Stark–Heegner points and special values of L-series

Massimo Bertolini
Henri Darmon
Samit Dasgupta

September 5, 2007

Introduction

Let E be an elliptic curve over $\mathbb{Q}$ attached to a newform f of weight two on $\Gamma_0(N)$. Let K be a real quadratic field, and let $p \| N$ be a prime of multiplicative reduction for E which is inert in K, so that the p-adic completion K_p of K is the quadratic unramified extension of $\mathbb{Q}_p$.

Subject to the condition that all the primes dividing $M := N/p$ are split in K, the article [Dar] proposes an analytic construction of "Stark–Heegner points" in $E(K_p)$, and conjectures that these points are defined over specific class fields of K. More precisely, let

$$R := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}[1/p]) \text{ such that } M \text{ divides } c \right\}$$

be an Eichler $\mathbb{Z}[1/p]$-order of level M in $M_2(\mathbb{Q})$, and let $\Gamma := R_1^\times$ denote the group of elements in R of determinant 1. This group acts by Möbius transformations on the K_p-points of the p-adic upper half-plane

$$\mathcal{H}_p := \mathbb{P}^1(K_p) - \mathbb{P}^1(\mathbb{Q}_p),$$

and preserves the non-empty subset $\mathcal{H}_p \cap K$. In [Dar], modular symbols attached to f are used to define a map

$$\Phi : \Gamma \backslash (\mathcal{H}_p \cap K) \longrightarrow E(K_p), \tag{1}$$

whose image is conjectured to consist of points defined over ring class fields of K. Underlying this conjecture is a more precise one, analogous to the classical Shimura reciprocity law, which we now recall.

Given $\tau \in \mathcal{H}_p \cap K$, the collection $\mathcal{O}_\tau$ of matrices $g \in R$ satisfying

$$g \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \lambda_g \begin{pmatrix} \tau \\ 1 \end{pmatrix} \text{ for some } \lambda_g \in K, \tag{2}$$

is isomorphic to a $\mathbb{Z}[1/p]$-order in K, via the map $g \mapsto \lambda_g$. This order is also equipped with the attendant ring homomorphism $\eta : \mathcal{O}_\tau \longrightarrow \mathbb{Z}/M\mathbb{Z}$ sending g to its upper left-hand entry (taken modulo M). The map η is sometimes referred to as the *orientation* at M attached to τ. Conversely, given any $\mathbb{Z}[1/p]$-order $\mathcal{O}$ of discriminant prime to M equipped with an orientation η, the set $\mathcal{H}_p^{\mathcal{O}}$ of $\tau \in \mathcal{H}_p$ with associated oriented order equal to $\mathcal{O}$ is preserved under the action of Γ, and the set of orbits $\Gamma\backslash\mathcal{H}_p^{\mathcal{O}}$ is equipped with a natural simply transitive action of the group $G = \mathrm{Pic}^+(\mathcal{O})$, where $\mathrm{Pic}^+(\mathcal{O})$ denotes the narrow Picard group of oriented projective $\mathcal{O}$-modules of rank one. Denote this action by $(\sigma, \tau) \mapsto \tau^\sigma$, for $\sigma \in G$ and $\tau \in \Gamma\backslash\mathcal{H}_p^{\mathcal{O}}$. Class field theory identifies G with the Galois group of the *narrow ring class field* of K attached to $\mathcal{O}$, denoted H_K. It is conjectured in [Dar] that the points $\Phi(\tau)$ belong to $E(H_K)$ for all $\tau \in \mathcal{H}_p^{\mathcal{O}}$, and that

$$\Phi(\tau)^\sigma = \Phi(\tau^\sigma), \qquad \text{for all } \sigma \in \mathrm{Gal}(H_K/K) = \mathrm{Pic}^+(\mathcal{O}). \tag{3}$$

In particular it is expected that the point

$$P_K := \Phi(\tau_1) + \cdots + \Phi(\tau_h)$$

should belong to $E(K)$, where $\tau_1, \ldots, \tau_h$ denote representatives for the distinct orbits in $\Gamma\backslash\mathcal{H}_p^{\mathcal{O}}$. The article [BD3] shows that the image of P_K in $E(K_p) \otimes \mathbb{Q}$ is of the form $t \cdot \mathbf{P}_K$, where

1. t belongs to $\mathbb{Q}^\times$;

2. $\mathbf{P}_K \in E(K)$ is of infinite order precisely when $L'(E/K, 1) \neq 0$;

provided the following ostensibly extraneous assumptions are satisfied

1. $\bar{P}_K = a_p P_K$, where $\bar{P}_K$ is the Galois conjugate of P_K over K_p, and a_p is the pth Fourier coefficient of f.

2. The elliptic curve E has at least two primes of multiplicative reduction.

The main result of [BD3] falls short of being definitive because of these two assumptions, and also because it only treats the image of P_K modulo the torsion subgroup of $E(K_p)$.

The main goal of this article is to examine certain "finer" invariants associated to P_K and to relate these to special values of L-series, guided by the analogy between the point P_K and classical Heegner points attached to imaginary quadratic fields.

In setting the stage for the main formula, let $E/\mathbb{Q}$ be an elliptic curve of conductor M; it is essential to assume that all the primes dividing M are *split* in K. This hypothesis is very similar to the one imposed in [GZ] when K is imaginary quadratic, where it implies that $L(E/K, 1)$ vanishes systematically because the sign in its functional equation is -1. In the case where K is real quadratic the "Gross-Zagier hypothesis" implies that the sign in the functional equation for $L(E/K, s)$ is 1 so that $L(E/K, s)$ vanishes to even order and is expected to be frequently non-zero at $s = 1$. Consistent with this expectation is the fact that the Stark–Heegner construction is now unavailable, in the absence of a prime $p \| M$ which is inert in K.

The main idea is to bring such a prime into the picture by "raising the level at p" to produce a newform g of level $N = Mp$ which is *congruent* to f. The congruence is modulo an appropriate ideal λ of the ring $\mathcal{O}_g$ generated by the Fourier coefficients of g. Let A_g denote the abelian variety quotient of $J_0(N)$ attached to g by the Eichler-Shimura construction. The main objective, which can now be stated more precisely, is to relate the *local behaviour at* p of the Stark–Heegner points in $A_g(K_p)$ to the algebraic part of the special value of $L(E/K, 1)$, taken modulo λ.

The first key ingredient in establishing such a relationship is an extension of the map Φ of (1) to arbitrary eigenforms of weight 2 on $\Gamma_0(Mp)$ such as g, and not just eigenforms with rational Fourier coefficients attached to elliptic curves, in a precise enough form so that phenomena related to congruences between modular forms can be analyzed. Let $\mathbb{T}$ be the full algebra of Hecke operators acting on the space of forms of weight two on $\Gamma_0(Mp)$. The theory presented in Section 1, based on the work of the third author [Das], produces a torus T over K_p equipped with a natural $\mathbb{T}$-action, whose character group (tensored with $\mathbb{C}$) is isomorphic as a $\mathbb{T} \otimes \mathbb{C}$-module to the space of weight 2 modular forms on $\Gamma_0(Mp)$ which are new at p. It also builds a Hecke-stable lattice $L \subset T(K_p)$, and a map Φ generalising (1)

$$\Phi : \Gamma\backslash(\mathcal{H}_p \cap K) \longrightarrow T(K_p)/L. \tag{4}$$

It is conjectured in Section 1 that the quotient T/L is isomorphic to the rigid analytic space associated to an abelian variety J defined over $\mathbb{Q}$. A strong partial result in this direction is proven in [Das], where it is shown that T/L is isogenous over K_p to the rigid analytic space associated to the p-new quotient $J_0(N)^{p\text{-new}}$ of the jacobian $J_0(N)$. In Section 1, it is further conjectured that the points $\Phi(\tau) \in J(K_p)$ satisfy the same algebraicity properties as were stated for the map Φ of (1).

