Periods of Hilbert modular forms and rational points on elliptic curves

Henri Darmon
Adam Logan

May 12, 2003

Abstract

Let E be a modular elliptic curve over a totally real field. Chapter 8 of [Dar2] formulates a conjecture allowing the construction of canonical algebraic points on E by suitably integrating the associated Hilbert modular form. The main goal of the present work is to obtain numerical evidence for this conjecture in the first case where it asserts something nontrivial, namely, when E has everywhere good reduction over a real quadratic field.

First published in International Mathematics Research Notices in 2003, published by Hindawi Publishing Corporation.

Introduction

To put the calculations of this paper in context, it is useful to recall how, when E is a (modular) elliptic curve over $\mathbb{Q}$, the theory of complex multiplication allows the construction of a distinguished collection of algebraic points on E—the so-called *Heegner points* which were studied systematically by Birch [Bi] and provide the setting for the formula of Gross and Zagier [GZ]. These points are obtained by letting τ be a quadratic irrationality in the Poincaré upper half-plane $\mathcal{H}$ and considering the images, under the Weierstrass uniformisation associated to an appropriate choice of complex lattice, of expressions of the form

$$J_\tau := \int_{i\infty}^{\tau} \omega_f = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n\tau}, \tag{1}$$

where

$$f(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n\tau}, \qquad \omega_f = 2\pi i f(\tau)d\tau, \tag{2}$$

are the normalised eigenform of weight 2 on $\Gamma_0(N)$ attached to E, and the corresponding $\Gamma_0(N)$-invariant differential form on $\mathcal{H}$, respectively. The resulting points P_τ are defined over ring class fields of the imaginary quadratic field

$K = \mathbb{Q}(\tau)$. The conductor of this extension, and the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the collection of all P_τ's, are understood precisely thanks to the Shimura reciprocity law ([Sh4], Theorem 5.4).

The Heegner point construction is based on the following facts:

1. The open modular curve $Y_0(N)$ whose complex points are described by the quotient $\mathcal{H}/\Gamma_0(N)$ admits a canonical model over $\mathbb{Q}$ arising from its interpretation as a (coarse) moduli space for elliptic curves with extra level structures. The modularity of E implies the existence of a parametrisation

$$\Phi : X_0(N) \longrightarrow E, \tag{3}$$

a morphism of algebraic curves over $\mathbb{Q}$. To compute it numerically, let c be the so-called *Manin constant* attached to Φ, the non-zero rational number defined by

$$\Phi^* \omega_E = c \cdot \omega_f, \tag{4}$$

where ω_E is a generator of the free rank one $\mathbb{Z}$-module of global relative regular one-forms on the Néron model for E—a *Néron differential* on E. Let Λ_E denote the Néron lattice of E and let Λ_f denote the sublattice of $c^{-1}\Lambda_E$ defined by

$$\begin{aligned} \Lambda_f &:= \left\langle \int_\tau^{\gamma\tau} \omega_f, \quad \text{for } \gamma \in \Gamma_0(N) \right\rangle & (5) \\ &= \left\langle c^{-1} \int_\alpha \omega_E, \quad \text{for } \alpha \in \Phi_*(H_1(X_0(N), \mathbb{Z}) \right\rangle. & (6) \end{aligned}$$

If $\eta : \mathbb{C}/\Lambda_E \longrightarrow E(\mathbb{C})$ is the Weierstrass uniformisation attached to ω_E, then

$$\Phi(\tau) = \eta(c \cdot J_\tau). \tag{7}$$

2. The quadratic irrationalities $\tau \in \mathcal{H} \cap K$ correspond, under the moduli interpretation of $Y_0(N)$, to elliptic curves with complex multiplication by an order in K. By the theory of complex multiplication these curves are defined over ring class fields of K and hence correspond to points in $Y_0(N)(K^{\mathrm{ab}})$.

In seeking to extend the Heegner point construction to modular elliptic curves defined over a totally real field F of degree $d > 1$, we are faced with the difficulty that the most obvious generalisation of modular curves—the Hilbert modular varieties—are d-dimensional and do not parametrise E in a natural way. Thus, a direct analogue of (3) with $Y_0(N)$ replaced by a Hilbert modular variety does not appear to exist. The usual extension of the theory of complex multiplication to Hilbert modular varieties shows that these varieties are equipped with an abundant collection of algebraic points defined over class fields of certain CM extensions of F; however, these points do not seem to yield points on E, and in light of the remarks made in Chapters 7 and 8 of [Dar2] they should not be expected to.

The known extensions of the Heegner point construction to totally real fields rely on replacing modular curves by Shimura curves rather than by Hilbert modular varieties. More precisely, if E is defined over a field F of odd degree, or if E has multiplicative reduction at a prime ideal of F, then E is equipped with a parametrisation analogous to (3):

$$\Phi : \mathrm{Jac}(X) \longrightarrow E, \tag{8}$$

where X is a *Shimura curve* with a canonical model over F obtained by realising X as (a quotient of) a parameter space for certain abelian varieties with quaternionic multiplication. Heegner points arising from Shimura curve parametrisations have been studied intensively in recent years, leading, for example, to an almost complete generalisation of the Gross-Zagier formula for such points ([Zh1], [Zh2], [Zh3]). But there are still a number of reasons for wishing to push the Heegner point construction beyond the realm of Shimura curve parametrisations:

1. It appears difficult to compute the uniformisation of (8) in practice, in all but the smallest examples; modular forms on quaternion algebras which are not division algebras are hard to work with explicitly, the absence of cusps on the associated curves precluding the existence of Fourier expansions which are so useful in the numerical calculation of expressions such as those in (1).

2. The generalised Heegner point construction—and indeed any method that relies on the known extensions of the theory of complex multiplication—can only yield points defined over ring class fields of a CM extension of a totally real field. Yet the Birch and Swinnerton–Dyer conjecture leads to the expectation that E ought to be equipped with an abundant collection of algebraic points defined over ring class fields of certain quadratic extensions of F which are not CM. (See [Dar2], Chapters 7 and 8 for a discussion of this point.)

3. For a given E/F, a Shimura curve parametrisation as in (8) is not always available. The simplest case where no modular or Shimura curve parametrisation is known or indeed expected to exist in general is that where F is a real quadratic field and E has everywhere good reduction over F.

This article presents numerical evidence for the conjectural generalisation of the Heegner point construction based on periods of Hilbert modular forms described in [Dar2], Chapter 8 and Section 7 of [BDG]. We have confined our experiments to elliptic curves with everywhere good reduction over a real quadratic field, this case being the most computationally tractable, while still presenting a great deal of theoretical interest in light of remark 3 above. For the sake of being self-contained, Sections 1 and 2 recall the construction of Chapter 8 of [Dar2]. Our presentation of this construction, based on the elegant treatment given in [Das], differs from the original description of [Dar2]. Section 3 describes the numerical evidence and Section 4 discusses in further details the algorithms and some of the theoretical and practical issues that arose in their implementation.

1 Hilbert modular forms

The assignment $\tau \mapsto J_\tau$ of equation (1) gives rise to a well-defined map

$$J : \mathcal{H}/\Gamma_0(N) \longrightarrow \mathbb{C}/\Lambda_f, \tag{9}$$

where Λ_f is the canonical period lattice attached to f in equation (5). This section discusses a generalisation of (9) when f is replaced by a Hilbert modular form, closely following the presentation given in [Das] and specialising to the simplest case where F is a real quadratic field of narrow class number 1 and Γ is the full Hilbert modular group attached to F.

Let $S = \{\infty_0, \infty_1\}$ denote the set of archimedean places of F, and write v_0 and v_1 for the corresponding embeddings of F into $\mathbb{R}$. Given $x \in F$ it will occasionally be convenient to write x_j for $v_j(x)$, and to denote by $|x| := x_0 x_1$ the norm of x. Denote likewise by $|n|$ the norm of an integral or fractional ideal n of F. Let ε be a fundamental unit of $\mathcal{O}_F$, chosen such that $\varepsilon_0 < 0$ and $\varepsilon_1 > 0$.

The group $\Gamma = \mathbf{PSL}_2(\mathcal{O}_F)$ acts discretely on the product $\mathcal{H}_0 \times \mathcal{H}_1$ of two copies of the Poincaré upper half-plane, using the real embeddings v_0 and v_1 to make Γ act on $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively by Möbius transformations. The complex-analytic variety

$$X := (\mathcal{H}_0 \times \mathcal{H}_1)/\Gamma \tag{10}$$

describes the complex points of (a singular model of) the Hilbert modular surface parametrising abelian surfaces with real multiplications by $\mathcal{O}_F$—although this moduli interpretation, and the attendant model over F to which it gives rise, will be of no use to us in this article.

