A BIRCH AND SWINNERTON-DYER CONJECTURE FOR THE MAZUR-TATE CIRCLE PAIRING

MASSIMO BERTOLINI and HENRI DARMON

Abstract

Let E be an elliptic curve over $\mathbb{Q}$ attached to a newform f of weight 2 on $\Gamma_0(N)$, and let K be a real quadratic field in which all the primes dividing N are split. This paper relates the canonical $\mathbb{R}/\mathbb{Z}$-valued "circle pairing" on $E(K)$ defined by Mazur and Tate [MT1] to a period integral $I'(f, K)$ defined in terms of f and K. The resulting conjecture can be viewed as an analogue of the classical Birch and Swinnerton-Dyer conjecture, in which $I'(f, K)$ replaces the derivative of the complex L-series $L(f, K, s)$ and the circle pairing replaces the Néron-Tate height. It emerges naturally as an archimedean fragment of the theory of anticyclotomic p-adic L-functions developed in [BD], and has been tested numerically in a variety of situations. The last section formulates a conjectural variant of a formula of Gross, Kohnen, and Zagier [GKZ] for the Mazur-Tate circle pairing.

Contents

0. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Fix a real quadratic field $K \subset \mathbb{R}$, and let $\varepsilon_K > 1$ denote the fundamental unit of K of positive norm. Write $E(K)^+$ (resp., $E(K)^-$) for the subgroup of the Mordell-Weil group $E(K)$ on which the generator of $\text{Gal}(K/\mathbb{Q})$ acts as multiplication by 1 (resp., -1), so that $E(K)^+ = E(\mathbb{Q})$.

In [MT1, §3.5], Mazur and Tate define (under the assumption that K has class

number one) a canonical $\mathbb{Z}$-bilinear "circle pairing"

$$E(K)^- \times E(\mathbb{Q}) \longrightarrow \mathbb{R}/(\mathbb{Z} \cdot \log \varepsilon_K) \tag{1}$$

and raise the question of what meaning can be ascribed to this pairing (cf. [MT1, Remark 3.5.3]).

By the results of [W], [TW], and [BCDT], the elliptic curve E is known to be modular. Let f be the associated normalised eigenform of weight 2 on $\Gamma_0(N)$. This paper formulates a conjecture relating the circle pairing of (1) to a period integral $I'(f, K)$ defined in terms of f and K. Conjecture 3.1 of Section 3 should be viewed as an analogue of the classical Birch and Swinnerton-Dyer conjecture, in which $I'(f, K)$ replaces the derivative of the complex L-series $L(f, K, s)$ and the circle pairing replaces the Néron-Tate height. It emerges naturally as an archimedean fragment of the theory of anticyclotomic p-adic L-functions developed in [BD], and has been tested numerically in a variety of situations, which are described in Section 4. Section 5 formulates a conjectural variant of a formula of Gross, Kohnen, and Zagier [GKZ] for the Mazur-Tate circle pairing whose proof would give strong evidence for Conjecture 3.1.

1. The circle pairing

For any place v of K, let K_v denote the completion of K at v, and let $\mathcal{O}_v$ (if v is nonarchimedean) be the ring of integers of K_v. Let

$$U_v = \begin{cases} \mathcal{O}_v^\times & \text{if } v \text{ is nonarchimedean,} \\ \{1\} & \text{if } v \text{ is real.} \end{cases}$$

Denote by $\mathrm{Div}^0(E(K_v)) \dot{\times} \mathrm{Div}^0(E(K_v))$ the set of pairs of degree zero divisors on $E(K_v)$ with disjoint supports. The classical Néron-Tate canonical height on $E(K)$ is defined in terms of the local Néron symbols

$$[\ ,\ ]_v : \mathrm{Div}^0\big(E(K_v)\big) \dot{\times} \mathrm{Div}^0\big(E(K_v)\big) \longrightarrow K_v^\times/U_v \tag{2}$$

characterised uniquely (cf. [N, Théorème 3 and Remarque (d) following its proof]) by the following properties.

(1)   The function $[\ ,\ ]_v$ is biadditive and symmetric.

(2)   For any principal divisor (f) and any divisor D with support disjoint from that of (f),

$$[(f), D]_v = f(D) \pmod{U_v}.$$

(3)   The symbol $[\ ,\ ]_v$ is *translation-invariant*; that is,

$$[D_1^x, D_2^x]_v = [D_1, D_2] \quad \text{for all } x \in E(K_v),$$

where D_i^x denotes the translate of the divisor D_i by the point x.

(4)   For fixed D, the function $x \mapsto [(x)-(x_0), D]_v$ is bounded on bounded subsets
        of $E(K_v) - \mathrm{supp}(D)$.

The symbol (2) is defined using arithmetic intersection theory on the Néron model of
E over $\mathscr{O}_v$ when v is nonarchimedean and using capacity theory (Green's functions)
on $E(K_v)$ when v is archimedean (cf. [N] and the discussion in [MT1, §§2, 3]).

Let $\mathbb{A}_K^\times \subset \prod_v K_v^\times$ denote the group of idèles of K. It is convenient to package
the local symbols $[\ ,\ ]_v$ in the obvious way into an idèlic symbol

$$[\ ,\ ] : \mathrm{Div}^0\left(E(K)\right) \times \mathrm{Div}^0\left(E(K)\right) \longrightarrow \mathbb{A}_K^\times / \left(\prod_v U_v\right).$$

Consider the quotient $C_K := \mathbb{A}_K^\times / \left(\prod_v U_v\right) K^\times$ of the idèle class group of K. If (f)
is a principal divisor on $E(K)$ and D is an arbitrary degree zero divisor with support
disjoint from that of (f), note that

$$[(f), D] = \left(f(D)\right) \text{ belongs to } K^\times,$$

so that $[\ ,\ ]$ descends to a C_K-valued pairing

$$\langle\ ,\ \rangle : E(K) \times E(K) \longrightarrow C_K.$$

If $|\cdot| : C_K \longrightarrow (\mathbb{R}^+)^\times$ denotes the homomorphism induced by the idèlic norm (which
is trivial on $K^\times$ by the product formula), then the classical Néron-Tate canonical
height is given by the formula

$$\langle P, Q \rangle_{NT} := \log(|\langle P, Q \rangle|)$$

(cf. [MT1, Proposition 2.3.1]).

Let $\mathrm{Cl}(K)$ and $\mathrm{Cl}^+(K)$ denote, respectively, the class group and narrow class
group of K, and denote by h and h^+ their orders so that

$$h^+ = \begin{cases} h & \text{if } \mathscr{O}_K \text{ has a unit of negative norm,} \\ 2h & \text{otherwise.} \end{cases}$$

Let $C_K^- \subset C_K$ denote the kernel of the idèlic norm on C_K. It is a compact group,
sitting in the middle of an exact sequence

$$0 \longrightarrow \mathbb{R}/(\mathbb{Z} \cdot \log \varepsilon_K) \xrightarrow{\ \alpha\ } C_K^- \xrightarrow{\ \beta\ } \mathrm{Cl}^+(K) \longrightarrow 0,$$

where β is the canonical map that assigns to the idèle class c the corresponding narrow
ideal class, and α sends x to the class of the idèle $(1, \ldots, 1, e^x, e^{-x})$.

Let τ be the generator of $\mathrm{Gal}(K/\mathbb{Q})$, and let $\eta : C_K \longrightarrow C_K^-$ be the homomor-
phism sending x to x/x^τ. The information lost in the passage from $\langle\ ,\ \rangle$ to $\langle\ ,\ \rangle_{NT}$ is
encoded for the most part in the *Mazur-Tate circle pairing*

$$\langle\ ,\ \rangle_{\mathrm{circle}} : E(K) \times E(K) \longrightarrow C_K^-, \quad \text{defined by } \langle P, Q \rangle_{\mathrm{circle}} = \eta(\langle P, Q \rangle).$$

The terminology arises from the fact that $\langle\,,\,\rangle_{\text{circle}}$ takes its values in C_K^-, an extension of a finite group by a circle. The Mazur-Tate circle pairing is a $\mathbb{Z}$-bilinear form on $E(K)$ satisfying the Galois equivariance property

$$\langle P^\tau, Q^\tau \rangle_{\text{circle}} = -\langle P, Q \rangle_{\text{circle}}.$$

In fact, the subspaces $E(\mathbb{Q})$ and $E(K)^-$ are isotropic for $\langle\,,\,\rangle_{\text{circle}}$; for if P and Q belong to the same eigenspace for τ, then the idèle class $\langle P, Q \rangle$ is fixed by τ and hence is in the kernel of η. (For further discussion of the Mazur-Tate circle pairing, see [MT1], [MT2], [C], [B], [H].)