Letting Φ_p denote the group of connected components in the Néron model of J over the maximal unramified extension of $\mathbb{Q}_p$, one has a natural Hecke-equivariant projection

$$\partial_p : J(\mathbb{C}_p) \longrightarrow \Phi_p. \tag{5}$$

The group Φ_p is described explicitly in Section 1, yielding a concrete description of the Hecke action on Φ_p and a description of the primes dividing the cardinality of Φ_p in terms of "primes of fusion" betwen forms on $\Gamma_0(M)$ and forms on $\Gamma_0(Mp)$ which are new at p.

This description also makes it possible to attach to E and K an explicit element

$$\mathcal{L}(E/K, 1)_{(p)} \in \bar{\Phi}_p,$$

where $\bar{\Phi}_p$ is a suitable f-isotypic quotient of Φ_p. Thanks to a theorem of Popa [Po], this element is closely related to the special value $L(E/K, 1)$, and, in particular, one has the equivalence

$$L(E/K, 1) = 0 \iff \mathcal{L}(E/K, 1)_{(p)} = 0 \text{ for all } p.$$

Section 2 contains an exposition of Popa's formula.

Section 3 is devoted to a discussion of $\mathcal{L}(E/K, 1)_{(p)}$; furthermore, by combining the results of Sections 1 and 2, it proves the main theorem of this article, an avatar of the Gross-Zagier formula which relates Stark–Heegner points to special values of L-series.

Main Theorem. *For all primes p which are inert in K,*

$$\partial_p(P_K) = \mathcal{L}(E/K, 1)_{(p)}.$$

Potential arithmetic applications of this theorem (conditional on the validity of the deep conjectures of Section 1) are briefly discussed in Section 4.

Aknowledgements. It is a pleasure to thank the anonymous referee, for some comments which led us to improve our exposition.

1 Stark–Heegner points on $J_0(Mp)^{p\text{-new}}$

Heegner points on an elliptic curve E defined over $\mathbb{Q}$ can be defined analytically by certain complex line integrals involving the modular form

$$f := \sum_{n=1}^{\infty} a_n(E) e^{2\pi i n z}$$

corresponding to E, and the Weierstrass parametrization of E. To be precise, let τ be any point of the complex upper half plane $\mathcal{H} := \{z \in \mathbb{C} | \Im z > 0\}$. The complex number

$$J_\tau := \int_{\infty}^{\tau} 2\pi i f(z) dz \in \mathbb{C}$$

gives rise to an element of $\mathbb{C}/\Lambda_E \cong E(\mathbb{C})$, where Λ_E is the Néron lattice of E, and hence to a complex point $P_\tau \in E(\mathbb{C})$. If τ also lies in an imaginary quadratic subfield K of $\mathbb{C}$, then P_τ is a *Heegner point* on E. The theory of complex multiplication shows that this analytically defined point is actually defined over an abelian extension of K, and it furthermore prescribes the action of the Galois group of K on this point.

The Stark–Heegner points of [Dar], defined on elliptic curves over $\mathbb{Q}$ with multiplicative reduction at p, are obtained by replacing complex integration on $\mathcal{H}$ with a double integral on the product of a p-adic and a complex upper half plane $\mathcal{H}_p \times \mathcal{H}$.

We now very briefly describe this construction. Let E be an elliptic curve over $\mathbb{Q}$ of conductor $N = Mp$, with $p \nmid M$. The differential $\omega := 2\pi i f(z) dz$ and its anti-holomorphic counterpart $\bar{\omega} = -2\pi i f(\bar{z}) d\bar{z}$ give rise to two elements in the DeRham cohomology of $X_0(N)(\mathbb{C})$:

$$\omega^{\pm} := \omega \pm \bar{\omega}.$$

To each of these differential forms is attached a *modular symbol*

$$m_E^{\pm}\{x \to y\} := (\Omega_E^{\pm})^{-1} \int_x^y \omega^{\pm}, \quad \text{for } x, y \in \mathbb{P}^1(\mathbb{Q}).$$

Here $\Omega_E^\pm$ is an appropriate complex period chosen so that $m_E^\pm$ takes values in $\mathbb{Z}$ and in no proper subgroup of $\mathbb{Z}$.

The group Γ defined in the Introduction acts on $\mathbb{P}^1(\mathbb{Q}_p)$ by Möbius transformations. For each pair of cusps $x, y \in \mathbb{P}^1(\mathbb{Q})$ and choice of sign $\pm$, a $\mathbb{Z}$-valued additive measure $\mu^\pm\{x \to y\}$ on $\mathbb{P}^1(\mathbb{Q}_p)$ can be defined by

$$\mu^\pm\{x \to y\}(\gamma \mathbb{Z}_p) = m_E^\pm\{\gamma^{-1}x \to \gamma^{-1}y\}, \tag{6}$$

where γ is an element of Γ. Since the stabilizer of $\mathbb{Z}_p$ in Γ is $\Gamma_0(N)$, equation (6) is independent of the choice of γ by the $\Gamma_0(N)$-invariance of $m_E^\pm$. The motivation for this definition, and a proof that it extends to an additive measure on $\mathbb{P}^1(\mathbb{Q}_p)$, comes from "spreading out" the modular symbol $m_E^\pm$ along the Bruhat-Tits tree of $\mathbf{PGL}_2(\mathbb{Q}_p)$ (see [Dar], [Das], and Section 1.2 below). For any $\tau_1, \tau_2 \in \mathcal{H}_p$ and $x, y \in \mathbb{P}^1(\mathbb{Q}_p)$, a multiplicative double integral on $\mathcal{H}_p \times \mathcal{H}$ is then defined by (multiplicatively) integrating the function $(t-\tau_1)/(t-\tau_2)$ over $\mathbb{P}^1(\mathbb{Q}_p)$ with respect to the measure $\mu^\pm\{x \to y\}$:

$$\begin{aligned} \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_x^y \omega_\pm &:= \times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu^\pm\{x \to y\}(t) \\ &= \lim_{||\mathcal{U}|| \to 0} \prod_{U \in \mathcal{U}} \left(\frac{t_U - \tau_2}{t_U - \tau_1}\right)^{\mu^\pm\{x \to y\}(U)} \in \mathbb{C}_p^\times. \end{aligned} \tag{7}$$

Here the limit is taken over uniformly finer disjoint covers $\mathcal{U}$ of $\mathbb{P}^1(\mathbb{Q}_p)$ by open compact subsets U, and t_U is an arbitrarily chosen point of U. Choosing special values for the limits of integration, in a manner motivated by the classical Heegner construction described above, one produces special elements in $\mathbb{C}_p^\times$. These elements are transferred to E using Tate's p-adic uniformization $\mathbb{C}_p^\times/q_E \cong E(\mathbb{C}_p)$ to define Stark–Heegner points.

In order to lift the Stark–Heegner points on E to the Jacobian $J_0(N)^{p\text{-new}}$, one can replace the modular symbols attached to E with the universal modular symbol for $\Gamma_0(N)$. In this section, we review this construction of Stark–Heegner points on $J_0(N)^{p\text{-new}}$, as described in fuller detail in [Das].

1.1 The universal modular symbol for $\Gamma_0(N)$

The first step is to generalize the measures $\mu^\pm\{x \to y\}$ on $\mathbb{P}^1(\mathbb{Q}_p)$. As we will see, the new measure naturally takes values in the p-new quotient of the homology group $H_1(X_0(N), \mathbb{Z})$. Once this measure is defined, the construction of Stark–Heegner points on $J_0(N)^{p\text{-new}}$ can proceed as the construction of Stark–Heegner points on E given in [Dar]. The Stark–Heegner points on $J_0(N)^{p\text{-new}}$ will map to those on E under the modular parametrization $J_0(N)^{p\text{-new}} \to E$.

We begin by recalling the universal modular symbol for $\Gamma_0(N)$. Let $\mathcal{M} := \mathrm{Div}_0\, \mathbb{P}^1(\mathbb{Q})$ be the group of degree zero divisors on the set of cusps of the complex upper half plane, defined by the exact sequence

$$0 \to \mathcal{M} \to \mathrm{Div}\, \mathbb{P}^1(\mathbb{Q}) \to \mathbb{Z} \to 0. \tag{8}$$

The group Γ acts on $\mathcal{M}$ via its action on $\mathbb{P}^1(\mathbb{Q})$ by Möbius transformations.