A *Hilbert modular form* of weight $(2,2)$ on Γ is a holomorphic function $f(\tau_1, \tau_2)$ on $\mathcal{H}_0 \times \mathcal{H}_1$ with the property that the associated differential form $f(\tau_0, \tau_1) d\tau_0 d\tau_1$ descends to a holomorphic two-form on X (i.e., is invariant under Γ) and is moreover holomorphic at the cusps. Such a form is in particular invariant under translation by elements of $\mathcal{O}_F$, and therefore admits a Fourier expansion at ∞:

$$f(\tau_0, \tau_1) = \sum_{n \gg 0} a_n e^{2\pi i (\frac{n_0}{d_0}\tau_0 + \frac{n_1}{d_1}\tau_1)}. \tag{11}$$

Here the sum is taken over all totally positive elements of $\mathcal{O}_F$, and d is a totally positive generator of the different ideal of $\mathcal{O}_F$. (For more details on Hilbert modular forms the reader may consult Chapter 1 of [Bu].)

For $j = 0, 1$, let $x_j, y_j \in \mathcal{H}_j$ be points on the j-th upper half-plane indexed by the place v_j of F. Write

$$\int_{x_0}^{y_0}\int_{x_1}^{y_1} \omega_f = \sqrt{|d|} \sum_{n \gg 0} \frac{a_n}{|n|} \left(e^{2\pi i \frac{n_0}{d_0} y_0} - e^{2\pi i \frac{n_0}{d_0} x_0}\right)\left(e^{2\pi i \frac{n_1}{d_1} y_1} - e^{2\pi i \frac{n_1}{d_1} x_1}\right) \tag{12}$$

for the usual multiple integral attached to the differential form

$$\omega_f = -4\pi^2 \sqrt{|d|}^{-1} f(\tau_0, \tau_1) d\tau_0 d\tau_1. \tag{13}$$

The form ω_f can be written as an average of two forms ω_f^+ and ω_f^- which are holomorphic only in the first variable:

$$\omega_f^{\pm} := -4\pi^2 \sqrt{|d|}^{-1} \left\{ f(\tau_0, \tau_1) d\tau_0 d\tau_1 \pm f(\varepsilon_0 \tau_0, \varepsilon_1 \bar{\tau}_1) d(\varepsilon_0 \tau_0) d(\varepsilon_1 \bar{\tau}_1) \right\} \tag{14}$$

The differential forms ω_f^+ and ω_f^- enjoy the same properties of invariance under Γ as the form ω_f. In particular,

$$\int_{\gamma x_0}^{\gamma y_0} \int_{\gamma x_1}^{\gamma y_1} \omega_f^{\pm} = \int_{x_0}^{y_0} \int_{x_1}^{y_1} \omega_f^{\pm} \tag{15}$$

for all $\gamma \in \Gamma$. Let $\mathrm{Div}^0(\mathcal{H}_0)$ and $\mathrm{Div}^0(\mathcal{H}_1)$ denote the $\mathbb{Z}[\Gamma]$-module of degree zero divisors supported on $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively. Integration of ω_f^+ and ω_f^- define two homomorphisms

$$\mathrm{Int}^+, \mathrm{Int}^- : (\mathrm{Div}^0(\mathcal{H}_0) \otimes \mathrm{Div}^0(\mathcal{H}_1))_\Gamma \longrightarrow \mathbb{C}, \tag{16}$$

where the subscript of Γ denotes the module of Γ-coinvariants. If D_0 and D_1 denote degree 0 divisors on $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively, then we write

$$\mathrm{Int}^{\pm}(D_0 \otimes D_1) =: \int_{D_0} \int_{D_1} \omega_f^{\pm}. \tag{17}$$

Following [Das], we conjecturally attach to ω_f^+ and ω_f^- two canonical *period lattices* Λ_f^+ and $\Lambda_f^- \subset \mathbb{C}$. To do this, let $\mathbb{Z}[\Gamma]$ denote the group ring of Γ and let I_Γ denote its augmentation ideal. Tensoring the exact sequence

$$0 \longrightarrow I_\Gamma \longrightarrow \mathbb{Z}[\Gamma] \longrightarrow \mathbb{Z} \longrightarrow 0 \tag{18}$$

with I_Γ and taking the Γ-coinvariants yields the exact sequence

$$0 \longrightarrow K_\Gamma \longrightarrow (I_\Gamma \otimes I_\Gamma)_\Gamma \xrightarrow{r} (\mathbb{Z}[\Gamma] \otimes I_\Gamma)_\Gamma \longrightarrow \Gamma_{\mathrm{ab}} \longrightarrow 0, \tag{19}$$

where K_Γ is defined to be the kernel of r and the cokernel I_Γ / I_Γ^2 of r is identified with the abelianisation Γ_{ab} of Γ in the usual way.

Choosing base points τ_0 and τ_1 in $\mathcal{H}_0$ and $\mathcal{H}_1$ respectively, one may define homomorphisms

$$I_{\tau_0,\tau_1}^{\pm} : (I_\Gamma \otimes I_\Gamma)_\Gamma \longrightarrow \mathbb{C} \tag{20}$$

by setting

$$I_{\tau_0,\tau_1}^{\pm}(\theta_0 \otimes \theta_1) = \int_{\theta_0 \tau_0} \int_{\theta_1 \tau_1} \omega_f^{\pm}. \tag{21}$$

It is not hard to see that the restriction of $I_{\tau_0,\tau_1}^{\pm}$ to the subgroup K_Γ is *independent of the choices of* τ_0 *and* τ_1, so the subgroup

$$\Lambda_f^{\pm} := I_{\tau_0,\tau_1}^{\pm}(K_\Gamma) \subset \mathbb{C} \tag{22}$$

depends only on the form f and not on the choices of τ_0 and τ_1 that were made in defining it.

Conjecture 1.1 *Suppose that f is an eigenform with rational Hecke eigenvalues. Then the subgroups Λ_f^+ and Λ_f^- are lattices in $\mathbb{C}$.*

The next section will make a more precise conjecture about the commensurability classes of Λ_f^+ and Λ_f^- by relating them to the Néron lattices of certain associated elliptic curves.

From now on we grant conjecture 1.1.

Definition 1.2 *The lattices Λ_f^+ and Λ_f^- are called the* even *and* odd *period lattice attached to f.*

Let $\overline{I}^{\pm}_{\tau_0,\tau_1}$ denote the reduction of $I^{\pm}_{\tau_0,\tau_1}$ modulo $\Lambda_f^{\pm}$. It follows directly from the definition of $\Lambda_f^{\pm}$ that the maps $\overline{I}^{\pm}_{\tau_0,\tau_1}$ vanish on K_Γ and therefore give rise, by passing to the quotient via the map r of (19), to natural homomorphisms

$$\widetilde{I}^{\pm}_{\tau_0,\tau_1} : \mathrm{Im}(r) \longrightarrow \mathbb{C}/\Lambda_f^{\pm}. \tag{23}$$

To extend this map to all of $(\mathbb{Z}[\Gamma]\otimes I_\Gamma)_\Gamma$, we use the following proposition which implies that the cokernel of r is finite:

Proposition 1.3 *The abelianisation Γ_{ab} of Γ is finite.*

Proof: By the hypothesis that F has narrow class number one, it follows that Γ is generated by the involution $R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, by the translation matrices $T_\theta = \begin{pmatrix} 1 & \theta \\ 0 & 1 \end{pmatrix}$, and by powers of the matrix $U = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}$. Since

$$UT_\theta U^{-1} = T_{\varepsilon^2\theta}, \quad RUR^{-1} = U^{-1}, \tag{24}$$

it follows that

$$T_\theta \equiv T_{\varepsilon^2\theta}, \quad U^2 \equiv 1 \pmod{[\Gamma,\Gamma]}, \tag{25}$$

so that

$$\#\Gamma_{\mathrm{ab}} \text{ divides } 4N_{K/\mathbb{Q}}(\varepsilon^2-1) = -16u^2, \qquad \text{where } \varepsilon = u+v\sqrt{D}. \tag{26}$$

