}^\times$ such that*

$$\log_E(P_\chi)=t\log_E(\mathbf{P}_\chi). \tag{3}$$

2. *The point $\mathbf{P}_\chi$ is of infinite order if and only if $L'(E/K,\chi,1)\neq 0$.*

Remark 2. Theorem 1 shows that P_χ coincides with the image of a global point in $E(K_p)\otimes\mathbb{Q}$. This implies that a suitable integral multiple of P_χ belongs to the natural image of $E(H_\chi)^\chi$ in $E(K_p)$.

By way of providing a context for the proof of Theorem 1, we note the analogy between the approach that it follows and Kronecker's "solution to Pell's equation" in terms of special values of the Dedekind eta-function. (See Chapter IX of [Wei76] for a historical account, and Chapter II.1 of [Sie80] for a more detailed treatment.) In the classical setting considered by Kronecker, the fundamental discriminant D is taken to be *negative*, and corresponds to an imaginary quadratic subfield K of $\mathbb{C}$. The p-adic upper half plane is replaced by its archimedean counterpart $\mathcal{H}$, and $\mathcal{H}^D$ is given the obvious meaning (with $M=1$). This set is preserved under the action of $\mathbf{SL}_2(\mathbb{Z})$ by Möbius transformations, and the quotient $\mathbf{SL}_2(\mathbb{Z})\backslash\mathcal{H}^D$ is equipped with a natural action of the class group G_D of K. A quadratic character χ of G_D—assumed to be non-trivial, although the trivial character requires no special consideration in the setting of Stark-Heegner points—corresponds to a pair

of Dirichlet characters χ_1 and χ_2 which are even and odd respectively, cutting out quadratic extensions K_1 and K_2 of $\mathbb{Q}$. Let $\epsilon_1 > 1$ be the fundamental unit of the real quadratic field K_1, denote by h_j (for $j = 1, 2$) the class number of K_j, and write w_2 for the number of roots of unity in K_2. After setting

$$\eta^*(\tau) := |D|^{-1/4}\sqrt{2y}|\eta(\tau)|^2,$$

Kronecker shows (cf. Theorem 6 of Chapter II.1 of [Sie80]) that for any $\tau \in \mathscr{H}^D$,

$$\sum_{\sigma \in G_D} \chi(\sigma) \log \eta^*(\tau^\sigma) = -\frac{2h_1h_2}{w_2}\log(\epsilon_1). \tag{4}$$

This expresses a solution to the Pell equation $x^2 - D_1y^2 = 1$ in terms of the function η^* evaluated at suitable quadratic imaginary arguments. Kronecker's proof is obtained by combining the following three ingredients:

1. The *Kronecker limit formula*, which expresses the left-hand side of (4) in terms of the L-series $\zeta(K, \chi, s) = \sum_{\mathfrak{a}} \chi(\mathfrak{a})N(\mathfrak{a})^{-s}$, where the sum is taken over all the ideals $\mathfrak{a}$ of K:

$$-\sum_{\sigma \in G_D} \chi(\sigma) \log \eta^*(\tau^\sigma) = \frac{d}{ds}\zeta(K, \chi, s)|_{s=0}. \tag{5}$$

2. A *factorisation* of $\zeta(K, \chi, s)$ as a product of the Dirichlet L-series attached to χ_1 and χ_2:

$$\zeta(K, \chi, s) = L(\chi_1, s)L(\chi_2, s). \tag{6}$$

3. *Dirichlet's class number formula* which asserts that

$$L'(\chi_1, 0) = h_1 \log(\epsilon_1), \qquad L(\chi_2, 0) = \frac{2h_2}{w_2}. \tag{7}$$

Kronecker's identity (4) is a direct consequence of (5), (6) and (7). It can also be understood in the framework of the theory of complex multiplication, which relates the individual quantities $\eta^*(\tau^\sigma)$ to elliptic units defined over H_D. Kronecker's approach is noteworthy in that it *makes no use* of the theory of complex multiplication. This represents an advantage in the setting of Stark-Heegner points attached to real quadratic fields, where no analogue of the theory of complex multiplication is known, and where the algebraicity of the individual quantities P_τ remains conjectural.

The proof of Theorem 1 is explained in Section 4. At this stage we limit ourselves to some general remarks on the counterparts to steps 1, 2, and 3 above in our approach.

1. The role of Kronecker's limit formula is played by Theorem 4.1, which relates the Stark-Heegner point P_χ to the leading term of a *Hida p-adic L-function*

$L_p(f_\infty/K, \chi, k)$ attached to the datum of a Hida family $\{f_\infty\}$ interpolating f in weight two. The relation that emerges between periods of Hida families and Stark-Heegner points represents a new insight that was suggested by combining the calculations in [Das04] and [DD06] with the main result of [BD98]. It is hoped that Theorem 4.1 may be of some independent interest beyond its role in the proof of Theorem 1.

2. The Hida L-function $L_p(f_\infty/K, \chi, k)$ interpolates the central critical values $L(f_k/K, \chi, k/2)$ of the weight k specialisations of f_∞. This interpolation property is a direct consequence of a formula of Popa [Pop06] expressing these values in terms of certain "geodesic cycle integrals" attached to f and K, à la Shintani. This interpolation property is the key to expressing $L_p(f/K, \chi, k)$ as a product of two Mazur-Kitagawa p-adic L-functions $L_p(f_\infty, \chi_j, k, s)$ attached to $\{f_\infty\}$ and the Dirichlet characters χ_1 and χ_2, restricted to the central critical line $s = k/2$.

3. One is finally reduced to expressing the leading term in a neighbourhood of $k = 2$ of $L_p(f_\infty, \chi_j, k, k/2)$ in terms of rational quantities and logarithms of global points. This last ingredient is supplied by Theorem 5.4 of [BD07], whose precise formulation is recalled in Section 4, and whose proof relies on a p-adic analytic construction of (classical) Heegner points coming from Shimura curve parametrisations, via the Cerednik-Drinfeld theory of p-adic uniformisation of these curves. It is this reliance on parametrisations by Shimura curves over $\mathbb{Q}$ which forces the assumption in Theorem 1 that E has at least two primes of multiplicative reduction.

Acknowledgements. The authors would like to thank the anonymous referee for detailed comments and suggestions which led to significant improvements in the exposition. The second author also acknowledges Samit Dasgupta for a stimulating collaboration [DD06] which led to some key insights which are used in the present work.

1. **A review of Stark-Heegner points**

This section reviews the definition of Stark-Heegner points given in [Dar01], presenting it in a way that is adapted to the subsequent proof of Theorem 1.

1.1. *Modular symbols.* Let $g \in S_k(\Gamma_0(N))$ be a normalised cusp form of even weight $k \geq 2$ on $\Gamma_0(N)$, and let K_g denote the finite extension of $\mathbb{Q}$ generated by its Fourier coefficients $a_n(g)$ $(n \geq 1)$. We view K_g as a subfield both of $\mathbb{C}$ and $\mathbb{C}_p$, by fixing complex and p-adic embeddings of K_g.

Let F be a field, and let $\mathcal{P}_k(F)$ denote the space of homogeneous polynomials in two variables of degree $k-2$ with coefficients in F. It is equipped with a right

action of $\mathbf{GL}_2(\mathbb{Q})$ given by the rule

$$(P|\gamma)(x,y) := P(ax+by, cx+dy), \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{8}$$

Let $V_k(F)$ denote the F-linear dual of $\mathcal{P}_k(F)$.

A *modular symbol* with values in an abelian group G is a function

$$I : \mathbb{P}_1(\mathbb{Q}) \times \mathbb{P}_1(\mathbb{Q}) \longrightarrow G, \text{ denoted } (r,s) \mapsto I\{r \to s\},$$

satisfying

$$I\{r \to s\} + I\{s \to t\} = I\{r \to t\}, \quad \text{for all } r,s,t \in \mathbb{P}_1(\mathbb{Q}).$$

The group $\mathbf{GL}_2(\mathbb{Q})$ acts on the space of $V_k(\mathbb{C})$-valued modular symbols by the rule

$$(I|\gamma)\{r \to s\}(P) := I\{\gamma r \to \gamma s\}(P|\gamma^{-1}).$$

The periods of the form g are encoded in such a modular symbol, denoted $\tilde{I}_g$ and defined by

$$\tilde{I}_g\{r \to s\}(P) := 2\pi i \int_r^s g(z) P(z,1) dz.$$

This symbol is invariant under $\Gamma_0(N)$.

The matrix $c = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ normalises $\Gamma_0(N)$ and hence induces an involution on the space $\mathrm{MS}(V_k(\mathbb{C}))^{\Gamma_0(N)}$ of $\Gamma_0(N)$-invariant, $V_k(\mathbb{C})$-valued modular symbols. Let $\tilde{I}_g^+$ and $\tilde{I}_g^-$ denote the plus and minus eigencomponents of $\tilde{I}_g$ for this involution.

PROPOSITION 1.1. *There exist complex periods Ω_g^+ and Ω_g^- with the property that the modular symbols*

$$I_g^+ := (\Omega_g^+)^{-1} \tilde{I}_g^+, \qquad I_g^- := (\Omega_g^-)^{-1} \tilde{I}_g^-$$

belong to $\mathrm{MS}(V_k(K_g)))$. *These periods can be chosen to satisfy*

$$\Omega_g^+ \Omega_g^- = \langle g, g \rangle, \tag{9}$$

where $\langle g, g \rangle$ is the Petersson scalar product of g with itself.