For any abelian group G, a *G-valued modular symbol* is a homomorphism $m : \mathcal{M} \longrightarrow G$; we write $m\{x \to y\}$ for $m([x] - [y])$. Let $\mathcal{M}(G)$ denote the left Γ-module of G-valued modular symbols, where the action of Γ is defined by the rule

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

Note that the natural projection onto the group of coinvariants

$$\mathcal{M} \longrightarrow \mathcal{M}_{\Gamma_0(N)} = H_0(\Gamma_0(N), \mathcal{M})$$

is a $\Gamma_0(N)$-invariant modular symbol. Furthermore, this modular symbol is universal, in the sense that any other $\Gamma_0(N)$-invariant modular symbol factors through this one.

One can interpret $H_0(\Gamma_0(N), \mathcal{M})$ geometrically as follows. Given a divisor $[x] - [y] \in \mathcal{M}$, consider any path from x to y in the completed upper half plane $\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$. Identifying the quotient $\Gamma_0(N)\backslash(\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}))$ with $X_0(N)(\mathbb{C})$, this path gives a well-defined element of $H_1(X_0(N), \text{cusps}, \mathbb{Z})$, the singular homology of the Riemann surface $X_0(N)(\mathbb{C})$ relative to the cusps. Manin [Man] proves that this map induces an isomorphism between the maximal torsion-free quotient $H_0(\Gamma_0(N), \mathcal{M})_T$ and $H_1(X_0(N), \text{cusps}, \mathbb{Z})$. Furthermore, the torsion of $H_0(\Gamma_0(N), \mathcal{M})$ is finite and supported at 2 and 3. The projection

$$\mathcal{M} \to \mathcal{M}_{\Gamma_0(N)} \to H_1(X_0(N), \text{cusps}, \mathbb{Z})$$

is called the *universal modular symbol for* $\Gamma_0(N)$.

The points of $X_0(N)$ over $\mathbb{C}$ correspond to isomorphism classes of pairs (E, C_N) of (generalized) elliptic curves $E/\mathbb{C}$ equipped with a cyclic subgroup $C_N \subset E$ of order N. To such a pair we can associate two points of $X_0(M)$, namely the points corresponding to the pairs (E, C_M) and $(E/C_p, C_N/C_p)$, where C_p and C_M are the subgroups of C_N of size p and M, respectively. This defines two morphisms of curves

$$f_1 : X_0(N) \to X_0(M) \text{ and } f_2 : X_0(N) \to X_0(M), \tag{9}$$

each of which is defined over $\mathbb{Q}$. The map f_2 is the composition of f_1 with the Atkin-Lehner involution W_p on $X_0(N)$. Write $f_* = f_{1*} \oplus f_{2*}$ and $f^* = f_1^* \oplus f_2^*$ (resp. $\overline{f_*}$ and $\overline{f^*}$) for the induced maps on singular homology (resp. relative singular homology):

$$\begin{array}{ll} f_* : & H_1(X_0(N), \mathbb{Z}) \to H_1(X_0(M), \mathbb{Z})^2 \\ \overline{f_*} : & H_1(X_0(N), \text{cusps}, \mathbb{Z}) \to H_1(X_0(M), \text{cusps}, \mathbb{Z})^2 \\ f^* : & H_1(X_0(M), \mathbb{Z})^2 \to H_1(X_0(N), \mathbb{Z}) \\ \overline{f^*} : & H_1(X_0(M), \text{cusps}, \mathbb{Z})^2 \to H_1(X_0(N), \text{cusps}, \mathbb{Z}). \end{array}$$

The abelian variety $J_0(N)^{p\text{-new}}$ is defined to be the quotient of $J_0(N)$ by the images of the Picard maps on Jacobians associated to f_1 and f_2. Define $\overline{H}$ and H to be the maximal torsion-free quotients of the cokernels of $\overline{f^*}$ and f^*, respectively:

$$\overline{H} := (\operatorname{coker} \overline{f^*})_T \text{ and } H := (\operatorname{coker} f^*)_T.$$

If we write g for the dimension of $J_0(N)^{p\text{-new}}$, the free abelian groups $\overline{H}$ and H have ranks $2g+1$ and $2g$, respectively, and the natural map $H \to \overline{H}$ is an injection ([Das, Prop. 3.2]).

The groups H and $\overline{H}$ have Hecke actions generated by T_ℓ for $\ell \nmid N$, U_ℓ for $\ell | N$, and W_p. We omit the proof of the following proposition.

Proposition 1.1. *The group $(\overline{H}/H)_T \cong \mathbb{Z}$ is Eisenstein; that is, T_ℓ acts as $\ell+1$ for $\ell \nmid N$, U_ℓ acts as ℓ for $\ell | M$, and W_p acts as -1.*

Proposition 1.1 implies that it is possible to choose a Hecke equivariant map $\psi : \overline{H} \to H$ such that the composition

$$H \longrightarrow \overline{H} \xrightarrow{\psi} H \tag{10}$$

has finite cokernel. For example, we may take ψ to be the Hecke operator $(p^2-1)(T_r - (r+1))$ for any prime $r \nmid N$. We fix a choice of ψ for the remainder of the paper.

1.2 A p-adic uniformization of $J_0(N)^{p\text{-new}}$

For any free abelian group G, let $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), G)$ denote the Γ-module of G-valued measures on $\mathbb{P}^1(\mathbb{Q}_p)$ with total measure zero, where Γ acts by $(\gamma\mu)(U) := \mu(\gamma^{-1}U)$.

In order to construct a Γ-invariant $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), H)$-valued modular symbol, we recall the Bruhat-Tits tree $\mathcal{T}$ of $\mathbf{PGL}_2(\mathbb{Q}_p)$. The set of vertices $\mathcal{V}(\mathcal{T})$ of $\mathcal{T}$ is identified with the set of homothety classes of $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^2$. Two vertices v and v' are said to be adjacent if they can be represented by lattices L and L' such that L contains L' with index p. Let $\mathcal{E}(\mathcal{T})$ denote the set of oriented edges of $\mathcal{T}$, that is, the set of ordered pairs of adjacent vertices of $\mathcal{T}$. Given $e = (v_1, v_2)$ in $\mathcal{E}(\mathcal{T})$, call $v_1 = s(e)$ the source of e, and $v_2 = t(e)$ the target of e. Define the standard vertex v^o to be the class of $\mathbb{Z}_p^2$, and the standard oriented edge $e^o = (v^o, v)$ to be the edge whose source is v^o and whose stabilizer in Γ is equal to $\Gamma_0(N)$. Note that $\mathcal{E}(\mathcal{T})$ is equal to the disjoint union of the Γ-orbits of e^o and $\bar{e}^o$, where $\bar{e}^o = (v, v^o)$ is the opposite edge of e^o. A *half line* of $\mathcal{T}$ is a sequence (e_n) of oriented edges such that $t(e_n) = s(e_{n+1})$. Two half lines are said to be equivalent if they have in common all but a finite number of edges. It is known that the boundary $\mathbb{P}^1(\mathbb{Q}_p)$ of the p-adic upper half plane bijects onto the set of equivalence classes of half lines. For an oriented edge e, write U_e for the subset of $\mathbb{P}^1(\mathbb{Q}_p)$ whose elements correspond to classes of half lines passing through e. The sets U_e are determined by the rules: (1) $U_{\bar{e}^o} = \mathbb{Z}_p$, (2) $U_{\bar{e}} = \mathbb{P}^1(\mathbb{Q}_p) - U_e$, and (3) $U_{\gamma e} = \gamma U_e$ for all $\gamma \in \Gamma$. The U_e give a covering of $\mathbb{P}^1(\mathbb{Q}_p)$ by compact open sets. Finally, recall the existence of a Γ-equivariant reduction map

$$r : (K_p - \mathbb{Q}_p) \longrightarrow \mathcal{V}(\mathcal{T}),$$

defined on the K_p-points of $\mathcal{H}_p$. (As before, K_p is an unramified extension of $\mathbb{Q}_p$.) See [GvdP] for more details.