Let r^+ and r^- denote the ranks of $E(\mathbb{Q})$ and $E(K)^-$, respectively, and let $(P_1^+, \ldots, P_{r^+}^+)$ and $(P_1^-, \ldots, P_{r^-}^-)$ denote bases for $E(\mathbb{Q})$ and $E(K)^-$, respectively, modulo torsion. The pairing matrix attached to the Mazur-Tate circle pairing and to the basis $(P_1^+, \ldots, P_{r^+}^+, P_1^-, \ldots, P_{r^-}^-)$ of $E(K) \otimes \mathbb{Q}$ is of the form

$$\begin{pmatrix} 0_{r^+} & M \\ M^t & 0_{r^-} \end{pmatrix},$$

where M is an $(r^+ \times r^-)$-matrix with entries in C_K^- given by

$$M_{ij} = \langle P_i^+, P_j^- \rangle_{\text{circle}}.$$

It is tempting to define the *Mazur-Tate regulator* in this context (or rather, a quantity akin to its *square root*) by the formula

$$R_{\text{circle}}^{1/2} \overset{?}{=} \begin{cases} \det(M) & \text{if } r^+ = r^-, \\ 0 & \text{otherwise.} \end{cases}$$

But since the Mazur-Tate pairing matrix has entries in a product of a finite group by a circle, which is not endowed with a ring structure, one is hard pressed to define its determinant in a sensible way—the one notable exception arising when $r^+ = r^- = 1$.

Thus we set

$$R_{\text{circle}}^{1/2} = \begin{cases} \langle P_1^+, P_1^- \rangle & \text{if } r^+ = r^- = 1, \\ 0 & \text{otherwise.} \end{cases}$$

This definition (or lack thereof in the higher-rank case) reflects a difficulty in our variant of the Birch and Swinnerton-Dyer conjecture which arises on two levels.

(1)   On the arithmetic side, we are unable to propose an interesting definition of a regulator for a pairing matrix whose entries take values in a circle group when r^+ or r^- is at least 1.

(2)   On the analytic side, as is seen in Section 2, the derived period $I'(f, K)$ defined there and playing the role of $L'(f, K, 1)$ is conjectured to vanish when r^+ or r^- is strictly greater than one, and no obvious candidate for a *higher derived period* playing the role of higher derivatives of L-series has emerged from the formalism described in Section 2.

2. Derived periods

Let

$$\omega_f := 2\pi i f(z)\, dz = \sum_{n>0} a_n q^n \frac{dq}{q}, \quad \text{where } q = e^{2\pi i z},$$

denote the $\Gamma_0(N)$-invariant differential on $\mathscr{H}$ associated to f.

Assume in the rest of the article that the real quadratic field K satisfies the following:

$$\text{the discriminant of } K \text{ is prime to } N. \tag{3}$$

Definition 2.1
An algebra embedding

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

is said to be *optimal* (with respect to N) if

$$\Psi(K) \cap M_0(N) = \Psi(\mathscr{O}_K),$$

where $M_0(N)$ is the algebra of matrices with entries in $\mathbb{Z}$ which are upper-triangular modulo N.

LEMMA 2.2
An optimal embedding of K of level N exists if and only if all the prime divisors of N are split in $K/\mathbb{Q}$.

Proof
If Ψ is an optimal embedding with respect to N, then the map

$$\mathfrak{o}_\Psi : \mathscr{O}_K \longrightarrow \mathbb{Z}/N\mathbb{Z},$$

which to x associates the lower right-hand entry of $\Psi(x)$ (taken modulo N), is a ring homomorphism; such a homomorphism can only exist, in light of assumption (3), if all the primes dividing N are split in $K/\mathbb{Q}$. Conversely, if this condition is satisfied, then there is a cyclic ideal $\mathscr{N}$ of $\mathscr{O}_K$ of norm N. Choose a $\mathbb{Z}$-basis (e_1, e_2) of $\mathscr{O}_K$ in such a way that e_1 belongs to $\mathscr{N}$. The action of $\mathscr{O}_K$ on itself by left multiplication, expressed in this basis, yields the desired optimal embedding. More precisely,

$$\Psi(\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{where } \begin{cases} \alpha e_1 = a e_1 + c e_2, \\ \alpha e_2 = b e_1 + d e_2. \end{cases} \tag{4}$$
□

Motivated by Lemma 2.2, assume that

$$\text{all primes dividing } N \text{ are split in } K/\mathbb{Q}. \tag{5}$$

In that case one has

$$\text{sign}(E, K) = 1, \tag{6}$$

where $\text{sign}(E, K)$ denotes the sign in the functional equation for $L(E, K, s)$. In particular, the Birch and Swinnerton-Dyer conjecture predicts that $E(K)$ has *even rank* when assumption (5) holds.

Fix a ring homomorphism $\mathfrak{o}_0 : \mathcal{O}_K \longrightarrow \mathbb{Z}/N\mathbb{Z}$ (or what amounts to the same thing, a cyclic ideal $\ker \mathfrak{o}_0$ of $\mathcal{O}_K$ of norm N, or a choice of square root of $\text{Disc}(K)$ modulo N).

Definition 2.3
The optimal embedding Ψ is said to be *oriented* (with respect to the choice of $\mathfrak{o}_0$) if the homomorphism $\mathfrak{o}_\Psi$ associated to it as in the proof of Lemma 2.2 is equal to $\mathfrak{o}_0$.

Note that if Ψ is an oriented optimal embedding, then so is the conjugate embedding $\alpha \Psi \alpha^{-1}$ for any $\alpha \in M_0(N)^\times$.

One may attach to an ideal class $\mathscr{C}$ of K an oriented optimal embedding $\Psi_\mathscr{C}$ by choosing a representative ideal $\mathfrak{c} \in \mathscr{C}$ of norm prime to N, choosing a $\mathbb{Z}$-basis (e_1, e_2) for $\mathfrak{c}$ such that e_1 belongs to $\mathfrak{c} \cap \mathcal{N}$, and defining Ψ as in (4). The resulting embedding is independent of the choice of $\mathfrak{c}$ and (e_1, e_2) up to conjugation by $M_0(N)^\times$, so that the assignment $\mathscr{C} \mapsto \Psi_\mathscr{C}$ sets up a bijection

$$\left\{ \begin{array}{c} \text{Ideal classes} \\ \text{of } K \end{array} \right\} \xrightarrow{\simeq} \left\{ \begin{array}{c} \text{Oriented optimal embeddings} \\ \text{of } \mathcal{O}_K \text{ into } M_0(N) \end{array} \right\} / M_0(N)^\times.$$

If $\mathscr{C}$ is a narrow ideal class, one may also insist that the basis of $\mathfrak{c}$ be *oriented*, that is, that

$$\det \begin{pmatrix} e_1 & \tau e_1 \\ e_2 & \tau e_2 \end{pmatrix} > 0.$$

Then $\Psi_\mathscr{C}$ becomes well defined up to conjugation by $\Gamma_0(N)$, the group of elements of $M_0(N)^\times$ of positive determinant, and the assignment $\mathscr{C} \mapsto \Psi_\mathscr{C}$ sets up a bijection

$$\left\{ \begin{array}{c} \text{Narrow ideal classes} \\ \text{of } K \end{array} \right\} \xrightarrow{\simeq} \left\{ \begin{array}{c} \text{Oriented optimal} \\ \text{embeddings} \\ \text{of } \mathcal{O}_K \text{ into } M_0(N) \end{array} \right\} / \Gamma_0(N).$$

Thanks to these identifications, the set of oriented optimal embeddings of $\mathcal{O}_K$ into $M_0(N)$, taken up to conjugation by $M_0(N)^\times$ (resp., $\Gamma_0(N)$), becomes a principal homogeneous space for the action of $\text{Cl}(K)$ (resp., $\text{Cl}^+(K)$). In particular, we have the following.

LEMMA 2.4
There are exactly h (resp., h^+) distinct oriented optimal embeddings of K of level N, up to conjugation by $M_0(N)^\times$ (resp., $\Gamma_0(N)$).

