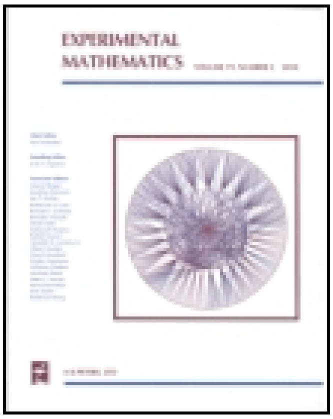

Experimental Mathematics

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uexm20

Elliptic Curves and Class Fields of Real Quadratic Fields: Algorithms and Evidence

Henri Darmon [a] & Peter Green [b]

[a] Department of Mathematics , McGill University , Montreal , Quebec , Canada , H3A 2K6 E-mail:

[b] Department of Mathematics , Harvard University , Cambridge , MA , 02138 E-mail:

Published online: 03 Apr 2012.

To cite this article: Henri Darmon & Peter Green (2002) Elliptic Curves and Class Fields of Real Quadratic Fields: Algorithms and Evidence, Experimental Mathematics, 11:1, 37-55, DOI: 10.1080/10586458.2002.10504467

To link to this article: http://dx.doi.org/10.1080/10586458.2002.10504467

Elliptic Curves and Class Fields of Real Quadratic Fields: Algorithms and Evidence

Henri Darmon and Peter Green

CONTENTS

The article [Darmon 02] proposes a conjectural p-adic analytic construction of points on (modular) elliptic curves, points which are defined over ring class fields of real quadratic fields. These points are related to classical Heegner points in the same way as Stark units to circular or elliptic units.[1] For this reason they are called "Stark-Heegner points," following a terminology introduced in [Darmon 98].

If K is a real quadratic field, the Stark-Heegner points attached to K are conjectured to satisfy an analogue of the Shimura reciprocity law, so that they can in principle be used to find explicit generators for the ring class fields of K. It is also expected that their heights can be expressed in terms of derivatives of the Rankin L-series attached to E and K, in analogy with the Gross-Zagier formula.

The main goal of this paper is to describe algorithms for calculating Stark-Heegner points and supply numerical evidence for the Shimura reciprocity and Gross-Zagier conjectures, focussing primarily on elliptic curves of prime conductor.

1. HEEGNER POINT ALGORITHMS

1.1 Heegner Points Attached to Imaginary Quadratic Fields

The theory of complex multiplication. It is instructive to briefly recall the theory behind the classical Heegner point construction. Fix a positive integer N, and let $X_0(N)$ be the modular curve classifying pairs (A, A') of generalized elliptic curves together with a cyclic isogeny $A \rightarrow A'$ of degree N. Its set of complex points is a Riemann surface admitting the complex uniformisation:

$$\eta : \mathcal{H}^*/\Gamma_0(N) \xrightarrow{\sim} X_0(N)(\mathbb{C})$$

where $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}_1(\mathbb{Q})$ is the extended upper half plane and $\Gamma_0(N)$ is the set of elements of $\mathrm{SL}_2(\mathbb{Z})$ whose reductions (mod N) are upper triangular. The map η sends

2000 AMS Subject Classification: Primary 11G40; Secondary 11F67

Keywords: Elliptic curves, modular forms, Heegner points, periods, real quadratic fields

[1] See for example the discussion in [Bertolini and Darmon 2001] relating these points to derivatives of p-adic L-functions.

$\tau \in \mathcal{H}$ to the point of $X_0(N)(\mathbb{C})$ associated to the pair $(\mathbb{C}/\langle\tau,1\rangle, \mathbb{C}/\langle\tau,1/N\rangle)$ of elliptic curves over $\mathbb{C}$ related by the obvious cyclic N-isogeny.

Let $\mathcal{O}$ be an order in a quadratic imaginary subfield K of $\mathbb{C}$. Such an order is completely determined by its discriminant D. The Heegner points attached to $\mathcal{O}$ correspond to the pairs (A, A') of N-isogenous elliptic curves satisfying

$$\mathrm{End}(A) \simeq \mathrm{End}(A') \simeq \mathcal{O}.$$

Assume for simplicity that D is prime to N. Then such a pair (A, A') is of the form $(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda')$ where (up to homothety) Λ and Λ' are projective $\mathcal{O}$-submodules of K satisfying $\Lambda = \mathfrak{n}\Lambda'$, for some factorization

$$(N) = \mathfrak{n}\bar{\mathfrak{n}}$$

of N as a product of cyclic $\mathcal{O}$-ideals. The set of Heegner points associated to $\mathcal{O}$ forms a $\mathrm{Pic}(\mathcal{O})$-affine space via

$$\mathfrak{a} * (A, A') = (\mathrm{Hom}(\mathfrak{a}, A), \mathrm{Hom}(\mathfrak{a}, A')),$$
$$\mathfrak{a} \in \mathrm{Pic}(\mathcal{O}), \quad (A, A') \in X_0(N).$$

On the level of complex tori, this action is described by the rule

$$\mathfrak{a} * (\mathbb{C}/\Lambda, \mathbb{C}/\mathfrak{n}^{-1}\Lambda) = (\mathbb{C}/\mathfrak{a}^{-1}\Lambda, \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{n}^{-1}\Lambda).$$

The natural action of $G_K := \mathrm{Gal}(\overline{K}/K)$ preserves the set of Heegner points attached to $\mathcal{O}$, and commutes with the action of $\mathrm{Pic}(\mathcal{O})$. Hence the action of G_K on the collection of Heegner points attached to $\mathcal{O}$ is determined by a homomorphism $\delta : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Pic}(\mathcal{O})$ satisfying

$$\delta(\sigma) * (A, A') = (A, A')^\sigma,$$

for all Heegner points (A, A') with $\mathrm{End}(A) = \mathcal{O}$. In particular, δ factors through the Galois group of an abelian extension $\tilde{H}$ of K, and the Heegner points attached to $\mathcal{O}$ are defined over $\tilde{H}$.

Let $\mathfrak{p}$ be a prime of K which is unramified in $\tilde{H}$ and for which A with $\mathrm{End}(A) \simeq \mathcal{O}$ has good reduction. Let $\mathfrak{P}$ be a prime of $\tilde{H}$ above $\mathfrak{p}$. A direct calculation shows that the elliptic curve obtained by reducing $A \pmod{\mathfrak{P}}$ and raising its coefficients to the $(\#\mathcal{O}_K/\mathfrak{p})$-power is isomorphic to $\mathfrak{p} * A$ reduced $\pmod{\mathfrak{P}}$. It follows that

$$\delta(\mathrm{Frob}_\mathfrak{p}) = [\mathfrak{p}] \in \mathrm{Pic}(\mathcal{O}). \tag{1–1}$$

Thus δ is the inverse of the Artin reciprocity map

$$\mathrm{rec} : \mathrm{Pic}(\mathcal{O}) \xrightarrow{\sim} \mathrm{Gal}(H/K)$$

of class field theory. The extension $H = \tilde{H}$ is the so-called ring class field attached to $\mathcal{O}$. The compatibility between rec and δ is known as the *Shimura reciprocity law*; it is the central result of the theory of complex multiplication.

Finding the Heegner points. The following recipe for calculating Heegner points on $\mathcal{H}/\Gamma_0(N)$ attached to the order $\mathcal{O}$ of discriminant D prime to N is decribed in [Zagier 85]. Choose an integer $s \in \mathbb{Z}$ satisfying

$$s^2 \equiv D \pmod{4N},$$

giving rise to the cyclic $\mathcal{O}$-ideal $\mathfrak{n} := (N, \frac{s-\sqrt{D_0}}{2})$ of norm N. The Heegner points (A, A') attached to $\mathcal{O}$ for which

$$\ker(A \to A') = A[\mathfrak{n}]$$

are in bijection with the $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of primitive integral binary quadratic forms

$$Ax^2 + Bxy + Cy^2 \text{ satisfying}$$
$$B^2 - 4AC = D, \quad N|A, \quad B \equiv s \pmod{2N}.$$

Under this bijection, the point on $\mathcal{H}/\Gamma_0(N)$ identified by η with the Heegner point corresponding to such a quadratic form is the class of τ where $\tau \in \mathcal{H}$ is the unique root of the dehomogenized form $Ax^2 + Bx + C$. Thus a list of representatives $\tau_1, \ldots, \tau_h \in \mathcal{H}$ (where h is the class number of $\mathcal{O}$) of Heegner points can be computed efficiently by using Gauss' theory of reduced primitive integral binary quadratic forms (see for example the explanation at the end of section 5.2 of [Cohen 94]).

Heegner points on elliptic curves. Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N. By the modularity theorem ([Wiles 95], [Taylor and Wiles 95], [Breuil et al. 2001]), E is equipped with a nonconstant morphism of curves over $\mathbb{Q}$, commonly referred to as the *Weil parametrisation* attached to E:

$$\phi : X_0(N) \to E$$

mapping the cusp ∞ to the identity element of E. It has proved eminently fruitful to consider the images under the Weil parametrisation of Heegner points of $X_0(N)$ (cf. Kolyvagin's work on Euler systems).

While it is difficult to write down explicit algebraic equations for $X_0(N)$ (not to mention ϕ), complex uniformisation of $E(\mathbb{C})$ and of $X_0(N)(\mathbb{C})$ provides a method for calculating the Weil parametrisation in practice. More precisely, the Riemann surface $E(\mathbb{C})$ is isomorphic to $\mathbb{C}/\Lambda$, where Λ is the lattice generated by the periods of a Néron differential ω on E (which is well-defined up to sign). Generators for Λ can be computed by Gauss's arithmetic-geometric mean formula for complete elliptic integrals, a quadratically convergent algorithm which works extremely well in practice. The curve E is then given up to isomorphism (over $\mathbb{C}$) by the equation

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

and the complex analytic isomorphism

$$\eta_E : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$$

is decribed by the formula

$$\eta_E(z) = (\wp_\Lambda(z), \wp'_\Lambda(z)),$$

where $\wp_\Lambda$ is the Weierstrass $\wp$-function attached to Λ. Explicit formulae for Λ, $g_2(\Lambda)$, $g_3(\Lambda)$ and $\wp_\Lambda$ can be found in [Silverman 86] for example.

Let f be the normalised cusp form of weight two attached to E, with Fourier expansion given by

$$f(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n\tau}, \quad a_1 = 1.$$

To calculate the coefficients a_n, it is enough to compute a_p for p prime, in light of the identity

$$\prod_{p|N}(1 - a_p p^{-s})^{-1} \prod_{p\not| N}(1 - a_p p^{-s} + p^{1-2s})^{-1} = \sum_n a_n n^{-s}.$$

This question in turn is reduced to counting the number of points of E over the finite fields with p elements, since $a_p = 0$ (resp. $1, -1$) if E has additive (resp. split multiplicative, non-split multiplicative) reduction at p, and

$$a_p = p + 1 - \#E(\mathbb{F}_p)$$

if E has good reduction at p. The pull-back $\phi^*(\omega)$ of ω by ϕ is a non-zero rational multiple of the differential

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

Assume for simplicity that $\phi^*(\omega) = \omega_f$. (After replacing E by a curve which is isogenous to it over $\mathbb{Q}$ – the so-called *strong Weil curve* in its isogeny class – it is conjectured that ϕ can be chosen to satisfy this condition. When E is a semistable strong Weil curve, it is in fact known that $\phi^*(\omega) = \pm\omega_f$ or $\pm 2\omega_f$. See the discussion in [Edixhoven 91].) Given $\tau \in \mathcal{H}$, and setting

$$J_\tau := \int_{i\infty}^{\tau} \omega_f,$$

a direct calculation shows that the following diagram commutes:

$$\begin{tikzcd}
\mathcal{H}^*/\Gamma_0(N) \arrow[r, "\eta"] \arrow[d, "\tau \mapsto J_\tau"'] & X_0(N)(\mathbb{C}) \arrow[d, "\phi"'] \\
\mathbb{C}/\Lambda \arrow[r, "\eta_E"] & E(\mathbb{C}).
\end{tikzcd}$$

More precisely, for all $\tau \in \mathcal{H}$, the point $P_\tau = (x, y) \in E(\mathbb{C})$ corresponding to it under the Weil uniformisation is given by the formula

$$P_\tau = (\wp_\Lambda(J_\tau), \wp'_\Lambda(J_\tau)).$$

It is of some interest to consider the complexity of calculating (x, y) as a function of τ.