Define a function

$$\kappa\{x \to y\} : \mathcal{E}(\mathcal{T}) \longrightarrow H$$

as follows. When e belongs to the Γ-orbit of e^o and $\gamma \in \Gamma$ is chosen so that $\gamma e = e^o$, let $\kappa\{x \to y\}(e)$ be ψ applied to the image of $\gamma^{-1}([x] - [y])$ in $\overline{H}$ under the universal modular symbol for $\Gamma_0(N)$. Let $\kappa\{x \to y\}(e)$ be the negative of this value when the relation $\gamma e = \bar{e}^o$ holds.

The function $\kappa\{x \to y\}$ is a *harmonic cocycle on* $\mathcal{T}$, that is, it obeys the rules

1. $\kappa\{x \to y\}(\bar{e}) = -\kappa\{x \to y\}(e)$ for all $e \in \mathcal{E}(\mathcal{T})$, and
2. $\sum_{s(e)=v} \kappa\{x \to y\}(e) = 0$ for all $v \in \mathcal{V}(\mathcal{T})$, where the sum is taken over the $p+1$ oriented edges e whose source $s(e)$ is v.

Furthermore, we have the Γ-invariance property

$$\kappa\{\gamma x \to \gamma y\}(\gamma e) = \kappa\{x \to y\}(e)$$

for all $\gamma \in \Gamma$.

The natural bijection between $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), H)$ and the group of harmonic cocycles on $\mathcal{T}$ valued in H shows that the definition

$$\mu\{x \to y\}(U_e) := \kappa\{x \to y\}(e)$$

yields a Γ-invariant $\mathrm{Meas}(\mathbb{P}^1(\mathbb{Q}_p), H)$-valued modular symbol μ ([Das, Prop. 3.1]). When $m = [x] - [y] \in \mathcal{M}$, we write μ_m for $\mu\{x \to y\}$.

We can now define, for $\tau_1, \tau_2 \in \mathcal{H}_p$ and $m \in \mathcal{M}$, a multiplicative double integral attached to the universal modular symbol for $\Gamma_0(N)$:

$$\begin{aligned} \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_m \omega &:= \times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{t-\tau_2}{t-\tau_1}\right) d\mu_m(t) \\ &= \lim_{||\mathcal{U}||\to 0} \prod_{U\in\mathcal{U}} \left(\frac{t_U-\tau_2}{t_U-\tau_1}\right) \otimes \mu_m(U) \in \mathbb{C}_p^\times \otimes_{\mathbb{Z}} H, \end{aligned}$$

with notations as in (7). One shows that this integral is Γ-invariant:

$$\times\!\!\!\!\!\!\int_{\gamma\tau_1}^{\gamma\tau_2}\int_{\gamma m} \omega = \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_m \omega \qquad \text{for } \gamma \in \Gamma.$$

Letting T denote the torus $T = \mathbb{G}_m \otimes_{\mathbb{Z}} H$, we thus obtain a homomorphism

$$\begin{aligned} ((\mathrm{Div}_0\,\mathcal{H}_p) \otimes \mathcal{M})_\Gamma &\to T \\ ([\tau_1] - [\tau_2]) \otimes m &\mapsto \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_m \omega. \end{aligned} \tag{11}$$

Consider the short exact sequence of Γ-modules defining $\mathrm{Div}_0\,\mathcal{H}_p$:

$$0 \to \mathrm{Div}_0\,\mathcal{H}_p \to \mathrm{Div}\,\mathcal{H}_p \to \mathbb{Z} \to 0.$$

After tensoring with $\mathcal{M}$, the long exact sequence in homology gives a boundary map

$$\delta_1 : H_1(\Gamma, \mathcal{M}) \to ((\mathrm{Div}_0 \, \mathcal{H}_p) \otimes \mathcal{M})_\Gamma. \tag{12}$$

The long exact sequence in homology associated to the sequence (8) defining $\mathcal{M}$ gives a boundary map

$$\delta_2 : H_2(\Gamma, \mathbb{Z}) \to H_1(\Gamma, \mathcal{M}). \tag{13}$$

Define L to be the image of $H_2(\Gamma, \mathbb{Z})$ under the composed homomorphisms in (11), (12), and (13): $H_2(\Gamma, \mathbb{Z}) \to T(\mathbb{Q}_p)$. Note that the Hecke algebra $\mathbb{T}$ of H acts on T.

Theorem 1.2 ([Das], Thm. 3.3). *Let K_p denote the quadratic unramified extension of $\mathbb{Q}_p$. The group L is a discrete, Hecke stable subgroup of $T(\mathbb{Q}_p)$ of rank $2g$. The quotient T/L admits a Hecke-equivariant isogeny over K_p to the rigid analytic space associated to the product of two copies of $J_0(N)^{p\text{-new}}$.*

Remark 1.3. If one lets the nontrivial element of $\mathrm{Gal}(K_p/\mathbb{Q}_p)$ act on T/L by the Hecke operator U_p, the isogeny of Theorem 1.2 is defined over $\mathbb{Q}_p$.

Remark 1.4. As described in [Das, §5.1], Theorem 1.2 is a generalization of a conjecture of Mazur, Tate, and Teitelbaum [MTT, Conjecture II.13.1] which was proven by Greenberg and Stevens [GS].

Theorem 1.2 implies that T/L is isomorphic to the rigid analytic space associated to an abelian variety J defined over a number field (which can be embedded in $\mathbb{Q}_p$). We now state a conjectural refinement of Theorem 1.2.

Conjecture 1.5. *The quotient T/L is isomorphic over K_p to the rigid analytic space associated to an abelian variety J defined over $\mathbb{Q}$.*

Presumably, the abelian variety J will have a natural Hecke action, and the isomorphism of Conjecture 1.5 will be Hecke equivariant; furthermore we expect that if one lets the nontrivial element of $\mathrm{Gal}(K_p/\mathbb{Q}_p)$ act on T/L by the Hecke operator U_p, the isomorphism will be defined over $\mathbb{Q}_p$.

The abelian variety J breaks up (after perhaps an isogeny of 2-power degree) into a product $J^+ \times J^-$, where the signs represent the eigenvalues of complex conjugation on H, and Theorem 1.2 (or rather its proof) implies that each of $J^\pm$ admits an isogeny denoted $\nu_\pm$ to $J_0(N)^{p\text{-new}}$.

Throughout this article, we will need to avoid a certain set of bad primes. Let S denote a finite set of primes containing those dividing $6\varphi(M)(p^2-1)$ or the size of the cokernel of the composite map (10). We say that two abelian varieties (or two analytic spaces) are S-isogenous if there is an isogeny between them whose degree is divisible only by primes in S. We expect that $\nu_\pm$ may be chosen to be S-isogenies defined over $\mathbb{Q}$, but as we will not need this result in the current article, we refrain from stating it as a formal conjecture.

1.3 Stark–Heegner points on J and $J_0(N)^{p\text{-new}}$

Fix $\tau \in \mathcal{H}_p$ and $x \in \mathbb{P}^1(\mathbb{Q})$. The significance of the subgroup L is that it is the smallest subgroup of T such that the cohomology class in $H^2(\Gamma, T/L)$ given by the 2-cocycle

$$d_{\tau,x}(\gamma_1,\gamma_2) := \times\!\!\!\!\!\!\int_{\tau}^{\gamma_1^{-1}\tau}\int_{x}^{\gamma_2 x}\omega \pmod{L}$$

vanishes (the cohomology class of this cocycle, and hence the smallest trivializing subgroup L, is independent of τ and x). Thus there exists a map $\beta_{\tau,x} : \Gamma \to T/L$ such that

$$\beta_{\tau,x}(\gamma_1\gamma_2) - \beta_{\tau,x}(\gamma_1) - \beta_{\tau,x}(\gamma_2) = \times\!\!\!\!\!\!\int_{\tau}^{\gamma_1^{-1}\tau}\int_{x}^{\gamma_2 x}\omega \pmod{L}. \tag{14}$$

The 1-cochain $\beta_{\tau,x}$ is defined uniquely up to an element of $\mathrm{Hom}(\Gamma, T/L)$. The following proposition, which follows from the work of Ihara and whose proof is reproduced in [Das, Prop. 3.7], allows us to deal with this ambiguity.