Proof. The proof is explained, for example, in Section 1.1 of [KZ84]. (See in particular the first corollary and the third theorem in that section.) □

Remark 1.2. Note that the periods $\Omega_g^{\pm}$ are only well-defined up to multiplication by a non-zero scalar in $K_g^{\times}$. This ambiguity seems unavoidable, because no obvious choice of $\Omega_g^{\pm}$ imposes itself naturally, even though the product $\Omega_g^+ \Omega_g^-$ is uniquely defined by (9).

Choose a "sign at infinity" $w_\infty \in \{+1, -1\}$, and set

$$\Omega_g := \begin{cases} \Omega_g^+ & \text{if } w_\infty = +1; \\ \Omega_g^- & \text{if } w_\infty = -1; \end{cases} \qquad I_g := \begin{cases} I_g^+ & \text{if } w_\infty = +1; \\ I_g^- & \text{if } w_\infty = -1. \end{cases}$$

Note that the modular symbol I_g can be viewed as an element of $\mathrm{MS}(V_k(\mathbb{C}_p))$ thanks to the chosen embedding of K_g into $\mathbb{C}_p$.

1.2. *Double integrals.* In the case where f is a modular form of weight 2 on $\Gamma_0(N)$ with rational Fourier coefficients, the modular symbol $I_f := I_f(1)$ is $\mathbb{Q}$-valued, and can even be rescaled so that it takes values in $\mathbb{Z}$. Assume that this has been done from now on.

A measure on $\mathbb{P}_1(\mathbb{Q}_p)$ is an element of the continuous $\mathbb{Q}_p$-linear dual of the space of continuous $\mathbb{Q}_p$-valued functions on $\mathbb{P}_1(\mathbb{Q}_p)$, equipped with the topology of uniform convergence. Given a measure μ, and a compact open subset U of $\mathbb{P}_1(\mathbb{Q}_p)$, set $\mu(U) := \mu(\chi_U)$, where χ_U denotes the characteristic function of U. The function $U \mapsto \mu(U)$ is a bounded, finitely additive $\mathbb{Q}_p$-valued function on the set of compact open subsets of $\mathbb{P}_1(\mathbb{Q}_p)$. Conversely, any such function gives rise to a $\mathbb{Q}_p$-valued measure on $\mathbb{P}_1(\mathbb{Q}_p)$. The measure μ is said to be *integral*, or *$\mathbb{Z}$-valued*, if $\mu(U)$ belongs to $\mathbb{Z}$ for all compact open $U \subset \mathbb{P}_1(\mathbb{Q}_p)$.

Recall the group Γ of equation (1) in the introduction. Fix a subset $\mathbb{P}$ of $\mathbb{P}_1(\mathbb{Q})$ on which Γ acts transitively by Möbius transformations.

The following elementary proposition is key to the definition of Stark-Heegner points attached to real quadratic fields.

PROPOSITION 1.3. *There exists a unique system of $\mathbb{Z}$-valued measures on $\mathbb{P}_1(\mathbb{Q}_p)$, indexed by $r, s \in \mathbb{P}$ and denoted $\mu_f\{r \to s\}$, satisfying the following properties.*

1. *For all $r, s \in \mathbb{P}$,*

$$\mu_f\{r \to s\}(\mathbb{P}_1(\mathbb{Q}_p)) = 0, \qquad \mu_f\{r \to s\}(\mathbb{Z}_p) = I_f\{r \to s\}.$$

2. *For all $\gamma \in \Gamma$, and all compact open $U \subset \mathbb{P}_1(\mathbb{Q}_p)$,*

$$\mu_f\{\gamma r \to \gamma s\}(\gamma U) = \mu_f\{r \to s\}(U).$$

Proof. The proof of this proposition is identical to that of Proposition 2.6 of [DD06], which considered the case where the newform f is replaced by the logarithmic derivative of a modular unit, a weight two Eisenstein series. The main property of this Eisenstein series that is used is the fact that it is fixed by the Hecke operator U_p^2. Since this is also true of f, the proof of Proposition 2.6 can be adapted to the setting at hand with essentially no modifications. □

Remark 1.4. We have chosen to consider modular symbols defined on $\mathbb{P}\times\mathbb{P}$, largely for convenience: for example, this will guarantee the uniqueness of the "indefinite integral" of Proposition 1.5.

The measures μ_f can be used to define a "double multiplicative integral" attached to $\tau_1, \tau_2 \in \mathscr{H}_p$ and $r, s \in \mathbb{P}$ as in equation (71) of [Dar01], by setting

$$\text{(10)} \qquad \prod_{\tau_1}^{\tau_2}\int_r^s \omega_f := \prod_{\mathbb{P}_1(\mathbb{Q}_p)} \left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_f\{r\to s\}(t).$$

The "multiplicative integral" notation appearing on the right indicates that a limit of Riemann products is being taken, rather than a limit of Riemann sums, i.e., that the integration is relative to the multiplicative structure on $\mathbb{C}_p^\times$. Such a definition is made possible by the fact that for each $r, s \in \mathbb{P}$, the measure $\mu_f\{r\to s\}$ is $\mathbb{Z}$-valued, and that the integrand is a continuous $K_p^\times$-valued function on $\mathbb{P}_1(\mathbb{Q}_p)$ relative to the natural topology on $K_p^\times$. (For a more detailed discussion of this multiplicative integral, and its basic properties, see the discussion following Lemma 1.10 in [Dar01].)

Recall the Tate period $q \in p\mathbb{Z}_p$ attached to $E/\mathbb{Q}_p$, and the branch $\log_q$ of the p-adic logarithm sending q to 0. Define

$$\text{(11)} \qquad \int_{\tau_1}^{\tau_2}\int_r^s \omega_f := \log_q\left(\prod_{\tau_1}^{\tau_2}\int_r^s \omega_f\right).$$

Note that the definition of this "additive integral" differs somewhat from the definition given in [Dar01], where the Iwasawa branch of the p-adic logarithm satisfying $\log(p) = 0$ is used. (Cf. equation (73) of [Dar01].)

1.3. *Indefinite integrals.* The following result justifies the choice of branch of p-adic logarithm that was made in (11).

PROPOSITION 1.5. *There is a unique function from $\mathscr{H}_p\times\mathbb{P}\times\mathbb{P}$ to $\mathbb{C}_p$, denoted*

$$(\tau, r, s) \mapsto \int^{\tau}\int_r^s \omega_f,$$

satisfying

1. *For all $\gamma \in \Gamma$,*
$$\int^{\gamma\tau}\int_{\gamma r}^{\gamma s} \omega_f = \int^{\tau}\int_r^s \omega_f.$$
2. *For all $\tau_1, \tau_2 \in \mathscr{H}$,*
$$\int^{\tau_2}\int_r^s \omega_f - \int^{\tau_1}\int_r^s \omega_f = \int_{\tau_1}^{\tau_2}\int_r^s \omega_f.$$

3. *For all* $r, s, t \in \mathbb{P}$,

$$\int_r^\tau \int_r^t \omega_f + \int_t^\tau \int_t^s \omega_f = \int_r^\tau \int_r^s \omega_f.$$

Proof. The proof of this proposition is explained in Section 3.1 of [Dar01], where it is reduced to the exceptional zero conjecture of Mazur, Tate and Teitelbaum proved by Greenberg and Stevens. (In the notation of Section 3.1 of [Dar01], and in particular of equation (162),

$$\int_r^\tau \int_r^s \omega_f = \log_q(\eta_{f,\tau}\{r \to s\}).)$$

A more direct proof, albeit one whose main idea can still be traced to the calculations of Greenberg and Stevens, can be obtained by specialising the approach described in [BDI] to weight 2 modular forms. □

The function which is characterised indirectly in Proposition 1.5 is called the *indefinite integral* attached to f. The articles [DG02] and [DP06] explain how Proposition 1.5 can be used to produce efficient algorithms for the numerical evaluation of the indefinite integral. Section 2.3 gives a direct formula for it in terms of the periods of the Hida family interpolating f, which is better adapted to the general calculations of this paper.

Remark 1.6. It is the *existence* of the indefinite integral that relies crucially on the branch of p-adic logarithm chosen in (11). Its *uniqueness* then follows when we note that the difference

$$\delta\{r \to s\} := \int_r^\tau \int_r^s \omega_f^{(1)} - \int_r^\tau \int_r^s \omega_f^{(2)}$$

of any two functions satisfying properties 1, 2 and 3 of Proposition 1.5 is independent of the choice of τ, and hence defines a Γ-invariant $\mathbb{C}_p$-valued modular symbol on $\mathbb{P} \times \mathbb{P}$. Since Γ acts transitively on $\mathbb{P}$, such a symbol is determined by the homomorphism $\varphi_\delta : \Gamma \longrightarrow \mathbb{C}_p$ defined by choosing a base point $r \in \mathbb{P}$ and setting $\varphi_\delta(\gamma) = \delta\{r \to \gamma r\}$. But this homomorphism is necessarily trivial, since Γ has finite abelianisation and $\mathbb{C}_p$ is torsion-free.