The result follows. □

Let e_Γ denote the exponent of Γ_{ab} (which can be crudely estimated by (26)). The maps $e_\Gamma \widetilde{I}^{\pm}_{\tau_0,\tau_1}$ admit obvious extensions to $(Z[\Gamma]\otimes I_\Gamma)_\Gamma$. More precisely, let $\theta_0 \in \mathbb{Z}[\Gamma]$ and $\theta_1 \in I_\Gamma$ be two group ring elements, and let $D_j = \theta_j\tau_j$ (for $j=0,1$) be the corresponding divisors supported on the Γ-orbit of τ_j. We define

$$\int_{D_0}\int_{D_1} e_\Gamma \cdot \omega_f^{\pm} := \widetilde{I}^{\pm}_{\tau_0,\tau_1}(e_\Gamma\cdot\theta_0\otimes\theta_1) \in \mathbb{C}/\Lambda_f^{\pm}. \tag{27}$$

Letting $\widetilde{\Lambda}_f^{\pm} := e_\Gamma^{-1}\Lambda_f^{\pm}$, an extended double integral with values in $\mathbb{C}/\widetilde{\Lambda}_f^{\pm}$ is defined by the rule

$$\int_{D_0}\int_{D_1} \omega_f^{\pm} := e_\Gamma^{-1}\int_{D_0}\int_{D_1} e_\Gamma\cdot\omega_f^{\pm} \in \mathbb{C}/\widetilde{\Lambda}_f^{\pm}. \tag{28}$$

When τ_1 and τ_2 are in the same Γ-orbit it will be convenient to define

$$\int^{\tau_0}\int_{\tau_1}^{\tau_2}\omega_f^{\pm} := \int_{(\tau_0)}\int_{(\tau_2)-(\tau_1)}\omega_f^{\pm}. \tag{29}$$

Given any $\tau \in \mathcal{H}_0$, let Γ_τ denote the stabiliser subgroup of τ in Γ.

Proposition 1.4 *The group Γ_τ is an abelian group of rank at most* 1.

Proof: Let $K \subset M_2(F)$ be the F-algebra generated by the invertible matrices satisfying

$$M\tau = \tau. \tag{30}$$

This K is a commutative subalgebra of $M_2(F)$, hence has rank at most 2 over F. If $K = F$, then Γ_τ is trivial. Otherwise, the fact that $K^\times$ has a fixed point in $\mathcal{H}_0$ implies that

$$K \otimes_{v_0} \mathbb{R} \simeq \mathbb{C}, \tag{31}$$

where the tensor product is taken over F relative to the real embedding v_0. Hence K is a quadratic extension of F which is complex at ∞_0. The ring $\mathcal{O} = K \cap M_2(\mathcal{O}_F)$ is an $\mathcal{O}_F$-order in K and

$$\Gamma_\tau = \left\{ x \in \mathcal{O}^\times \text{ such that } \mathrm{Norm}_{K/F}(x) = 1 \right\} / \pm 1.$$

By the Dirichlet unit theorem, it follows that Γ_τ has rank at most one, with equality occuring precisely when K is *real* at the place ∞_1. $\square$

Motivated by the proof of proposition 1.4, and following the terminology of [Dar2], ch. 8, we call a quadratic extension K of F an *ATR ("almost totally real")* extension if it is complex at v_0 and real at v_1. We say that $\tau \in \mathcal{H}_0$ is an ATR point if the stabiliser Γ_τ has rank one, i.e., if τ belongs to $\mathcal{H}_0 \cap v_0(K)$ for some ATR extension K of F (after extending v_0 to a complex embedding of K). The set of all ATR points in $\mathcal{H}_0$, equipped with the discrete topology – the only natural topology that presents itself in this setting – is denoted by $\mathcal{H}_0'$. Note that $\mathcal{H}_0'$ is preserved by the natural action of Γ.

Given $\tau \in \mathcal{H}_0'$, let γ_τ be a generator for the stabiliser subgroup of τ. We can now generalise the expression J_τ in (1) by choosing any $x \in \mathcal{H}_1$ and setting

$$J_\tau^{\pm} = \int^{\tau}\int_{x}^{\gamma_\tau x}\omega_f^{\pm}. \tag{32}$$

The assignments $\tau \mapsto J_\tau^{\pm}$ give rise to two well-defined maps

$$J^{\pm} : \mathcal{H}_0'/\Gamma \longrightarrow \mathbb{C}/\widetilde{\Lambda}_f^{\pm}, \tag{33}$$

which are defined analytically solely in terms of f and yield the desired analogue of (9).

2 Elliptic curves

Let E be an elliptic curve with everywhere good reduction over F. For each prime ideal p of F, an integer a_p is associated to E just as in the case where E is defined over $\mathbb{Q}$, by setting

$$a_p = |p| + 1 - \#E(\mathcal{O}_F/p). \tag{34}$$

Let

$$L(E,s) = \prod_p (1 - a_p|p|^{-s} + |p|^{1-2s})^{-1} =: \sum_n a_n |n|^{-s} \tag{35}$$

be the Hasse-Weil L-function attached to E/F, where the product (resp. the sum) is taken over the prime (resp. all) ideals of $\mathcal{O}_F$.

The Shimura-Taniyama conjecture (or rather its generalisation to totally real fields, which fits into the context of the general Langlands philosophy) predicts that the holomorphic function on $\mathcal{H}_0 \times \mathcal{H}_1$ given by the absolutely convergent Fourier series

$$f(\tau_0, \tau_1) = \sum_{n \gg 0} a_{(n)} e^{2\pi i (\frac{n_0}{d_0}\tau_0 + \frac{n_1}{d_1}\tau_1)}, \tag{36}$$

is a Hilbert modular form of weight $(2,2)$ on Γ, and a simultaneous eigenform for all the Hecke operators. We will suppose that this conjecture (which in many cases can be proved by the methods of Wiles) is true for E from now on.

Let $E_{\mathcal{O}_F}$ denote the Néron model of E over $\mathcal{O}_F$, and let $\Omega^1(E_{/\mathcal{O}_F})$ denote its module of global regular relative differential 1-forms. It is a projective (hence free, because of our standing assumption that $h_F = 1$) module of rank one over $\mathcal{O}_F$. Let ω_E be a generator for this module. For $j = 0, 1$, let E_j be the elliptic curve over $\mathbb{R}$ defined by applying the real embedding corresponding to v_j to E/F. Finally, write Λ_0 and Λ_1 for the period lattices obtained by integrating the real invariant differential $v_j(\omega_E)$ on $(E_j)_{/\mathbb{R}}$ against the homology of $E_j(\mathbb{C})$. Denote by λ_j^+ and λ_j^- $(j = 0, 1)$ the generators of $\Lambda_j \cap \mathbb{R}$ and of $\Lambda_j \cap i\mathbb{R}$ respectively, fixed so that λ_j^+ and λ_j^-/i are positive.

Note that ω_E is only well-defined up to multiplication by a power of ε, so that Λ_0 and Λ_1 are only well-defined up to multiplication by the corresponding power of ε_0 and ε_1 respectively. But the four products $\lambda_0^\pm \lambda_1^\pm$ are well-defined up to sign. In particular, the lattices

$$\Lambda_E^+ := \lambda_1^+ \Lambda_0 \quad \text{and} \quad \Lambda_E^- := \lambda_1^- \Lambda_0 \tag{37}$$

do not depend on the choice of Néron differential that was made in defining them.

Conjecture 2.1 *The lattice Λ_f^+ (resp. Λ_f^-) of Definition 1.2 is commensurable with the lattice Λ_E^+ (resp. Λ_E^-).*

Remarks: 1. This conjecture is a concrete reformulation of a conjecture of Oda [Oda] on periods of Hilbert modular forms. For further discussion see Chapter 8 of [Dar2].

2. In specific examples the lattices Λ_E^+ and Λ_E^- can be computed without difficulty using the known algorithms for computing minimal Weierstrass models and Néron differentials on elliptic curves. The calculation of the lattice $\Lambda_f^\pm$, requiring a concrete understanding of the second homology $H_2(\Gamma,\mathbb{Z})$ of Γ, poses more difficulties. We do not know, for example, whether Λ_f^+ and Λ_f^- always belong to the same similarity class of lattices, although one might suspect the answer to be "no".

We are now ready to define maps

$$\Phi^\pm : \mathcal{H}_0'/\Gamma \longrightarrow E_0(\mathbb{C}) \tag{38}$$

playing the role of the classical modular parametrisation in our context. Invoking conjecture 2.1, choose positive integers c^+ and c^- in such a way that

$$c^\pm \widetilde{\Lambda}_f^\pm \subset \Lambda_E^\pm. \tag{39}$$

The integers c^+ and c^- might be viewed as playing a role analogous to that of the Manin constant c in equation (4) of the introduction. Let

$$\eta^\pm : \mathbb{C}/\Lambda_E^\pm \longrightarrow E_0(\mathbb{C}) \tag{40}$$

denote the Weierstrass uniformisation attached to the lattice $\Lambda_E^\pm$. Let t denote the cardinality of the torsion subgroup of $E(K)$. By analogy with (7) we set

$$\Phi^\pm(\tau) := t \cdot \eta^\pm(c^\pm \cdot J_\tau^\pm) \tag{41}$$

for $\tau \in \mathcal{H}_0'$.