Proposition 1.1. *For $\tau \in \mathcal{H}$, the calculation of the associated point $(x, y) \in E(\mathbb{C})$ to d digits of decimal accuracy can be performed in $O(d^2 \log d/\mathrm{Im}(\tau)^2)$ elementary operations as $d \to \infty$ and $\mathrm{Im}(\tau) \to 0$.*

Proof: The naive estimate

$$\left|\sum_{n=M+1}^{\infty} \frac{a_n}{n} q^n\right| \le \sum_{n=M+1}^{\infty} \exp(-2\pi n \mathrm{Im}(\tau))$$

implies that the quantity J_τ can be evaluated with an error of at most 10^{-d} using not more than

$$M = \frac{\log 10^{-d}}{-2\pi \mathrm{Im}(\tau)} = O\left(\frac{d}{\mathrm{Im}\,\tau}\right)$$

Fourier coefficients attached to E. Using the algorithm of Shanks (see Algorithm 7.4.12 in Cohen's book [Cohen 94]), it is possible to compute M coefficients in time $O(M^2)$. The evaluation of the sum

$$J_\tau = \sum_{n=1}^{M} \frac{a_n}{n} q^n$$

can then be performed (using Horner's rule) with $O(M)$ multiplications. Each multiplication can be carried out in $O(d \log d)$ time using fast Fourier transform techniques. Since the subsequent calculation of $\wp(J_\tau)$ and $\wp'(J_\tau)$ is dominated by the time necessary to obtain J_τ (see Algorithm 7.4.5 of [Cohen 94]), the result follows. □

1.2 Stark-Heegner Points Attached to Real Quadratic Fields

Theory. The previous section motivates a conjectural p-adic analytic construction of so-called *Stark-Heegner points*, which are defined over ring class fields of real quadratic fields. The description of the method is simplified by the assumption that the conductor $N = p$ is a prime, an assumption that will be made from now on.

The elliptic curve E of conductor p has multiplicative reduction at p. Of key importance for the construction is Tate's p-adic uniformization of E

$$\phi_{\mathrm{Tate}} : \mathbb{C}_p^\times/q^{\mathbb{Z}} \xrightarrow{\sim} E(\mathbb{C}_p),$$

where $q \in p\mathbb{Z}_p$ is the Tate period attached to E.

Following the notations that were used in [Darmon 02], set $w = 1$ if E has split multiplicative reduction at p, and set $w = -1$ if E has non-split multiplicative reduction at p. Some important features of the behaviour of the Stark-Heegner points on E are governed by this sign. It is known that w is equal to

1. the negative of the eigenvalue of the Atkin-Lehner involution W_p at p acting on f;
2. the sign in the functional equation for $L(E/\mathbb{Q}, s)$, so that, conjecturally, $E(\mathbb{Q})$ has even (resp. odd) rank if $w = 1$ (resp. $w = -1$);
3. the eigenvalue of the Hecke operator U_p acting on f.

Let K be a real quadratic field in which p is inert, and let H be a ring class field of K of conductor prime to p. Considerations combining the Birch and Swinnerton-Dyer conjecture with a determination of the signs in the functional equations of $L(E/K, s)$ and its twists by characters of $\mathrm{Gal}(H/K)$ lead to the prediction that the Mordell-Weil group $E(H)$ is equipped with a large collection of points of infinite order. (Cf. the discussion in the introduction to [Darmon 02].)

Let $\mathcal{H}_p := \mathbb{P}_1(\mathbb{C}_p) - \mathbb{P}_1(\mathbb{Q}_p)$ denote the p-adic upper half-plane. Fix from now on an embedding of K into $\mathbb{C}_p$. Since p is inert in K, note that $K \cap \mathcal{H}_p$ is non-empty. The Stark-Heegner points are indexed by elements $\tau \in K \cap \mathcal{H}_p$, and are defined by the rule

$$P_\tau := \phi_{\mathrm{Tate}}(J_\tau),$$

where $J_\tau \in \mathbb{C}_p^\times/q^{\mathbb{Z}}$ is a period attached to τ and f whose definition will now be recalled briefly.

The role played by the line integral of the differential form ω_f in defining J_τ in the setting of Section 1.1 (when τ is quadratic imaginary) is now played by the double integral on $\mathcal{H}_p \times \mathcal{H}$ introduced in [Darmon 02]. More precisely (with only a minor modification to the notation) equations (71) and (72) of [Darmon 02] attach to a normalized newform for $\Gamma_0(p)$ having rational Fourier coefficents a period function

$$\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_x^y \omega \in \mathbb{C}_p^\times \otimes_{\mathbb{Z}} \tilde{\Lambda},$$
$$\text{with } \tau_1, \tau_2 \in \mathcal{H}_p, \quad x, y \in \mathbb{P}_1(\mathbb{Q}) \subset \mathcal{H}^*. \tag{1–2}$$

Here $\tilde{\Lambda}$ is the $\mathbb{Z}$-module of rank two

$$\left\{\int_\sigma f(z)dz \ : \ \sigma \in H_1(X_0(p),\ \text{cusps}; \mathbb{Z})\right\}.$$

Note that this lattice contains the period lattice Λ attached to E. The period of (1–2) is expressed as a limit of Riemann sums

$$\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_x^y \omega = \lim_{||\mathcal{U}||\to 0} \sum_{U\in\mathcal{U}} \left[\left(\frac{t_U-\tau_2}{t_U-\tau_1}\right) \otimes \left(\epsilon_U \int_{\alpha_U x}^{\alpha_U y} f(z)dz\right)\right] \tag{1–3}$$

where the limit is taken over uniformly finer disjoint covers of $\mathbb{P}_1(\mathbb{Q}_p)$ by sets of the form $U = \alpha_U^{-1}\mathbb{Z}_p$, with $\alpha_U \in \mathrm{GL}_2^+(\mathbb{Z}[1/p])$. In this limit, t_U is an arbitrarily chosen point of U, and $\epsilon_U := w^{\mathrm{ord}_p(\det \alpha)}$.

The form of the definition, familiar from the theory of p-adic L-functions, is based on the observation that the assignment

$$U \mapsto \epsilon_U \int_{\alpha_U 0}^{\alpha_U \infty} f(z)dz \tag{1–4}$$

satisfies a distribution relation. Since it takes values in the finitely generated $\mathbb{Z}$-module $\tilde{\Lambda}$, its values are p-adically bounded and hence this distribution gives rise to a p-adic measure against which locally analytic $\mathbb{C}_p$-valued functions on $\mathbb{P}_1(\mathbb{Q}_p)$ can be integrated.

As stated in Lemma 1.11 of [Darmon 02], the double integral of (1–2) is additive in the first and second set of variables of integration, i.e.,

$$\times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_x^y \omega + \times\!\!\!\!\!\!\int_{\tau_2}^{\tau_3}\int_x^y \omega = \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_3}\int_x^y \omega, \tag{1–5}$$
$$\text{for all } \tau_j \in \mathcal{H}_p, \quad x, y \in \mathbb{P}_1(\mathbb{Q}),$$

$$\times\!\!\!\!\!\!\int_{\tau_1}^{\tau 2}\int_x^y \omega + \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_y^z \omega = \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_x^z \omega, \tag{1–6}$$
$$\text{for all } \tau_j \in \mathcal{H}_p, \quad x, y, z \in \mathbb{P}_1(\mathbb{Q}).$$

(Note that these relations are written multiplicatively in Lemma 1.11 of [Darmon 02], because the double integral defined there takes its values in $\mathbb{C}_p^\times$. The notational discrepancy is in keeping with the common usage that the composition law on the abelian group $\mathbb{C}_p^\times \otimes \tilde{\Lambda}$ should be written additively in relations (1–5) and (1–6) above.)
By the third formula in Lemma 1.11 of [Darmon 02], the double integral attached to E also satisfies the key invariance property under $\Gamma := \mathrm{SL}_2(\mathbb{Z}[1/p])$:

$$\times\!\!\!\!\!\!\int_{\gamma\tau_1}^{\gamma\tau_2}\int_{\gamma x}^{\gamma y} \omega = \times\!\!\!\!\!\!\int_{\tau_1}^{\tau_2}\int_x^y \omega \quad \text{for all } \gamma \in \Gamma.$$

Given any distinct elements $a, b \in \mathbb{P}_1(\mathbb{Q})$, the group

$$\Gamma_{a,b} = \{\gamma \in \Gamma \mid \quad \gamma a = a, \quad \gamma b = b\}$$

is an abelian group of rank one. Assume for simplicity that E is alone in its $\mathbb{Q}$-isogeny class.

Lemma 1.2. *The double integral*

$$\times\!\!\!\!\!\!\int_z^{\gamma z}\int_a^b \omega$$

belongs to $q^{\mathbb{Z}} \otimes \tilde{\Lambda}$, *for all* $z \in \mathcal{H}_p$ *and for all* $\gamma \in \Gamma_{a,b}$.

Sketch of Proof. Since E has prime conductor, the assumption that E is alone in its isogeny class implies that $\operatorname{ord}_p(q) = 1$. Hence by Theorem 1 of [Darmon 02] (see also Remark 1 following the statement of Corollary 3 of [Darmon 02])

$$\times\!\!\!\!\!\!\int_z^{\gamma z}\int_a^b \omega \text{ belongs to } q^{\mathbb{Z}} \otimes \tilde{\Lambda}, \quad (\mathrm{mod}\ (\mathbb{Q}_p)^\times_{\mathrm{tors}} \otimes \tilde{\Lambda}). \quad (1\text{–}7)$$

The proof of Theorem 1 of [Darmon 02] is based on a deep conjecture of Mazur, Tate and Teitelbaum [Mazur et al. 86] proved by Greenberg and Stevens [Greenberg and Stevens 93]. A multiplicative refinement [Mazur and Tate 87] of these conjectures due to Mazur and Tate, which, for prime conductor, is proved by deShalit [de Shalit 95], allows the $(\mathbb{Q}_p)^\times_{\mathrm{tors}}$-ambiguity in formula (1–7) to be removed. Lemma 1.2 follows.

Formal considerations explained in [Darmon 02], involving the cohomology of M-symbols, imply the existence of "indefinite integrals"

$$\times\!\!\!\!\!\!\int^{\tau}\int_x^y \omega \in (\mathbb{C}_p^\times/q^{\mathbb{Z}}) \otimes \tilde{\Lambda}$$

satisfying the properties

$$\times\!\!\!\!\!\!\int^{\tau}\int_{\alpha^{-1}x}^{\alpha^{-1}y} \omega - \times\!\!\!\!\!\!\int^{\tau}\int_x^y \omega = \times\!\!\!\!\!\!\int_{\tau}^{\alpha\tau}\int_x^y \omega \qquad (\mathrm{mod}\ q^{\mathbb{Z}}),$$

$$\times\!\!\!\!\!\!\int^{\tau}\int_x^y \omega + \times\!\!\!\!\!\!\int^{\tau}\int_y^z \omega = \times\!\!\!\!\!\!\int^{\tau}\int_x^z \omega,$$

$$\text{for all } \tau \in \mathcal{H}_p, \quad \alpha \in \Gamma, \quad x, y, z \in \mathbb{P}_1(\mathbb{Q}).$$

The first relation completely determines the indefinite integral, in view of the fact that the space of Γ-invariant $(\mathbb{C}_p^\times/q^{\mathbb{Z}})\otimes\tilde{\Lambda}$-valued functions on $\mathbb{P}_1(\mathbb{Q})\times\mathbb{P}_1(\mathbb{Q})$ satisfying the second relation is trivial. (In fact, this is already true for the $\mathrm{SL}_2(\mathbb{Z})$-invariant functions.)

To define the period $\tilde{J}_\tau \in \mathbb{C}_p^\times/q^{\mathbb{Z}}\otimes\tilde{\Lambda}$ associated to $\tau \in K \cap \mathcal{H}_p$, we use the algebra embedding $\Psi : K \to M_2(\mathbb{Q})$ such that for $\lambda \in K$,

$$\Psi(\lambda)\begin{pmatrix} \tau \\ 1 \end{pmatrix} = \lambda \begin{pmatrix} \tau \\ 1 \end{pmatrix}.$$

Ψ is defined by

$$\Psi(\tau) = \begin{pmatrix} \mathrm{Tr}\,\tau & -\mathrm{Nm}\,\tau \\ 1 & 0 \end{pmatrix}.$$

Let $\mathcal{O} \subset K$ be the $\mathbb{Z}[1/p]$-order of K defined by $\mathcal{O} = \Psi^{-1}(M_2(\mathbb{Z}[1/p]))$. Let u be the generator of $\mathcal{O}_1^\times$, the group of units of $\mathcal{O}$ of norm one, which is greater than 1 with respect to the chosen real embedding of K. Then $\gamma_\tau = \Psi(u)$ is a generator for the stabilizer of τ in Γ. Define

$$\tilde{J}_\tau = \times\!\!\!\!\!\!\int^{\tau}\int_x^{\gamma_\tau x} \omega.$$

From the properties of the indefinite integral sketched above, it can be checked that $\tilde{J}_\tau$ is independent of the choice of $x \in \mathbb{P}_1(\mathbb{Q})$. Let $\beta : \tilde{\Lambda} \to \mathbb{Z}$ be a $\mathbb{Z}$-module homomorphism. The following assumption is made on β:

Assumption 1.3. *The image* $\beta(\Lambda)$ *is contained in* $2c_p\mathbb{Z}$, *where* c_p *is the Tamagawa factor attached to* E *at* p.