Remark 1.7. Proposition 1.5 can be refined (cf. Theorem 5.2 of [BDG04], or Theorem 3.3 of [Das05]) to yield the existence of a lattice $Q \subset \mathbb{C}_p^\times$ which is commensurable with $q^{\mathbb{Z}}$, and an "indefinite multiplicative integral"

$$\oint_r^\tau \int_r^s \omega_f \in \mathbb{C}_p^\times / Q$$

satisfying the obvious multiplicative analogues of the properties listed in Proposition 1.5. (Cf. equations (163)–(165) of [Dar01].) Roughly speaking, the lattice Q appears

as the obstruction to splitting a two-cocycle in $H^2(\Gamma, \mathbb{C}_p^\times)$ constructed in terms of the double multiplicative integral. Note that $\log_q(Q) = 0$, and that we can write

$$\int\!\!\int_r^s \omega_f = \log_q\left(\not\int\!\!\int_r^s \omega_f\right).$$

1.4. *Stark-Heegner points.* Given $\tau \in \mathscr{H}_p \cap K$, let $\gamma_\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ denote the unique generator for the stabiliser of τ in Γ satisfying

$$c\tau + d > 1. \tag{12}$$

(In this inequality, we have made use of the fixed real embedding of K.) Associate to τ a multiplicative and additive period by choosing any base point $r \in \mathbb{P}$ and setting

$$J_\tau^\times := \not\int\!\!\int_r^{\gamma_\tau r} \omega_f \ \in K_p^\times/Q, \qquad J_\tau := \log_q(J_\tau^\times) = \int\!\!\int_r^{\gamma_\tau r} \omega_f. \tag{13}$$

Since $\Phi_{\mathrm{Tate}}(Q)$ is contained in $E(K_p)_{\mathrm{tors}}$, the image of $J_\tau^\times$ under Φ_{Tate} is well-defined in $E(K_p) \otimes \mathbb{Q}$, and is called the *Stark-Heegner point* attached to τ and f:

$$P_\tau := \Phi_{\mathrm{Tate}}(J_\tau^\times); \qquad \text{hence } \log_E(P_\tau) = J_\tau. \tag{14}$$

Let D be the discriminant of K. The modified Heegner hypothesis imposed on K in the first paragraph of the introduction implies the existence of an element $\delta \in \mathbb{Z}/M\mathbb{Z}$ satisfying

$$\delta^2 \equiv D \pmod{M}.$$

Fix such a δ once and for all. Let $\mathscr{F}^D$ denote the set of primitive binary quadratic forms $Ax^2 + Bxy + Cy^2$ of discriminant D satisfying

$$M|A, \quad B \equiv \delta \pmod{M}.$$

The set $\mathscr{F}^D$ is preserved under the natural action of $\Gamma_0(M)$ defined by (8). Recall the class group G_D of $\mathbf{SL}_2(\mathbb{Z})$-equivalence classes of primitive binary quadratic forms of discriminant D. The natural map

$$\Gamma_0(M)\backslash\mathscr{F}^D \longrightarrow G_D$$

obtained by sending the class of the quadratic form Q to its corresponding $\mathbf{SL}_2(\mathbb{Z})$-equivalence class is readily seen to be a bijection, and hence $\Gamma_0(M)\backslash\mathscr{F}^D$ is endowed with the stucture of a principal homogeneous space under G_D. If $Q(x, y)$ belongs to $\Gamma_0(M)\backslash\mathscr{F}^D$, and σ to G_D, write Q^σ for the image of Q by σ. Let H_D denote the narrow Hilbert class field of K, whose Galois group is identified with G_D, and let

$$\mathrm{rec} : G_D \longrightarrow \mathrm{Gal}(H_D/K)$$

denote the isomorphism arising from the reciprocity law of global class field theory.

Given $Q = Ax^2 + Bxy + Cy^2 \in \Gamma_0(M)\backslash\mathscr{F}^D$, let

$$\tau_Q := \frac{-B + \sqrt{D}}{2A} \tag{15}$$

be a fixed root of the quadratic polynomial $Q(x, 1)$. Note that τ_Q belongs (via the fixed p-adic embedding of K) to $\mathscr{H}_p^D$, and that its image in $\Gamma\backslash\mathscr{H}_p^D$ is well-defined. Given $\sigma \in G_D$, write $\tau^\sigma \in \mathscr{H}_p^D$ for the root of any quadratic form in the $\Gamma_0(M)$-equivalence class of Q^σ. This definition gives a precise meaning to the conjectural equation (2) of the introduction.

Since the definition of Stark-Heegner points is purely p-adic analytic, little can be said about the action of $\mathrm{Gal}(H_D/K)$ on these points independently of assertion (2) in the introduction. However, something unconditional can be asserted about the action of the Frobenius element at p, denoted $\tau_p \in \mathrm{Gal}(H_D/\mathbb{Q})$. Since the prime p is inert in K, the element τ_p, which is only defined up to conjugation, corresponds to a reflection in the generalised dihedral group $\mathrm{Gal}(H_D/\mathbb{Q})$. This reflection corresponds to the involution in $\mathrm{Gal}(K_p/\mathbb{Q}_p)$ after fixing an embedding $H_D \longrightarrow K_p$, i.e., a prime of H_D above p. Proposition 5.10 of [Dar01] asserts the existence of an element σ_τ in G_D satisfying

$$\tau_p(J_\tau) = -w_M J_{\tau^{\sigma_\tau}}, \qquad \tau_p(P_\tau) = w_N P_{\tau^{\sigma_\tau}}. \tag{16}$$

Note the sign difference in the two equations, which arises from the fact that τ_p does not commute with Φ_{Tate} in general, but rather satisfies

$$\tau_p \Phi_{\mathrm{Tate}} \tau_p = a_p \Phi_{\mathrm{Tate}} = -w_p \Phi_{\mathrm{Tate}}.$$

The element σ_τ is denoted by σ in Proposition 5.10 of [Dar01], but we have denoted it here by σ_τ to emphasize its dependence on τ. Indeed, replacing τ by τ^α, for some $\alpha \in G_D$, one can see that

$$\sigma_{\tau^\alpha} = \sigma_\tau \alpha^{-2}. \tag{17}$$

This identity is a consequence of the fact that τ_p does not commute with the elements of G_D, but rather satisfies

$$\tau_p \sigma = \sigma^{-1} \tau_p, \quad \text{for all } \sigma \in G_D.$$

Equation (17) shows that the image of σ_τ in G_D/G_D^2 is independent of $\tau \in \Gamma\backslash\mathscr{H}_p^D$. Denote this element by σ, in keeping with the notation of Proposition 5.10 of [Dar01].

It will be necessary to have a precise description of σ. To do this, we give a formula for $\chi(\sigma)$, as χ runs over the characters of G_D/G_D^2. These characters are precisely the genus characters attached to the discriminant D, and correspond to pairs (χ_1, χ_2) of primitive quadratic Dirichlet characters of coprime conductor

satisfying $\chi_1\chi_2 = \epsilon_K$. (Cf. the discussion in the introduction preceding the statement of Theorem 1.) The unordered pair (χ_1, χ_2) is characterised by the properties

$$\begin{aligned}(18)\qquad \chi(\mathrm{frob}_\lambda) = \chi(\mathrm{frob}_{\bar\lambda}) &= \chi_1(\ell) = \chi_2(\ell),\\ \chi(\mathrm{frob}_\infty) &= \chi_1(-1) = \chi_2(-1),\end{aligned}$$

for any rational prime ℓ which splits completely as a product $\ell = \lambda\bar\lambda$ of prime ideals of K of norm ℓ. (Here, frob_∞ denotes the conjugacy class of complex conjugation in G_D.)

PROPOSITION 1.8. *For any genus character χ attached to the discriminant D, corresponding to the pair (χ_1, χ_2) of quadratic Dirichlet characters,*

$$\chi(\sigma) = \chi_1(-M).$$

Proof. We will show that the element σ corresponds to the class in G_D/G_D^2 of the element $\infty\lambda_1^{e_1}\cdots\lambda_t^{e_t} \in \mathrm{Pic}^+(\mathbb{O})$, where

1. ∞ stands for the class of a principal ideal generated by an element $x \in K$ of negative norm for which $\mathrm{ord}_p(x)$ is even, and corresponds to complex conjugation in G_D/G_D^2;
2. $M = \ell_1^{e_1}\cdots\ell_t^{e_t}$ is the factorisation of M into a product of distinct prime powers, and λ_j is some ideal of K above ℓ_j.