Our main conjecture asserts that the point $\Phi(\tau)$ is defined over a specific class field of the ATR extension $F(\tau)$. More precisely, fix an ATR extension K of F, let c be a non-zero ideal of $\mathcal{O}_F$, and let $\mathcal{O} = \mathcal{O}_F + c\mathcal{O}_K$ be the order in K of conductor c. An embedding

$$\Psi : K \longrightarrow M_2(F) \tag{42}$$

of F-algebras is said to be *optimal* (relative to $\mathcal{O}$), or *of conductor c*, if

$$\Psi(K) \cap M_2(F) = \Psi(\mathcal{O}). \tag{43}$$

Let h_+ denote the narrow class number of $\mathcal{O}$ and let h denote its usual class number (i.e., the cardinality of the Picard group of isomorphism classes of projective $\mathcal{O}$-modules of rank one).

Lemma 2.2 *There are exactly h_+ distinct Γ-conjugacy classes of embeddings of K into $M_2(F)$ of conductor c.*

For further discussion of this lemma see Section 8.5 of [Dar2]. The image of $\Psi(K^\times)$ acting on $\mathcal{H}_0$ by Möbius transformations has a unique fixed point τ which by definition is an ATR point.

Let H be the ring class field of K of conductor c, and let $H^+ \supset H$ denote the narrow ring class field of K. The group $\mathrm{Gal}(H^+/H)$ is of order at most two; let σ denote its generator (which corresponds to the complex conjugation attached to the real place v_1). Fix a complex embedding of H^+ extending the embedding v_0. The following is the main conjecture that we have endeavoured to test numerically:

Conjecture 2.3 *The local points $\Phi^+(\tau)$ (resp. $\Phi^-(\tau)$) in $E_0(\mathbb{C})$ are the image of global points in $E(H)$ (resp. in $E(H^+)$). The automorphism σ acts trivially on the image of Φ^+, and as multiplication by -1 on the image of Φ^-.*

Remarks: 1. It is expected that the heights of the points $\Phi^+(\tau)$ and $\Phi^-(\tau)$ interpolate the first derivatives of $L(E/K, s)$ at $s = 1$ twisted by even and odd characters of $\mathrm{Gal}(H^+/K)$ respectively. For example, if H has degree one over K, the Néron-Tate height of $\Phi^+(\tau) \in E(K)$ is expected to agree with $L'(E/K, 1)$ up to multiplication by a simple non-zero fudge factor, by analogy with the classical Gross-Zagier formula. Combining this expectation with the classical Birch and Swinnerton-Dyer conjecture for E/K, it follows that if $E(K)$ has rank strictly greater than 1, resp. rank 1, the subgroup generated by $\Phi^+(\tau)$ should be finite, resp. of index essentially equal to the square root of the order of the Shafarevich-Tate group of E/K. Experience suggests that the latter quantity ought to be a small integer in the (of necessity, atypical) ranges that were treated in our numerical experiments.

2. Conjecture 2.3 was suggested by the strong analogy with the p-adic conjectures formulated in [Dar1] and tested numerically in [DG].

3 Numerical experiments

Elliptic curves with everywhere good reduction over real quadratic fields have been studied by Shimura (cf. [Sh1], [Sh2], and [Sh3]) who has shown that the abelian variety quotient of $J_1(N)$ associated to a primitive eigenform in $S_2(\Gamma_0(N), \varepsilon)$, where $\varepsilon : \mathbb{Z}/N\mathbb{Z}^\times \longrightarrow \pm 1$ is a primitive even Dirichlet character, has everywhere good reduction over the corresponding real quadratic field F. According to tables given in [Cr], up to isogeny there are exactly three elliptic curves of this sort defined over a real quadratic field with prime discriminant ≤ 100, corresponding to the fields $F = \mathbb{Q}(\sqrt{29})$, $\mathbb{Q}(\sqrt{37})$, and $\mathbb{Q}(\sqrt{41})$.

Note that the curves obtained by Shimura's construction are examples of $\mathbb{Q}$-curves, i.e., they are isogenous to their Galois conjugate over F. It appears that for the real quadratic fields F of narrow class number 1 with $\mathrm{Disc}(F) \leq 100$, all elliptic curves with everywhere reduction over F have this property. The prevalence of $\mathbb{Q}$-curves seems to be an artifact of the small ranges in which data has been tabulated, and is not expected to persist in larger ranges. To the best of our knowledge, the first example of a curve of conductor 1 over a real quadratic field with narrow class number 1 which is not a $\mathbb{Q}$-curve occurs over the field F of discriminant 509 generated by $\omega = \frac{1+\sqrt{509}}{2}$ and is given by the equation [Pi]

$$y^2 - xy - \omega y = x^3 + (2+2\omega)x^2 + (162+3\omega)x + (71+34\omega). \qquad (44)$$

Since $\mathbb{Q}$-curves are always expected to appear in the Jacobians of the modular curve $J_1(N)$, some variant of the Heegner point construction could perhaps be used to construct algebraic points on such curves. For a curve such as (44) no such method appears to be available.

The field $F = \mathbb{Q}(\sqrt{29})$. Fix the real embeddings ∞_0 and ∞_1 of F in such a way that v_0 sends $\sqrt{29}$ to the negative square root, and v_1 sends it to the positive square root. Write ω for $(1+\sqrt{29})/2$ (so that $v_0(\omega) < 0$ and $v_1(\omega) > 0$). A fundamental unit of F is

$$\varepsilon = 2 + \omega. \qquad (45)$$

An elliptic curve with everywhere good reduction over F has been found by Tate. Its minimal Weierstrass equation is given by

$$E : y^2 + xy + \varepsilon^2 y = x^3, \qquad (46)$$

and its discriminant is equal to $-\varepsilon^{10}$. It has a rational subgroup of order 3 generated by the point $(0,0)$, and is of rank 0 over F. (See [Se], Section 5.10 for a detailed discussion of the curve E.) The period lattices Λ_j $(j = 0,1)$ attached to the choice of Néron differential $\omega_E = \frac{dx}{2y+x+\varepsilon^2}$ are index two sublattices of $\langle \lambda_j^+, \lambda_j^- \rangle$, where

$$\lambda_0^+ = 10.8794721724\ldots \qquad \lambda_1^+ = (3\sqrt{29}-16)\lambda_0^+,$$
$$\lambda_0^- = 34.2340042602\ldots i \qquad \lambda_1^- = \frac{(3\sqrt{29}-16)}{5}\lambda_0^-.$$

(In these equations $\sqrt{29}$ denotes the *positive* square root.) The fact that Λ_1 is homothetic to an index 5 sublattice of Λ_0 reflects the fact that E is 5–isogenous to its Galois conjugate over $\mathbb{Q}$.

The canonical lattice Λ_E^+ attached to E is given by

$$\Lambda_E^+ = \langle 18.404772944..., -9.2023864724... + 28.9567851002...i \rangle, \qquad (47)$$

while Λ_E^- is given by

$$\Lambda_E^- = \langle 11.58271404011...i, 5.79135702005735...i - 18.2234337984... \rangle. \qquad (48)$$

Table 29.1 below lists a few quadratic ATR extensions $K = F(\beta)$ of small discriminant, together with the norms D_K of their relative discriminants (over F), wide and narrow class numbers, and relative fundamental units. Note that Table 29.1 lists two extensions with $D_K = -35$, which are denoted -35_1 and -35_2 in order to be distinguished.

D_K	β^2	h_K	h_K^+	ε_K
-7	$-1+\omega$	1	1	$(\beta^2+\beta-1)/2$
-16	$2+\omega$	1	1	$2\beta^3+5\beta^2+\beta$
-23	$17+8\omega$	1	1	$(\beta^2-1)/8$
-35_1	$19+9\omega$	2	2	$(\beta^2+9\beta-1)/18$
-35_2	$4+3\omega$	2	4	$(\beta^2+3\beta-1)/6$
-59	$61+28\omega$	1	1	$(\beta^2+14\beta+9)/28$
-63	3ω	1	2	$(\beta^2+6)/3$
-64	$4+2\omega$	1	1	$\beta^2/2$
-80	$1+\omega$	2	2	β^2+1
-91	$7+5\omega$	1	2	$(\beta^2-5\beta+3)/10$
-175	$-5+5\omega$	4	4	$\beta^2/10+\beta/2+1/2$

Table 29.1. ATR extensions of $\mathbb{Q}(\sqrt{29})$ with small discriminant

Table 29.2 lists, next to each ATR extension K of F with $D = D_K$, the x and y coordinates of a point P_D of small height on $E(K)$ found by computer using a simple point-searching algorithm. In all cases we believe this point to be a generator of $E(K)$ modulo torsion, although this has not been checked rigorously. The fourth column of the table lists, in the case where the class number of K is equal to 2, an extra point P' such that P' and P_D generate $E(H^+)$ up to finite index. This point is always to be found among the points P_D already tabulated.