Proposition 1.6. *The abelianization of* Γ *is finite, and any prime dividing its size divides* $6\varphi(M)(p^2-1)$.

We may now define Stark–Heegner points on J and $J_0(N)^{p\text{-new}}$. Let K be a real quadratic field such that p is inert in K, and choose a real embedding σ of K. For each $\tau \in \mathcal{H}_p \cap K$, consider its associated order $\mathcal{O}_\tau$ as defined in (2). Let γ_τ be the generator of the group of units in $\mathcal{O}_\tau^\times$ of norm 1 whose associated λ_γ (see (2)) is greater than 1 under σ. Finally, choose any $x \in \mathbb{P}^1(\mathbb{Q})$, and let t denote the exponent of the abelianization of Γ. We then define the *Stark–Heegner point associated to* τ by

$$\Phi(\tau) := t \cdot \beta_{\tau,x}(\gamma_\tau) \in T(K_p)/L.$$

The multiplication by t ensures that this definition is independent of the choice of $\beta_{\tau,x}$, and one also checks that $\Phi(\tau)$ is independent of x. Furthermore, the point $\Phi(\tau)$ depends only on the Γ-orbit of τ, so we obtain a map

$$\Phi : \Gamma\backslash(\mathcal{H}_p \cap K) \to T(K_p)/L = J(K_p). \tag{15}$$

Following [Das], we conjecture that the images of Φ satisfy explicit algebraicity properties analogous to those mentioned in the Introduction. Fix a $\mathbb{Z}[1/p]$-order $\mathcal{O}$ in K, and let H_K be the narrow ring class field of K attached to $\mathcal{O}$, whose Galois group is canonically identified by class field theory with $\mathrm{Pic}^+(\mathcal{O})$. If h is the size of this Galois group, there are precisely h distinct Γ-orbits of points in $\mathcal{H}_p \cap K$ whose associated order is $\mathcal{O}$. Let $\tau_1, \ldots, \tau_h$ be representatives for these orbits.

Conjecture 1.7. *The points $\Phi(\tau_i)$ are global points defined over H_K:*

$$\Phi(\tau_i) \in J(H_K). \tag{16}$$

They are permuted simply transitively by $\mathrm{Gal}(H_K/K)$*, so the point*

$$P_K := \Phi(\tau_1) + \cdots + \Phi(\tau_h) \tag{17}$$

lies in $J(K)$.

While a proof of this conjecture (particularly, of equation (16)) seems far from the methods we have currently developed, one may still hope to glean some information from the p-adic invariants of Stark–Heegner points, and it seems of independent interest to relate such invariants to special values of Rankin L-series. Let $P_K = J(K_p)$ be as in (17). The goal of Section 3 is to relate P_K to a certain *algebraic part* of $L(E/K, 1)$, the latter being defined in terms of a formula of Popa that is explained in Section 2. This approach lends itself to generalisations to linear combinations of the points $\Phi(\tau_i)$ associated to the complex characters of $\mathrm{Gal}(H_K/K)$ (see Section 4 for more details).

We conclude this section by remarking that Stark–Heegner points on $J_0(N)^{p\text{-new}}$ are defined by composing the map Φ of (15) with the maps $\nu_\pm$ resulting from Theorem 1.2. In [Das] it is conjectured that Stark–Heegner points on $J_0(N)^{p\text{-new}}$ are defined over H_K; Conjecture 1.7 may thus be viewed as a refinement.

2 Popa's formula

Let D denote the discriminant of K, and fix an orientation $\eta : \mathcal{O}_K \longrightarrow \mathbb{Z}/M\mathbb{Z}$ of the ring of integers $\mathcal{O} := \mathcal{O}_K$ of K. With notations as in the Introduction, there are exactly $h = \#G$ different $R_0(M)^\times$ conjugacy classes of oriented optimal embeddings of $\mathcal{O}$ into the order $R_0(M)$ of matrices in $M_2(\mathbb{Z})$ which are upper triangular modulo M. Let $\Psi_1, \ldots, \Psi_h$ denote representatives for these classes of embeddings. After fixing a fundamental unit ϵ_K of K of norm one, normalised so that $\epsilon_K > 1$ with respect to the fixed real embedding of K, set

$$\gamma_j := \Psi_j(\epsilon_K) \in \Gamma_0(M). \tag{18}$$

Let f be the normalised eigenform attached to E. Then we have

Proposition 2.1 (Popa). *The equality*

$$L(E/K,1) \cdot (D^{1/2}/4\pi^2) = \left(\sum_{j=1}^{h} \int_{z_0}^{\gamma_j z_0} f(z)dz \right)^2$$

holds, for any choice of z_0 in the extended complex upper half plane.

Proof. See Theorem 6.3.1 of [Po]. □

Remark 2.2. The result of Popa, which is stated here for simplicity in the case of the trivial character, deals more generally with twists of the L-series of E/K by complex characters of $\mathrm{Pic}^+(\mathcal{O})$ (and even with twists by complex characters attached to more general orders of K). In order to formulate the result in this more general form, one needs to define an action of $\mathrm{Pic}(\mathcal{O}_K)$ on the set of conjugacy classes of oriented optimal embeddings of $\mathcal{O}$ into the order $R_0(M)$. See [Po] for more details.

The eigenform f determines an algebra homomorphism $\varphi_f : \mathbb{T} \longrightarrow \mathbb{Z}$ satisfying

$$\varphi_f(T_n) = a_n(f), \quad \text{for } (n,N) = 1, \quad \varphi_f(U_\ell) = a_\ell(f), \quad \text{for } \ell | N.$$

Write I_f for the kernel of φ_f. For a $\mathbb{T}$-module A, let $A_f := A/I_f A$ be the largest quotient of A on which $\mathbb{T}$ acts via φ_f. Note that $H_1(X_0(M), \mathbb{Z})_f$ is a $\mathbb{Z}$-module of rank 2. Given a finite set of primes S, let $\mathbb{Z}_S$ denote the localization of $\mathbb{Z}$ in which the primes of S are inverted. By possibly enlarging

S, we may assume that $H_1(X_0(M), \mathbb{Z}_S)_f$ is torsion-free, and hence a free $\mathbb{Z}_S$-module of rank 2.

For any such S, denote by $[\gamma_j] \in H_1(X_0(M), \mathbb{Z}_S)$ the homology class corresponding to γ_j, and let

$$[\gamma_K] := \sum_{j=1}^{h} [\gamma_j].$$

Define the *algebraic part* of $L(E/K, 1)$ by the formula

$$\mathcal{L}(E/K, 1) = \mathcal{L}(E/K, 1)_S := \text{the natural image of } [\gamma_K] \text{ in } H_1(X_0(M), \mathbb{Z}_S)_f.$$

Proposition 2.1 directly implies the following

Corollary 2.3. *$L(E/K, 1) \neq 0$ if and only if $\mathcal{L}(E/K, 1) \neq 0$.*

3 The main formula

The goal of this section is to compute the image of the Stark-Heegner point P_K in the group of connected components at p of the abelian variety J introducted in Section 1, and relate it to $\mathcal{L}(E/K, 1)$.

3.1 The p-adic valuation

The image of the multiplicative double integral under the p-adic valuation map has a simple combinatorial description.

Proposition 3.1 ([BDG], Lemma 2.5 or [Das], Lemma 4.2). *For τ_1, $\tau_2 \in K_p - \mathbb{Q}_p$, and $x, y \in \mathbb{P}^1(\mathbb{Q})$, the equality*

$$\mathrm{ord}_p \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2} \int_x^y \omega = \sum_{e: v_1 \to v_2} \kappa\{x \to y\}(e)$$

holds in H, where $v_i \in \mathcal{V}(\mathcal{T})$, $i = 1, 2$ is the image of τ_i by the reduction map, and the sum is taken over the edges in the path joining v_1 to v_2.