We now associate to f and K a canonical *derived period* $I'(f, K) \in C_K^-$ whose value is conjecturally related to the circle regulator of the previous section. The description is simpler when K has narrow class number one, so we begin by treating this case, postponing the general case to the end of the section.

Let Ψ be any optimal embedding of K into $M_2(\mathbb{Q})$, which is unique up to conjugation in $\Gamma_0(N)$, by Lemma 2.4. Let

$$\gamma_\Psi := \Psi(\varepsilon_K) \in \Gamma_0(N).$$

Choose an arbitrary base point x in the extended Poincaré upper half-plane $\mathscr{H}^* = \mathscr{H} \cup \mathbb{P}_1(\mathbb{Q})$. To this data is associated the period integral

$$I_{\Psi,x} = \int_x^{\gamma_\Psi x} \omega_f. \tag{7}$$

It follows directly from the $\Gamma_0(N)$-invariance of ω_f that the period $I_{\Psi,x}$ is independent of the choice of x. Hence one may, when it is convenient, suppress the base point x from the notation and set $I_\Psi := I_{\Psi,x}$. A direct computation also shows that, if α belongs to $\Gamma_0(N)$, then

$$I_{\alpha\Psi\alpha^{-1}} = I_{\alpha\Psi\alpha^{-1},x} = I_{\Psi,\alpha^{-1}x} = I_\Psi.$$

Hence I_Ψ depends only on the $\Gamma_0(N)$-conjugacy class of Ψ. Set

$$I(f, K) = I_\Psi \tag{8}$$

for any choice of optimal embedding Ψ and base point x. By the assumption that K has narrow class number one, this period does not depend on the choice of Ψ thanks to Lemma 2.4. Furthermore, this canonical period is related to special values of L-series as follows.

LEMMA 2.5
The period $I(f, K)$ vanishes if and only if $L(f, K, 1) = 0$.

Sketch of proof
A formula that is spelled out precisely in [P] (see also [GKZ, Chapter II]) implies that

$$I(f, K)^2 \doteq L(f, K, 1),$$

where the symbol $\doteq$ denotes equality up to an explicit nonzero fudge factor. The result follows from this.   □

Assume henceforth that $L(f, K, 1) = 0$, so that

$$I(f, K) = 0. \tag{9}$$

The group $\Psi(K^\times)$ acting by Möbius transformations on $\mathbb{P}_1(\mathbb{C})$ has two fixed points x_Ψ and y_Ψ in $\mathbb{P}_1(\mathbb{R})$. Order these fixed points in such a way that γ_Ψ has x_Ψ as a repulsive fixed point and y_Ψ as an attractive fixed point.

Under assumption (9) it becomes natural to consider the *derived period integral*

$$I'_{\Psi,x} = \int_x^{\gamma_\Psi x} \log\left(\frac{z - x_\Psi}{z - y_\Psi}\right)\omega_f. \tag{10}$$

To analyse the dependence of this quantity on the choice of base point $x \in \mathscr{H}^*$, note that

$$I'_{\Psi,x} - I'_{\Psi,y} = \int_x^y \log\left(\frac{z - x_\Psi}{z - y_\Psi}\right)\omega_f - \int_{\gamma_\Psi x}^{\gamma_\Psi y} \log\left(\frac{z - x_\Psi}{z - y_\Psi}\right)\omega_f.$$

Performing the change of variable $w = \gamma_\Psi^{-1} z$ in the second term, and noting that

$$\left(\frac{\gamma_\Psi w - x_\Psi}{\gamma_\Psi w - y_\Psi}\right) = \varepsilon_K^2 \cdot \left(\frac{w - x_\Psi}{w - y_\Psi}\right),$$

yields

$$I'_{\Psi,x} - I'_{\Psi,y} = 2\log \varepsilon_K \cdot \int_x^y \omega_f. \tag{11}$$

Thus the value of $I'_{\Psi,x}$ depends strongly on the choice of x. One resolves this ambiguity by requiring that

$$\text{the base point } x \text{ belong to } \mathbb{P}_1(\mathbb{Q}) \subset \mathscr{H}^*. \tag{12}$$

A theorem of Manin [M] and Drinfeld asserts that the subgroup of $\mathbb{C}$ generated by the expressions of the form $\int_x^y \omega_f$, where x and y belong to $\mathbb{P}_1(\mathbb{Q})$, is a lattice Λ_f which is commensurable to the Néron lattice of E. This result is crucial in our definition of the derived period for it implies the following.

LEMMA 2.6
The natural image of $I'_{\Psi,x}$ in $\mathbb{C}/2\Lambda_f \log \varepsilon_K$ is independent of the choice of $x \in \mathbb{P}_1(\mathbb{Q})$. Furthermore, it depends only on the $\Gamma_0(N)$-conjugacy class of Ψ.

Proof
The first assertion follows directly from (11). By a slight abuse of notation, we may therefore denote by I'_Ψ the natural image of $I'_{\Psi,x}$ in $\mathbb{C}/2\Lambda_f \log \varepsilon_K$ for any choice of base point $x \in \mathbb{P}_1(\mathbb{Q})$. To prove the second assertion, let $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be an element of $\Gamma_0(N)$. Then a direct calculation shows that

$$I'_{\alpha\Psi\alpha^{-1}, \alpha x} - I'_{\Psi,x} = c_\alpha \cdot I(f, K), \tag{13}$$

where

$$c_\alpha = \log \frac{(\alpha z - \alpha x_\Psi)(z - y_\Psi)}{(\alpha z - \alpha y_\Psi)(z - x_\Psi)} = \log \left(\frac{cy_\Psi + d}{cx_\Psi + d} \right) \tag{14}$$

is a constant independent of z. It follows from (9) that

$$I'_{\alpha \Psi \alpha^{-1}} = I'_\Psi \quad (\text{mod } 2\Lambda_f \cdot \log \varepsilon_K). \tag{15}$$

$\square$

It is useful to supplement (15) by the following equation, which describes the variation of I'_Ψ under conjugation of Ψ by an element $\alpha \in M_0(N)^\times - \Gamma_0(N)$ of determinant -1:

$$I'_{\alpha \Psi \alpha^{-1}} = \bar{I}'_\Psi \quad (\text{mod } 2\Lambda_f \cdot \log \varepsilon_K). \tag{16}$$

Lemmas 2.4 and 2.6 make it possible (under the narrow class number one hypothesis) to associate to f and K a canonical *derived period*

$$I'(f, K) \in \mathbb{C}/(\Lambda_f \cdot \log \varepsilon_K),$$

defined as the natural image of $I'_{\Psi, x}$, for any choice of optimal embedding Ψ of $\mathscr{O}_K$ in $M_0(N)$ and of base point $x \in \mathbb{P}_1(\mathbb{Q})$.

Let Ω^+ be the real period attached to f, defined as the unique positive generator of the lattice $\Lambda_f \cap \mathbb{R}$.

LEMMA 2.7
The period $I'(f, K)$ is fixed under complex conjugation. Its image in $\mathbb{C}/(\Lambda_f \cdot \log \varepsilon_K)$ belongs to the subgroup $\mathbb{R}/(\Omega^+ \cdot \log \varepsilon_K)$.

Proof
Let $\varepsilon \in \mathscr{O}_K^\times$ be a unit of negative norm (which can be chosen, for instance, so that $\varepsilon^2 = \varepsilon_K$), and let $\alpha = \Psi(\varepsilon) \in M_0(N)^\times$. Since α commutes with $\Psi(K^\times)$, we have

$$\alpha \Psi \alpha^{-1} = \Psi; \quad \text{hence } I'_{\alpha \Psi \alpha^{-1}} = I'_\Psi \quad (\text{mod } 2\Lambda_f \cdot \log \varepsilon_K).$$

The result now follows from (16). $\square$

Let $\text{sign}(E, \mathbb{Q}) = \pm 1$ denote the sign in the functional equation of the L-series $L(E/\mathbb{Q}, s)$. This sign is known to be the *negative* of the eigenvalue of the Atkin-Lehner involution acting on ω_f.

LEMMA 2.8
If $\text{sign}(E, \mathbb{Q}) = 1$, then $I'(f, K) = 0$.