D_K	x	y	P'
-7	β^2+3	$-5\beta^3/2-3\beta^2-8\beta-19/2$	
-16	$\beta^2/2$	$-5\beta^3/4-11\beta^2/4-\beta/4-1/2$	
-23	$(11\beta^2+5)/8$	$-13\beta^3/8-\beta^2-7\beta/8-1/2$	
-35_1	$(2\beta^2+1)/5$	$-59\beta^3/225-43\beta^2/90-89\beta/450-29/90$	P_{-7}
-35_2	$(-4\beta^2-11)/15$	$(-17\beta^3-105\beta^2-43\beta-270)/150$	P_{-7}
-59	$-1/9$	$-11\beta^3/1512-5\beta^2/56-\beta/1512+1/504$	
-63	$7\beta^2/9+5$	$-59\beta^3/225-43\beta^2/90-89\beta/450-29/90$	
-64	$-1/4$	$-3\beta^3/8-5\beta^2/4-\beta/4-3/8$	
-80	$(43\beta^2+51)/10$	$-517/50\beta^3-93/20\beta^2-1233/100\beta$ $-111/20$	P_{-16}
-91	$(98\beta^2+387)/13$	$-18939\beta^3/845-111\beta^2/26$ $-150109\beta/1690-439/26$	
-175	$(-3\beta^2-13)/5$	$-\beta^3/10-11\beta^2/25-37\beta/25-67/10$	See †

Table 29.2. Generators of $E(K)$ modulo torsion

† **Remark**: When $D_K = -175$, the class number of K is equal to 4 and $E(H)\otimes\mathbb{Q}$ appears to be generated by the points P_{-175}, P_{-7}, P_{-35_1}, and P_{-35_2}.

Finally, Table 29.3 below summarises the experimental evidence that has been gathered for the uniformisation Φ^+.

1. The leftmost column indicates the discriminant of the field K that is involved in the calculation.

2. The second column lists the imaginary part of J_τ^+/λ_1^+ that was computed, where τ is any element in $\mathcal{H}'_0/\Gamma$ with associated order isomorphic to $\mathcal{O}_K$. In all cases, since the corresponding K has class number one, the value of J_τ^+ is well-defined modulo the lattice $\widetilde{\Lambda}_f^+$, so that J_τ^+/λ_1^+ is well-defined modulo $(\lambda_1^+)^{-1}\widetilde{\Lambda}_f^+$.

3. For each global point P listed in Table 29.2, let $\widetilde{P}$ be a lift to the group $\mathbb{C}/\Lambda_0$ via the Weierstrass uniformisation attached to Λ_0. (It is well-defined modulo this lattice.) The third column gives the imaginary part of $\widetilde{P}$.

4. Conjecture 2.1 implies that the lattices $(\lambda_1^+)^{-1}\widetilde{\Lambda}_f^+$ and Λ_0 are commensurable so that columns 2 and 3 of Table 29.3 can be naturally compared. Conjecture 2.3 (and the remark after it) suggests that there should be a linear dependence relation *with small integer coefficients* between J_τ^+/λ_1^+, $\widetilde{P}$, and the generators of Λ_0. It was checked that the real parts of both J_τ^+/λ_1^+ and $\widetilde{P}$ are easily recognised rational multiples of λ_0^+, with small denominators bounded by the size of the torsion subgroup of $E(F)$, as expected since $E(F)$ has rank 0.

   The imaginary parts yield more interesting linear relations – as is to be expected since $E(F)$ has rank 0, so that $\Phi^+(\tau)$ should belong to the minus-eigenspace in $E(K)$ for the generator of $\mathrm{Gal}(K/F)$, which is given by complex conjugation attached to the place v_0. The relations involving the imaginary parts were found numerically to hold within the calculated numerical accuracy of at least 12 decimal digits. Here a, b, c are the integers that ostensibly satisfy, when $h = 1$, the relation

   $$\mathrm{Imag}\left(a \cdot J_\tau^+/\lambda_1^+ + b \cdot \widetilde{P} + c \cdot \lambda_0^-\right) \stackrel{?}{=} 0, \qquad (49)$$

   to within the calculated accuracy. For the relative discriminants -35_1, -35_2, and -80 attached to fields of class number 2, for which H is a quadratic extension of K, the linear relation was found to involve (as expected) both the points P and P' of Table 29.2. In those cases the lifts of P and P' are listed in column 3 on consecutive lines and the coefficients involved in the linear relation are listed in the corresponding position in the column labelled b.

D_K	imag(J_τ^+/λ_1^+)	imag$(\widetilde{P})$	a	b	c
-7	-4.1065886757855	-3.079941506839	-3	4	0
-16	2.2268825202458	5.176638961858	15	20	-4
-23	-8.7234515079459	10.574413499142	3	-4	2
-35_1	0.6541186390204	4.835246135965	15	10	1
		-3.079941506839		30	
-35_2	1.3559957321827	-1.748436897948	15	-5	15
		-3.079941506839		15	
-59	2.3399309289739	8.515253081333	-15	-20	6
-63	0.1407578729538	10.059064468632	-15	-10	3
-64	-5.8375918830394	-2.468606939763	15	20	4
-80	-3.4771883041218	0.205296785629	15	10	6
		5.176638961858		-30	
-91	2.1415937032841	6.635790980948	15	-10	1
-175	1.4909906157837	1.290594724488	15	-5	2
		See rmk. 4 below			

Table 29.3. Numerical evidence for conjecture 2.4.

Remarks: 1. In all the examples listed in Table 29.3, the period J_τ^+ could in particular be used to recover a point $P \in E(K)$ of infinite order and relatively small height. While most of the calculations were only carried out to between 12 and 30 digits, one of them, involving the field whose relative discriminant has norm -64, has been checked to 200 decimal places of accuracy.

2. The data in Table 29.3 suggests an expression for $\eta_0(J_\tau^+/\lambda_1^+)$ as an element of $E(H^+)\otimes\mathbb{Q}$. Let P_K denote the trace from H^+ to K of this element. For the 11 examples in Table 29.3, the equality

$$P_K \stackrel{?}{=} \pm 4/3 \cdot P =: 2\ell_F \cdot P \quad \text{holds in } E(K)\otimes\mathbb{Q}. \tag{50}$$

It is noteworthy that the coefficient ℓ_F in this relation is (unlike the point P) independent of K. This suggests that, for these examples, the Shafarevich-Tate group of E twisted by the quadratic character of $\mathrm{Gal}(\bar{F}/F)$ attached to K is probably trivial, so that the position of P_K in $E(K)\otimes\mathbb{Q}$ is entirely controlled by the algebraic part of $L(E/F,1)$, a quantity which does not depend on K. In fact the following equality was checked to 20 digits of decimal accuracy:

$$\int_0^{i\infty}\int_{i\varepsilon^{-1}}^{i\varepsilon} \omega_f^+ = -\ell_F^2 \cdot \lambda_0^+\lambda_1^+. \tag{51}$$

Note that the expression on the left in (51) is a multiple of the special value $L(E/F,1)$ by a simple non-zero fudge factor.

3. For the three cases in which $h = 2$, we can introduce the non-trivial character of order two

$$\chi : \mathrm{Gal}(H^+/K) \longrightarrow \mathrm{Gal}(H/K) = \pm 1 \tag{52}$$

and set

$$P^{\chi} := \sum_{\sigma\in \mathrm{Gal}(H^+/K)} \chi(\sigma)\eta_0(J_\tau^+/\lambda_1^+)^\sigma. \tag{53}$$

In the three cases with $h = 2$ listed in Table 29.2, it appears that

$$P^{\chi} \stackrel{?}{=} \pm 4P, \tag{54}$$

an identity which is analogous to (50) with χ replacing the trivial character.

4. The example with $D = -175$ and class number 4 appears to yield the relation

$$\mathrm{Imag}\left(15J_\tau^+/\lambda_1^+ - 5\widetilde{P}_{175} + 15(\widetilde{P}_{-7} + \widetilde{P}_{-35_1} + \widetilde{P}_{-35_2}) - 2\lambda_0^-\right) \stackrel{?}{=} 0. \tag{55}$$

Notice that the values of P_K and P^{χ} suggested by this relation continue to satisfy (50) and (54) respectively.