This proposition implies:

Proposition 3.2 ([Das], Props. 4.1, 4.9). *The image of L under*

$$\partial_p = \mathrm{ord}_p \otimes \mathrm{Id} : T(\mathbb{Q}_p) = \mathbb{Q}_p^\times \otimes H \to \mathbb{Z} \otimes H = H$$

is equal to the image of $\ker \bar{f}_*$ by the composition of ψ with the natural projection $H_1(X_0(N), \mathrm{cusps}, \mathbb{Z}) \longrightarrow \bar{H}$.

3.2 Connected components and primes of fusion

Let Φ_p denote the quotient

$$\mathrm{coker}\, f^*/\ker f_*.$$

Let S be a finite set of primes chosen as at the end of section 1.2, that is, S contains the primes dividing $6\varphi(M)(p^2-1)$ or the size of the cokernel of the composite map (10).

The group Φ_p is finite, and the primes dividing the cardinality of $\Phi_p \otimes \mathbb{Z}_S$ are "congruence primes." This will be discussed further below.

Let $\Phi_{p,S}$ denote the $\mathbb{Z}_S$-module $\Phi_p \otimes \mathbb{Z}_S$. By Proposition 3.2, combined with the results of [Das], pp. 438-441, for any unramified extension K_p of $\mathbb{Q}_p$, the p-adic valuation gives a well-defined homomorphism

$$\partial_{p,S} : T(K_p)/L \to \Phi_{p,S}.$$

By the theory of p-adic uniformisation of abelian varieties, the group of connected components of the Néron model of J over the maximal unramified extension of $\mathbb{Q}_p$, tensored with $\mathbb{Z}_S$, is equal to $\Phi_{p,S}$.

Let $\tilde{\mathbb{T}}$, resp. $\mathbb{T}$ denote the Hecke algebra acting faithfully on $H_1(X_0(N), \mathbb{Z})$, resp. $H_1(X_0(M), \mathbb{Z})$. This algebra is generated by the Hecke operators $\tilde{T}_q$ for $q \not| N$ and $\tilde{U}_q$ for $q \mid N$, resp. T_q for $q \not| M$ and U_q for $q \mid M$.

Identify

$$H_1(X_0(M), \mathbb{Z})^2$$

with a submodule of $H_1(X_0(N), \mathbb{Z})$ via f^*. Note that $H_1(X_0(M), \mathbb{Z})^2$ is stable for the action of $\tilde{\mathbb{T}}$. For $(n, p) = 1$, the action of the operator $\tilde{T}_n \in \tilde{\mathbb{T}}$ on $H_1(X_0(M), \mathbb{Z})^2$ is equal to the diagonal action of $T_n \in \mathbb{T}$; moreover, the action of $\tilde{U}_p \in \tilde{\mathbb{T}}$ is equal to that of the operator $U_p := \begin{pmatrix} T_p & -1 \\ p & 0 \end{pmatrix}$. Note that U_p and T_p (with T_p acting diagonally) satisfy the relation

$$U_p^2 - T_p U_p + p = 0.$$

The maximal quotient of $\tilde{\mathbb{T}}$ acting on $H_1(X_0(M), \mathbb{Z})^2$ is called the p-old quotient of $\tilde{\mathbb{T}}$, and is denoted $\tilde{\mathbb{T}}^{p\text{-old}}$.

Proposition 3.3. *There is a $\tilde{\mathbb{T}}$-equivariant isomorphism*

$$\Phi_{p,S} \simeq H_1(X_0(M), \mathbb{Z}_S)^2/\mathrm{Im}(f_* \circ f^*). \tag{19}$$

Proof. The module $\Phi_{p,S}$ is isomorphic to the quotient of $H_1(X_0(N), \mathbb{Z}_S)$ by the $\mathbb{Z}_S$-submodule generated by the image of f^* and the kernel of f_*. It follows from a result of Ribet that the size of the cokernel of f_* divides $\varphi(M)$ (see [Rib1, Thm 4.3]). Thus, having tensored with $\mathbb{Z}_S$, we find that $\Phi_{p,S}$ is isomorphic to the cokernel of the endomorphism $f_* \circ f^*$ of $H_1(X_0(M), \mathbb{Z}_S)^2$. □

Corollary 3.4. *There is an isomorphism*

$$\Phi_{p,S} \cong H_1(X_0(M), \mathbb{Z}_S)/(T_p^2 - (p+1)^2), \tag{20}$$

which is compatible for the action of the Hecke operators $\tilde{T}_n \in \tilde{\mathbb{T}}$, resp. $T_n \in \mathbb{T}$, for $(n,p) = 1$, on the left-, resp. right-hand side.

Proof. The endomorphism $f_* \circ f^*$ is given explicitly by the matrix

$$f_* \circ f^* = \begin{pmatrix} p+1 & T_p \\ T_p & p+1 \end{pmatrix}.$$

Since $p+1$ is invertible in $\mathbb{Z}_S$, the cokernel of this map is isomorphic to

$$H_1(X_0(M), \mathbb{Z}_S)/(T_p^2 - (p+1)^2).$$

□

Remark 3.5. In this remark, assume as in Section 2 that f is the normalised eigenform attached to E, and write $a_n(f) \in \mathbb{Z}$ for the n-th Fourier coefficient of f. Let $S = S_f$ be a finite set of primes containing those dividing $6\varphi(M)(p^2-1)(a_r(f) - (r+1))$, for a prime r not dividing N. An argument similar to the proof of Corollary 3.4 shows that there is an isomorphism

$$(\Phi_{p,S})_f = \Phi_{p,S}/I_f\Phi_{p,S} \cong H_1(X_0(M), \mathbb{Z}_S)_f/(a_p(f)^2 - (p+1)^2). \tag{21}$$

Let λ be a maximal ideal of $\mathbb{T}$ belonging to the support of the module $H_1(X_0(M), \mathbb{Z}_S)/(T_p^2 - (p+1)^2)$, and let ℓ be the characteristic of the finite field $\mathbb{T}/\lambda\mathbb{T}$. The algebra homomorphism

$$\pi : \mathbb{T} \longrightarrow \mathbb{T}/\lambda\mathbb{T}$$

is identified with the reduction in characteristic ℓ of a modular form f on $\Gamma_0(M)$. (The normalised eigenform attached to an elliptic curve of conductor M has Fourier coefficients in $\mathbb{Z}$, and therefore arises in this way.)

Let $\tilde{\lambda}$ be a maximal ideal of $\tilde{\mathbb{T}}$ compatible with λ, in the sense that $\tilde{\lambda}$ arises from a maximal ideal $\bar{\lambda}$ of $\tilde{\mathbb{T}}^{p\text{-old}}$, and both λ and $\bar{\lambda}$ are contained in a maximal ideal of the Hecke ring $\mathbb{T}[U_p]$. (Note that the existence of $\tilde{\lambda}$ is guaranteed by the going-up theorem of Cohen-Seidenberg.) The isomorphism (19) shows that $\tilde{\lambda}$ is p-new (besides being p-old), since it appears in the support of the component group $\Phi_{p,S}$, on which $\tilde{\mathbb{T}}$ acts via its maximal p-new quotient. Therefore, $\tilde{\lambda} = \tilde{\lambda}_g$ corresponds to the reduction in characteristic ℓ of a p-new modular form g on $\Gamma_0(N)$.

In the terminology of Mazur, $\tilde{\lambda}$ is an *ideal of fusion* between the p-old and the p-new subspaces of modular forms on $\Gamma_0(N)$. The forms f and g are called *congruent* modular forms. For more details on these concepts, see [Rib2].

3.3 Specialisation of Stark-Heegner points

This section computes the image $\partial_{p,S}(\Phi(\tau))$ of a Stark-Heegner point $\Phi(\tau)$ in the group of connected components $\Phi_{p,S}$.

Assume that S contains the primes dividing $6\varphi(M)(p^2-1)(a_r(f)-(r+1))$, for a prime r not dividing N, and is such that $H_1(X_0(M), \mathbb{Z}_S)_f$ is a free $\mathbb{Z}_S$-module of rank 2.