To see this, we first recall the description of the action of G_D on $\Gamma\backslash\mathcal{H}_p^D$ given in Section 2.4 of [DD06]. If τ belongs to $\mathcal{H}_p^D$, one may choose a representative element (denoted τ again by abuse of notation) in its Γ-orbit in such a way that both $\Lambda_1 = \langle\tau, 1\rangle$ and $\Lambda_2 = \langle M\tau, 1\rangle$ are fractional ideals of $\mathbb{O}$ with $\tau > \bar\tau$ and $\mathrm{ord}_p(\tau - \bar\tau)$ even. The ratio $\lambda = \Lambda_1/\Lambda_2$ is a cyclic integral $\mathbb{O}$-ideal of norm M. Using the bijection $\underline{\tau}$ described in Section 2.4 of [DD06], the element $W_M(\bar\tau) = -1/(M\bar\tau)$ corresponds to the pair of fractional ideals

$$\Lambda_1' = \langle -x, Mx\bar\tau\rangle, \quad \Lambda_2' = \langle -Mx, Mx\bar\tau\rangle.$$

Now a direct calculation shows that

$$(\Lambda_1', \Lambda_2') = \mathfrak{c} * (\Lambda_1, \Lambda_2),$$

where

$$\mathfrak{c} = (x)\bar\lambda(\bar\Lambda_1/\Lambda_1).$$

The fractional ideal $(\bar\Lambda_1/\Lambda_1) = \frac{\Lambda_1\bar\Lambda_1}{\Lambda_1^2}$ represents the trivial element in G_D/G_D^2. It follows that σ is represented by the class of $(x)\bar\lambda$ in G_D/G_D^2, as was to be shown. Proposition 1.8 now follows from (18). □

2. **Hida theory**

The definition of Stark-Heegner points given in Section 1.4 is ill-suited for theoretical calculations, because of the indirect nature of the definition of the indefinite integral of Proposition 1.5. The present chapter gives a useful definition of the indefinite integral and of Stark-Heegner points in terms of periods attached to Hida families.

2.1. *Hida families.* Let

$$\tilde{\Lambda} := \mathbb{Z}_p[[\mathbb{Z}_p^\times]], \quad \Lambda = \mathbb{Z}_p[[(1+p\mathbb{Z}_p)^\times]]$$

denote the usual Iwasawa algebras, and let

$$\mathscr{X} = \hom(\mathbb{Z}_p^\times, \mathbb{Z}_p^\times) \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$$

be the space of continuous p-adic characters of $\mathbb{Z}_p^\times$, equipped with its natural topology. Elements of $\mathscr{X}$ can also be viewed in a natural way as continuous algebra homomorphisms from $\tilde{\Lambda}$ to $\mathbb{Z}_p$. The space $\mathscr{X}$ contains $\mathbb{Z}$ as a dense subset by sending $k \in \mathbb{Z}$ to the character $\theta_k(x) := x^{k-2}$. Note the shift by two in our convention, which means that $k = 2$ corresponds to the augmentation map on $\tilde{\Lambda}$.

Following the discussion in Section 1.2 of [BD07], we associate to f a so-called *Hida family*

$$f_\infty := \sum_{n=1}^{\infty} a_n(k) q^n.$$

This is a formal q-expansion with coefficients in the ring $\mathscr{A}(U)$ of p-adic analytic functions on U, where U is an appropriate neighbourhood of $2 \in \mathscr{X}$. Assume for simplicity that U is contained in the residue disc of 2 modulo $p-1$, and let $\mathbb{Z}^{\geq 2}$ denote the set of integers which are ≥ 2. The formal q-expansion f_∞ is characterised by the following properties:

1. If k belongs to $U \cap \mathbb{Z}^{\geq 2}$, the q-expansion
$$f_k := \sum_{n=1}^{\infty} a_n(k) q^n$$
is a normalised eigenform of weight k on $\Gamma_0(N)$. For this reason it is referred to as the *weight k specialisation* of f_∞.
2. $f_2 = f$.

Note in particular that the field K_{f_k} generated by the Fourier coefficients of the normalised eigenform f_k is a finite extension of $\mathbb{Q}$. For each $k \in U \cap \mathbb{Z}^{\geq 2}$, we fix the Shimura periods $\Omega_k^+ := \Omega_{f_k}^+$ and $\Omega_k^- := \Omega_{f_k}^-$ as in Proposition 1.1. This choice of periods allows us to talk about the $V_k(\mathbb{C}_p)$-valued modular symbols $I_{f_k}^+$

and $I_{f_k}^-$ associated to each f_k. The modular symbol I_{f_k} will be taken to be $I_{f_k}^+$ or $I_{f_k}^-$ depending on the choice of w_∞ that was made.

2.2. *Periods attached to Hida families.* Let $L_* := \mathbb{Z}_p^2$ denote the standard $\mathbb{Z}_p$-lattice in $\mathbb{Q}_p^2$, and let L'_* denote its set of *primitive vectors*, i.e., the vectors in L_* which are not divisible by p. Let $\mathbb{D}$ denote the space of compactly supported $\mathbb{Q}_p$-valued measures on $\mathcal{W} := \mathbb{Q}_p^2 - \{0\}$, and let $\mathbb{D}_*$ denote the subspace of measures that are supported on L'_*. The action of the group $\mathbb{Z}_p^\times$ on $\mathcal{W}$ and L'_* given by $\lambda(x, y) = (\lambda x, \lambda y)$ gives rise to $\tilde{\Lambda}$ and Λ module structures on $\mathbb{D}$ and $\mathbb{D}_*$. The module $\mathbb{D}$ is also equipped with a right $\tilde{\Lambda}$-linear action of $\mathbf{GL}_2(\mathbb{Q}_p)$ defined by the rule

$$\int_{\mathcal{W}} F d(\mu|\gamma) = \int_{\mathcal{W}} (F|\gamma^{-1}) d\mu, \tag{19}$$

where $\mathbf{GL}_2(\mathbb{Q}_p)$ operates on the continuous functions on $\mathcal{W}$ by the rule extending (8):

$$(F|\gamma)(x, y) := F(ax + by, cx + dy), \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{20}$$

Denote by $\Gamma_0(p\mathbb{Z}_p)$ the group of matrices in $\mathbf{GL}_2(\mathbb{Z}_p)$ which are upper triangular modulo p. Our interest in the space $\mathbb{D}_*$ lies in the fact that it is equipped, for all $k \in \mathbb{Z}^{\geq 2}$, with a $\Gamma_0(p\mathbb{Z}_p)$-equivariant homomorphism

$$\rho_k : \mathbb{D}_* \longrightarrow V_k$$

defined by

$$\rho_k(\mu)(P) := \int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} P(x, y) d\mu(x, y).$$

(Note that ρ_k does not respect the full action of $\mathbf{GL}_2(\mathbb{Z}_p)$, because the domain of integration that appears in its definition is only preserved by $\Gamma_0(p\mathbb{Z}_p)$.) The homomorphism ρ_k gives rise to a homomorphism, denoted by the same letter by abuse of notation:

$$\rho_k : \mathrm{MS}_{\Gamma_0(M)}(\mathbb{D}_*) \longrightarrow \mathrm{MS}_{\Gamma_0(N)}(V_k(\mathbb{C}_p)).$$

The space $\mathrm{MS}_{\Gamma_0(M)}(\mathbb{D}_*)$ is equipped with a natural action of the Hecke operators, and of the operator U_p in particular. Let $\mathrm{MS}^{\mathrm{ord}}_{\Gamma_0(M)}(\mathbb{D}_*)$ denote the *ordinary subspace* of $\mathrm{MS}_{\Gamma_0(M)}(\mathbb{D}_*)$.

Proposition (6.1) of [GS93] asserts that this module is free and of finite rank over Λ.

The Iwasawa algebra Λ is identified in the usual way with a subring of the ring of analytic functions on $\mathscr{X}$. Let $\Lambda^\dagger$ denote the larger ring of $\mathbb{C}_p$-valued functions

on $\mathscr{X}$ which can be represented by a convergent power series expansion in some neighbourhood of $2 \in \mathscr{X}$, and set

$$\mathbb{D}_*^\dagger := \mathbb{D}_* \otimes_\Lambda \Lambda^\dagger, \qquad \mathrm{MS}^{\mathrm{ord}}_{\Gamma_0(M)}(\mathbb{D}_*)^\dagger := \mathrm{MS}^{\mathrm{ord}}_{\Gamma_0(M)}(\mathbb{D}_*) \otimes_\Lambda \Lambda^\dagger.$$

Similar notations are adopted, with the obvious meanings, when $\mathbb{D}_*$ is replaced by $\mathbb{D}$. If $\mu = \lambda_1\mu_1 + \cdots + \lambda_t\mu_t$, with $\lambda_i \in \Lambda^\dagger$ and $\mu_i \in \mathbb{D}$, is any element of $\mathbb{D}^\dagger$, then there exists a neighbourhood U_μ of $2 \in \mathscr{X}$ on which all the λ_j are defined. Call such a region a *neighbourhood of regularity* for μ. Given $k \in \mathbb{Z}$, a function F on $\mathscr{W}$ is said to be *homogeneous of degree* k if $F(\lambda x, \lambda y) = \lambda^k F(x, y)$ for all $\lambda \in \mathbb{Z}_p$. Observe that for any $k \in U_\mu \cap \mathbb{Z}^{\geq 2}$, and any homogeneous function $F(x, y)$ of degree $k-2$, one can integrate F against μ on any compact open region $X \subset \mathscr{W}$ by the rule

$$\int_X F d\mu := \lambda_1(k) \int_X F d\mu_1 + \cdots + \lambda_t(k) \int_X F d\mu_t.$$

The following result of Greenberg and Stevens plays a key role in the constructions of this section.