5. The calculations involving J_τ^- instead of J_τ^+ are frequently less interesting in the ranges that were tabulated, since conjecture 2.3 predicts that $\Phi^-(\tau)$ is trivial when $H^+ = H$, which occurs in all examples except $D = -35_2$, -63, and -91. It was checked numerically for a few values of D_K with $h^+ = h$ that $\Phi^-(\tau)$ is in fact trivial in $E(K)\otimes\mathbb{Q}$, while a closer study of the case $D_K = -91$ suggested the relation

$$3J_\tau^-/\lambda_1^- - 6\widetilde{P}' + 2\lambda_0^+ \stackrel{?}{=} 0, \tag{56}$$

where P' is the point

$$(\beta^2 - 2, \beta^3/2 + 2\beta^2 - \beta - 9/2)$$

(for β the negative real root of $x^4 + x^2 - 7$) and $\widetilde{P}'$ is its lift to $\mathbb{C}/\Lambda_0$. Note that P' is defined over the narrow Hilbert class field H^+ of K and is sent to its negative by the generator of $\mathrm{Gal}(H^+/K)$.

The field $F = \mathbb{Q}(\sqrt{37})$. Fix again the real embeddings ∞_0 and ∞_1 in such a way that v_0 sends $\sqrt{37}$ to the negative square root, and v_1 sends it to the positive square root. We now write ω for $(1+\sqrt{37})/2$, and the fundamental unit of F is

$$\varepsilon = 5 + 2\omega. \tag{57}$$

There is, up to isogeny, a unique elliptic curve with everywhere good reduction over F, with minimal Weierstrass equation given by

$$y^2 + y = x^3 + 2x^2 - (19 + 8\omega)x + (28 + 11\omega). \tag{58}$$

Its discriminant is equal to ε^6, and its Mordell-Weil group is finite (of order 5). The period lattices Λ_j $(j = 0, 1)$ attached to the choice of Néron differential $\omega_E = \frac{dx}{2y+1}$ are equal to $\langle\lambda_j^+, \lambda_j^-\rangle$, where

$$\begin{array}{ll} \lambda_0^+ = 14.326245329177\ldots & \lambda_1^+ = -\lambda_0^+(6 - \sqrt{37}) \\ \lambda_0^- = 11.114695464434\ldots i & \lambda_1^- = -\lambda_0^-(6 - \sqrt{37}) \end{array}$$

(In these equations $\sqrt{37}$ denotes the *positive* square root.) The fact that Λ_1 is homothetic to Λ_0 reflects the fact that E is isomorphic to its Galois conjugate over $\mathbb{Q}$.

The canonical lattice Λ_E^+ attached to E is given by

$$\Lambda_E^+ = \langle 16.986289742692\ldots, 13.178431139675\ldots i\rangle, \tag{59}$$

while Λ_E^- is given by

$$\Lambda_E^- = \langle 13.178431139675\ldots i, -10.224189621979\ldots\rangle. \tag{60}$$

Tables 37.1, 37.2 and 37.3 below list a few quadratic ATR extensions of the form $K = F(\beta)$ of F of small discriminant and the data in support of conjecture 2.3 that has been gathered for these extensions, following the same conventions as in the case $F = \mathbb{Q}(\sqrt{29})$.

D_K	β^2	h_K	h_K^+	ε_K
-3	$\omega - 3$	1	1	$(\beta^2 - \beta - 1)/2$
-7	$\omega + 1$	1	1	$(\beta^3 - 4\beta - 1)/2$
-11	$15\omega + 38$	1	1	$(\beta^2 - 15\beta + 7)/30$
-16	$2\omega + 5$	1	1	$(\beta^3 - 5\beta^2 + 5\beta + 1)/2$
-48	$\omega + 2$	1	2	$\beta^3 + 2\beta^2 + 2$
-64	$4\omega + 10$	1	1	$(5\beta^3 - 24\beta^2 - 2\beta - 1)/4$
-75	$5\omega - 15$	2	2	$\beta^2/10 - \beta/2 + 1/2$

Table 37.1. ATR extensions of $\mathbb{Q}(\sqrt{37})$ with small discriminant

D_K	x	y	P'
-3	$-2\beta^2/3 - 13/3$	$-61\beta^3/18 - 169\beta/9 - 1/2$	
-7	$\beta^2/7 - 3/7$	$-57\beta^3/98 - 44/49\beta - 1/2$	
-11	$-2\beta^2/165 - 104/165$	$-17\beta^3/1210 - 2\beta/605 - 1/2$	
-16	$\beta^2/8 - 5/8$	$-\beta^3/8 - 1/2$	
-48	$115\beta^2/588 - 80/147$	$-11225\beta^3/24696 - 1529/6174\beta - 1/2$	
-64	$-\beta^2/8 - 3/4$	$-\beta^3/8 - 1/2$	
-75	$-196\beta^2/675 - 20/9$	$-1559\beta^3/12150 - 25732/6075\beta - 1/2$	P_{-3}

Table 37.2. Generators of $E(K)$ modulo torsion

D_K	$\mathrm{imag}(J_\tau^+/\lambda_1^+)$	$\mathrm{imag}(\widetilde{P})$	a	b	c
-3	4.8353604732654	2.5352474364262	5	8	-4
-7	6.3896987259283	4.3424598946205	5	8	-6
-11	-0.4402203556346	0.2751377222716	5	8	0
-16	7.5409894304028	1.9344445278926	-5	8	2
-48	6.3896987259283	4.7919606979801	5	4	6
-64	23.0031166062165	6.7048953912383	5	16	-20
-75	-0.5228238836020	0.6535298545025	5	4	0
		2.5352474364262		0	

Table 37.3. Numerical evidence for conjecture 2.3.

Remarks: 1. With only one exception (the case $D_K = -64$) it appears that

$$P_K \stackrel{?}{=} \pm 2\ell_F \cdot P \quad \text{in } E(K) \otimes \mathbb{Q}, \qquad \text{with } \ell_F = 4/5. \tag{61}$$

This is consistent with the numerical observation that (with an accuracy of at least 20 decimal digits)

$$\int_0^{i\infty} \int_{i\varepsilon^{-1}}^{i\varepsilon} \omega_f^+ = -\ell_F^2 \cdot \lambda_0^+ \lambda_1^+, \tag{62}$$

just as in equation (51) for the case of $F = \mathbb{Q}(\sqrt{29})$.

2. Even though the field with $D_K = -75$ has $h_K = 2$, nevertheless the coefficient in the relation of the auxiliary point P_{-3} is 0. This contrasts with the three examples over $\mathbb{Q}(\sqrt{29})$ in which this coefficient is nonzero. It is reasonable to suppose that this is connected with the fact that the curve E has rank ≥ 2 (presumably equal to 2) over $\mathbb{Q}(\sqrt{5}, \sqrt{37})$, the totally real extension of degree 4 contained in the Hilbert class field of K. (The points

$$\left(\frac{-7+\sqrt{37}}{2}, \frac{\sqrt{185}-6\sqrt{5}-1}{2}\right) \text{ and } \left(\frac{29-5\sqrt{37}}{2}, \frac{12\sqrt{185}-73\sqrt{5}+1}{2}\right)$$

are independent elements of the Mordell-Weil group and appear to generate it modulo torsion.)

The field $F = \mathbb{Q}(\sqrt{41})$ Fix the real embeddings ∞_0 and ∞_1 as before. The symbol ω now represents $(1+\sqrt{41})/2$, and the fundamental unit of F is

$$\varepsilon = 27 + 10\omega. \tag{63}$$

Up to isogeny there is a unique elliptic curve over $\mathbb{Q}(\sqrt{41})$ with everywhere good reduction. It can be chosen to have minimal Weierstrass equation

$$y^2 + xy = x^3 - \varepsilon x. \tag{64}$$

Its discriminant is $\Delta = \varepsilon^4$ and its Mordell-Weil group $E(F)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

The period lattices Λ_j $(j = 0, 1)$ attached to the choice of Néron differential $\omega_E = \frac{dx}{2y+x}$ are equal to $\langle \lambda_j^+, \lambda_j^- \rangle$, where

$$\lambda_0^+ = 8.886172490171\ldots \qquad \lambda_1^+ = \frac{(-19+3\sqrt{41})}{2}\lambda_0^+$$

$$\lambda_0^- = 17.645928598111\ldots i \qquad \lambda_1^- = \frac{(-19+3\sqrt{41})}{4}\lambda_0^+$$

(In these equations $\sqrt{41}$ denotes the *positive* square root.) The fact that Λ_1 is homothetic to an index 2 sublattice Λ_0 reflects the fact that E is 2-isogenous to its Galois conjugate over $\mathbb{Q}$.