Proof

Let $\alpha_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ be the matrix in terms of which the Atkin-Lehner involution is defined. Since α_N normalises $\Gamma_0(N)$, the embedding $\alpha_N \Psi \alpha_N^{-1}$ is also an optimal embedding of K of level N. A direct computation using the change of variables formula and the fact that $w_N f = -f$ shows that

$$I'_{\alpha_N \Psi \alpha_N^{-1}} = -I'_\Psi \quad (\text{mod } 2\Lambda_f \cdot \log \varepsilon_K). \tag{17}$$

Observe that $\alpha_N \Psi \alpha_N^{-1}$, although it is an optimal embedding, is not *oriented*; more precisely, its orientation corresponds to the choice of the ideal $\bar{\mathcal{N}} = \tau\mathcal{N}$ rather than $\mathcal{N}$. Hence $\alpha_N \Psi \alpha_N^{-1}$ is $\Gamma_0(N)$-conjugate to the embedding $\Psi' = \Psi \circ \tau$. Note that $\gamma_{\Psi'} = \gamma_\Psi^{-1}$, so that $(x_{\Psi'}, y_{\Psi'}) = (y_\Psi, x_\Psi)$. Hence

$$\begin{aligned}
I'_{\alpha_N \Psi \alpha_N^{-1}} = I'_{\Psi'} &= \int_x^{\gamma_\Psi^{-1} x} \log\left(\frac{z - y_\Psi}{z - x_\Psi}\right) \omega_f \\
&= \int_x^{\gamma_\Psi x} \log\left(\frac{z - x_\Psi}{z - y_\Psi}\right) \omega_f = I'_\Psi \quad (\text{mod } 2\Lambda_f \cdot \log \varepsilon_K).
\end{aligned} \tag{18}$$

The result follows after comparing (17) and (18).   □

Because of Lemma 2.8, it is natural to assume that $\text{sign}(E, \mathbb{Q}) = -1$. The Birch and Swinnerton-Dyer conjecture then predicts—in light of assumption (6)—that both $E(\mathbb{Q})$ and $E(K)^-$ have *odd* rank.

   We now turn to the derived period in the general case where h^+ is not necessarily equal to 1. In this case we define an invariant $J'(f, K) \in C_K^-$, which, when $h^+ = 1$, is simply the class represented by the period $I'(f, K)$ with the real period Ω^+ factored out. The definition of $J'(f, K)$ (like the definition of the group to which it belongs) is best given adelically.[*]

   It is worthwhile to allow more generality by introducing a quadratic character χ of the narrow ideal class group of K. The character χ is said to be *even* if it is trivial on the group of principal ideals (so that it factors through the class group of K) and is said to be *odd* otherwise (in which case it cuts out, by class field theory, a totally imaginary quadratic extension of K). We set the local sign w to be 1 if χ is even and -1 if χ is odd.

   Let $\mathscr{C}_1, \ldots, \mathscr{C}_{h^+}$ be a full set of representatives for the narrow ideal classes of K, and let $\Psi_1, \ldots, \Psi_{h^+}$ denote representatives for the corresponding $\Gamma_0(N)$-conjugacy

---

[*]The reader may wish in a first reading to skip the rest of this section and jump directly to Section 3, where the Birch and Swinnerton-Dyer–type conjecture relating $I'(f, K)$ to the circle pairing is described.

classes of oriented optimal embeddings of $\mathscr{O}_K$ into $M_0(N)$. Setting

$$I(f, \chi) = \sum_{j=1}^{h^+} \chi(\mathscr{C}_j) I_{\Psi_j}, \tag{19}$$

one has the following (see the references given for Lemma 2.5).

LEMMA 2.9
The period $I(f, \chi)$ vanishes if and only if $L(E/K, \chi, 1) = 0$.

The invariant $J'(f, \chi)$ to be defined below (which we seek to interpret when $I(f, \chi) = 0$) plays the role of $L'(E/K, \chi, 1)$ in the conjectures of Section 3. It is defined as a weighted linear combination of periods

$$J'_{\Psi_j} \in C_K^-$$

indexed by the oriented optimal embeddings Ψ_j of $\mathscr{O}_K$ into $M_0(N)$. Fix such an embedding $\Psi = \Psi_j$, and let x_Ψ and $y_\Psi \in \mathbb{P}_1(K)$ be the fixed points of $\Psi(K^\times)$, normalised as before. Choose a rational function $g_\Psi \in K(x)$ satisfying

$$\mathrm{Div}(g_\Psi) = (y_\Psi) - (x_\Psi).$$

Note that this condition makes g_Ψ well defined up to multiplication by an element of $K^\times$.

Let v be a prime of K, let p be the rational prime that lies below it, and let K_v and k_v denote the corresponding completion and residue field. Reduction modulo v gives a natural map $\mathbb{P}_1(K_v) \longrightarrow \mathbb{P}_1(k_v)$, denoted $x \mapsto \bar{x}$. Define a compact open subset $U_{\Psi,v} \subset \mathbb{P}_1(\mathbb{Q}_p)$ by the rule

$$U_{\Psi,v} = \begin{cases} \mathbb{P}_1(\mathbb{Q}_p) & \text{if } p \text{ is inert or ramified in } K/\mathbb{Q}, \\ \{t \in \mathbb{P}_1(\mathbb{Q}_p) \text{ such that } \bar{t} \neq \bar{x}_\Psi \text{ and } \bar{t} \neq \bar{y}_\Psi\} & \text{otherwise.} \end{cases}$$

The key properties of $U_{\Psi,v}$ are summarised in the following two lemmas.

LEMMA 2.10
If t_1 and t_2 belong to $U_{\Psi,v}$, then the cross ratio

$$\left(\frac{t_1 - y_\Psi}{t_1 - x_\Psi}\right)\left(\frac{t_2 - y_\Psi}{t_2 - x_\Psi}\right)^{-1} = \frac{g_\Psi(t_1)}{g_\Psi(t_2)}$$

belongs to $\mathscr{O}_v^\times$.

Proof

If v is inert or ramified in K, then the expression on the left belongs to $K_v^\times$ and is of norm one. In any case, the reduction of the expression on the left modulo a uniformiser π_v (i.e., its image in $\mathbb{P}_1(k_v)$ under the reduction map) is simply the cross ratio of $\bar{t}_1$, $\bar{t}_2$, $\bar{x}_\Psi$, and $\bar{y}_\Psi$. By definition of $U_{\Psi,v}$, the points $\bar{t}_1$ and $\bar{t}_2$ are different from $\bar{x}_\Psi$ and $\bar{y}_\Psi$, and hence the lemma follows from the familiar properties of the cross ratio.   □

LEMMA 2.11
For all $\alpha \in \Gamma_0(N)$,
$$U_{\alpha\Psi\alpha^{-1},v} = \alpha U_{\Psi,v}.$$

Proof

This follows directly from the fact that $\Gamma_0(N) \subset \mathbf{SL}_2(\mathscr{O}_v)$ acts naturally on $\mathbb{P}_1(K_v)$ and $\mathbb{P}_1(k_v)$ in a manner that is compatible with the reduction map
$$\mathbb{P}_1(K_v) \longrightarrow \mathbb{P}_1(k_v). \qquad\qquad □$$

For each finite place v of K, fix a choice of local base points $t_v \in U_{\Psi,v}$, and choose a base point $t_\infty \in \mathbb{P}_1(\mathbb{Q})$. Write
$$\underline{t} = (\dots, t_v, \dots; t_\infty) \in \prod_v \mathbb{P}_1(\mathbb{Q}_v) \times \mathbb{P}_1(\mathbb{Q})$$

for the infinite tuple corresponding to these choices.