We begin by imitating the definition of the map κ, with the group $\Gamma_0(M)$ replacing $\Gamma_0(N)$. Let $\tilde{\Gamma} = R^\times$, where R is the order appearing in the Introduction. Define a function

$$\bar{\kappa}\{x \to y\} : \mathcal{V}(\mathcal{T}) \longrightarrow H_1(X_0(M), \text{cusps}, \mathbb{Z}_S)$$

by setting $\bar{\kappa}\{x \to y\}(v) =$ image of $([\gamma x] - [\gamma y])$, where $\gamma \in \tilde{\Gamma}$ is chosen so that $\gamma v = v^o$. Since the stabilizer of v^o in $\tilde{\Gamma}$ is $\Gamma_0(M)$, and the natural homomorphism from $\mathcal{M}$ to $H_1(X_0(M), \text{cusps}, \mathbb{Z}_S)$ factors through $\Gamma_0(M)$, it follows that the map $\bar{\kappa}$ is well defined.

Recall the compatible ideals $\lambda_f \subset \mathbb{T}$ and $\tilde{\lambda}_g \subset \tilde{\mathbb{T}}$ introduced in Section 3.2. Assume in the sequel that f is the eigenform with rational coefficients attached to E, and that the p-th Hecke operator $\tilde{U}_p \in \tilde{\mathbb{T}}$ maps to 1 in the quotient ring $\tilde{\mathbb{T}}/\tilde{\lambda}_g$. (Since $\tilde{\lambda}_g$ is p-new, $\tilde{U}_p$ maps to ± 1 in $\tilde{\mathbb{T}}/\tilde{\lambda}_g$; the condition we are imposing is equivalent to requiring that λ_f belongs to the support of the module $H_1(X_0(M), \mathbb{Z}_S)/(T_p - (p+1))$.)

The identification

$$H_1(X_0(M), \text{cusps}, \mathbb{Z}_S)/\lambda_f H_1(X_0(M), \text{cusps}, \mathbb{Z}_S) = H/\tilde{\lambda}_g H = \Phi_{p,S}/\tilde{\lambda}_g \Phi_{p,S},$$

which follows from Remark 3.5, implies that the reduction modulo λ_f of $\bar{\kappa}$ can also be viewed as a $\Phi_{p,S}/\tilde{\lambda}_g\Phi_{p,S}$-valued function.

Lemma 3.6. *The relation*

$$\bar{\kappa}\{x \to y\}(v') - \bar{\kappa}\{x \to y\}(v) = \kappa\{x \to y\}(e) \pmod{\tilde{\lambda}_g\Phi_{p,S}}$$

holds for all the oriented edges $e = (v, v')$.

Proof. By our choice of S, the reduction modulo λ_f of $\bar{\kappa}$ yields a map

$$\eta_f : \mathcal{V}(\mathcal{T}) \longrightarrow H_1(X_0(M), \mathbb{Z}_S)/\lambda_f H_1(X_0(M), \mathbb{Z}_S) \simeq \mathbf{F}^2,$$

where $\mathbf{F}$ is the finite field with ℓ elements. The map

$$\eta_f^\sharp : \mathcal{E}(\mathcal{T}) \longrightarrow \mathbf{F}^2$$

given by the rule $\eta_f^\sharp(e) = \eta_f(v') - \eta_f(v)$, for $e = (v, v')$, defines the p-stabilised eigenform associated to η_f. It satisfies the relation $\tilde{U}_p\eta_f^\sharp = \eta_f^\sharp$, where the operator $\tilde{U}_p$ acts by sending an oriented edge e to the formal sum of the oriented edges originating from e. Since $\tilde{\lambda}_g$ is a prime of fusion, it follows that $\eta_f^\sharp$ coincides with the reduction of κ modulo $\tilde{\lambda}_g$. ☐

Let $v \in \mathcal{V}(\mathcal{T})$ denote the reduction of τ. Define a 1-cochain

$$\bar{\beta}_{\tau,x} : \Gamma \to \Phi_{p,S}/\tilde{\lambda}_g\Phi_{p,S}$$

by the rule

$$\bar{\beta}_{\tau,x}(\gamma) = \bar{\kappa}\{x \to \gamma x\}(v).$$

A direct calculation using the equation

$$\bar{\kappa}\{x \to y\}(\gamma v) = \bar{\kappa}\{\gamma^{-1}x \to \gamma^{-1}y\}(v)$$

along with Lemma 3.6 and Proposition 3.1 shows that

$$\bar{\beta}_{\tau,x}(\gamma_1\gamma_2) - \bar{\beta}_{\tau,x}(\gamma_1) - \bar{\beta}_{\tau,x}(\gamma_2) = \mathrm{ord}_p\left(⨍_{\tau}^{\gamma_1^{-1}\tau}\int_x^{\gamma_2 x}\omega\right) \tag{22}$$

in $\Phi_{p,S}/\tilde{\lambda}_g\Phi_{p,S}$. From equation (14) defining $\beta_{\tau,x}$ and the fact that $\beta_{\tau,x}$ is unique up to translation by a homomorphism from Γ, it follows that

$$t \cdot \mathrm{ord}_p\left(\beta_{\tau,x}(\gamma)\right) = t \cdot \bar{\beta}_{\tau,x}(\gamma)$$

in $\Phi_{p,S}/\tilde{\lambda}_g\Phi_{p,S}$. In particular, we have

Proposition 3.7. *The equality*

$$\partial_{p,S}(\Phi(\tau)) = t \cdot \bar{\kappa}\{x \to \gamma_\tau x\}(v)$$

holds in $\Phi_{p,S}/\tilde{\lambda}_g \Phi_{p,S}$.

With notations as in the Introduction, let $\tau = \tau_1, \ldots, \tau_h$ be representatives for the distinct Γ-orbits of points in $\mathcal{H}_p \cap K$ corresponding to a real quadratic order $\mathcal{O}$. Define the Stark-Heegner point

$$P_K := \Phi(\tau_1) + \ldots + \Phi(\tau_h).$$

Write v_j, $j = 1, \ldots, h$ for the image of τ_j by the reduction map, and $\gamma_j \in \mathcal{O}_1^\times$ for the element appearing in the definition of $\Phi(\tau_j)$. Normalise the τ_j so that the associated γ_j are defined as in equation (18). This implies that the vertices v_j all coincide with the standard vertex v^o.

One finds

Corollary 3.8. *The equality*

$$\partial_{p,S}(P_K) = \sum_{i=1}^{h} t \cdot \bar{\kappa}\{x \to \gamma_i x\}(v^o)$$

holds in $\Phi_{p,S}/\tilde{\lambda}_g \Phi_{p,S}$.

Recall the homology element $\mathcal{L}(E/K, 1) \in H_1(X_0(M), \mathbb{Z}_S)$ defined in Section 2. In light of Proposition 3.3, let $\mathcal{L}(E/K, 1)_{(p)}$ denote the natural image of $t \cdot \mathcal{L}(E/K, 1)$ in $\Phi_{p,S}/\tilde{\lambda}_g \Phi_{p,S}$. (Note that t is a unit in $\mathbb{Z}_S$ by Proposition 1.6, so that $\mathcal{L}(E/K, 1)_{(p)}$ is non-zero if and only if the image of $\mathcal{L}(E/K, 1)$ in $\Phi_{p,S}/\tilde{\lambda}_g \Phi_{p,S}$ is non-zero.) Then, combining Corollary 3.8 with Proposition 2.1 yields the main theorem of the Introduction:

Theorem 3.9. *For all primes p which are inert in K,*

$$\partial_{p,S}(P_K) = \mathcal{L}(E/K, 1)_{(p)}.$$

Remark 3.10. The element $\mathcal{L}(E/K, 1)_{(p)}$ depends on the choice of primes p and ℓ (the residue characteristic of λ_f), and of the set S. Given a rational prime p which is inert in K, it is certainly possible that the module $H_1(X_0(M), \mathbb{Z}_S)_f/(a_p(f) - (p + 1))$ be zero, and that no modular form g, congruent to f, be available for which the quotient $\Phi_{p,S}/\tilde{\lambda}_g\Phi_{p,S}$ is non-zero. For such a choice of p, the statement of Theorem 3.9 amounts to a trivial equality. However, the Chebotarev density theorem can be used to produce infinitely many p (for a fixed ℓ) for which the equality of Theorem 3.9 is non-trivial. Assume that $L(E/K,1)$ is non-zero, or equivalently by Corollary 2.3, that $\mathcal{L}(E/K,1) = \mathcal{L}(E/K,1)_S$ is non-zero, where S is such that $H_1(X_0(M),\mathbb{Z}_S)_f$ is a free $\mathbb{Z}_S$-module of rank 2. By a theorem of Serre, for all but finitely many primes ℓ, the element $\mathcal{L}(E/K,1)$ is non-zero modulo ℓ and the Galois representation $\rho_{E,\ell}$ attached to $E[\ell]$—the ℓ-torsion of E—is surjective. A standard application of the Chebotarev density theorem (see for example [BD2]) shows that there exist infinitely many primes p which are inert in K and such that the following conditions are satisfied:

1. ℓ divides the integer $a_p(f) - (p+1)$,
2. ℓ does not divide $6\varphi(M)(p^2-1)(a_r(f)-(r+1))$, for a prime $r \nmid Mp$.