The canonical lattice Λ_E^+ attached to E is given by

$$\Lambda_E^+ = \langle 8.266459867807\ldots, 16.415319503174\ldots i\rangle, \tag{65}$$

while Λ_E^- is given by

$$\Lambda_E^- = \langle 8.207659751587\ldots i, -16.298555772387\ldots\rangle. \tag{66}$$

The three tables below summarise the numerical evidence that has been gathered in support of conjecture 2.3, for six ATR extensions of F of small relative discriminant, following the notational conventions that were used in the previous sections.

D_K	β^2	h_K	h_K^+	ε_K
-4	$27+10\omega$	1	1	$(\beta^3-\beta^2-57\beta+7)/10$
-8	$-181-67\omega$	1	1	$(17\beta^3+\beta^2+7298\beta+516)/134$
-20	$697+258\omega$	1	2	$(3\beta^3-\beta^2-4929\beta+439)/516$
-20	$-697-258\omega$	1	2	$(19\beta^3-\beta^2+31389\beta-1729)/86$
-23	$389+144\omega$	1	1	$(\beta^3-\beta^2-893/\beta+29)/144$
-32	$1+\omega$	2	2	$\beta^3/2-\beta^2-5\beta/2+5$

Table 41.1. ATR extensions of $\mathbb{Q}(\sqrt{41})$ with small discriminant

D_K	x	y	P'
-4	$-1/4$	$-\beta/2+1/8$	
-8	$(-3\beta^2-1481)/268$	$(-254\beta^3+3\beta^2-108954\beta+1481)/536$	
-20	$(\beta^2-9)/43$	$(-\beta^3-3\beta^2+181\beta+27)/258$	
-20	$(-\beta^2-1729)/258$	$(-67\beta^3+\beta^2-110683\beta+1729)/516$	
-23	See remark below	See remark below	
-32	$(29\beta^2+49)/4$	$(-359\beta^3-58\beta^2-611\beta-98)/16$	P_{-4}

Table 41.2. Generators of $E(K)$ modulo torsion

Remark: In the case $D_K = -23$, the point P has coordinates given by

$$\begin{aligned} x &= (-71027\beta^2 - 1271153)/9884736 \\ y &= (-1095348\beta^3 + 9304537\beta^2 + 16459332\beta + 166521043)/2589800832 \end{aligned}$$

The height of P was somewhat too large for it to be found by the (fairly rudimentary) point-searching algorithm that was used. Instead, P was discovered by computing the period J_τ^+ to several hundred digits of decimal accuracy and recognising the coordinates of the resulting complex point as algebraic numbers. This example vividly illustrates how conjecture 2.3 can (in favorable circumstances) be used to produce global points on E by analytic means.

D_K	imag(J_τ^+/λ_1^+)	imag$(\widetilde{P})$	a	b	c
-4	9.78222836348	15.1529745774	-8	4	1
-8	1.25106319555	-1.25106319556	1	1	0
20	1.50677322258	14.7412196711	-4	4	3
-20	-2.23232801736	15.466774659	4	4	-3
-23	2.78771530996	7.19919745949	-4	4	-1
-32	10.2755917186	3.37115554850	4	-4	5
		15.1529745774		4	

Table 41.3. Numerical evidence for conjecture 2.4.

Remark: Note that all of the examples of Table 41.3 appear to yield

$$P_K = \pm P \quad \text{in } E(K) \otimes \mathbb{Q} \tag{67}$$

to within a factor of 2, consistent with the fact that

$$\int_0^{i\infty} \int_{i\varepsilon^{-1}}^{i\varepsilon} \omega_f^+ = -\lambda_0^+ \lambda_1^+. \tag{68}$$

It is possible that the greater variation in the factor of 2 in this case reflects the fact that elliptic curves with full level-2 structure are more likely to have elements of order 2 in their Tate-Shafarevich group.

4 Algorithmic issues

Concretely, to compute the map Φ^+ it is necessary to evaluate semi-indefinite integrals entering in the definition of J_τ^+ (see [Dar2], ch. 8), which are of the form

$$\int^\tau \int_{c_1}^{c_2} \omega_f^+, \qquad \text{with } c_1, c_2 \in \mathbb{P}_1(F). \tag{69}$$

Adopting the terminology of Section 9.6 of [Dar2], we say that two cusps a/b and c/d are *adjacent* if $ad - bc$ is a unit in $\mathcal{O}_F$. This definition is an obvious replacement of the one given for $F = \mathbb{Q}$, where it is required that $ad - bc = \pm 1$. Our method relies on connecting any two cusps by a sequence of adjacent ones. It is of course sufficient to join an arbitrary cusp a/b to the cusp ∞, which amounts to expressing a/b as a continued fraction.

The three fields $F = \mathbb{Q}(\sqrt{29})$, $\mathbb{Q}(\sqrt{37})$ and $\mathbb{Q}(\sqrt{41})$ that were treated in our numerical experiments enjoy the crucial property of being *norm-Euclidean*. Continued fractions can therefore be obtained using the standard Euclidean algorithm for calculating GCD's described in [Op]. This paper shows that, given nonzero $a, b \in \mathcal{O}_F$, an element $c \in \mathcal{O}_F$ such that $|N(a - bc)| < |N(b)|$ may be found not far from a/b, and so it is a simple matter to find this element.

Since Γ acts transitively on pairs of adjacent cusps, one is then reduced to calculating expressions of the form

$$\begin{aligned} \int^{\tau}\int_0^{\infty}\omega_f^+ &= \int^{\tau}\int_0^{1}\omega_f^+ + \int^{\tau}\int_1^{\infty}\omega_f^+ \\ &= \int^{-1/\tau}\int_{\infty}^{-1}\omega_f^+ + \int^{\tau-1}\int_0^{\infty}\omega_f^+ = \int_{1-1/\tau}^{\tau-1}\int_0^{\infty}\omega_f^+. \end{aligned}$$

This integral can be evaluated by breaking it into a sum of two integrals with all but one limit in the (open) upper half-plane and translating the remaining limit by a matrix in Γ to the cusp ∞ which is in the region of convergence for the Fourier expansion (36). The resulting integrals can then be computed using equation (12), reducing the problem to one of adding suitable products of Fourier coefficients, exponentials, and other easily-computed quantities.

It would be interesting to understand the complexity of this algorithm for calculating J_τ as a function of τ. This raises subtle questions about the continued fraction representations of elements of real quadratic fields of class number 1. For example, the Euclidean algorithm used to find the GCD of two rational integers a, b requires $O(\log(\max(a, b)))$ steps, but how many steps are needed to find a sequence of adjacent cusps leading from ∞ to an arbitrary element of $\mathbb{Q}(\sqrt{29})$? The Euclidean algorithm presented in [Op] shows that such a sequence exists and gives an algorithm for producing it. According to [Co], any cusp can be even be connected to ∞ by a sequence of adjacent cusps of length at most eight (whether or not F is Euclidean for the norm). But if such a sequence yields double integrals with limits very close to the real axis, the shortness of the sequence will in all likelihood come at too high a cost.

Since so little is understood about the complexity of calculating J_τ as a function of τ, we focus on the simpler question of analysing the complexity of calculating the integral given in (12), where the size of the problem is measured by the desired number M of digits of decimal accuracy.

It is convenient to group the totally positive elements according to the ideals that they generate. Thus, let u be a generator of the group of totally positive units. We may choose u such that $u_0 > 1$. Also, given a totally positive element μ, we may find ν generating the same ideal such that $1 < \nu_1 < u_0$. With this done, the individual terms appearing in the right-hand sum in (12) are of the form

$$(e^{2\pi i\frac{n_0}{d_0}y_0u_0^a} - e^{2\pi i\frac{n_0}{d_0}x_0u_0^a})(e^{2\pi i\frac{n_1}{d_1}y_1u_1^a} - e^{2\pi i\frac{n_1}{d_1}x_1u_1^a}). \tag{70}$$

As a approaches ∞, the absolute value of the first factor tends to 0 exponentially fast, while the second factor is bounded. The situation as a approaches $-\infty$ is similar with the roles of the two factors interchanged. In fact only a small number values of a are needed in each sum for a specified degree of accuracy.