THEOREM 2.1. *There exists a $\mathbb{D}_*^\dagger$-valued modular symbol $\mu_* \in \mathrm{MS}^{\mathrm{ord}}_{\Gamma_0(M)}(\mathbb{D}_*)^\dagger$ such that*

1. $\rho_2(\mu_*) = I_f$;
2. *For all $k \in U_{\mu_*} \cap \mathbb{Z}^{\geq 2}$, there exists a scalar $\lambda(k) \in \mathbb{C}_p$ such that*

$$\rho_k(\mu_*) = \lambda(k) I_{f_k}.$$

Proof. This is Theorem 1.5 of [BD07], which follows from Theorem (5.13) of [GS93] and whose proof is explained in Section 6 of that paper. See also [BDI] where extensions of this result to modular forms that are not necessarily ordinary are discussed. □

Remark 2.2. Note that the scalar $\lambda(k)$ depends on the choice of complex period used to define I_{f_k}. Since no attempt was made to choose these complex periods "coherently" as k varies (and in fact, the authors ignore whether such a choice can meaningfully be made *a priori*), the function $k \mapsto \lambda(k)$ cannot be expected to extend to a continuous function on U_{μ_*}.

Since $R^\times$ acts transitively on the set of $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^2$, and the stabiliser of L_* for this action is precisely $\Gamma_0(M)$, we may define a collection of $\mathbb{D}^\dagger$-valued modular symbols μ_L indexed by the $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^2$ as in Proposition 1.8 of [BD07], by imposing the rules:

$$\mu_{L_*} = \mu_*, \qquad \int_{\gamma X} (F|\gamma^{-1}) d\mu_{\gamma L}\{\gamma r \to \gamma s\} = \int_X F d\mu_L\{r \to s\},$$

for all $\gamma \in \Gamma$, for all lattices $L \subset \mathbb{Q}_p^2$, and all compact open regions $X \subset \mathcal{W}$.

Let

$$U := U_{\mu_*} = U_{\mu_L}$$

denote a region of regularity for the measures μ_L. The measures $\mu_L\{r \to s\}$ are supported on the compact subsets L' of $\mathcal{W}$, and they satisfy the following property:

LEMMA 2.3. *Suppose that $L_2 \subset L_1$ is a sublattice of index p in L_1. For all $k \in U \cap \mathbb{Z}^{\geq 2}$, for all homogeneous polynomials $P(x, y)$ of degree $k-2$, and for all $r, s \in \mathbb{P}$,*

$$\int_{L_1' \cap L_2'} P d\mu_{L_2}\{r \to s\} = a_p(k) \int_{L_1' \cap L_2'} P d\mu_{L_1}\{r \to s\}.$$

Proof. See Lemma 1.10 of [BD07]. □

The basic property of the measures $\mu_*\{r \to s\}$ given in Theorem 2.1 can be re-written as

$$\int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} P(x, y) d\mu_*\{r \to s\}(x, y) = \lambda(k) I_{f_k}\{r \to s\}(P), \tag{21}$$

for all $P \in \mathcal{P}_k(\mathbb{Q})$, and for all $r, s \in \mathbb{P}$. It will be useful to understand the value of the integral appearing on the left in (21), when the region of integration is taken to be the full $L_*' = (\mathbb{Z}_p^2)'$ instead of the subset $\mathbb{Z}_p \times \mathbb{Z}_p^\times$.

To write down such a formula, we first remark that for each integer $k > 2$, the form f_k is old at p, and there is a unique normalised eigenform $f_k^\sharp$ of weight k on $\Gamma_0(M)$ satisfying

$$f_k(z) = f_k^\sharp(z) - p^{k-1} a_p(k)^{-1} f_k^\sharp(pz).$$

(By convention, we set $f_2^\sharp := 0$.) Let $I_{f_k^\sharp}$ be the modular symbol attached to $f_k^\sharp$ via the choice of complex period Ω_k. This modular symbol satisfies the relation

$$I_{f_k}\{r \to s\}(P) = I_{f_k^\sharp}\{r \to s\}(P) - p^{k-2} a_p(k)^{-1} I_{f_k^\sharp}\{r/p \to s/p\}(P(x, y/p)).$$

PROPOSITION 2.4. *For all $k \in U \cap \mathbb{Z}^{\geq 2}$, for all $P \in \mathcal{P}_k(\mathbb{C}_p)$ and for all $r, s \in \mathbb{P}$,*

$$\int_{(\mathbb{Z}_p^2)'} P(x, y) d\mu_*\{r \to s\}(x, y) = \lambda(k)(1 - a_p(k)^{-2} p^{k-2}) I_{f_k^\sharp}\{r \to s\}(P).$$

Proof. This proposition is inspired from Lemma 4.17 of [DD06] which treats the case of the Hida family of Eisenstein series. The proof given here follows the argument of [DD06] closely. (The essential, comparatively minor difference is that one has $\lambda(k) = a_p(k)^2 = 1$ in the context of Lemma 4.17 of [DD06].) Let L_* and L_∞ denote the lattices

$$L_* = \mathbb{Z}_p^2, \quad L_\infty = \mathbb{Z}_p \oplus p\mathbb{Z}_p.$$

Note that

$$(L'_* \cap L'_\infty) = \mathbb{Z}_p^\times \times p\mathbb{Z}_p, \quad \left(L'_* \cap \frac{1}{p}L'_\infty\right) = \mathbb{Z}_p \times \mathbb{Z}_p^\times. \tag{22}$$

Let $\theta \in R^\times$ be any matrix of determinant p satisfying

$$\theta(L_*) = L_\infty, \quad \theta(L_\infty) = pL_*; \quad \text{then } \theta(\mathbb{Z}_p^\times \times p\mathbb{Z}_p) = p(\mathbb{Z}_p \times \mathbb{Z}_p^\times). \tag{23}$$

Observe that L'_* can be written as a disjoint union of the two regions appearing in (22). Hence we may write

$$\int_{(\mathbb{Z}_p^2)'} P(x,y) d\mu_*\{r \to s\}(x,y) = J_1 + J_2,$$

where

$$\begin{aligned}
J_1 &= \int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} P d\mu_f\{r \to s\} = \lambda(k) I_{f_k}\{r \to s\}(P), \\
J_2 &= \int_{\mathbb{Z}_p^\times \times p\mathbb{Z}_p} P d\mu_f\{r \to s\} \\
&= \int_{p(\mathbb{Z}_p \times \mathbb{Z}_p^\times)} (P|\theta^{-1}) d\mu_{L_\infty}\{\theta r \to \theta s\} \\
&= p^{k-2} \int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} (P|\theta^{-1}) d\mu_{\frac{1}{p}L_\infty}\{\theta r \to \theta s\} \\
&= a_p(k)^{-1} p^{k-2} \int_{\mathbb{Z}_p \times \mathbb{Z}_p^\times} (P|\theta^{-1}) d\mu_{L_*}\{\theta r \to \theta s\} \\
&= a_p(k)^{-1} p^{k-2} \lambda(k) I_{f_k}\{\theta r \to \theta s\}(P|\theta^{-1}),
\end{aligned}$$

and the penultimate equality follows from Lemma 2.3. To evaluate the contributions J_1 and J_2 in terms of the form $f_k^\sharp$, note that, for any choice of θ satisfying (23),

$$f_k(z) = f_k^\sharp(z) - p^{k-1} a_p(k)^{-1} (f_k^\sharp|\theta)(z).$$

A direct calculation, using a change of variables, then shows that

$$I_{(f_k^\sharp|\theta)}\{r \to s\}(P) = p^{-1} I_{f_k^\sharp}\{\theta r \to \theta s\}(P|\theta^{-1}).$$

Hence

$$\begin{aligned}
J_1 &= \lambda(k) \left(I_{f_k^\sharp}\{r \to s\}(P) - p^{k-1} a_p(k)^{-1} I_{(f_k^\sharp|\theta)}\{r \to s\}(P) \right) \\
&= \lambda(k) \left(I_{f_k^\sharp}\{r \to s\}(P) - p^{k-2} a_p(k)^{-1} I_{f_k^\sharp}\{\theta r \to \theta s\}(P|\theta^{-1}) \right),
\end{aligned}$$

while

$$J_2 = \lambda(k)a_p(k)^{-1}\,p^{k-2}\left(I_{f_k^\sharp}\{\theta r \to \theta s\}(P|\theta^{-1}) - p^{k-2}a_p(k)^{-1}I_{f_k^\sharp}\{\theta^2 r \to \theta^2 s\}(P|\theta^{-2})\right).$$

Note that $\theta^2 = p\gamma$, for some $\gamma \in \Gamma_0(N)$. Since $I_{f_k^\dagger}$ is $\Gamma_0(N)$-invariant, it follows that

$$I_{f_k^\sharp}\{\theta^2 r \to \theta^2 s\}(P|\theta^{-2}) = p^{-k+2}I_{f_k^\sharp}\{r \to s\}(P),$$

and therefore

$$J_1 + J_2 = \lambda(k)(1 - a_p(k)^{-2}p^{k-2})I_{f_k^\sharp}\{r \to s\}(P).$$

The proposition follows. □

2.3. *Indefinite integrals revisited.* Recall the indefinite integral defined in Section 1.3. The relevance of Hida families to Stark-Heegner points can be explained by the fact that the system of distribution-valued modular symbols $\mu_L\{r \to s\}$ introduced in Section 2.2 can be used to give a direct formula for this indefinite integral.