Enlarge the set S above by including all the primes dividing the quantity $6\varphi(M)(p^2-1)(a_r(f)-(r+1))$. For such an S, the results of Section 3.2—see in particular Remark 3.5—show that there exists a congruent form g for which $\mathcal{L}(E/K,1)_{(p)}$ is a non-zero element of $\Phi_{p,S}/\tilde{\lambda}_g\Phi_{p,S}$. (Note that in this case, the latter quotient is identified with $\Phi_p/\tilde{\lambda}_g\Phi_p$, since all the primes in S are units modulo ℓ. Thus, the formula of Theorem 3.9 can be written by omitting a reference to S.)

4 Arithmetic applications

The Shimura reciprocity law implies that the points $\Phi(\tau)$, as τ varies over $\mathcal{H}_p \cap K$, satisfy the same norm-compatibility properties as classical Heegner points attached to an imaginary quadratic K, and it is expected that they should yield an "Euler system" in the sense of Kolyvagin. (Cf. [BD1], Prop. 6.18). Theorem 3.9 gives a relationship between Stark–Heegner points and special values of related Rankin L-series, and one might ask whether this result could have applications to the arithmetic of elliptic curves analogous to those of the Gross-Zagier theorem.

For example, assume Conjecture 1.7 that P_K belongs to $J(K)$. Theorem 3.9 then shows that, when $L(E/K,1) \neq 0$, the points P_K are of infinite order for infinitely many p (in fact, for precisely those p for which $\mathcal{L}(E/K,1)_{(p)} \neq$

0). The P_K can then be used to construct a large and well-behaved supply of cohomology classes in $H^1(K, E_p)$. Following the methods of Kolyvagin, such classes could be used to prove the following theorem:

Theorem 4.1. *Assume Conjecture 1.7. If $L(E/K, 1) \neq 0$, the Mordell-Weil group and Shafarevich-Tate group of E over K are finite.*

We omit the details of the proof, but point out that such a proof would follow that same strategy as in [BD2], but with Stark-Heegner points replacing the classical Heegner points that are used in [BD2]. (See also [Lo] where a similar strategy is used to prove the Birch and Swinnerton-Dyer conjecture for elliptic curves of analytic rank 0 defined over totally real fields which do *not* necessarily arise as quotients of modular or Shimura curves.)

Theorem 4.1 has the drawback of being conditional on Conjecture 1.7—a limitation that appears all the more flagrant when one notes that the conclusion of this theorem already follows, unconditionally, from earlier results of Kolyvagin (or of Kato) applied in turn to $E/\mathbb{Q}$ and to the twist of E by the even Dirichlet character associated to K.

However, greater generality could be achieved by introducing a ring class character

$$\chi : \mathrm{Gal}(H_K/K) \longrightarrow \mathbb{C}^\times$$

and considering twisted special values of $L(E/K, \chi, 1)$ along with related eigencomponents of the Mordell-Weil group $E(H_K)$ and of the Shafarevich-Tate group $Ш := Ш(E/H_K)$:

$$E(H_K)^\chi := \{P \in E(H_K) \otimes \mathbb{C} \text{ such that } \sigma P = \chi(\sigma)P, \quad \forall\ \sigma \in \mathrm{Gal}(H_K/K)\};$$

$$Ш^\chi := \{x \in Ш \otimes \mathbb{Z}[\chi] \text{ such that } \sigma x = \chi(\sigma)x, \quad \forall\ \sigma \in \mathrm{Gal}(H_K/K)\}.$$

In light of Proposition 2.1 and Remark 2.2, Theorem 3.9 generalises directly to a relation between the special value $L(E/K, \chi, 1)$ and the images of the χ-parts of Stark-Heegner points in connected components. Furthermore, when χ is not a quadratic character an unconditional proof of the following theorem would appear to lie beyond the scope of the known Euler systems discovered by Kolyvagin and Kato, and would yield a genuinely new arithmetic application of the conjectural Euler system made from Stark–Heegner points:

Theorem 4.2. *Assume conjecture 1.7 of Section 1. If $L(E/K, \chi, 1) \neq 0$, then the Mordell-Weil group $E(H_K)^\chi$ is trivial and the Shafarevich-Tate group $Ш^\chi$ is finite.*

Part of the inspiration for Theorem 3.9 is the strong analogy between it and the "first explicit reciprocity law" of chapter 4 of [BD2] in the setting where K is imaginary. (See in particular the displayed formula in lemma 8.1 of [BD2].) In [BD2] this first explicit reciprocity law was used in conjunction with a "second explicit reciprocity law" to prove one divisibility in the anti-cyclotomic Main Conjecture of Iwasawa Theory (for K imaginary quadratic). Such a main conjecture has no counterpart when K is real quadratic (since K has no "anti-cyclotomic $\mathbb{Z}_p$-extension") but versions of this statement over ring class fields of K (of finite degree) remain non-trivial and meaningful. Note in this connection that it may be interesting to formulate a convincing substitute for the "second explicit reciprocity law" of [BD2] describing the local behaviour of the point P_K at primes different from p.

References

[BD1] M. Bertolini, H.Darmon. *The p-adic L-functions of modular elliptic curves.* in Mathematics unlimited—2001 and beyond, 109–170, Springer, Berlin, 2001.

[BD2] M. Bertolini, H. Darmon. *The main conjecture of Iwasawa theory for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions.* Annals of Mathematics (2) 162 (2005), no. 1, 1–64.

[BD3] M. Bertolini, H. Darmon. *The rationality of Stark-Heegner points over genus fields of real quadratic fields.* Annals of Mathematics, to appear.

[BDG] M. Bertolini, H. Darmon, and P. Green. *Periods and points attached to quadratic algebras.* MSRI Publ. 49, Cambridge Univ. Press, 323-367, 2004.

[Dar] H. Darmon, *Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications.* Ann. of Math. (2) **154** (2001), no. 3, 589–639.

[Das] S. Dasgupta, *Stark–Heegner points on modular Jacobians.* Ann. Scient. Éc. Norm. Sup., 4e sér., 38 (2005), 427-469.

[DG] H. Darmon, P. Green, *Elliptic curves and class fields of real quadratic fields: algorithms and verifications.* Experimental Mathematics, 11:1, 2002, 37-55.

[GvdP] L. Gerritzen, M. van der Put, *Shottky 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.

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

[Lo] M. Longo, *On the Birch and Swinnerton-Dyer for modular elliptic curves over totally real fields,* Ann. Inst. Fourier, to appear.

[Man] J.I. Manin, *Parabolic Points and Zeta Functions of Modular Curves.* Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), no. 1, 19–66.

[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.

[Po] A. Popa. *Central values of Rankin L-series over real quadratic fields.* Submitted.

[Rib1] K. Ribet, *Congruence Relations Between Modular Forms.* Proceedings of the International Congress of Mathematicians, Warsaw, August 16-24, 1983.

[Rib2] K. Ribet, *On modular representation of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms,* Invent. Math. **100** (1990) 431-476.

[Se] J.P. Serre, *Trees.* Springer, Berlin, 1980.

[W] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem,* Ann. Math. **141** (1995) 443-551.