Let Ω_w be the unique positive generator of $\Lambda_f \cap \mathbb{R}$ if $w = 1$ and of $i^{-1}\Lambda_f \cap \mathbb{R}$ if $w = -1$. We define an element
$$J'_{\Psi,\underline{t}} \in C_K = \mathbb{A}_K^\times / \left(\prod_v U_v\right) K^\times$$

by specifying each of its local components,
$$(J'_{\Psi,\underline{t}})_v \in K_v^\times / \mathscr{O}_v^\times = \mathbb{Z}, \qquad (J'_{\Psi,\underline{t}})_{\infty_i} \in \mathbb{R}^\times, \quad i = 1, 2.$$

Each v of K (either finite or one of the two archimedean places ∞_1 or ∞_2) yields an embedding $K(z) \longrightarrow K_v(z)$ of rational function fields, and in this way $g_\Psi(z)$ gives rise to elements denoted $g_\Psi^v(z)$ in each $K_v(z)$. The components of $J'_{\Psi,\underline{t}}$ are defined as follows:
$$(J'_{\Psi,\underline{t}})_v = \begin{cases} \operatorname{ord}_v g_\Psi^v(t_v) \cdot \operatorname{Re}(I_\Psi)\Omega_+^{-1} & \text{if } w = 1, \\ \operatorname{ord}_v g_\Psi^v(t_v) \cdot \operatorname{Imag}(I_\Psi)\Omega_-^{-1} & \text{if } w = -1; \end{cases} \tag{20}$$
$$(J'_{\Psi,\underline{t}})_{\infty_j} = \begin{cases} \exp\left(\operatorname{Re}\left(\int_{t_\infty}^{\gamma_\Psi t_\infty} \log g_\Psi^{\infty_j}(z)\omega_f\right)\Omega_+^{-1}\right) & \text{if } w = 1, \\ \exp\left(\operatorname{Imag}\left(\int_{t_\infty}^{\gamma_\Psi t_\infty} \log g_\Psi^{\infty_j}(z)\omega_f\right)\Omega_-^{-1}\right) & \text{if } w = -1. \end{cases} \tag{21}$$

We note the following.

(1)   The idèle class in C_K corresponding to $J'_{\Psi,\underline{t}}$ does not depend on the choice of g_Ψ. This is because multiplying g_Ψ by a scalar in $K^\times$ changes $J'_{\Psi,\underline{t}}$ by the corresponding principal idèle.

(2)   For each nonarchimedean place v, the local component $(J'_{\Psi,\underline{t}})_v$ does not depend on the choice of base point t_v which was made to define it. This follows directly from Lemma 2.10.

(3)   The archimedean components $(J'_{\Psi,\underline{t}})_{\infty_j}$ do not depend on the choice of base point $t_\infty \in \mathbb{P}_1(\mathbb{Q})$ which was made to define them. This follows from the same manipulations as were used to derive formula (11).

Finally, we have the following.

LEMMA 2.12
The derived period $J'_{\Psi,\underline{t}}$ depends only on the $\Gamma_0(N)$-conjugacy class of Ψ.

Proof
Let $\Psi' = \alpha\Psi\alpha^{-1}$ be an oriented optimal embedding of $\mathscr{O}_K$ into $M_0(N)$ which is conjugate to Ψ under a matrix $\alpha \in \Gamma_0(N)$. The fixed points for this embedding are $(x_{\Psi'}, y_{\Psi'}) = (\alpha x_\Psi, \alpha y_\Psi)$, and we may set

$$
\begin{aligned}
g_{\Psi'}(z) &= g_\Psi(\alpha^{-1}z), \\
\gamma_{\Psi'} &= \alpha\gamma_\Psi\alpha^{-1}, \\
U_{\Psi',v} &= \alpha U_{\Psi,v} \quad \text{(hence } t'_v = \alpha t_v), \\
t'_\infty &= \alpha t_\infty, \\
\underline{t}' &= (\ldots, t'_v, \ldots; t'_\infty).
\end{aligned}
$$

With these choices it follows by a direct computation (using change of variables for the archimedean component) that

$$
(J'_{\Psi,\underline{t}})_v = (J'_{\Psi',\underline{t}'})_v \quad \text{for all } v.
$$

The lemma now follows from the fact that $J'_{\Psi,\underline{t}}$ does not depend on $\underline{t}$.   □

By an abuse of notation, let J'_Ψ denote the natural image of $J'_{\Psi,\underline{t}}$ in C_K^-. As before, let $\mathscr{C}_1, \ldots, \mathscr{C}_{h^+}$ be a full set of representatives for the narrow ideal classes of K, and let $\Psi_1, \ldots, \Psi_{h^+}$ denote representatives for the corresponding $\Gamma_0(N)$-conjugacy classes of oriented optimal embeddings of $\mathscr{O}_K$ into $M_0(N)$. Since J'_{Ψ_j} depends only on $\mathscr{C}_j$

and not on the particular choice of representative, we may define

$$J'(f, K) = \sum_{j=1}^{h^+} J'_{\Psi_j} \quad \text{(with } w = 1\text{)},$$

$$J'(f, \chi) = \sum_{j=1}^{h^+} \chi(\mathscr{C}_j) J'_{\Psi_j}.$$

Question

In the simpler approach that was described, where $h^+ = 1$, the fact that $I'(f, K)$ was well defined depended on the vanishing of $I(f, K)$ (cf. formula (13)). The adelic approach we adopted in the general case, involving a more careful integral normalisation of the factor $g_\Psi(t)$ appearing in the integrand, makes the derived periods J'_Ψ and $J'(f, K)$ well defined in C_K^- without any assumption on the vanishing of the corresponding periods I_Ψ and $I(f, K)$. What meaning (if any) can be ascribed to $J'(f, K)$ when $I(f, K) \neq 0$?

3. The conjecture

We begin by formulating the main conjecture in the special case where $h^+ = 1$, following the notation of Section 2 which was introduced for this setting. Let e denote the exponent of the torsion subgroup of $E(K)$.

CONJECTURE 3.1

The derived period $I'(f, K)$ is nonzero (and, even, of infinite order) if and only if $E(\mathbb{Q})$ and $E(K)^-$ both have rank one. In that case,

$$I'(f, K) \cdot t = \pm \langle P^+, P^- \rangle_{\text{circle}} \cdot \sqrt{\#\text{Ш}} \cdot \Omega_E^+ \cdot \prod_{p|N} c_p \left(\text{mod } \Omega^+ \cdot \frac{1}{e} \log \varepsilon_K \right), \quad (22)$$

where

(1)   *the points P^+ and P^- are generators for $E(\mathbb{Q})$ and $E(K)^-$, respectively, modulo torsion;*

(2)   *t is the index in $E(K)$ of the group generated by P^+ and P^-;*

(3)   *Ш is the conjecturally finite Shafarevich-Tate group of E over K;*

(4)   *Ω_E^+ is the real Néron period for $E/\mathbb{Q}$;*

(5)   *c_p is the local Tamagawa factor attached to $E/\mathbb{Q}_p$.*

Remark

Note that the right-hand side in Conjecture 3.1 can be rewritten as

$$\pm R_{\text{circle}}^{1/2} \cdot \sqrt{\#\text{Ш}} \cdot \Omega_E^+ \cdot \prod_{p|N} c_p$$

and is analogous to the *square root* of the kind of expression in the leading term of $L(E/K, s)$ predicted by the classical Birch and Swinnerton-Dyer conjecture. This is clear for the Tamagawa factors (since all the primes dividing N are split in $K/\mathbb{Q}$), for the factor Ω_E^+ (since K is real quadratic), and for the term involving the order of the Shafarevich-Tate group. Finally, it was explained in Section 1 that $R_{\text{circle}}^{1/2}$ should be thought of as the "square root" of a hypothetical circle pairing regulator for $E(K)$.

In the case where $h^+ > 1$, let H be the extension of K which is cut out by χ. Thus $H = K$ if χ is the trivial character, and H is an unramified quadratic extension of K otherwise.

Let σ be a generator for $\text{Gal}(H/K)$, and let

$$E(H)^\chi := \{P \in E(H) \text{ such that } \sigma P = \chi(\sigma)P \text{ for all } \sigma \in \text{Gal}(H/K)\},$$
$$\text{Ш}^\chi := \{\alpha \in \text{Ш}(E/H) \text{ such that } \sigma\alpha = \chi(\sigma)\alpha \text{ for all } \sigma \in \text{Gal}(H/K)\}$$

denote the χ-parts of the Mordell-Weil group $E(H)$ and of the Shafarevich-Tate group of E over H, respectively.

Choose a lift of τ to $\text{Gal}(H/\mathbb{Q})$. Since τ commutes with $\text{Gal}(H/K)$, it acts on $E(H)^\chi$, and one denotes by $E(H)^{\chi,\pm}$ the eigenspaces for this action and by $r_{\chi,\pm}$ the corresponding ranks. Considerations involving the signs on the functional equation for $L(E/K, \chi, s)$ lead to the expectation that $E(H)^\chi$ has even rank, so that r_χ^+ and r_χ^- should have the same parity.