We content ourselves with doing this when τ belongs to $\mathcal{H}_p \cap K_p$, and hence is defined over a quadratic unramified extension of $\mathbb{Q}_p$. In that case, the function

$$(x, y) \mapsto x - \tau y$$

identifies $\mathbb{Q}_p^2$ with K_p. Let L_τ be the $\mathbb{Z}_p$-lattice in $\mathbb{Q}_p^2$ defined by

$$L_\tau = \{(x, y) \text{ such that } x - \tau y \text{ belongs to } \mathcal{O}_K \otimes \mathbb{Z}_p\}.$$

The following theorem is a direct generalisation of Proposition 4.7 of [DD06].

THEOREM 2.5. *For all $\tau \in \mathcal{H}_p \cap K_p$, and for all $r, s \in \mathbb{P}$,*

$$\int_r^\tau\int_r^s \omega_f = \int_{L'_\tau} \log(x - \tau y)d\mu_{L_\tau}\{r \to s\}(x, y),$$

where $\log : K_p^\times \longrightarrow K_p$ *is any branch of the p-adic logarithm.*

Proof. Note that the expression $(x - \tau y)$ belongs to $(\mathcal{O}_K \otimes \mathbb{Z}_p)^\times$ for any $(x, y) \in L'_\tau$, and hence the integrand on the right is independent of the branch of the p-adic logarithm that was chosen to define it. To prove Theorem 2.5, it suffices to check that the three defining properties of the indefinite integral listed in Proposition 1.5 are satisfied by the expression appearing on the right in Theorem 2.5. The invariance under Γ stated as property 1 is a consequence of Proposition 4.6 of [BDI]. As for property 2, it follows from Proposition 4.7 of [BDI], which holds for any branch of the p-adic logarithm, including $\log_q$ for which the extra

term appearing in Proposition 4.7 of [BDI] vanishes. Finally, property 3 is a direct consequence of the definitions. □

COROLLARY 2.6. *The Stark-Heegner point P_τ associated to*

$$Q \in \Gamma_0(M)\backslash \mathscr{F}^D$$

satisfies

$$\log_E P_\tau = J_\tau = \int_{(\mathbb{Z}_p^2)'} \log(x - \tau y) d\mu_*\{r \to \gamma_\tau r\}(x, y).$$

Proof. This follows from (14) and Theorem 2.5, after we note that $L_\tau = \mathbb{Z}_p^2$ when $\tau = \tau_Q$ and Q is an element of $\mathscr{F}^D$. □

3. p-adic L-functions

3.1. *The Mazur-Kitagawa p-adic L-function.* Let $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \{\pm 1\}$ be a primitive quadratic Dirichlet character of conductor m with $\chi(-1) = w_\infty$, and let

$$\tau(\chi) := \sum_{a=1}^{m} \chi(a) e^{2\pi i a/m}$$

denote the Gauss sum attached to χ. For each $k \in U \cap \mathbb{Z}^{\geq 2}$, and $1 \leq j \leq k-1$ with j odd, the expression

$$L^*(f_k, \chi, j) := \frac{(j-1)!\tau(\chi)}{(-2\pi i)^{j-1}\Omega_k} L(f_k, \chi, j) \tag{24}$$

belongs to K_{f_k}; it is called the *algebraic part* of the special value $L(f_k, \chi, j)$. Recall that the period Ω_k that appears in the definition of $L^*(f_k, \chi, j)$ was chosen at the end of Section 2.1 and depends on the sign w_∞ that was fixed in that section, and therefore on the parity of χ.

One defines $L^*(f_k^\sharp, \chi, j)$ similarly, by replacing f_k by $f_k^\sharp$ in the definition above. Note that

$$L^*(f_k, \chi, j) = (1 - \chi(p)a_p(k)^{-1} p^{k-1-j}) L^*(f_k^\sharp, \chi, j). \tag{25}$$

The measures $\mu_*\{r \to s\}$ can be used to define the *Mazur-Kitagawa two-variable p-adic L-function* of $(k, s) \in U \times \mathscr{X}$ by the rule:

$$L_p(f_\infty, \chi, k, s) = \sum_{a=1}^{m} \chi(pa) \int_{\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times} \Big(x - \frac{pa}{m} y\Big)^{s-1} y^{k-s-1} d\mu_* \left\{\infty \to \frac{pa}{m}\right\}.$$

This function satisfies the following interpolation property with respect to special values of the classical L-functions $L^*(f_k, \chi, j)$.

THEOREM 3.1. *Suppose that* $k \in U \cap \mathbb{Z}^{\geq 2}$, *and that* $1 \leq j \leq k-1$ *satisfies* $\chi(-1) = (-1)^{j-1} w_\infty$. *Then*

$$L_p(f_\infty, \chi, k, j) = \lambda(k)(1 - \chi(p)a_p(k)^{-1} p^{j-1}) L^*(f_k, \chi, j).$$

Proof. See Theorem 1.12 of [BD07]. □

It will be useful to have a formula expressing $L_p(f_\infty, \chi, k, j)$ in terms of the special value $L^*(f_k^\sharp, \chi, j)$. Theorem 3.1 and equation (25) imply that

$$L_p(f_\infty, \chi, k, j)$$
$$= \lambda(k)(1 - \chi(p)a_p(k)^{-1} p^{j-1})(1 - \chi(p)a_p(k)^{-1} p^{k-1-j}) L^*(f_k^\sharp, \chi, j).$$

In particular, specialising at $j = k/2$ one obtains

COROLLARY 3.2. *Suppose that* χ *satisfies* $\chi(-1) = (-1)^{k/2-1} w_\infty$. *Then for all* $k \in U \cap \mathbb{Z}^{\geq 2}$,

$$L_p(f_\infty, \chi, k, k/2) = \lambda(k)(1 - \chi(p)a_p(k)^{-1} p^{\frac{k}{2}-1})^2 L^*(f_k^\sharp, \chi, k/2).$$

Note that the Euler factor appearing in this last expression is a perfect square.

3.2. *p-adic L-functions attached to real quadratic fields.* Given $Q = Ax^2 + Bxy + Cy^2$ in $\mathscr{F}^D$, let $\tau = \tau_Q$ and $\bar{\tau}$ be the roots of the quadratic polynomial $Q(x, 1)$, ordered as in (15). These belong to K, and can be viewed as elements of $\mathbb{C}_p$ via the chosen embedding of K into $\mathbb{C}_p$.

The quadratic form Q has a stabiliser in $\Gamma_0(M)$ of rank one, generated by the element $\gamma_\tau \in \Gamma_0(M)$ normalised as in (12). Let $\epsilon = c\tau + d$ denote the corresponding fundamental unit of K. By analogy with the definition of the Mazur-Kitagawa p-adic L-function, it is tempting to associate to f_∞ and Q a "two-variable p-adic L-function" by the rule

$$\mathscr{L}_p(f_\infty, Q, k, s) := A^{\frac{k}{2}-1} \int_{(\mathbb{Z}_p^2)'} (x - \tau y)^{s-1} (x - \bar{\tau} y)^{k-s-1} d\mu_*\{r \to \gamma_\tau r\}(x, y).$$

Note that this expression depends on the choice of base point r in a crucial way: replacing r by $r' \in \mathbb{P}$ has the effect of modifying $L_p(f_\infty, Q, k, s)$ by the term

$$A^{\frac{k}{2}-1}(1 - \epsilon^{k-2s}) \int_{(\mathbb{Z}_p^2)'} (x - \tau y)^{s-1} (x - \bar{\tau} y)^{k-s-1} d\mu_*\{r \to r'\}(x, y).$$

It follows that the restriction of $\mathscr{L}_p(f_\infty, Q, k, s)$ to the *central critical line* $s = k/2$ is independent of the choice of r. This motivates the following definitions.

Definition 3.3. Let $r \in \mathbb{P}$ be any base point. The *partial square root p-adic L-function* attached to f_∞ and Q is the function of $k \in U$ defined by

$$\mathscr{L}_p(f_\infty, Q, k) := \int_{(\mathbb{Z}_p^2)'} Q(x, y)^{\frac{k-2}{2}} d\mu_*\{r \to \gamma_\tau r\}(x, y).$$

Let χ be a fixed genus character of G_D. This character is said to be *even* (resp. *odd*) if it cuts out a totally real, resp. imaginary, quadratic extension of K. If χ is even (resp. odd), then the associated Dirichlet characters χ_1 and χ_2 are both even (resp. odd). Recall the sign at infinity w_∞ chosen in defining the modular symbols I_{f_k} and in choosing the Shimura period Ω_k.

Definition 3.4. Let χ be a genus character. Assume that $w_\infty = 1$ if χ is even, and that $w_\infty = -1$ if χ is odd.