The homomorphism β induces a homomorphism (denoted by the same letter by abuse of notation)

$$\beta : \mathbb{C}_p^\times/q^{\mathbb{Z}} \otimes \tilde{\Lambda} \to \mathbb{C}_p^\times/q^{\mathbb{Z}}.$$

Define

$$J_\tau = \beta(\tilde{J}_\tau).$$

Definition 1.4. The point $P_\tau := \phi_{\mathrm{Tate}}(J_\tau) \in E(\mathbb{C}_p)$ is called the *Stark-Heegner point* attached to $\tau \in K \cap \mathcal{H}_p$ (and to the choice of functional β).

The *conductor* of τ is the conductor of the $\mathbb{Z}[1/p]$-order $\mathcal{O}$ attached to τ.

A point $\tau \in K \cap \mathcal{H}$ is said to be *even* if $\operatorname{ord}_p(\tau - \bar{\tau})$ is even, and odd otherwise. The action of Γ on $\mathcal{H}_p$ preserves both the order associated to τ, and its parity. There are exactly h distinct Γ-orbits of even τ with associated order $\mathcal{O}$, where h is the cardinality of $\mathrm{Pic}^+(\mathcal{O})$, the group of narrow ideal classes attached to $\mathcal{O}$. In fact, the group $\mathrm{Pic}^+(\mathcal{O})$ acts simply transitively on the set of these Γ-orbits. (Cf. [Darmon 02], sec. 5.2). Denote by $\mathfrak{a} * \tau$ the image of $\mathfrak{a}$ acting on τ by this action. Let H^+ denote the so-called *narrow ring class field* attached to the order $\mathcal{O}$, and let

$$\mathrm{rec} : \mathrm{Pic}^+(\mathcal{O}) \xrightarrow{\sim} \mathrm{Gal}(H^+/K)$$

be the reciprocity map of global class field theory. The following is a restatement of Conjecture 5.6 and 5.9 of [Darmon 02] (in light of the fact that the integer denoted t in conjecture 5.6 is equal to 1 when the conductor of E is prime).

Conjecture 1.5. *If* $\tau \in K \cap \mathcal{H}_p$ *is a real quadratic point, then the Stark-Heegner point* $P_\tau \in E(\mathbb{C}_p)$ *is a global point* *defined over H^+. Furthermore,*

$$P_{\mathfrak{a}*\tau} = \mathrm{rec}([\mathfrak{a}])^{-1} P_\tau.$$

A slightly weaker form of this conjecture is

Conjecture 1.6. *If $\tau_1, \dots, \tau_h$ is a complete set of representatives for the Γ-orbits of even τ attached to the order $\mathcal{O}$ of discriminant D, then the points P_{τ_j} are defined over H^+ and are permuted by $Gal(H^+/K)$, so that collectively these points are defined over K.*

Computations. We now describe an algorithm for computing J_τ. Set

$$\mathcal{R} = \left\{ a + b\sqrt{s} \,:\, a \in \mathbb{Z}_p, b \in \mathbb{Z}_p^\times \right\},$$

where s is a nonsquare element of $\mathbb{Z}_p - p\mathbb{Z}_p$. If K is a real quadratic field in which p is inert, any point $\tau \in K \cap \mathcal{H}_p$ is equivalent under Γ to a point in $\mathcal{R}$. Hence, it suffices to describe an algorithm for computing

$$\beta\left(\times\!\!\!\!\!\!\int^\tau \int_x^y \omega \right) \qquad \text{for } \tau \in \mathcal{R}, \quad x, y \in \mathbb{P}_1(\mathbb{Q}). \tag{1–8}$$

Let $\frac{a_0}{b_0}, \frac{a_1}{b_1}, \dots, \frac{a_n}{b_n}$ be a *Farey sequence* from x to y, i.e., a sequence of fractions in lowest terms satisfying

$$\frac{a_0}{b_0} = x, \quad \frac{a_n}{b_n} = y, \quad a_{i-1}b_i - b_{i-1}a_i = \pm 1 \ \text{ for } i = 1, \dots, n.$$

Let $\sigma_1, \dots, \sigma_n \in SL_2(\mathbb{Z})$ be elements satisfying

$$\sigma_j 0 = \frac{a_{j-1}}{b_{j-1}}, \quad \sigma_j \infty = \frac{a_j}{b_j} \quad \text{for } j = 1, \dots, n.$$

By the additivity and $\mathrm{SL}_2(\mathbb{Z})$-invariance properties of the indefinite integral, the period of (1–8) is equal to

$$\prod_{j=1}^n \beta\left(\times\!\!\!\!\!\!\int^{\sigma_j^{-1}\tau} \int_0^\infty \omega \right).$$

Since $\mathcal{R}$ is preserved by the action of $\mathrm{SL}_2(\mathbb{Z})$ it thus suffices to compute periods of the form

$$\beta\left(\times\!\!\!\!\!\!\int^\tau \int_0^\infty \omega \right), \qquad \text{with } \tau \in \mathcal{R}.$$

To carry out this last calculation, note that

$$\begin{aligned} \times\!\!\!\!\!\!\int^\tau \int_0^\infty \omega &= \times\!\!\!\!\!\!\int^\tau \int_1^\infty \omega - \times\!\!\!\!\!\!\int^\tau \int_1^0 \omega = \times\!\!\!\!\!\!\int^\tau \int_1^\infty \omega - \times\!\!\!\!\!\!\int^{\frac{2\tau-1}{\tau}} \int_1^\infty \omega \\ &= \times\!\!\!\!\!\!\int_{\frac{2\tau-1}{\tau}}^\tau \int_1^\infty \omega = \times\!\!\!\!\!\!\int_{\frac{1}{1-\tau}}^{\frac{\tau}{1-\tau}} \int_0^\infty \omega \\ &= \times\!\!\!\!\!\!\int_{\frac{\tau}{1-\tau}}^{\frac{1}{1-\tau}-1} \int_0^\infty \omega (\mathrm{mod}\ q^{\mathbb{Z}}). \end{aligned}$$

Hence, it suffices to compute

$$\beta\left(\times\!\!\!\!\!\!\int_\tau^{\tau-1} \int_0^\infty \omega \right) = \lim_{||\mathcal{U}|| \to 0} \prod_{U \in \mathcal{U}} \left(1 + \frac{1}{t_U - \tau} \right)^{\beta\left(\epsilon_U \int_{\alpha_U 0}^{\alpha_U \infty} f(z)dz \right)}$$

where the notation is as before. Observe now that when $\tau \in \mathcal{R}$ the function

$$1 + \frac{1}{t - \tau}$$

is constant (mod p^N) on the sets

$$\begin{pmatrix} p^{-N} & -jp^{-N} \\ 0 & 1 \end{pmatrix}^{-1} \mathbb{Z}_p = j + p^N \mathbb{Z}_p, \qquad j = 0, \dots, p^N - 1$$

$$\begin{pmatrix} jp^{1-N} & p^{-N} \\ -1 & 0 \end{pmatrix}^{-1} \mathbb{Z}_p = (-jp + p^N \mathbb{Z}_p)^{-1}, \qquad j = 0, \dots, p^{N-1} - 1,$$

which cover $\mathbb{P}_1(\mathbb{Q}_p)$. It follows therefore from the additivity of the distribution (1–4) and the formula (1–3) that

$$\beta\left(\times\!\!\!\!\!\!\int_\tau^{\tau+1} \int_0^\infty \omega \right) \equiv \left(\prod_{j=0}^{p^N-1} \left(1 + \frac{1}{j - \tau} \right)^{\beta\left(w^N \int_{-jp^{-N}}^\infty f(z)dz \right)} \right) \tag{1–9}$$

$$\times \left(\prod_{j=0}^{p^{N-1}-1} \left(1 + \frac{1}{pj - \tau} \right)^{\beta\left(w^N \int_\infty^{-jp^{1-N}} f(z)dz \right)} \right) \tag{1–10}$$

$$\equiv \prod_{j \in (\mathbb{Z}/p^N\mathbb{Z})^\times} \left(1 + \frac{1}{j - \tau} \right)^{\beta\left(w^N \int_{-jp^{-N}}^\infty f(z)dz \right)} \ (\mathrm{mod}\ p^N). \tag{1–11}$$

The computation of the values

$$\beta\left(\int_x^y f(z)dz \right)$$

can in turn be performed efficiently using Manin's continued fraction method for calculating modular symbols. (Cf. for example [Cremona 97].)

Note that the running time of the above algorithm for computing J_τ is dominated by the $(p^N - p^{N-1})$-fold product of (1–11) needed to approximate the double p-adic integral to a precision of p^{-N}. Taking $\log(p^N)$ as a natural measure for the size of this problem, this algorithm has exponential running time. Motivated by Proposition 1.1, it is natural to ask:

Question. Is there an algorithm for computing J_τ to a p-adic acuracy of p^{-N} in subexponential time?

Remark 1.7. A prospect for a polynomial-time algorithm (albeit one that is neither as efficient nor as simple as the method described in Proposition 1.1) is offered by the conjectures of [Darmon 02]. Observe that J_τ can be recovered from its p-adic logarithm and its value (mod p). Thus it suffices to provide a polynomial-time algorithm for computing

$$\log\, J_\tau = \lim_{||\mathcal{U}||\to 0} \sum_{U\in\mathcal{U}} \left[\beta\left(\epsilon_U \int_{\alpha_U 0}^{\alpha_U\infty} f(z)dz\right)\right.$$
$$\left. \times \log\left(1+\frac{1}{t_U-\tau}\right)\right]$$

when $\tau \in \mathcal{R}$. Taking local expansions of the logarithm, this expression can be rewritten as

$$\sum_{k\in\mathbb{P}_1(\mathbb{Z}/p\mathbb{Z})} \sum_{j=0}^{\infty} c_{j,k}\, g_{j,k}(\tau)$$

where $c_{j,k} \in p^j\mathbb{Z}_p[\sqrt{s}]$ are constants independent of τ, and $g_{j_k}(\tau) \in \mathbb{Z}_p[\sqrt{s}]$ are functions of τ that can be calculated in linear time. Thus to calculate J_τ for any $\tau \in \mathcal{R}$ to a precision of p^{-N}, it suffices to calculate the $(p+1)N$ constants $c_{j,k}$, $k \in \mathbb{P}_1(\mathbb{Z}/p\mathbb{Z})$ and $j = 0, \dots, N-1$. The Shimura reciprocity and Gross-Zagier conjectures (to be discussed below) might provide a method for accomplishing this by predicting the values of J_τ for sufficiently many τ to the necessary precision, thus reducing the calculation of the $c_{j,k}$ to a problem of linear algebra provided the values of τ can be chosen to produce a linearly independent set of equations.

2. CLASS FIELDS OF REAL QUADRATIC FIELDS

The experiments summarised in this section test the prediction of Conjecture 1.6 that Stark-Heegner points are defined over ring class fields of real quadratic fields. All of the calculations were carried out using Pari-GP running on a Unix workstation.[2]

Choose a $\mathbb{Z}[1/p]$-order $\mathcal{O}$ in a real quadratic field K. Of particular interest is the case where $\mathrm{Pic}(\mathcal{O})$ is not of exponent two, since in this case the associated ring class field H is not abelian over $\mathbb{Q}$, and no method is known for constructing points on $E(H)$ without an *a priori* knowledge of H. Thus, in all the cases to be examined in this section, the order $\mathcal{O}$ has been chosen so that $\mathrm{Pic}^+(\mathcal{O})$ is a cyclic group of odd order h.