The adèlic pairing

$$\langle\,,\,\rangle : E(H) \times E(H) \longrightarrow C_H$$

gives rise, by its functorial nature, to a pairing on $E(H)^\chi$ with values in C_K. Composing this pairing with $\eta : C_K \longrightarrow C_K^-$ yields the corresponding circle pairing

$$\langle\,,\,\rangle_{\text{circle}} : E(H)^\chi \times E(H)^\chi \longrightarrow C_K^-,$$

which satisfies properties similar to the case where χ is the trivial character. For example, both the submodules $E(H)^{\chi,+}$ and $E(H)^{\chi,-}$ are isotropic for this pairing.

For each rational prime $p|N$, let $\mathfrak{p}$ be a prime of K above it, and let $\sigma_\mathfrak{p}$ denote the Frobenius element in $\text{Gal}(H/K)$ attached to $\mathfrak{p}$. One may attach to E and χ a Tamagawa factor c_p^χ by letting c_{p^2} denote the Tamagawa factor attached to E over the quadratic unramified extension of $\mathbb{Q}_p$ and setting

$$c_p^\chi = \begin{cases} c_p & \text{if } \chi(\sigma_\mathfrak{p}) = 1, \\ c_{p^2}/c_p & \text{if } \chi(\sigma_\mathfrak{p}) = -1. \end{cases}$$

Let Ω_E^w denote the real (resp., imaginary) Néron period for $E/\mathbb{Q}$ if $w = 1$ (resp., $w = -1$). The ratio (Ω_E^w/Ω_w) is known to be a rational number. Let $d_0 > 0$ be

its denominator, and let $d = d_0 e$, where e is, as before, the exponent of the torsion subgroup of $E(K)$. Let $C_K^-[d]$ denote the d-torsion subgroup of the group C_K^-.

Our conjecture can now be formulated as follows.

CONJECTURE 3.2

The derived period $J'(f, K)$ is nonzero if and only if $E(H)^{\chi,+}$ and $E(H)^{\chi,-}$ both have rank one. In that case

$$J'(f, \chi) \cdot t \doteq \pm \langle P_\chi^+, P_\chi^- \rangle_{\text{circle}} \cdot \sqrt{\# III^\chi} \cdot (\Omega_E^w / \Omega^w) \cdot \prod_{p | N} c_p^\chi \quad \text{in } C_K^- / C_K^-[d],$$

where

(1)   *the symbol $\doteq$ denotes equality up to multiplication by a power of 2;*

(2)   *the points P_χ^+ and P_χ^- are generators for $E(H)^{\chi,+}$ and $E(H)^{\chi,-}$, respectively, modulo torsion;*

(3)   *t is the index of the group generated by P_χ^+ and P_χ^- in $E(H)^\chi$.*

Remark

Applying the natural projection

$$C_K^- \longrightarrow \text{Cl}^+(K)$$

to Conjecture 3.2 yields a variant of the conjectures of [MT2] for real quadratic fields which is spelled out precisely in [D, Conjecture 3.6]. Thus Conjecture 3.2 can be viewed as a (partial) lift of [D, Conjecture 3.6] to the full idèle class group C_K^-, including the connected component of the identity of which class field theory does not provide a Galois-theoretic interpretation.

4. Numerical evidence

We summarise some of the numerical evidence for Conjecture 3.1 which has been gathered. Since the complexity of the period calculation increases with the size of the discriminant and fundamental unit of K, the experiments focused on the real quadratic fields of small discriminant $D = 5$ and $D = 13$.

Calculations with $\mathbb{Q}(\sqrt{5})$

Let $K = \mathbb{Q}(\sqrt{5})$ be the real quadratic field of discriminant 5. It has narrow class number one, and its fundamental unit of norm one is given by

$$\varepsilon_K = \frac{3 + \sqrt{5}}{2}.$$

There are exactly 3 elliptic curves of conductor at most 100 with $\text{sign}(E, \mathbb{Q}) = -1$, all of whose prime factors are split in $\mathbb{Q}(\sqrt{5})$: the curves denoted $61A$, $79A$, and $89A$

in the tables of Cremona [Cr]. The equations for these curves, the coordinates for the points P^+ and P^-, and the circle pairings for these points (with ten significant digits after the decimal point) are in Table 1.

Table 1

E	Equation	P^+	P^-	$\langle P^+, P^- \rangle_{\text{circle}}$
61A	$y^2 + xy = x^3 - 2x + 1$	$(1, 0)$	$(\frac{4}{5}, \frac{-10+3\sqrt{5}}{25})$	-0.9723644825
79A	$y^2 + xy + y = x^3 + x^2 - 2x$	$(0,0)$	$(\frac{1}{5}, \frac{-15+\sqrt{5}}{25})$	-0.4284370106
89A	$y^2 + xy + y = x^3 + x^2 - x$	$(0,0)$	$(\frac{-1}{5}, \frac{-10+7\sqrt{5}}{25})$	-1.5571998775

(For the explicit formulae allowing the calculation of $\langle P^+, P^- \rangle_{\text{circle}}$, see [MT1] or [C], for example.) The values of t are readily calculated from Table 1: one has $t = 2$, 1, and 2 for $E = 61A$, $79A$, and $89A$, respectively.

To compute the derived period I'_ψ, we set

$$F(z) = \int_\infty^z \omega_f = \sum_{n=1}^\infty \frac{a_n}{n} e^{2\pi i n z}.$$

The assumption that $I(f, K) = 0$ implies that $F(z) = F(\gamma_\psi z)$ for all $z \in \mathcal{H}^*$, so that, in particular, $F(\gamma_\psi \infty) = 0$. Applying integration by parts,

$$\int_\infty^{\gamma_\psi \infty} \log \left(\frac{z - x_\psi}{z - y_\psi} \right) \omega_f = -\int_\infty^{\gamma_\psi \infty} F(z) \, d \log \left(\frac{z - x_\psi}{z - y_\psi} \right). \tag{23}$$

Since the differential appearing on the right-hand side of (23) is invariant under γ_ψ, one can replace ∞ by any other $\tau \in \mathcal{H}^*$ in this expression without affecting its value. The optimal choice of τ is to take a value for which both $\text{Imag}(\tau)$ and $\text{Imag}(\gamma_\psi \tau)$ are maximized:

$$\tau = \frac{-d + i}{c}, \quad \text{so that } \gamma_\psi \tau = \frac{a + i}{c}, \quad \text{where } \gamma_\psi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Table 2 lists the choices of γ_ψ which were made for the calculation of $I'_\psi = I'(f, K)$, together with the value of the corresponding derived period. Finally, Table 3 summarises the calculations of the left- and right-hand sides occurring in Conjecture 3.1. Here

- LHS denotes $t \cdot I'(f, K)$;
- $\#\text{III}^?$ denotes the putative value of $\#\text{III}$ which makes (22) hold;
- RHS denotes $\pm \langle P^+, P^- \rangle_{\text{circle}} \cdot \sqrt{\#\text{III}^?} \cdot \Omega^+ \cdot \prod_{p|N} c_p$;
- δ denotes $(\text{LHS} - \text{RHS})/(\Omega^+ \cdot \log \varepsilon_K)$.

Table 2

E	$61A$	$79A$	$89A$
γ_Ψ	$\begin{pmatrix} 19 & -5 \\ 61 & -16 \end{pmatrix}$	$\begin{pmatrix} -28 & -11 \\ 79 & 31 \end{pmatrix}$	$\begin{pmatrix} -8 & -1 \\ 89 & 11 \end{pmatrix}$
I'_Ψ	-0.0304845228	-1.2747715571	1.6512851401

Table 3

E	LHS	$\#III^?$	RHS	δ
$61A$	-0.0609690456	1	-5.9636991823	1
$79A$	-1.2747715571	1	-1.2747715571	0
$89A$	3.3025702803	1	8.6465494063	-1

The last column in Table 3 indicates that in these three calculations the quantity δ was always found to be an integer to within the calculated degree of accuracy, lending support for (but of course not proving) Conjecture 3.1 in these examples. Although only 10 digits of numerical accuracy are indicated in the tables, the calculations were actually carried out to over 20 significant digits. The pari programs and script used to perform these calculations can be downloaded from Darmon's Web site at http://math.mcgill.ca/darmon/programs.html

Calculations with $\mathbb{Q}(\sqrt{13})$
Let $K = \mathbb{Q}(\sqrt{13})$ be the real quadratic field of discriminant 13. It has narrow class number one, and its fundamental unit of norm one is given by

$$\varepsilon_K = \frac{11 + 3\sqrt{13}}{2}.$$

There are exactly 4 elliptic curves of conductor $N \leq 100$ with $\text{sign}(E, \mathbb{Q}) = -1$, all of whose prime factors are split in $\mathbb{Q}(\sqrt{13})$: the curves denoted $43A$, $53A$, $61A$, and $79A$ in the tables of Cremona [Cr]. The equations for these curves, the coordinates for the points P^+ and P^-, and the circle pairings for these points (with ten significant digits after the decimal point) are given in Table 4. From this table it can be checked, by a direct calculation, that $t = 2$ in all cases; that is, the point $P^+ + P^-$ is always divisible by two in $E(K)$. Table 5 lists the derived period I'_Ψ in each case to ten digits of numerical accuracy, together with the value of γ_Ψ used to compute it using (23). Table 6 summarises the calculations of the left- and right-hand sides occurring in Conjecture 3.1, with the same conventions as before.