1. The *square root p-adic L-function* attached to f_∞ and χ is the function of $k \in U$ defined by
$$\mathscr{L}_p(f_\infty/K, \chi, k) := \sum_{\sigma \in G_D} \chi(\sigma) \mathscr{L}_p(f_\infty, Q^\sigma, k).$$
2. The *p-adic L-function* attached to f_∞ and χ is the function of $k \in U$ defined by
$$L_p(f_\infty/K, \chi, k) := \mathscr{L}_p(f_\infty/K, \chi, k)^2.$$

We now prove the interpolation property for $L_p(f_\infty/K, \chi, k)$ which justifies its designation as a p-adic L-function.

THEOREM 3.5. *For all* $k \in U \cap \mathbb{Z}^{\geq 2}$,
$$L_p(f_\infty/K, \chi, k) = \lambda(k)^2 (1 - a_p(k)^{-2} p^{k-2})^2 D^{\frac{k-2}{2}} L^*(f_k^\sharp/K, \chi, k/2),$$
where
$$L^*(f_k^\sharp/K, \chi, k/2) = \frac{(\frac{k}{2}-1)!^2 \sqrt{D}}{(2\pi i)^{k-2} \Omega_k^2} L(f_k^\sharp/K, \chi, k/2). \tag{26}$$

Proof. By definition,
$$\begin{aligned}\mathscr{L}_p(f_\infty/K, Q, k) &= \int_{(\mathbb{Z}_p^2)'} Q(x,y)^{\frac{k-2}{2}} d\mu_*\{r \to \gamma_Q r\}(x,y) \\ &= \lambda(k)(1 - a_p(k)^{-2} p^{k-2}) I_{f_k^\sharp}\{r \to \gamma_Q r\}(Q^{\frac{k-2}{2}}),\end{aligned}$$
where the last equality follows from Proposition 2.4. Hence
$$\begin{aligned}&L_p(f_\infty/K, \chi, k) \\ &= \lambda(k)^2 (1 - a_p(k)^{-2} p^{k-2})^2 \Big(\sum_{\sigma \in G_D} \chi(\sigma) I_{f_k^\sharp}\{r \to \gamma_{Q^\sigma} r\} \left((Q^\sigma)^{\frac{k-2}{2}} \right) \Big)^2 \\ &= \lambda(k)^2 (1 - a_p(k)^{-2} p^{k-2})^2 (2\pi i)^2 \Omega_k^{-2} \mathbb{L}_\chi,\end{aligned} \tag{27}$$
where
$$\mathbb{L}_\chi = \Big(\sum_{\sigma \in G_D} \chi(\sigma) \int_{z_0}^{\gamma_Q z_0} f_k^\sharp(z) Q^\sigma(z,1)^{\frac{k-2}{2}} dz \Big)^2.$$

The crucial ingredient in the proof of Theorem 3.5 is Theorem 6.3.1 of [Pop06], which asserts that

$$\mathbb{L}_\chi = D^{\frac{k-1}{2}}(2\pi)^{-k}\left(\frac{k-2}{2}\right)!^2 L(f_k^\sharp/K,\chi,k/2). \tag{28}$$

It follows readily from (27) and (28) that

$$L_p(f_\infty/K,\chi,k) = \lambda(k)^2(1-a_p(k)^{-2}p^{k-2})^2 D^{\frac{k-2}{2}} L^*(f_k^\sharp/K,\chi,k/2),$$

as was to be shown. □

3.3. *A factorisation formula.* We come to the following factorisation relating the Mazur-Kitagawa p-adic L-functions (more precisely, their restrictions to the central critical line) with the p-adic L-functions attached to the real quadratic field K in the previous section.

THEOREM 3.6. *For all* $k \in U$,

$$L_p(f_\infty/K,\chi,k) = D^{\frac{k-2}{2}} L_p(f_\infty,\chi_1,k,k/2)L_p(f_\infty,\chi_2,k,k/2).$$

Proof. By comparing the Euler product expansions on both sides (and noting that $\mathrm{Ind}_{G_K}^{G_\mathbb{Q}}(\chi) = \chi_1 \oplus \chi_2$) we see that

$$L(f_k^\sharp/K,\chi,k/2) = L(f_k^\sharp,\chi_1,k/2)L(f_k^\sharp,\chi_2,k/2). \tag{29}$$

Gauss's classical calculation of quadratic Gauss sums, in the case of fundamental discriminants, shows that

$$\tau(\chi_i) = \sqrt{D_i}, \quad i = 1,2. \tag{30}$$

Combining (29) and (30) with definitions (24) and (26), we see that

$$L^*(f_k^\sharp/K,\chi,k/2) = L^*(f_k^\sharp,\chi_1,k/2)L^*(f_k^\sharp,\chi_2,k/2).$$

Also, because p is inert in K, the Dirichlet characters χ_1 and χ_2 satisfy $\chi_1(p) = -\chi_2(p)$, and hence the product of the Euler factors at p appearing in Corollary 3.2 with χ replaced by χ_1 and χ_2 is equal to the Euler factor appearing in Theorem 3.5. Hence Theorem 3.5 and Corollary 3.2 imply that for all $k \in U \cap \mathbb{Z}^{\geq 2}$,

$$L_p(f_\infty/K,\chi,k) = D^{\frac{k-2}{2}} L_p(f_\infty,\chi_1,k,k/2)L_p(f_\infty,\chi_2,k,k/2). \tag{31}$$

Since $U \cap \mathbb{Z}^{\geq 2}$ is dense in U, and the two sides of (31) are continuous on U, they necessarily agree on this region. □

4. **Proof of the main result**

We begin by noting the following connection between the Stark-Heegner point P_χ and the leading term of the p-adic L-function that was introduced in Section 3.2. This relation can be viewed as a somewhat exotic p-adic variant of the Gross-Zagier formula since it relates Stark-Heegner points to derivatives of p-adic L-series. It is even more closely related in the spirit of the main theorem of [BD98] and its extension to Hida families stated in Theorem 4.9 of [BD07].

Recall first from Definition 3.3 that, for all $Q \in \mathscr{F}^D$,

$$\mathscr{L}_p(f_\infty/K, Q, 2) = \int_{(\mathbb{Z}_p^2)'} d\mu_*\{r \to \gamma_\tau r\}(x, y) = \mu_f\{r \to \gamma_\tau r\}(\mathbb{P}_1(\mathbb{Q}_p)) = 0.$$

It follows that $\mathscr{L}_p(f_\infty/K, \chi, 2) = 0$ for all characters χ of G_D.

THEOREM 4.1. *For all genus characters χ of G_D,*

$$\frac{d}{dk}\mathscr{L}_p(f_\infty/K, \chi, k)_{k=2} = \frac{1}{2}\,(1 - \chi_1(-M)w_M)\log_E(P_\chi).$$

Proof. By definition for each $Q \in \Gamma_0(M)\backslash\mathscr{F}^D$ with associated roots τ and $\bar\tau$,

$$\begin{aligned}\frac{d}{dk}\mathscr{L}_p(f_\infty, Q, k)_{k=2} &= \frac{1}{2}\int_{(\mathbb{Z}_p^2)'} (\log(x - \tau y) + \log(x - \bar\tau y))\, d\mu_*\{r \to \gamma_\tau r\} \\ &= \frac{1}{2}(J_\tau + \tau_p J_\tau) \\ &= \frac{1}{2}(J_\tau - w_M J_{\tau^{\sigma_\tau}}),\end{aligned}$$

where the last equality is a consequence of equation (16). It follows from Proposition 1.8 that

$$\frac{d}{dk}\mathscr{L}_p(f_\infty/K, \chi, k)_{k=2} = \frac{1}{2}\,(1 - \chi_1(-M)w_M)\left(\sum_{\sigma\in G_D}\chi(\sigma)J_{\tau^\sigma}\right),$$

as was to be proved. □

COROLLARY 4.2. *For all genus characters χ of G_D,*

$$\frac{d^2}{dk^2}L_p(f_\infty/K, \chi, k)_{k=2} = \begin{cases} 2\log_E^2(P_\chi) & \text{if } \chi_1(-M) = -w_M \\ 0 & \text{if } \chi_1(-M) = w_M. \end{cases}$$

We are now ready to prove Theorem 1 of the introduction.

THEOREM 4.3. *Let χ be the genus character attached to the pair of Dirichlet characters χ_1 and χ_2. Suppose that E has at least two primes of multiplicative reduction, and that $\chi_1(-M) = -w_M$.*

1. *There is a point* $\mathbf{P}_\chi \in E(H_\chi)^\chi$ *and* $t \in \mathbb{Q}^\times$ *such that*

$$\log_E(P_\chi) = t \log_E(\mathbf{P}_\chi).$$

2. *The point* $\mathbf{P}_\chi$ *is of infinite order if and only if* $L'(E/K, \chi, 1) \neq 0$.

Proof. The proof proceeds in three stages, which are parallel to Kronecker's "solution to Pell's equation" described in the last paragraph of his introduction.

1. Corollary 4.2 expresses the logarithm of the Stark-Heegner point P_χ in terms of special values of L-series:

$$\log_E^2(P_\chi) = \frac{1}{2}\frac{d^2}{dk^2} L_p(f_\infty/K, \chi, k)_{k=2}. \tag{32}$$

2. Theorem 3.6 asserts that

$$L_p(f_\infty/K, \chi, k) = D^{\frac{k-2}{2}} L_p(f_\infty, \chi_1, k, k/2) L_p(f_\infty, \chi_2, k, k/2). \tag{33}$$

Hence we are now reduced to understanding the leading terms of the Mazur-Kitagawa p-adic L-functions attached to χ_1 and χ_2 in a neighbourhood of $k = 2$.