Let E be an elliptic curve of prime conductor p, where p is inert in K and prime to the discriminant of $\mathcal{O}$. Let $\tau_1, \dots, \tau_h$ be a complete set of representatives for the $\mathrm{SL}_2(\mathbb{Z}[1/p])$-orbits of even $\tau \in \mathcal{H}_p$ having stabiliser in $M_2(\mathbb{Z}[1/p])$ isomorphic to $\mathcal{O}$, and let $P_{\tau_1}, \dots, P_{\tau_h}$ be the associated Stark-Heegner points.

Example 2.1. Let $\mathcal{O} = \mathbb{Z}\left[\sqrt{37}\right]$ be the order of discriminant $D = 4\cdot 37$, the smallest positive discriminant of narrow class number 3. The smallest prime p which is inert in $\mathbb{Q}(\sqrt{37})$ and for which the modular curve $X_0(p)^+$ admits an elliptic curve quotient is $p = 43$. Let

$$E\,:\, y^2 + y = x^3 + x^2$$

be the eliptic curve of conductor $p = 43$ denoted by $43A1$ in Cremona's tables. The elements $\tau_1, \tau_2, \tau_3 \in \mathbb{Q}(\sqrt{37}) \cap \mathcal{H}_{43}$ attached to the order $\mathcal{O}$ can be chosen to be

$$\tau_1 = -6 + \sqrt{37}, \quad \tau_2 = \frac{-3+\sqrt{37}}{4}, \quad \tau_3 = \frac{-3+\sqrt{37}}{7}.$$

Let Ω_+ and Ω_- denote the real and imaginary half-periods of E and define $\beta : \tilde{\Lambda} \to \mathbb{Z}$ by $\beta(\Omega_+) = \beta(\Omega_-) = \frac{1}{2}$. The points

$$P_j := \Phi_{\mathrm{Tate}}(\beta \tilde{J}_\tau)$$

were computed to 5 significant 43-adic digits to obtain, after setting $(x_j, y_j) := P_j$:

$$x_1 = 29{+}26{\cdot}43{+}36{\cdot}43^2{+}36{\cdot}43^3{+}15{\cdot}43^4{+}34{\cdot}43^5{+}\cdots$$
$$x_2 = (31 + 29\cdot 43 + 24\cdot 43^2 + 24\cdot 43^3 + 13\cdot 43^4 + 4\cdot 43^5 + \cdots)$$
$$+ (16 + 37\cdot 43 + 29\cdot 43^2 + 39\cdot 43^3 + 26\cdot 43^4 + 25\cdot 43^5 + \cdots)\sqrt{37}$$
$$x_3 = (31 + 29\cdot 43 + 24\cdot 43^2 + 24\cdot 43^3 + 13\cdot 43^4 + 4\cdot 43^5 + \cdots)$$
$$+ (27 + 5\cdot 43 + 13\cdot 43^2 + 3\cdot 43^3 + 16\cdot 43^4 + 17\cdot 43^5 + \cdots)\sqrt{37}.$$

$$y_1 = 21 + 28\cdot 43 + 23\cdot 43^2 + 43^3 + 42\cdot 43^4 + 4\cdot 43^5 + \cdots$$
$$y_2 = (18 + 7\cdot 43 + 31\cdot 43^2 + 20\cdot 43^3 + 19\cdot 43^5 + \cdots)$$
$$+ (41 + 36\cdot 43 + 10\cdot 43^2 + 14\cdot 43^3 + 9\cdot 43^4 + 30\cdot 43^5 + \cdots)\sqrt{37}$$
$$y_3 = (18 + 7\cdot 43 + 31\cdot 43^2 + 20\cdot 43^3 + 19\cdot 43^5 + \cdots)$$
$$+ (2 + 6\cdot 43 + 32\cdot 43^2 + 28\cdot 43^3 + 33\cdot 43^4 + 12\cdot 43^5 + \cdots)\sqrt{37}.$$

Since the sign of the Atkin-Lehner involution at 43 acting on f_E is equal to 1, Conjecture 5.9 of [Darmon 02] (together with Proposition 5.10) predicts that the 43-adic points $P_j = (x_j, y_j)$ are algebraic and conjugate to each other over $\mathbb{Q}$, and that their coordinates generate the ring class field of $\mathbb{Q}(\sqrt{37})$ of conductor 2. A direct calculation reveals that

$$\prod_{j=1}^{3}(t - x_j) = t^3 - 5t^2 - 5t - 1 \pmod{43^6} \qquad (2\text{–}1)$$

$$\prod_{j=1}^{3}(t - y_j) = t^3 - 14t^2 - 14t + 2 \pmod{43^6}. \qquad (2\text{–}2)$$

[2] The routines that were written for this purpose can be downloaded from the web site http://www.math.mcgill.ca/darmon/heegner/heegner.html

Let $f_x(t)$ and $f_y(t)$ denote the polynomials appearing on the right hand side of (2–1) and (2–2) respectively. The small size of their coefficients suggest that the mod 43^6 congruences in these equations are in fact genuine *equalities*. This guess is reinforced by the fact that $f_x(t)$ and $f_y(t)$ each have splitting field equal to H, and that, if $x \in H$ is a root of $f_x(t)$, and y is the unique root of $f_y(t)$ defined over $\mathbb{Q}(x)$, then the pair (x, y) is an algebraic point on $E(H)$.

A similar calculation—with the same value $D = 4 \cdot 37$, and the same values of τ_1, τ_2, and τ_3, but viewed this time as elements of the 61-adic upper half plane $\mathcal{H}_{61}$—was performed with the elliptic curve

$$E : y^2 + xy = x^3 - 2x + 1$$

of conductor 61 denoted $61A1$ in Cremona's tables. The x and y-coordinates of the Stark-Heegner points attached to this order were computed to 5 significant 61-adic digits, and found to satisfy (to this accuracy) the polynomials with small integer coefficients

$$x^3 - 3x^2 - x + 1, \qquad \text{and} \qquad y^3 - 5y^2 + 3y + 5.$$

As before, the splitting field of each of these polynomials is the ring class field H, and their roots, paired appropriately, give global points on the elliptic curve $E = 61A$ over H.

Example 2.2. Let $K = \mathbb{Q}(\sqrt{401})$. It is the smallest real quadratic field of (narrow) class number 5. The prime $p = 61$ is inert in $K/\mathbb{Q}$, and $X_0(p)^+$ admits an elliptic curve quotient; the curve E of conductor 61 denoted $61A1$ in Cremona's tables, which already appeared in Example 2.1. The following $\tau_j \in \mathcal{H}_{61}$:

$$\tau_1 = \frac{-1+\sqrt{401}}{20}, \quad \tau_2 = \frac{-11+\sqrt{401}}{10}, \quad \tau_3 = \frac{-11+\sqrt{401}}{28},$$

$$\tau_4 = \frac{-7+\sqrt{401}}{16}, \quad \tau_5 = \frac{-7+\sqrt{401}}{22},$$

form a complete system of representatives for the $\mathrm{SL}_2(\mathbb{Z}[1/61])$-orbits of even $\tau \in \mathcal{H}_{61}$ whose stabiliser in $M_2(\mathbb{Z}[1/61])$ is the maximal $\mathbb{Z}[1/61]$-order $\mathcal{O} = \mathbb{Z}[1/61][\frac{1+\sqrt{401}}{2}]$ of K.

As in Example 2.1, let Ω_+ and Ω_- denote the real and imaginary half-periods of E and define $\beta : \tilde{\Lambda} \to \mathbb{Z}$ by $\beta(\Omega_+) = \beta(\Omega_-) = \frac{1}{2}$. The five points $P_{\tau_j} = (x_j, y_j)$ were calculated to 4 significant 61-adic digits, yielding the values:

$$\begin{aligned}
x_1 &= 19 + 34 \cdot 61 + 17 \cdot 61^2 + 46 \cdot 61^3 + 32 \cdot 61^4 + \cdots\\
x_2 &= (29 + 26 \cdot 61 + 36 \cdot 61^2 + 7 \cdot 61^3 + 12 \cdot 61^4 + \cdots)\\
&\quad + (52 + 11 \cdot 61 + 21 \cdot 61^2 + 32 \cdot 61^3 + 48 \cdot 61^4 + \cdots)\sqrt{401}\\
x_3 &= (29 + 26 \cdot 61 + 36 \cdot 61^2 + 7 \cdot 61^3 + 12 \cdot 61^4 + \cdots)\\
&\quad + (9 + 49 \cdot 61 + 39 \cdot 61^2 + 28 \cdot 61^3 + 12 \cdot 61^4 + \cdots)\sqrt{401}\\
x_4 &= (59 + 47 \cdot 61 + 15 \cdot 61^2 + 30 \cdot 61^3 + 32 \cdot 61^4 + \cdots)\\
&\quad + (28 + 6 \cdot 61 + 40 \cdot 61^2 + 36 \cdot 61^3 + 4 \cdot 61^4 + \cdots)\sqrt{401}\\
x_5 &= (59 + 47 \cdot 61 + 15 \cdot 61^2 + 30 \cdot 61^3 + 32 \cdot 61^4 + \cdots)\\
&\quad + (33 + 54 \cdot 61 + 20 \cdot 61^2 + 24 \cdot 61^3 + 56 \cdot 61^4 + \cdots)\sqrt{401}.
\end{aligned}$$

$$\begin{aligned}
y_1 &= 19 + 37 \cdot 61 + 57 \cdot 61^2 + 11 \cdot 61^3 + 34 \cdot 61^4 + \cdots\\
y_2 &= (48 + 53 \cdot 61 + 8 \cdot 61^2 + 59 \cdot 61^3 + 12 \cdot 61^4 + \cdots)\\
&\quad + (58 + 60 \cdot 61 + 9 \cdot 61^2 + 28 \cdot 61^3 + 51 \cdot 61^4 + \cdots)\sqrt{401}\\
y_3 &= (48 + 53 \cdot 61 + 8 \cdot 61^2 + 59 \cdot 61^3 + 12 \cdot 61^4 + \cdots)\\
&\quad + (3 + 51 \cdot 61^2 + 32 \cdot 61^3 + 9 \cdot 61^4 + \cdots)\sqrt{401}\\
y_4 &= (37 + 49 \cdot 61 + 53 \cdot 61^2 + 56 \cdot 61^3 + 30 \cdot 61^4 + \cdots)\\
&\quad + (50 + 2 \cdot 61 + 38 \cdot 61^2 + 6 \cdot 61^3 + 11 \cdot 61^4 + \cdots)\sqrt{401}\\
y_5 &= (37 + 49 \cdot 61 + 53 \cdot 61^2 + 56 \cdot 61^3 + 30 \cdot 61^4 + \cdots)\\
&\quad + (11 + 58 \cdot 61 + 22 \cdot 61^2 + 54 \cdot 61^3 + 49 \cdot 61^4 + \cdots)\sqrt{401}
\end{aligned}$$

Conjecture 1.6 (combined with proposition 5.10 of [Darmon 02]) predicts that the 61-adic points $P_{\tau_1}, \ldots, P_{\tau_5}$ are algebraic and conjugate to each other over $\mathbb{Q}$, and together generate the Hilbert class field H of $\mathbb{Q}(\sqrt{401})$. One finds:

$$\prod_{j=1}^{5}(t - x_j) = t^5 - 12t^4 + 34t^3 - 5t^2 - 24t + 9 \pmod{61^5}$$

$$\prod_{j=1}^{5}(t - y_j) = t^5 - 6t^4 - 181t^3 - 428t^2 - 346t - 93 \pmod{61^5},$$

and observes that the polynomials $f_x(t)$ and $f_y(t)$ appearing on the right both have H as splitting field. Furthermore, if x is a root of $f_x(t)$ and y is the unique root of f_y defined over $\mathbb{Q}(x)$, then the pair (x, y) is an algebraic point on $E(H)$.