Table 4

E	Equation	P^+	P^-	$\langle P^+, P^-\rangle_{\text{circle}}$
$43A$	$y^2 + y = x^3 + x^2$	$(0,0)$	$\left(\frac{61}{52}, \frac{-676+675\sqrt{13}}{1352}\right)$	0.9717293862
$53A$	$y^2 + xy + y = x^3 - x^2$	$(0,0)$	$\left(\frac{1}{13}, \frac{-91+25\sqrt{13}}{13^2}\right)$	-2.4475758590
$61A$	$y^2 + xy = x^3 - 2x + 1$	$(1,0)$	$\left(\frac{4}{13}, \frac{-26+31\sqrt{13}}{13^2}\right)$	0.8669460262
$79A$	$y^2 + xy + y =$ $x^3 + x^2 - 2x$	$(0,0)$	$\left(\frac{-23}{13}, \frac{65+53\sqrt{13}}{13^2}\right)$	0.7180776230

Table 5

E	$43A$	$53A$	$61A$	$79A$
γ_Ψ	$\begin{pmatrix} 40 & -9 \\ 129 & -29 \end{pmatrix}$	$\begin{pmatrix} -17 & -3 \\ 159 & 28 \end{pmatrix}$	$\begin{pmatrix} -65 & -27 \\ 183 & 76 \end{pmatrix}$	$\begin{pmatrix} -41 & -9 \\ 237 & 52 \end{pmatrix}$
I'_Ψ	2.6570431602	5.4645636685	-4.6691398640	2.1365682861

A calculation with the curve of conductor 5077

The elliptic curve E of the smallest conductor with rank three is given by the minimal Weierstrass equation

$$y^2 + y = x^3 - 7x + 6.$$

This curve has conductor 5077. The real quadratic field of narrow class number one with the smallest discriminant in which 5077 splits is $K = \mathbb{Q}(\sqrt{53})$. It was checked for this field that the period $I'(f, K)$ belongs to the lattice $\Lambda_f \log \varepsilon_K$. (In fact, in this computation the value of $I'(f, K)$ turned out to be zero to within the calculated accuracy of roughly 12 decimal digits.) This supports the prediction of Conjecture 3.1 that the derived period $I'(f, K)$ should be trivial whenever either r^+ or r^- is strictly greater than one.

Table 6

E	LHS	#$\amalg$?	RHS	δ
$43A$	5.3140863205	1	5.3140863205	0
$53A$	10.9291273370	1	-11.4733570670	2
$61A$	-9.3382797281	1	5.3171474282	-1
$79A$	4.2731365722	4	4.2731365722	0

5. A Gross-Kohnen-Zagier formula

We begin by recalling a formula proved in [GKZ] which relates the height pairings between Heegner points coming from different imaginary quadratic fields to special values of certain L-series.

Given any (not necessarily fundamental) discriminant D, let $K_D = \mathbb{Q}(\sqrt{D})$ denote the corresponding quadratic field, let H_D denote the ring class field attached to the order of discriminant D, and let h_D denote the degree of H_D over K_D.

In order to state [GKZ, Theorem B] precisely, it is useful to recall some of the notation used in this work. If $D < -4$ is a negative discriminant satisfying

$$D \equiv r^2 \pmod{2N},$$

then there are exactly h_D distinct $\Gamma_0(N)$-orbits of integral binary quadratic forms $ax^2 + bxy + cz^2$ of discriminant D satisfying

$$a > 0, \qquad a \equiv 0 \pmod{N}, \qquad b \equiv r \pmod{2N},$$

the roots of which give representatives in $\mathcal{H}/\Gamma_0(N)$ for the distinct Heegner points in $X_0(N)(H_D)$ attached to the order of discriminant D, with orientation corresponding to the choice r of the square root of D (modulo N). Let $\alpha_{D,r}$ be one of these points, and let

$$P_{D,r} = \sum_{\sigma \in \mathrm{Gal}(H_D/K_D)} \sigma \alpha_{D,r} \in \mathrm{Div}\big(X_0(N)\big)(K_D) \tag{24}$$

denote the K_D-rational divisor of degree h_D on $X_0(N)$ formed by taking the trace of $\alpha_{D,r}$. Finally, let

$$y_{D,r} = P_{D,r} - h_D(\infty) \tag{25}$$

denote both the degree zero divisor on $X_0(N)$ and, by a slight abuse of notation, its class in $J_0(N)(K_D)$. We write $P^*_{D,r}$ and $y^*_{D,r}$ for the images of $P_{D,r}$ and $y_{D,r}$ in $X_0^*(N)$ and $J_0^*(N)$, respectively, where $X_0^*(N)$ denotes the quotient of $X_0(N)$ by the Atkin-Lehner involution W_N and $J_0^*(N)$ denotes its Jacobian.

LEMMA 5.1
The element $y^*_{D,r}$ belongs to $J_0^*(N)(\mathbb{Q})$.

Proof
We already know that $y_{D,r}$ belongs to $J_0(N)(K_D)$. To analyse the action of $\mathrm{Gal}(K_D/\mathbb{Q}) = \langle \tau \rangle$ on $y_{D,r}$, note the equality of divisor classes on $X_0(N)$:

$$\tau y_{D,r} = W_N y_{D,r} + h_D\big((0) - (\infty)\big).$$

It follows immediately from this that the class of $y^*_{D,r}$ is fixed by τ and hence belongs to $J_0^*(N)(\mathbb{Q})$. $\square$

Let $\mathbb{T}$ be the subring of $\mathrm{End}(J_0^*(N))$ generated by the Hecke operators T_p ($p \nmid N$) and U_q ($q|N$). Fix a rational multiple $\mathbf{t}_f \in \mathbb{T} \otimes \mathbb{Q}$ of the idempotent attached to f. Such a $\mathbf{t}_f$ is only well defined up to multiplication by a nonzero rational scalar, but one may choose to normalise $\mathbf{t}_f$ so that it belongs to $\mathbb{T}$ and is not divisible by any integer in $\mathbb{T}$. Let $\lambda_f \in \mathbb{Z}$ be the integer scalar defined by the rule

$$\mathbf{t}_f f = \lambda_f f,$$

and set $(y_{D,r}^*)_f := \mathbf{t}_f y_{D,r}^*$.

Finally, define a number d_E by the identity

$$4\pi^2 \|f\|^2 = d_E \Omega_E^+ \Omega_E^-.$$

It is known that d_E is a rational number. In fact, if E is the strong Weil curve of conductor N, it is equal (up to a possible factor of 2) to the degree of the minimal modular parametrisation attached to E (cf. the last equation in [Z, §1].) Furthermore, we have the following.

LEMMA 5.2
The denominator of the rational number $\lambda_f/(2d_E)$ divides $2N^i$ for some i and divides 2 if N is prime.

Proof
The integer denoted r in the proof of [Z, Theorem 3] clearly divides λ_f. The proof of [Z, Theorem 3] (note, in particular, the last sentence) shows that d_E divides $\lambda_f N^i$ for some exponent i which can be taken to be zero if N is prime. □

Let D_1 and D_2 be two negative coprime fundamental discriminants with $D_i \equiv r_i$ (mod $4N$). The product $D = D_1 D_2$ is a positive fundamental discriminant, and the factorisation $D = D_1 D_2$ corresponds, by genus theory, to an odd genus character

$$\chi_{D_1,D_2} : \mathrm{Gal}(H_D/K_D) \longrightarrow \{\pm 1\}.$$

Recall the period $I(f, \chi_{D_1,D_2})$ associated to D and χ_{D_1,D_2} in equation (19).