3. Let

$$\mathrm{sign}(E, \chi_j) := -w_N \chi_j(-N)$$

denote the sign in the functional equation for the complex L-series $L(E, \chi_j, s)$. Since $\chi_1(-N)\chi_2(-N) = \epsilon_K(-N) = -1$, it follows that $\mathrm{sign}(E, \chi_1)$ and $\mathrm{sign}(E, \chi_2)$ are *opposite*. Order χ_1 and χ_2 in such a way that

$$\mathrm{sign}(E, \chi_1) = -1, \qquad \mathrm{sign}(E, \chi_2) = 1. \tag{34}$$

Then $\chi_1(-N) = w_N$, and the running hypothesis that $\chi_1(-M) = -w_M$ implies that

$$\chi_1(p) = -w_p = a_p. \tag{35}$$

Therefore the Mazur-Kitagawa p-adic L-function $L_p(f, \chi_1, k, s)$ has an exceptional zero at $(k, s) = (2, 1)$. Conditions (34) and (35) imply that we are in the situation where Theorem 5.4 of [BD07] can be applied to $L_p(f, \chi_1, k, k/2)$. Hence, this p-adic analytic function vanishes to order ≥ 2 at $k = 2$, and there is a global point $\mathbf{P}_{\chi_1} \in E(\mathbb{Q}(\sqrt{D_1}))$ and a rational number $\ell_1 \in \mathbb{Q}^\times$ satisfying three properties:

A.

$$\frac{d^2}{dk^2} L_p(f_\infty, \chi_1, k, k/2)_{k=2} = \ell_1 \log^2(\mathbf{P}_{\chi_1}). \tag{36}$$

B. The point $\mathbf{P}_{\chi_1}$ is of infinite order if and only if $L'(E, \chi_1, 1) \neq 0$.

C. The rational number ℓ_1 satisfies

$$\ell_1 \equiv L^*(f, \psi, 1) \pmod{(\mathbb{Q}^\times)^2}, \tag{37}$$

for *any* primitive quadratic Dirichlet character ψ for which $L(f,\psi,1)\neq 0$ and such that

$$\psi(\ell)=\chi_1(\ell) \text{ for } \ell|M, \qquad \psi(p)=-\chi_1(p).$$

On the other hand, the quantity

$$L_p(f_\infty,\chi_2,2,1)=2L^*(E,\chi_2,1)=:2\ell_2 \tag{38}$$

is a rational number, which is non-zero if and only if $L(E,\chi_2,1)$ does not vanish. Note that in this case $\ell_1\ell_2$ is a rational square by (37). Choose $t\in\mathbb{Q}^\times$ such that

$$t^2=\begin{cases}\ell_1\ell_2 & \text{if } \ell_2\neq 0,\\ 1 & \text{otherwise,}\end{cases}$$

and let

$$\mathbf{P}_\chi:=\begin{cases}\mathbf{P}_{\chi_1} & \text{if } L'(E/K,\chi,1)=L'(E,\chi_1,1)L(E,\chi_2,1)\neq 0,\\ 0 & \text{otherwise,}\end{cases}$$

Equations (32), (33), (36) and (38) imply Theorem 4.3, after possibly adjusting the sign of t. □

Remark 4.4. The condition $\chi_1(-M)=-w_M$ imposed in Theorem 4.3 is needed both in the first and third steps of the argument. When $\chi_1(-M)=w_M$, the signs in the functional equations for both $L_p(f_k,\chi_1,s)$ and $L_p(f_k,\chi_2,s)$ are -1.

1. In the case of $L_p(f_k,\chi_1,s)$, this arises from the fact that the sign in the classical functional equation for $L(f_k,\chi_1,s)$ is -1, while $L_p(f_k,\chi_1,s)$ does not have an exceptional zero, because $\chi_1(p)=w_p=-a_p$.
2. For $L_p(f_\infty,\chi_2,k,s)$, the classical L-function $L(f_k,\chi_2,s)$ vanishes to even order, but its p-adic counterpart has an exceptional zero and therefore vanishes to odd order at the central critical point. (This latter situation is precisely the one that was studied by Greenberg and Stevens in [GS93], where the vanishing of $L_p(f_\infty,\chi_2,k,s)$ on the central critical line was used to prove the "exceptional zero conjecture" of Mazur, Tate and Teitelbaum.)

Thus, in the setting where $\chi_1(-M)=w_M$, equation (33) implies that the p-adic L-function $\mathscr{L}_p(f_\infty/K,\chi,k)$ vanishes identically. Hence no arithmetic information is to be extracted from this function, and a proof of Theorem 1 would seem to require a different approach. (An eventual extension of equation (36) to the setting of Hilbert modular forms attached to the real quadratic field K seems a promising avenue.)

Remark 4.5. In the case where χ is not quadratic, the crucial factorisation (33) ceases to be available. This reflects the presence of a serious obstacle, and the ideas explored in his paper appear to shed no light on the algebraicity of the individual Stark-Heegner points P_τ when G_D is not of exponent 2. Indeed, the reader will

have noted that no "genuinely new" Stark-Heegner points are produced in this article. Rather, it is shown that where the classical theory of Heegner points and the theory of Stark-Heegner points intersect—namely, genus fields—the Stark-Heegner points can be expressed in terms of Heegner points. To go beyond genus characters, one would probably need to develop a theory of "real multiplication" yielding an independent construction of Stark-Heegner points and an "explicit class field theory" for real quadratic fields.

References

[BD98] M. BERTOLINI and H. DARMON, Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization, *Invent. Math.* **131** (1998), 453–491. MR 99f:11080

[BD07] _____, Hida families and rational points on elliptic curves, *Invent. Math.* **168** (2007), 371–431. MR 2008c:11076 Zbl 1129.11025

[BDG04] M. BERTOLINI, H. DARMON, and P. GREEN, Periods and points attached to quadratic algebras, in *Heegner points and Rankin L-series*, *Math. Sci. Res. Inst. Publ.* **49**, Cambridge Univ. Press, Cambridge, 2004, pp. 323–367. MR 2005e:11062

[BDI] M. BERTOLINI, H. DARMON, and A. IOVITA, Families of modular forms on definite quaternion algebras and Teitelbaum's conjecture.

[Dar01] H. DARMON, Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications, *Ann. of Math.* **154** (2001), 589–639. MR 2003j:11067 Zbl 1035.11027

[DD06] H. DARMON and S. DASGUPTA, Elliptic units for real quadratic fields, *Ann. of Math.* **163** (2006), 301–346. MR 2007a:11079 Zbl 1130.11030

[DG02] H. DARMON and P. GREEN, Elliptic curves and class fields of real quadratic fields: algorithms and evidence, *Experiment. Math.* **11** (2002), 37–55. MR 2004c:11112 Zbl 1040.11048

[DP06] H. DARMON and R. POLLACK, Efficient calculation of Stark-Heegner points via overconvergent modular symbols, *Israel J. Math.* **153** (2006), 319–354. MR 2007k:11077 Zbl 1157.11028

[Das04] S. DASGUPTA, Gross-Stark units, Stark-Heegner points, and class fields of real quadratic fields, Ph.d. thesis, Univ. of California, Berkeley, 2004.

[Das05] _____, Stark-Heegner points on modular Jacobians, *Ann. Sci. École Norm. Sup.* **38** (2005), 427–469. MR 2006e:11080

[GS93] R. GREENBERG and G. STEVENS, p-adic L-functions and p-adic periods of modular forms, *Invent. Math.* **111** (1993), 407–447. MR 93m:11054 Zbl 0778.11034

[KZ84] W. KOHNEN and D. ZAGIER, Modular forms with rational periods, in *Modular Forms* (*Durham*, 1983), Horwood, Chichester, 1984, pp. 197–249. MR 87h:11043 Zbl 0618.10019

[Pop06] A. A. POPA, Central values of Rankin L-series over real quadratic fields, *Compos. Math.* **142** (2006), 811–866. MR 2007m:11070 Zbl 1144.11041

[Sie80] C. L. SIEGEL, *Advanced Analytic Number Theory*, second ed., *TIFR Studies in Math.* **9**, Tata Institute of Fundamental Research, Bombay, 1980. MR 83m:10001 Zbl 0478.10001

[Wei76] A. WEIL, *Elliptic Functions According to Eisenstein and Kronecker*, Springer-Verlag, New York, 1976, *Ergeb. Math. Grenzgeb.* **88**. MR 58 #27769a Zbl 0318.33004

(Received May 30, 2005)
(Revised January 31, 2006)

E-mail address: massimo.bertolini@unimi.it
DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI MILANO, VIA SALDINI, 50, 20133 MILANO, ITALY

E-mail address: darmon@math.mcgill.ca
DEPARTMENT OF MATHEMATICS, MCGILL UNIVERSITY, 805 SHEBROOKE STREET WEST, MONTREAL, QC H3A 2K6, CANADA