Example 2.3. Similar calculations were performed on the real quadratic field $K = \mathbb{Q}(\sqrt{577})$ of class number 7. When applied to the elliptic curve $E = 61A$ whose conductor is inert in K, the method produces seven 61-adic points whose x and y coordinates ostensibly (i.e., to the calculated accuracy of 4 significant 61-adic digits) satisfy the polynomials with small integer coefficients:

$$\begin{aligned}
f_x(x) &= x^7 - 23x^6 + 109x^5 - 102x^4 - 137x^3\\
&\quad + 271x^2 - 145x + 25,\\
f_y(y) &= y^7 + 71y^6 - 589y^5 + 204y^4 + 1582y^3\\
&\quad - 533y^2 - 22y + 5.
\end{aligned}$$

D	h	h_+	P_D^+	P_D^-
8	1	1	$2 \cdot \left(\frac{9}{2}, -\frac{1}{2} + \frac{7}{4}\sqrt{2}\right)$	O
13	1	1	$2 \cdot \left(\frac{553}{36}, -\frac{1}{2} - \frac{3397}{216}\sqrt{13}\right)$	O
17	1	1	$2 \cdot \left(\frac{21}{4}, -\frac{1}{2} + \frac{13}{8}\sqrt{17}\right)$	O
21	1	2	$\left(\frac{384067}{86700}, -\frac{1}{2} - \frac{17413453}{44217000}\sqrt{21}\right)$	$5\left(-6, -\frac{1}{2} \pm \frac{11}{2}\sqrt{-7}\right)$
24	1	2	$\left(\frac{5281}{150}, -\frac{1}{2} + \frac{376621}{4500}\sqrt{6}\right)$	$5\left(-\frac{1}{2}, -\frac{1}{2} \pm \frac{11}{4}\sqrt{-2}\right)$
28	1	2	$\left(\frac{379}{36}, -\frac{1}{2} - \frac{2491}{216}\sqrt{7}\right)$	$5\left(-6, -\frac{1}{2} \pm \frac{11}{2}\sqrt{-7}\right)$
29	1	1	$2 \cdot \left(\frac{907428789}{5569600}, -\frac{1}{2} + \frac{5059406780519}{13144256000}\sqrt{29}\right)$	O
32	1	2	$3 \cdot \left(\frac{9}{2}, -\frac{1}{2} - \frac{7}{4}\sqrt{2}\right)$	$5\left(-\frac{1}{2}, -\frac{1}{2} \pm \frac{11}{4}\sqrt{-2}\right)$
40	2	2	$\left(\frac{66529}{810}, -\frac{1}{2} + \frac{17042077}{72900}\sqrt{10}\right) + 5 \cdot \left(\frac{9}{2}, -\frac{1}{2} \pm \frac{7}{4}\sqrt{2}\right)$	O
41	1	1	$2 \cdot \left(\frac{2589}{100}, -\frac{1}{2} + \frac{20003}{1000}\sqrt{41}\right)$	O
52	1	1	$2 \cdot \left(\frac{105557507041}{21602148048}, -\frac{1}{2} + \frac{15613525573072201}{11447669519372736}\sqrt{13}\right)$	O
57	1	2	$\left(\frac{103}{12}, -\frac{1}{2} - \frac{203}{72}\sqrt{57}\right)$	$5\left(\frac{9}{4}, -\frac{1}{2} \pm \frac{11}{8}\sqrt{-19}\right)$
61	1	1	$2 \cdot \left(\frac{330571544885629}{55217977574400}, -\frac{1}{2} - \frac{523005552890597564957}{410318165198057472000}\sqrt{61}\right)$	O
65	2	2	$\left(\frac{4833}{980}, -\frac{1}{2} - \frac{43847}{68600}\sqrt{65}\right) + 5 \cdot \left(\frac{553}{36}, -\frac{1}{2} \pm \frac{3397}{216}\sqrt{13}\right)$	O
68	1	1	$2 \cdot \left(\frac{1152668280488833798716 81}{260601227159006391332 48}, -\frac{1}{2} + \frac{727244198574136415939778113 6558209}{173455927426677980709046796384 55808}\sqrt{17}\right)$	O
72	1	2	$\left(\frac{9}{2}, -\frac{1}{2} - \frac{7}{4}\sqrt{2}\right)$	$5\left(-\frac{25}{6}, -\frac{1}{2} \pm \frac{121}{36}\sqrt{-6}\right)$
73	1	1	$2 \cdot \left(\frac{157}{36}, -\frac{1}{2} + \frac{19}{216}\sqrt{73}\right)$	O
76	1	2	$\left(\frac{34293031}{864900}, -\frac{1}{2} + \frac{45330699833}{804357000}\sqrt{19}\right)$	$5\left(\frac{9}{4}, -\frac{1}{2} \pm \frac{11}{8}\sqrt{-19}\right)$
84	1	2	$2 \cdot \left(\frac{384067}{86700}, -\frac{1}{2} + \frac{17413453}{44217000}\sqrt{21}\right)$	$10 \cdot \left(-6, -\frac{1}{2} \pm \frac{11}{2}\sqrt{-7}\right)$
85	2	2	$\left(\frac{161509609733}{263973780}, -\frac{1}{2} - \frac{15729396596529101}{9590167427400}\sqrt{85}\right) + 5 \cdot \left(\frac{21}{4}, -\frac{1}{2} \pm \frac{13}{8}\sqrt{17}\right)$	O
96	2	4	$\pm\Big(\frac{356973682910042736082542174429}{278370776850857336999564906 42} \pm \frac{130569573374110842287342220555}{278370776850857336999564906 42}\sqrt{3},$ $-\frac{1}{2} - \frac{205420898019081988398262688233144460221888187}{656826187966684076857319367559728112 2773524}\sqrt{2}$ $\mp \frac{128971256132268625320388516238463109582746165}{656826187966684076857319367559728112 2773524}\sqrt{6}\Big)$	$\pm 5\Big(-\frac{23}{2} \pm \frac{11}{2}\sqrt{3},$ $-\frac{1}{2} + \frac{143}{4}\sqrt{-2} \mp \frac{77}{4}\sqrt{-6}\Big)$

TABLE 1. Stark-Heegner points on $X_0(11)$, with $D \leq 100$.

As in Examples 2.1 and 2.2, the roots of these polynomials generate the Hilbert class field of $\mathbb{Q}(\sqrt{577})$, and are the coordinates of global points on E defined over this class field.

Remark 2.4. In all the examples presented in this section, the Stark-Heegner points are integral points of small height, a fortunate circumstance which facilitates their identification. There is no reason to expect this pattern to persist, and in fact it is known (cf. [Bertolini and Darmon 2001]) that there is no elliptic curve E for which all the Stark-Heegner points are integral—in contrast with the case of the classical Heegner point construction, which does yield integral points on any elliptic curve E whose associated Weil uniformisation maps only cuspidal points of $X_0(N)$ to the origin of E.

Remark 2.5. Certain elliptic curves—such as the curve $61A$—seemed more amenable to the types of calculations described in this section, than others, such as $11A$, on which the Stark-Heegner points appear generally to be of larger height. The authors can provide no explanation, even conjectural, for this phenomenon—nor would they vouch for the fact that this observation is not a mere accident, an artefact of the small ranges in which numerical data has been gathered. With this caveat, the following question still seems to merit some consideration: Is there a quantity which would play the role of the

D	h	h_+	P_D^+	P_D^-
101	1	1	$---$	O
105	2	4	$---$	$---$
109	1	1	$2\left(\frac{3667842483162901}{617920164000000}, -\frac{1}{2} + \frac{143246420081640994000033}{153602594367120000000000}\sqrt{109}\right)$	O
112	1	2	$3\left(\frac{379}{36}, -\frac{1}{2} + \frac{2491}{216}\sqrt{7}\right)$	$15\left(-6, -\frac{1}{2} - \frac{11}{2}\sqrt{-7}\right)$
116	1	1	$4\left(\frac{907428789}{5569600}, -\frac{1}{2} - \frac{5059406780519}{13144256000}\sqrt{29}\right)$	O
117	1	2	$3\left(\frac{553}{36}, -\frac{1}{2} + \frac{3397}{216}\sqrt{13}\right)$	$5\left(-\frac{7}{3}, -\frac{1}{2} + \frac{11}{18}\sqrt{-39}\right)$
120	2	4	$\left(\frac{925955556961}{13188452670}, -\frac{1}{2} - \frac{883710863425484731}{8295668613956700}\sqrt{30}\right)$ $+5\left(\frac{5281}{150}, -\frac{1}{2} + \frac{376621}{4500}\sqrt{6}\right)$	$---$
128	1	2	$4\left(\frac{9}{2}, -\frac{1}{2} + \frac{7}{4}\sqrt{2}\right)$	$---$
129	1	2	$\left(\frac{862869067}{193924800}, -\frac{1}{2} - \frac{828635680379}{4677466176000}\sqrt{129}\right)$	$---$
140	2	4	$\left(\frac{306622827130980667}{62124016807132020}, -\frac{1}{2} + \frac{3027993094559976479360401 3}{346237652804094781739802 00}\sqrt{35}\right)$ $+5\left(\frac{379}{36}, -\frac{1}{2} + \frac{2491}{216}\sqrt{7}\right)$	$5\left(-\frac{43}{20}, -\frac{1}{2} + \frac{121}{200}\sqrt{-35}\right)$ $+5\left(-6, -\frac{1}{2} + \frac{11}{2}\sqrt{-7}\right)$
145	4	4	$---$	O
149	1	1	$---$	O
153	1	2	$\left(\frac{21}{4}, -\frac{1}{2} - \frac{13}{8}\sqrt{17}\right)$	$5\left(-\frac{413}{12}, -\frac{1}{2} + \frac{2057}{72}\sqrt{-51}\right)$
156	2	4	$\left(\frac{2705296424336257}{26495677267500}, -\frac{1}{2} + \frac{38814934713661482518869}{2362235354622596250 00}\sqrt{39}\right)$ $+5\left(\frac{553}{36}, -\frac{1}{2} - \frac{3397}{216}\sqrt{13}\right)$	$5\left(-\frac{57}{4}, -\frac{1}{2} + \frac{121}{8}\sqrt{-13}\right)$ $+5\left(-\frac{7}{3}, -\frac{1}{2} - \frac{11}{18}\sqrt{-39}\right)$
160	2	4	$3\left(\frac{66529}{810}, -\frac{1}{2} - \frac{17042077}{72900}\sqrt{10}\right) + 5\left(\frac{9}{2}, -\frac{1}{2} + \frac{7}{4}\sqrt{2}\right)$	$---$
161	1	2	$\left(\frac{7542243}{57500}, -\frac{1}{2} - \frac{7796699851}{66125000}\sqrt{161}\right)$	$115\left(\frac{2293}{2300}, -\frac{1}{2} - \frac{227293}{529000}\sqrt{-161}\right)$
164	1	1	$8\left(\frac{2589}{100}, -\frac{1}{2} - \frac{20003}{1000}\sqrt{41}\right)$	O
172	1	2	$\left(\frac{2131747}{51984}, -\frac{1}{3} - \frac{467322401}{11852352}\sqrt{43}\right)$	$5\left(\frac{69}{16}, -\frac{1}{2} + \frac{11}{64}\sqrt{-43}\right)$
173	1	1	$---$	O
184	1	2	$\left(\frac{313445281}{38512350}, -\frac{1}{2} + \frac{4608082094021}{1620984811500}\sqrt{46}\right)$	$5\left(-\frac{1}{2}, -\frac{1}{2} \pm \frac{11}{4}\sqrt{-2}\right)$
189	1	2	$2\left(\frac{384067}{86700}, -\frac{1}{2} + \frac{17413453}{44217000}\sqrt{21}\right)$	O
193	1	1	$2\left(\frac{697}{144}, -\frac{1}{2} - \frac{581}{1728}\sqrt{193}\right)$	O
197	1	1	$---$	O
200	2	2	$\left(\frac{9}{2}, -\frac{1}{2} + \frac{7}{4}\sqrt{2}\right) + 5\left(\frac{66529}{810}, -\frac{1}{2} - \frac{17042077}{72900}\sqrt{10}\right)$	O

TABLE 2. Stark-Heegner points on $X_0(11)$, with $100 < D \leq 200$.

degree of the Weil parametrisation in the classical Heegner point construction by *controlling* the overall heights of Stark-Heegner points?

3. ELLIPTIC CURVES OF SMALL CONDUCTOR

3.1 Elliptic Curves with $\mathbf{w} = 1$

The elliptic curve curve $X_0(11)$. Let

$$E : y^2 + y = x^3 - x^2 - 10x - 20$$

be the elliptic curve of smallest conductor $N = 11$. Given a discriminant D (not necessarily fundamental) write P_D^+ (resp. P_D^-) for the Stark-Heegner points of discriminant D attached to the choice of functional sending Ω_+ to 5 (resp Ω_- to 5) and Ω_- (resp. Ω_+) to 0.