The Riemann hypothesis for elliptic curves over finite fields implies that $a(n) = O(|n|^{1/2+\varepsilon})$, so that

$$a(n)/|n| = O(|n|^{-1/2+\varepsilon}). \tag{71}$$

In addition, it is well-known that the number of ideals of norm n is $o(n^{\varepsilon})$. Hence the sum over generators of all ideals of norm n has order of magnitude

$$O(e^{-c|n|\min(\operatorname{im} x_i \operatorname{im} y_i)}).$$

Thus it is necessary to evaluate the sum in (12) up to the terms corresponding to elements n of norm $O(M/\min(\operatorname{im} x_i y_j)$ to obtain M digits of accuracy, which involves computing

$$O(M^2/\min(\operatorname{im} x_i y_j)) \tag{72}$$

partial sums attached to generators of an ideal. This complexity estimate accords well with experiment.

The Fourier coefficients $a(\mathfrak{p})$ for $\mathfrak{p}$ a prime ideal were computed by counting points on E over $\mathcal{O}_F/\mathfrak{p}$, using Shanks' "baby-step-giant-step" method, and the general coefficient $a(n)$ was then obtained using the recursion relations implied by (35). The time taken up by this part of the calculation is negligible both practically and theoretically. In practice the Fourier coefficients $a(p)$ for p a prime which is inert in K were precomputed, while built-in GP functions were used to compute the generators p_1, p_2 of split prime ideals and the corresponding coefficients $a(p_i)$. Gathering this data for the range $|p| \leq 20000^2$, which is more than enough for the numerical examples treated in the previous section, required less time than the computation of many of the individual examples. In fact, the time needed to evaluate an individual period $J_\tau^{\pm}$ to 12 places varied widely from about 2 minutes to about 12 hours, reflecting our lack of understanding of the complexity of this calculation as a function of τ.

Example. Here are the details of the computation for the fields

$$F = \mathbb{Q}(\sqrt{29}), \quad K = F(\beta) = F\left(\sqrt{-1+\omega}\right)$$

displayed on the first row of Table 29.1, where the relative discriminant of K/F is of norm -7. As indicated in Table 29.1, the field K has narrow class number 1, and its group of units is generated by

$$-1, \frac{5+\sqrt{29}}{2}, \text{ and } \varepsilon_K := \frac{\beta^2-\beta-1}{2}. \tag{73}$$

Since the norm of ε_K to F is not a square, it is necessary to work with the unit

$$\varepsilon_K^2 := (-\beta^3 - \beta^2 + \beta + 4)/2. \tag{74}$$

The ring of integers of K is generated as a $\mathbb{Z}$-module by

$$1, \beta, \frac{\beta^2+\beta+1}{2}, \text{ and } \frac{\beta^3+1}{2}. \tag{75}$$

Therefore the embedding $\widetilde{\Psi}$ of K into $M_2(F)$ which sends β to the matrix $\begin{pmatrix} 0 & -1+\omega \\ 1 & 0 \end{pmatrix}$ with fixed point $\widetilde{\tau} = \beta_0 \in \mathcal{H}_0$ is not optimal. An optimal embedding is obtained by conjugating $\widetilde{\Psi}$ by the matrix $\begin{pmatrix} 1 & \omega \\ 0 & 2 \end{pmatrix}$. The resulting embedding Ψ has associated fixed point

$$\tau := (\widetilde{\tau} + \omega_0)/2 = (\beta_0 + \omega_0)/2 \approx -1.09629120178 + 0.89338994895i. \tag{76}$$

Under the embedding Ψ the unit ε_K^2 gets sent to the matrix

$$\gamma_\tau := \Psi(\varepsilon_K^2) = \begin{pmatrix} -1 & -2\omega - 2 \\ 1+\omega & 5+\omega \end{pmatrix}. \tag{77}$$

The conjugate of $\frac{-1}{1+\omega}$ has an obvious continued fraction expansion:

$$\frac{1}{\omega - 2} = 0 + \frac{1}{\omega - 2}. \tag{78}$$

The desired quantity J_τ^+ is therefore

$$\begin{aligned} J_\tau^+ &= \int^\tau \int_\infty^{\frac{1}{\omega-2}} \omega_f^+ = \int^\tau \int_\infty^0 \omega_f^+ + \int^\tau \int_0^{\frac{1}{\omega-2}} \omega_f^+ \\ &= \int^\tau \int_\infty^0 \omega_f^+ + \int^{-1/\tau} \int_\infty^{-(\omega-2)} \omega_f^+ \\ &= \int^{-1/\tau} \int_\infty^0 \omega_f^+ + \int^{-1/\tau+\omega_0-2} \int_\infty^0 \omega_f^+ = \int_{-1/\tau+\omega_0-2}^{-1/\tau} \int_0^\infty \omega_f^+. \end{aligned}$$

For 12 places of accuracy, it is not necessary to evaluate any of the terms in the infinite sum (12) beyond those corresponding to elements n of norm ≤ 6000. A numerical evaluation yields

$$J_\tau^+ = 2.41766048277\cdots + 4.10658867578\ldots i. \tag{79}$$

The real part of this expression agrees with $2\lambda_0^+/9$ within the computed accuracy, so that the image of $9J_\tau^+$ in $\mathbb{C}/\Lambda_0$ appears to lie in the -1-eigenspace for complex conjugation.

A short search finds a point over $\mathbb{Q}(\omega)$ with x-coordinate $2+\omega$, and the built-in GP command `ellpointtoz` shows that this point is the image of

$$z \approx -3.079941506839i \text{ in } \mathbb{C}/\Lambda_0 \tag{80}$$

under the Weierstrass uniformisation. Numerically, it appears that

$$3J_\tau + 4z \stackrel{?}{=} 0. \tag{81}$$

This linear relation was checked to over 200 digits of decimal accuracy. Of course, we are unable to prove even the single identity (81), a situation not unlike that occurring in the numerical verifications of Stark's conjectures.

References

[BDG] M. Bertolini, H. Darmon, and P. Green. *Periods and points attached to quadratic algebras.* Proceedings of the MSRI workshop on Special Values of Rankin L-series, H. Darmon and S. Zhang, eds.

[Bi] B. Birch. *Heegner points: the beginnings.* Proceedings of an MSRI workshop on special values of Rankin L-series. H. Darmon and S. Zhang, eds. To appear.

[Bu] D. Bump. Automorphic forms and representations. Cambridge Studies in Advanced Mathematics, **55**. Cambridge University Press, Cambridge, 1997.

[Co] G. Cooke. *The weakening of the Euclidean property for integral domains and application to algebraic number theory I.* J. Reine Angew. Math. **282** (1976) 133-156.

[Cr] J. E. Cremona. *Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction.* Math. Proc. Cambridge Philos. Soc. **111** (1992), no. 2, 199–218.

[Dar1] H. Darmon. *Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications.* Annals of Math. (2) **154** (2001), no. 3, 589–639.

[Dar2] H. Darmon. *Rational points on modular elliptic curves.* NSF-CBMS notes. To appear.

[Das] S. Dasgupta. PhD Thesis, Berkeley, in progress.

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

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

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

[Op] A. Oppenheim, *Quadratic fields with and without Euclid's algorithm.* Math. Ann. **66** (1909) 109–112.

[Pi] R. Pinch, Private communication.

[Se] Serre, Jean-Pierre. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15** (1972), no. 4, 259–331.

[Sh1] Shimura, Goro. *Class fields over real quadratic fields and Hecke operators*. Seminar on Modern Methods in Number Theory (Inst. Statist. Math., Tokyo, 1971), Paper No. 6, 17 pp. Inst. Statist. Math., Tokyo, 1971.

[Sh2] Shimura, Goro. *Class fields over real quadratic fields and Hecke operators*. Ann. of Math. (2) **95** (1972), 130–190.

[Sh3] Shimura, Goro. *Class fields over real quadratic fields in the theory of modular functions*. Several complex variables, II (Proc. Internat. Conf., Univ. Maryland, College Park, Md., 1970), pp. 169–188. Lecture Notes in Math., Vol. 185, Springer, Berlin, 1971.

[Sh4] G. Shimura. Introduction to the arithmetic theory of automorphic functions. Princeton University Press, 1971.

[Zh1] S. Zhang. *Heights of Heegner points on Shimura curves*. Ann. of Math. (2) **153** (2001), no. 1, 27–147.

[Zh2] S. Zhang. *Gross-Zagier formula for* GL_2. Asian J. Math. **5** (2001), no. 2, 183–290.

[Zh3] S. Zhang. *Gross-Zagier formula for* GL_2. Proceedings of an MSRI workshop on special values of Rankin L-series. H. Darmon and S. Zhang, eds. To appear.