Theorem B of [GKZ] states that

$$\langle (y_{D_1,r_1}^*)_f, y_{D_2,r_2}^* \rangle = \frac{\lambda_f}{2d_E} \cdot \frac{I(f, \chi_{D_1,D_2})}{i\Omega_E^-} \cdot \frac{L'(E/\mathbb{Q}, 1)}{\Omega_E^+}. \tag{26}$$

Remark
(1) The statement given here differs slightly from [GKZ, Theorem B] in the way that we have grouped the terms, and in our definition of the f-isotypic elements $(y_{D_i,r_i}^*)_f$.

In [GKZ], the element $\mathbf{t}_f$ is chosen to be an idempotent in $\mathbb{T} \otimes \mathbb{Q}$ so that $\lambda_f = 1$. Requiring that $\mathbf{t}_f$ belong to the integral Hecke algebra $\mathbb{T}$ becomes essential for the analogue we wish to formulate next, in which the Néron-Tate height is replaced by the Mazur-Tate circle pairing on $J_0^*(N)(K)$ for a suitable real quadratic field K. This is because the circle pairing, whose value group is not uniquely divisible, does not extend naturally to $J_0^*(N)(K) \otimes \mathbb{Q}$.

(2) Note that the first factor in the expression

$$\frac{\lambda_f}{2d_E} \cdot \frac{I(f, \chi_{D_1, D_2})}{i\Omega_E^-} \tag{27}$$

on the right in (26) is a rational number that is not far from being an integer, by Lemma 5.2, and that the second factor is in fact an integer if the Manin constant attached to the modular parametrisation for E is equal to 1.

A circle pairing variant

We wish to express the circle pairing between two Heegner divisor classes in terms of a derived period integral. As before, we let D_1 and D_2 be negative fundamental discriminants, but in our setting we are forced to relinquish the simplifying assumption that D_1 and D_2 are relatively prime. Rather, we must assume that D_1 *divides* D_2, so that

$$D_2 = d \cdot D_1,$$

where d is a positive fundamental discriminant. To simplify the discussion, assume that the real quadratic field K_d has narrow class number one.

As in the Gross-Kohnen-Zagier formula, let

$$D = D_1 D_2 = d D_1^2.$$

This discriminant is not fundamental but corresponds to the order of conductor D_1 in $\mathbb{Q}(\sqrt{d})$. Let H_D be the ring class field attached to this order, and let χ_{D_1, D_2} denote the (generalised) genus character attached to the factorisation $D = D_1 D_2$.

We define the Heegner element y_{D_1, r_1}^* as in (25) and the sentence following it. Turning to the discriminant D_2, we let ϵ be the genus character of K_{D_2} corresponding to the factorisation $D_2 = dD_1$, which cuts out the quadratic extension $K_{D_2}(\sqrt{d})$ of K_{D_2}, and we set

$$y_{D_2, r_2, \epsilon} = \sum_{\sigma \in \mathrm{Gal}(H_{D_2}/K_{D_2})} \epsilon(\sigma) \sigma \alpha_{D_2, r_2} \in \mathrm{Div}^0\left(X_0(N)\right)\left(K_{D_2}(\sqrt{d})\right).$$

By abuse of notation, we let $y_{D_2, r_2, \epsilon}$ (resp., $y_{D_2, r_2, \epsilon}^*$) denote the corresponding divisor classes in $J_0(N)(K_{D_2}(\sqrt{d}))$ (resp., in $J_0^*(N)(K_{D_2}(\sqrt{d}))$).

LEMMA 5.3
The element $y^*_{D_2,r_2,\epsilon}$ belongs to $J^*_0(K_d)^-$.

Proof
The proof is similar to that of Lemma 5.1 and is left to the reader. □

Having in hand two explicit elements $y^*_{D_1,r_1}$ and $y^*_{D_2,r_2,\epsilon}$ in $J^*_0(\mathbb{Q})$ and $J^*_0(K_d)^-$, respectively, it is natural to ask for a formula for their Mazur-Tate circle pairing, in the spirit of the Gross-Kohnen-Zagier formula (26). Guided by Conjecture 3.1, the following suggests itself naturally.

CONJECTURE 5.4
Let m be the denominator of the rational number (27). Then

$$\langle (y^*_{D_1,r_1})_f, y^*_{D_2,r_2,\epsilon} \rangle_{\text{circle}} = \frac{\lambda_f}{2d_E} \cdot \frac{I(f, \chi_{D_1,D_2})}{i\Omega^-_E} \cdot \frac{I'(f, K_d)}{\Omega^+_E} \left(\bmod \, \mathbb{Z} \frac{\log \varepsilon_K}{m} \right).$$

This conjecture appears to be more tractable than Conjecture 3.1. Since it only involves terms that are explicitly defined, one may hope that it would lend itself to an assault analogous to what is carried out in [GKZ]. The authors plan to return to this matter in a future publication.

References

[BD]   M. BERTOLINI and H. DARMON, *Heegner points on Mumford-Tate curves*, Invent.
         Math. **126** (1996), 413–456. MR 1419003 181, 182
[BDG]   M. BERTOLINI, H. DARMON, and P. GREEN, "Periods and points attached to quadratic
         algebras" to appear in *Proceedings of the MSRI Workshop on Special Values of
         Rankin L-Series*, H. Darmon and S. Zhang, eds., Cambridge Univ. Press,
         Cambridge.
[B]   E. D. BONE, *The circle pairing on elliptic curves*, bachelor's thesis, Amherst College,
         Amherst, Mass., 1995. 184
[BCDT]   C. BREUIL, B. CONRAD, F. DIAMOND, and R. TAYLOR, *On the modularity of elliptic
         curves over* **Q***: Wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.
         MR 1839918 182
[C]   G. S. CALL, *Local heights on families of abelian varieties*, Ph.D. dissertation, Harvard
         University, Cambridge, Mass., 1986. 184, 197
[Cr]   J. E. CREMONA, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge Univ.
         Press, Cambridge, 1997. MR 1628193 197, 198
[D]   H. DARMON, "Heegner points, Heegner cycles, and congruences" in *Elliptic Curves
         and Related Topics*, CRM Proc. Lecture Notes **4**, Amer. Math. Soc., Providence,
         1994, 45–59. MR 1260954 196

[GKZ]   B. GROSS, W. KOHNEN, and D. ZAGIER, *Heegner points and derivatives of L-series, II*,
        Math. Ann. **278** (1987), 497–562. MR 0909238   181, 182, 187, 200, 201, 202,
        203

[H]   S. R. HAMBLEN, *Calculating the circle pairing over families of elliptic curves*,
        bachelor's thesis, Amherst College, Amherst, Mass., 1998.   184

[M]   JU. I. MANIN, *Parabolic points and zeta functions of modular curves* (in Russian), Izv.
        Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66; English translation in Math.
        USSR-Izv. **6** (1972), 19–64. MR 0314846   188

[MT1]   B. MAZUR and J. TATE, "Canonical height pairings via biextensions" in *Arithmetic and
        Geometry, Vol. I*, Progr. Math. **35**, Birkhäuser, Boston, 1983, 195–237.
        MR 0717595   181, 182, 183, 184, 197

[MT2]   ———, *Refined conjectures of the "Birch and Swinnerton-Dyer type,"* Duke Math. J.
        54 (1987), 711–750. MR 0899413   184, 196

[N]   A. NÉRON, *Quasi-fonctions et hauteurs sur les variétés abéliennes*, Ann. of Math. (2)
        82 (1965) 249–331. MR 0179173   182, 183

[P]   A. A. POPA, *Central values of Rankin L-series over real quadratic fields*, Ph.D.
        dissertation, Harvard University, Cambridge, Mass., 2003.   187

[TW]   R. TAYLOR and A. WILES, *Ring-theoretic properties of certain Hecke algebras*, Ann. of
        Math. (2) **141** (1995), 553–572. MR 1333036   182

[W]   A. WILES, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141**
        (1995), 443–551. MR 1333035   182

[Z]   D. ZAGIER, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (1985),
        372–384. MR 0790959   201

Bertolini

Dipartimento di Matematica, Università degli Studi di Milano, Via Saldini 50, I-20133 Milano,
Italy; Massimo.Bertolini@mat.unimi.it

Darmon

Department of Mathematics and Statistics, McGill University, 805 Sherbrooke Street West,
Montreal, Quebec H3A 2K6, Canada; darmon@math.mcgill.ca