Conjecture 5.9 and Proposition 5.13 of [Darmon 02] predict that P_D^+ belongs to $E(H)$, and that P_D^- belongs to $E(H^+)^-$, where H and H^+ are the ring class field and narrow ring class field of discriminant D respectively,

D	h	h_+	P_D^+	P_D^-
5	1	1	$2\left(3, -2-\sqrt{5}\right)$	O
12	1	2	$2\left(\frac{29}{6}, -\frac{35}{12} - \frac{185}{36}\sqrt{3}\right)$	$2\left(\frac{1}{2}, -\frac{3}{4} - \frac{15}{4}i\right)$
20	1	1	$2\left(3, -2+\sqrt{5}\right)$	O
24	1	2	$\left(\frac{131}{12}, -\frac{143}{24} - \frac{1015}{72}\sqrt{6}\right)$	$4\left(\frac{5}{8}, -\frac{13}{16} + \frac{85}{32}\sqrt{-2}\right)$
28	1	2	$\left(\frac{5231}{1134}, -\frac{6365}{2268} - \frac{439205}{142884}\sqrt{7}\right)$	$2\left(\frac{1}{2}, -\frac{3}{4} + \frac{15}{4}i\right)$
29	1	1	$2\left(\frac{5091}{1225}, -\frac{3158}{1225} - \frac{52207}{42875}\sqrt{29}\right)$	O
37	1	1	$2\left(\frac{88251563}{6497401}, -\frac{47374482}{6497401} + \frac{131903494275}{16561875149}\sqrt{37}\right)$	O
40	2	2	$2\left(5, -3+3\sqrt{10}\right) + 4\left(3, -2-\sqrt{5}\right)$	O
41	1	1	$2\left(\frac{27}{4}, -\frac{31}{8} - \frac{5}{2}\sqrt{41}\right)$	O
44	1	2	$\left(\frac{27101}{9702}, -\frac{36803}{19404} + \frac{1206545}{4482324}\sqrt{11}\right)$	$2\left(\frac{1}{2}, -\frac{3}{4} - \frac{15}{4}i\right)$
45	1	2	O	$16\left(\frac{4}{3}, -\frac{7}{6} + \frac{17}{18}\sqrt{-15}\right)$
48	1	2	$\left(\frac{29}{6}, -\frac{35}{12} + \frac{185}{36}\sqrt{3}\right)$	O
56	1	2	$\left(\frac{10469}{3388}, -\frac{13857}{6776} + \frac{46275}{65219}\sqrt{14}\right)$	$4\left(\frac{5}{8}, -\frac{13}{16} - \frac{85}{32}\sqrt{-2}\right)$
57	1	2	$\left(\frac{8522141}{1554124}, -\frac{10076265}{3108248} - \frac{6274142315}{4222554908}\sqrt{57}\right)$	$4\left(-\frac{63}{76}, -\frac{13}{152} - \frac{629}{722}\sqrt{-19}\right)$
61	1	1	$2\left(\frac{67}{9}, -\frac{38}{9} + \frac{65}{27}\sqrt{61}\right)$	O
65	2	2	$2\left(15, -8-7\sqrt{65}\right) + 4\left(3, -2+\sqrt{5}\right)$	O
73	1	1	$2\left(\frac{1543}{36}, -\frac{1579}{72} - \frac{3515}{108}\sqrt{73}\right)$	O
80	1	2	$2\left(3, -2+\sqrt{5}\right)$	$4\left(\frac{1}{2}, -\frac{3}{4} - \frac{15}{4}i\right)$
88	1	2	$\left(\frac{1168375625699}{393455082636}, -\frac{1561830708335}{786910165272} + \frac{3634412106732760\,55}{8185384455447774\,96}\sqrt{22}\right)$	$4\left(\frac{5}{8}, -\frac{13}{16} + \frac{85}{32}\sqrt{-2}\right)$
92	1	2	$\left(\frac{1621831557551}{2873040814}, -\frac{1624704598365}{5746081628} - \frac{2919003154601635125}{1044459511439932}\sqrt{23}\right)$	$2\left(\frac{1}{2}, -\frac{3}{4} - \frac{15}{4}i\right)$
96	2	4	$\left(\frac{131}{12}, -\frac{143}{24} + \frac{1015}{72}\sqrt{6}\right) + 2\left(\frac{29}{6}, -\frac{35}{12} - \frac{185}{36}\sqrt{3}\right)$	$2\left(\frac{1}{2}, -\frac{3}{4} + \frac{15}{4}i\right)$
97	1	1	$2\left(\frac{49765}{17424}, -\frac{67189}{34848} - \frac{330455}{2299968}\sqrt{97}\right)$	O

TABLE 3. Stark-Heegner points on $X_0(17)$, with $D \leq 100$.

and the $-$ superscript denotes the minus-eigenspace for complex conjugation. This prediction is borne out by the calculations whose outcome is summarised in Tables 1 and 2.

Remark 3.1. In Table 1 all the Stark-Heegner points for discriminants $D < 100$ (not necessarily fundamental) were calculated to an accuracy of 8 significant 11-adic digits. In all cases it was possible to find a global point defined over the appropriate class field, of fairly modest height, approximating the Stark-Heegner point to the calculated accuracy. In many cases, however, this accuracy was not enough to recognize these 11-adic points as global points over the appropriate class field H without making an a priori calculation of the Mordell-Weil groups $E(H)$. This calculation in turn was facilitated by the fact that the class fields that arise for discriminants $D < 100$ in which 11 is inert are composita of quadratic extensions of $\mathbb{Q}$.

Remark 3.2. Note that the points P_D^+ seem generally to be of larger heights than the points P_D^-. The authors know of no theoretical justification (even heuristic) for this empirical observation.

Remark 3.3. Table 2 lists the Stark-Heegner points on $X_0(11)$ in the range $100 \leq D \leq 200$.

Remark 3.4. The entries marked $- - -$ in Table 2 (as in the tables following it) correspond to situations where the Stark-Heegner points have not been calculated. In most cases, this is because the (rudimentary)

D	h	P_D^+
8	1	$2\left(\frac{17}{2}, -\frac{1}{2} + \frac{69}{4}\sqrt{2}\right)$
12	1	$\left(\frac{31}{4}, -\frac{1}{2} + \frac{97}{8}\sqrt{3}\right)$
13	1	$2\left(4, -\frac{1}{2} - \frac{3}{2}\sqrt{13}\right)$
21	1	$\left(\frac{958}{175}, -\frac{1}{2} + \frac{30479}{12250}\sqrt{21}\right)$
29	1	$2\left(\frac{187766}{50625}, -\frac{1}{2} + \frac{17260511}{22781250}\sqrt{29}\right)$
32	1	$\left(\frac{17}{2}, -\frac{1}{2} - \frac{69}{4}\sqrt{2}\right)$
33	1	$\left(\frac{839}{44}, -\frac{1}{2} + \frac{14209}{968}\sqrt{33}\right)$
37	1	$2\left(\frac{97}{4}, -\frac{1}{2} - \frac{159}{8}\sqrt{37}\right)$
40	2	$\left(\frac{1201}{10}, -\frac{1}{2} - \frac{41781}{100}\sqrt{10}\right) + 3\left(\frac{17}{2}, -\frac{1}{2} + \frac{69}{4}\sqrt{2}\right)$
41	1	$2\left(\frac{328071349}{100600900}, -\frac{1}{2} - \frac{173802949917}{1009027027000}\sqrt{41}\right)$
48	1	$\left(\frac{31}{4}, -\frac{1}{2} - \frac{97}{8}\sqrt{3}\right)$
52	1	O
53	1	$2\left(\frac{171802}{5929}, -\frac{1}{2} + \frac{19788441}{913066}\sqrt{53}\right)$
56	1	$\left(\frac{81689740196849}{3182668608350}, -\frac{1}{2} - \frac{747294455075136103407}{212447267076553355500}\sqrt{14}\right)$
60	2	$\left(\frac{177592727}{5304500}, -\frac{1}{2} + \frac{1380972233981}{27318175000}\sqrt{15}\right) + 3\left(\frac{31}{4}, -\frac{1}{2} + \frac{97}{8}\sqrt{3}\right)$
65	2	$\left(\frac{460138373}{2979920}, -\frac{1}{2} + \frac{2745872872863}{11502491200}\sqrt{65}\right) + 3\left(4, -\frac{1}{2} - \frac{3}{2}\sqrt{13}\right)$
69	1	$2\left(\frac{136}{25}, -\frac{1}{2} + \frac{339}{250}\sqrt{69}\right)$
72	1	$2\left(\frac{17}{2}, -\frac{1}{2} - \frac{69}{4}\sqrt{2}\right)$
84	1	O
88	1	$\left(\frac{3529}{1078}, -\frac{1}{2} + \frac{44589}{166012}\sqrt{22}\right)$
89	1	$---$
97	1	$2\left(\frac{78721}{3136}, -\frac{1}{2} + \frac{2270031}{175616}\sqrt{97}\right)$

TABLE 4. Stark-Heegner points on $19A$, with $D \leq 100$.

search algorithm that was used to compute the relevant Mordell-Weil group did not produce a point in the relevant Mordell-Weil group, even though the existence of such a point is guaranteed by the Birch and Swinnerton-Dyer conjecture. At any rate, the authors are satisfied with the strong evidence for Conjecture 1.5 provided by the data they have compiled, and believe that the missing entries in their tables are only a manifestation of their lack of persistence in fully carrying out their calculations.

The elliptic curve of conductor 17. Table 3 summarizes the calculation of Stark-Heegner points on the elliptic curve $17A1$ of coonductor 17, with equation given by

$$y^2 + xy + y = x^3 - x^2 - x - 14.$$

The points were computed to an accuracy of 5 significant 17-adic digits. When their height was too large to allow easy recognition of their coordinates as algebraic numbers, the Mordell-Weil group of E over the appropriate ring class field was computed, allowing the recognition of the points P_D^+ and P_D^- as global points in most cases. Here, P_D^+ (resp. P_D^-) is associated to the functional β sending Ω_+ to 8 (resp. Ω_- to 8) and Ω_- (resp. Ω_+) to 0.

The elliptic curve of conductor 19. Table 4 summarizes the data for the elliptic curve of conductor 19, denoted $19A1$ in Cremona's tables, and with equation given by

$$y^2 + y = x^3 + x^2 - 9x - 15.$$

In this case only the point P_D^+—defined by letting β be the functional sending Ω_+ to 6 and Ω_- to 0—was calculated, to an accuracy of 4 significant 19-adic digits.

D	h	h_+	P_D^+	P_D^-
5	1	1	$2 \cdot (0,0)$	O
8	1	1	$2 \cdot (0,0)$	O
13	1	1	$2 \cdot (0,0)$	O
17	1	1	$2 \cdot (0,0)$	O
20	1	1	$-4 \cdot (0,0)$	O
24	1	2	$-(0,0)$	$\left(\frac{1}{2}, -\frac{1}{2} \pm \frac{1}{4}\sqrt{-2}\right)$
29	1	1	$4 \cdot (0,0)$	O
32	1	2	$-3 \cdot (0,0)$	$\left(\frac{1}{2}, -\frac{1}{2} \pm \frac{1}{4}\sqrt{-2}\right)$
45	1	2	$-3 \cdot (0,0)$	$\left(\frac{1}{3}, -\frac{1}{2} \pm \frac{1}{18}\sqrt{-15}\right)$
52	1	1	$-4 \cdot (0,0)$	O
56	1	2	$(0,0)$	$\left(\frac{1}{2}, -\frac{1}{2} \pm \frac{1}{4}\sqrt{-2}\right)$
57	1	2	$(0,0)$	$\left(\frac{149}{324}, -\frac{1}{2} \pm \frac{449}{5832}\sqrt{-19}\right)$
60	2	4	$\left(2 \pm \sqrt{3}, -4 \mp 2\sqrt{3}\right)$	$\pm\left(-1 \pm \sqrt{3}, -\frac{1}{2} - \sqrt{-5} \pm \frac{1}{2}\sqrt{-15}\right)$
61	1	1	O	O
68	1	1	$-8 \cdot (0,0)$	O
69	1	2	O	$\left(-2, -\frac{1}{2} \pm \frac{1}{2}\sqrt{-23}\right)$
72	1	2	$-3 \cdot (0,0)$	$\left(\frac{5}{6}, -\frac{1}{2} \pm \frac{1}{36}\sqrt{-6}\right)$
76	1	2	$(0,0)$	$\left(\frac{149}{324}, -\frac{1}{2} \pm \frac{449}{5832}\sqrt{-19}\right)$
80	1	2	$(0,0)$	$\left(\frac{3}{4}, -\frac{1}{2} \pm \frac{1}{8}\sqrt{-5}\right)$
88	1	2	$-(0,0)$	$\left(\frac{1}{2}, -\frac{1}{2} \pm \frac{1}{4}\sqrt{-2}\right)$
89	1	1	$-2 \cdot (0,0)$	O
92	1	2	$-2 \cdot (0,0)$	$\left(-2, -\frac{1}{2} \pm \sqrt{-23}\right)$
93	1	2	$2 \cdot (0,0)$	$\left(\frac{-10}{9}, -\frac{1}{2} \pm \frac{1}{54}\sqrt{-31}\right)$
96	2	4	$\left(1 \pm \sqrt{3}, 2 \pm \sqrt{3}\right)$	$\pm\left(-\frac{1}{2} \pm \frac{1}{2}\sqrt{3}, -\frac{1}{2} + \frac{1}{4}\sqrt{-2} \mp \frac{1}{4}\sqrt{-6}\right)$
97	1	1	O	O
105	2	4	$\left(\frac{8}{25} \pm \frac{3}{25}\sqrt{21}, -\frac{32}{125} \mp \frac{12}{125}\sqrt{21}\right)$	$\left(-\frac{1}{5} + \frac{1}{5}\sqrt{21}, -\frac{1}{2} + \frac{1}{50}\sqrt{-15} + \frac{1}{25}\sqrt{-35}\right)$
109	1	1	$2(0,0)$	O
113	1	1	O	O
116	1	1	$-8(0,0)$	O
117	1	2	$-5(0,0)$	$\left(\frac{2}{3}, -\frac{1}{2} \pm \frac{1}{18}\sqrt{-39}\right)$
124	1	2	O	$\left(-\frac{10}{9}, -\frac{1}{2} \pm \frac{1}{54}\sqrt{-31}\right)$
125	1	1	$-6(0,0)$	O
128	1	2	$4(0,0)$	$2\left(\frac{1}{2}, -\frac{1}{2} \pm \frac{1}{4}\sqrt{-2}\right)$
129	1	2	$-(0,0)$	$\left(\frac{14470973}{21902400}, -\frac{1}{2} \pm \frac{5466310441}{102503232000}\sqrt{-43}\right)$
133	1	2	$-(0,0)$	$\left(\frac{149}{324}, -\frac{1}{2} \pm \frac{49}{5832}\sqrt{-19}\right)$
140	2	4	$-(0,0) + \left(2 \pm \sqrt{7}, 4 \pm 2\sqrt{7}\right)$	$\left(-1 - \frac{1}{2}\sqrt{7}, -\frac{1}{2} - \frac{3}{4}\sqrt{-5} - \frac{1}{4}\sqrt{-35}\right)$
153	1	2	$-3(0,0)$	$\left(\frac{967}{1200}, -\frac{1}{2} \pm \frac{1819}{72000}\sqrt{-51}\right)$
156	2	4	$\left(2 \pm \frac{3}{,} - 4 \mp 2\sqrt{3}\right)$	$\left(-\frac{31}{39} - \frac{8}{13}\sqrt{3}, -\frac{1}{2} - \frac{48}{169}\sqrt{-13} - \frac{515}{3042}\sqrt{-39}\right)$
161	1	2	$2(0,0)$	$\left(-2, -\frac{1}{2} \pm \frac{1}{2}\sqrt{-23}\right)$
165	2	4	$\left(\frac{1}{8} \pm \frac{1}{8}\sqrt{33}, -\frac{15}{16} \pm \frac{1}{16}\sqrt{33}\right)$	$\left(-\frac{1}{6} + \frac{1}{6}\sqrt{33}, -\frac{1}{2} + \frac{1}{18}\sqrt{-15}\right)$
168	2	4	$\left(\frac{8}{25} \pm \frac{3}{25}\sqrt{21}, -\frac{32}{125} \mp \frac{12}{125}\sqrt{21}\right)$	$\left(-\frac{3}{4} - \frac{1}{4}\sqrt{21}, -\frac{1}{2} - \frac{1}{2}\sqrt{-6} - \frac{1}{4}\sqrt{-14}\right)$
172	1	2	$(0,0)$	$\left(\frac{14470973}{21902400}, -\frac{1}{2} \pm \frac{5466310441}{102503232000}\sqrt{-43}\right)$
177	1	2	O	$\left(-\frac{171}{100}, -\frac{1}{2} \pm \frac{227}{1000}\sqrt{-59}\right)$
180	1	2	$6(0,0)$	$2\left(\frac{1}{3}, -\frac{1}{2} \pm \frac{1}{18}\sqrt{-15}\right)$
193	1	1	$-2(0,0)$	O
200	2	2	$-2(0,0) + 2\left(-\frac{1}{2}, -\frac{1}{2} \pm \frac{1}{4}\sqrt{10}\right)$	O

TABLE 5. Stark-Heegner Points on $X_0(37)^+$, with $D \leq 200$.

D	h	h_+	P_D^+	P_D^-
5	1	1	$2(0,0)$	O
8	1	1	$-2(0,0)$	O
12	1	2	$-(0,0)$	$\left(-\frac{5}{4}, -\frac{1}{2} + \frac{3}{8}i\right)$
20	1	1	$-4(0,0)$	O
28	1	2	$(0,0)$	$\left(-\frac{5}{4}, -\frac{1}{2} + \frac{3}{8}i\right)$
29	1	1	$2(0,0)$	O
32	1	2	$3(0,0)$	$\left(-\frac{5}{4}, -\frac{1}{2} - \frac{3}{8}i\right)$
33	1	2	$(0,0)$	$\left(-\frac{141}{44}, -\frac{1}{2} - \frac{1381}{968}\sqrt{-11}\right)$
37	1	1	$2(0,0)$	O
45	1	2	$2(0,0)$	$---$
48	1	2	$3(0,0)$	$\left(-\frac{5}{4}, -\frac{1}{2} - \frac{3}{8}i\right)$
61	1	1	$2(0,0)$	O
65	2	2	$-(0,0) + \left(\frac{61}{52}, -\frac{1}{2} - \frac{675}{1352}\sqrt{13}\right)$	O
69	1	2	$(0,0)$	$\left(-\frac{36}{23}, -\frac{1}{2} + \frac{235}{1058}\sqrt{-23}\right)$
72	1	2	$2(0,0)$	$---$
73	1	1	$-2(0,0)$	O
76	1	2	O	$2\left(-\frac{5}{4}, -\frac{1}{2} + \frac{3}{8}i\right)$
77	1	2	$-3(0,0)$	$\left(-\frac{141}{44}, -\frac{1}{2} - \frac{1381}{968}\sqrt{-11}\right)$
80	1	2	$(0,0)$	$\left(-\frac{5}{4}, -\frac{1}{2} \pm \frac{3}{8}\sqrt{-1}\right)$
85	2	2	$-(0,0) + \left(-\frac{19}{17}, -\frac{1}{2} \pm \frac{45}{578}\sqrt{17}\right)$	O
88	1	2	$(0,0)$	$\left(-\frac{141}{44}, -\frac{1}{2} \pm \frac{1381}{968}\sqrt{-11}\right)$
89	1	1	$2(0,0)$	O
93	1	2	$3(0,0)$	$\left(-\frac{392}{31}, -\frac{1}{2} \pm \frac{14895}{1922}\sqrt{-31}\right)$
104	2	2	$(0,0) + \left(\frac{61}{52}, -\frac{1}{2} \pm \frac{675}{1352}\sqrt{13}\right)$	O
105	2	4	$\left(\frac{1}{4}, -\frac{1}{2} \pm \frac{1}{8}\sqrt{21}\right)$	$\left(-2, -\frac{1}{2} + \frac{1}{2}\sqrt{-15}\right) + \left(-\frac{47}{36}, -\frac{1}{2} + \frac{19}{216}\sqrt{-35}\right)$
108	1	2	$3(0,0)$	$\left(-\frac{5}{4}, -\frac{1}{2} \pm \frac{3}{8}\sqrt{-1}\right)$
112	1	2	$-3(0,0)$	$3\left(-\frac{5}{4}, -\frac{1}{2} \pm \frac{3}{8}\sqrt{-1}\right)$
113	1	1	$4(0,0)$	O
116	1	1	$-4(0,0)$	O
120	2	4	$\left(-\frac{1}{2}, -\frac{1}{2} \pm \frac{1}{4}\sqrt{6}\right)$	$\left(-\frac{209}{162}, -\frac{1}{2} + \frac{445}{2916}\sqrt{-10}\right) + \left(-2, -\frac{1}{2} + \frac{1}{2}\sqrt{-15}\right)$
125	1	1	$-10(0,0)$	O
128	1	2	$-4(0,0)$	$2\left(-\frac{5}{4}, -\frac{1}{2} \pm \frac{3}{8}\sqrt{-1}\right)$
132	1	2	$-4(0,0)$	O
136	2	4	$\left(\frac{3}{2} \pm \frac{1}{2}\sqrt{17}, 3 \pm \sqrt{17}\right)$	$---$
137	1	1	$4(0,0)$	O
141	1	2	$-2(0,0)$	$2\left(-7, -\frac{1}{2} \pm \frac{5}{2}\sqrt{-47}\right)$
148	3	3	Cf. example 1, sec. 2.	O
149	1	1	O	O
156	2	4	$\left(4 \pm \sqrt{13}, 11 \pm 3\sqrt{13}\right)$	$\left(-\frac{152233963}{56647368} - \frac{20226293}{56647368}\sqrt{13}\,,\right.$ $\left.-\frac{1}{2} - \frac{285199304263}{75369323124}\sqrt{-1} - \frac{127648135123}{150738646248}\sqrt{-13}\right)$
157	1	1	$-4(0,0)$	O
161	1	2	$(0,0)$	$\left(-\frac{36}{23}, -\frac{1}{2} \pm \frac{235}{1058}\sqrt{-23}\right)$
168	2	4	$-(0,0) + \left(\frac{1}{4}, -\frac{1}{2} - \frac{1}{8}\sqrt{21}\right)$	$\left(-\frac{3}{2}, -\frac{1}{2} + \frac{1}{4}\sqrt{-14}\right) + \left(-\frac{7}{2}, -\frac{1}{2} + \frac{9}{4}\sqrt{-6}\right)$
177	1	2	$-2(0,0)$	$2\left(-\frac{19}{16}, -\frac{1}{2} \pm \frac{1}{64}\sqrt{-59}\right)$
180	1	2	$4(0,0)$	$---$
184	1	2	$-(0,0)$	$\left(-\frac{36}{23}, -\frac{1}{2} \pm \frac{235}{1058}\sqrt{-23}\right)$
192	2	4	$-2(0,0) + \left(-\frac{1}{2}, -\frac{1}{2} \pm \frac{1}{4}\sqrt{6}\right)$	$\left(-\frac{7}{2}, -\frac{1}{2} \pm \frac{9}{4}\sqrt{-6}\right)$
200	2	2	$4(0,0) + 2\left(\frac{1}{2}, -\frac{1}{2} \pm \frac{1}{4}\sqrt{10}\right)$	O

TABLE 6. Stark-Heegner Points on $43A$, with $D \leq 200$.

3.2 Elliptic Curves with $w = -1$

The elliptic curve $X_0(37)^+$. Calculations similar to those of the previous section were performed for the elliptic curve

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

of conductor $N = 37$ denoted by $37A1$ in Cremona's tables. For all real quadratic discriminants D satisfying $(\frac{D}{37}) = -1$, write P_D^+ (resp. P_D^-) for the Stark-Heegner points of discriminant D attached to the choice of functional β sending Ω_+ (resp Ω_-) to 1 and Ω_- (resp. Ω_+) to 0.

Conjecture 5.9 of [Darmon 02], which apply directly in this situation because E is unique in its $\mathbb{Q}$-isogeny class, predicts that

1. The point P_D^+ belongs to $E(H)$, where H is the ring class field attached to the discriminant D.

2. The point P_D^- belongs to $E(H^+)$, where H^+ is the narrow ring class field of discriminant D, and is sent to its negative by complex conjugation, so that in particular it is a torsion point if $h = h^+$.

   In light of the fact that the eigenvalue of the Atkin-Lehner involution W_p at p acting on f_E is equal to 1, Proposition 5.10 of [Darmon 02] (which is conditional on Conjecture 5.9) also predicts that

3. If $\mathcal{O}$ has class number one, so that $H = K$, the point P_D^+ belongs to $E(\mathbb{Q})$.

These predictions are borne out by the calculations, performed to 5 significant 37-adic digits in the range $D \leq 200$, whose outcome is summarised in Table 5. In these calculations, the heights of the Stark-Heegner points are quite small, and so they could usually be recognised directly as algebraic points without an independent calculation of the Mordell-Weil groups $E(H)$.

The elliptic curve 43A. Table 6 displays the corresponding data for the elliptic curve

$$y^2 + y = x^3 + x^2$$

of conductor 43 (denoted $43A$ in Cremona's tables), which has rank one over $\mathbb{Q}$ and Mordell-Weil group generated by the point $P = (0, 0)$. The point P_D^+ (resp. P_D^-) corresponds to the choice of functional β sending the period Ω_+ to 2 (resp. Ω_+ to 0) and Ω_- to 0 (resp. Ω_- to 1).

The elliptic curve 61A. Table 7 displays the corresponding data for the elliptic curve

$$y^2 + xy = x^3 - 2x + 1$$

of conductor 61 (denoted $61A$ in Cremona's tables), which has rank one over $\mathbb{Q}$ and Mordell-Weil group generated by the point $P = (1, 0)$. The point P_D^+ (resp. P_D^-) corresponds to the choice of functional β sending the period Ω_+ to 2 (resp. Ω_+ to 0) and Ω_- to 0 (resp. Ω_- to 1).

4. A GROSS-ZAGIER CONJECTURE

If K is a real quadratic field of narrow class number h, and E is an elliptic curve of prime conductor p which is inert in K, let

$$P_K = P_{\tau_1} + \cdots + P_{\tau_h} \in E(\mathbb{C}_p),$$

where $\tau_1, \ldots, \tau_h$ range over a complete set of representatives for the $\mathrm{SL}_2(\mathbb{Z}[1/p])$-orbits of even $\tau \in \mathcal{H}_p$ with stabiliser isomorphic to the maximal $\mathbb{Z}[1/p]$-order $\mathcal{O}$ of K. The Shimura reciprocity law predicts that $P_{\tau_1}, \ldots, P_{\tau_h}$ belong to $E(H)$, where H is the Hilbert class field of K, and that these points are permuted simply transitively by $\mathrm{Gal}(H/K)$. This implies that P_K belongs to $E(K)$. Guided by the classical Gross-Zagier formula, the following conjecture is natural:

Conjecture 4.1. $L'(E/K, 1) = 4\frac{\Omega_+^2}{\sqrt{D}}h(P_K)$.

Assume furthermore that E satisfies the following additional assumption:

1. E is a quotient of $X_0(p)^+$
2. E is alone in its $\mathbb{Q}$-isogeny class, so that in particular it has no rational torsion.

In this case, the Shimura reciprocity law of [Darmon 02] predicts that the Stark-Heegner point P_K belongs to $E(\mathbb{Q})$.

Remark 4.2. The curves of conductor ≤ 101 satisfying these assumptions are the curves denoted $37A$, $43A$, $53A$, $61A$, $79A$, $83A$, $89A$, and $101A$ in Cremona's tables.

The assumptions on E imply that $w = 1$, and hence that the sign in the functional equation for $L(E/\mathbb{Q}, s)$ is -1, so that

$$L'(E/K, 1) = L'(E/\mathbb{Q}, 1)L(E^{(D)}/\mathbb{Q}, 1), \qquad (4\text{–}1)$$

D	h	h_+	P_D^+	P_D^-
8	1	1	$2(1,0)$	O
17	1	1	$-2(1,0)$	O
21	1	2	$(1,0)$	$\left(-\frac{79}{7}, \frac{79}{14} \pm \frac{1377}{98}\sqrt{-7}\right)$
24	1	2	O	$2\left(-2, 1-\sqrt{-2}\right)$
28	1	2	$-(1,0)$	$\left(-\frac{79}{7}, \frac{79}{14} - \frac{1377}{98}\sqrt{-7}\right)$
29	1	1	$-2(1,0)$	O
32	1	2	$-2(1,0)$	$\left(-2, 1+\sqrt{-2}\right)$
33	1	2	$(1,0)$	$\left(-\frac{20}{11}, \frac{10}{11} \pm \frac{27}{121}\sqrt{-11}\right)$
37	1	1	$2(1,0)$	O
40	2	2	$-1(1,0) + \left(\frac{4}{5}, -\frac{2}{5} \pm \frac{3}{25}\sqrt{5}\right)$	O
44	1	2	$(1,0)$	$\left(-\frac{20}{11}, \frac{10}{11} \pm \frac{27}{121}\sqrt{-11}\right)$
53	1	1	$-4(1,0)$	O
68	1	1	$6(1,0)$	O
69	1	2	$(1,0)$	$\left(-\frac{1039}{575}, \frac{1039}{1150} \pm \frac{18899}{132250}\sqrt{-23}\right)$
72	1	2	$-2(1,0)$	$---$
84	1	2	$-(1,0)$	$\left(-\frac{79}{7}, \frac{79}{14} \pm \frac{1377}{98}\sqrt{-7}\right)$
85	2	2	$(1,0) + \left(\frac{4}{5}, -\frac{2}{5} \pm \frac{3}{25}\sqrt{5}\right)$	O
89	1	1	O	O
92	1	2	$(1,0)$	$\left(-\frac{1039}{575}, \frac{1039}{1150} \pm \frac{18899}{132250}\sqrt{-23}\right)$
93	1	2	O	$2\left(-\frac{19}{9}, \frac{19}{18} \pm \frac{17}{54}\sqrt{-31}\right)$
96	2	4	$\left(\frac{1}{2}, -\frac{1}{4} \pm \frac{1}{4}\sqrt{3}\right)$	$\left(-\frac{7}{4}, \frac{7}{8} \pm \frac{1}{8}\sqrt{-6}\right)$
101	1	1	$2(1,0)$	O
104	2	2	$-(1,0) + \left(\frac{4}{13}, -\frac{2}{13} - \frac{31}{169}\sqrt{13}\right)$	O
105	2	4	$\left(-\frac{1}{2} \pm \frac{1}{2}\sqrt{5}, 0\right)$	$\left(-\frac{163}{14} - \frac{7}{2}\sqrt{5}, \frac{163}{28} + \frac{7}{4}\sqrt{5} + \frac{2909}{196}\sqrt{-7} + \frac{31}{4}\sqrt{-35}\right)$
112	1	2	$2(1,0)$	$2\left(-\frac{79}{7}, \frac{79}{14} \pm \frac{1377}{98}\sqrt{-7}\right)$
116	1	1	$2(1,0)$	O
120	2	4	$-(1,0)$	$\left(-\frac{962}{45}, \frac{481}{45} + \frac{20927}{675}\sqrt{-10}\right) + \left(-2, 1+\sqrt{-2}\right)$
124	1	2	O	$2\left(-\frac{19}{9}, \frac{19}{18} \pm \frac{17}{54}\sqrt{-31}\right)$
128	1	2	O	$2\left(-2, 1 \pm \sqrt{-2}\right)$
129	1	2	O	$4\left(-\frac{13}{4}, \frac{13}{8} \pm \frac{3}{4}\sqrt{-43}\right)$
132	1	2	$-3(1,0)$	$\left(-\frac{20}{11}, \frac{10}{11} \pm \frac{27}{121}\sqrt{-11}\right)$
133	1	2	$(1,0)$	$\left(-\frac{79}{7}, \frac{79}{14} \pm \frac{1377}{98}\sqrt{-7}\right)$
140	2	4	$\left(-\frac{1}{2} \pm \frac{1}{2}\sqrt{5}, \frac{1}{2} \mp \frac{1}{2}\sqrt{5}\right)$	$\left(-\frac{163}{14} - \frac{7}{2}\sqrt{5}, \frac{163}{28} + \frac{7}{4}\sqrt{5} + \frac{2909}{196}\sqrt{-7} + \frac{31}{4}\sqrt{-35}\right)$
145	4	4	$---$	O
148	3	3	Cf. example 1, sec. 2.	O
152	1	2	$-2(1,0)$	$2\left(-2, 1 \pm \sqrt{-2}\right)$
153	1	2	$2(1,0)$	$---$
157	1	1	$2(1,0)$	O
160	2	4	$(1,0)$	$\left(-\frac{962}{45}, \frac{481}{45} + \frac{20927}{675}\sqrt{-10}\right) + \left(-2, 1+\sqrt{-2}\right)$
165	2	4	$\left(-\frac{1}{2} \pm \frac{1}{2}\sqrt{5}, \frac{1}{2} \mp \frac{1}{2}\sqrt{5}\right)$	$\left(-\frac{486813}{76582} - \frac{13637}{6962}\sqrt{5}, \frac{486813}{153164} + \frac{13637}{13924}\sqrt{5} + \frac{536241399}{99403436}\sqrt{-11} + \frac{20169123}{9036676}\sqrt{-55}\right)$
172	1	2	$2(1,0)$	$4\left(-\frac{13}{4}, \frac{13}{8} \pm \frac{3}{4}\sqrt{-43}\right)$
173	1	1	$4(1,0)$	O
176	1	2	$-2(1,0)$	O
177	1	2	$(1,0)$	$\left(-\frac{79849300}{36542771}, \frac{39924650}{36542771} \pm \frac{434520424417}{1696790485843}\sqrt{-59}\right)$
181	1	1	O	O
185	2	2	$-(1,0) + \left(\frac{4}{5}, -\frac{2}{5} \pm \frac{3}{25}\sqrt{5}\right)$	O
189	1	2	$-3(1,0)$	$\left(-\frac{79}{7}, \frac{79}{14} \pm \frac{1377}{98}\sqrt{-7}\right)$
193	1	1	O	O
200	2	2	$-3(1,0) + \left(\frac{4}{5}, -\frac{2}{5} \pm \frac{3}{25}\sqrt{5}\right)$	O

TABLE 7. Stark-Heegner Points on $61A$, with $D \leq 200$.

D	$a(D)$	$A(D)$	D	$a(D)$	$A(D)$	D	$a(D)$	$A(D)$	D	$a(D)$	$A(D)$	D	$a(D)$	$A(D)$
5	2	4	193	−2	4	393	2	4	584	−6	36	796	0	0
8	2	4	204	2	4	401	2	4	597	0	0	797	−8	64
13	2	4	205	−2	4	409	0	0	609	0	0	808	2	4
17	2	4	209	−2	4	412	−2	4	616	2	4	809	4	16
24	−2	4	217	0	0	413	12	144	649	0	0	812	−8	64
29	4	16	220	−2	4	421	−2	4	652	2	4	829	0	0
56	2	4	236	−4	16	424	−2	4	653	0	0	849	0	0
57	2	4	237	6	36	429	6	36	661	−2	4	853	4	16
60	−2	4	241	0	0	449	2	4	664	2	4	856	0	0
61	0	0	253	0	0	457	−2	4	668	−14	196	857	6	36
69	0	0	257	−4	16	461	−10	100	680	4	16	865	2	4
76	2	4	264	2	4	473	−6	36	681	0	0	869	−6	36
88	−2	4	265	2	4	476	2	4	685	−4	16	893	6	36
89	−2	4	273	2	4	489	2	4	689	−2	4	901	2	4
92	−4	16	277	4	16	501	2	4	697	−2	4	905	−6	36
93	4	16	281	4	16	505	−2	4	701	−8	64	908	−12	144
97	0	0	301	−2	4	520	0	0	705	−2	4	917	−6	36
105	−2	4	309	−2	4	524	2	4	709	2	4	920	−4	16
109	2	4	313	2	4	533	−6	36	716	4	16	933	6	36
113	0	0	316	2	4	536	0	0	717	4	16	940	−2	4
124	0	0	328	−2	4	537	0	0	721	−2	4	949	−2	4
129	−2	4	341	8	64	541	−4	16	732	4	16	956	8	64
133	−2	4	348	4	16	553	2	4	745	2	4	957	0	0
140	−6	36	353	2	4	557	−16	256	748	−2	4	977	4	16
156	−2	4	357	6	36	561	−2	4	753	−2	4	984	2	4
161	4	16	364	2	4	568	−2	4	757	−4	16	985	2	4
165	2	4	365	6	36	569	4	16	760	0	0	993	0	0
168	−2	4	376	2	4	572	−6	36	764	0	0	997	−4	16
172	2	4	385	−2	4	573	0	0	769	0	0			
177	0	0	389	−4	16	577	−2	4	785	−2	4			

TABLE 8. Traces of Stark-Heegner points on $X_0(37)^+$, with $D \leq 1000$.

D	$a(D)$	$A(D)$	D	$a(D)$	$A(D)$	D	$a(D)$	$A(D)$	D	$a(D)$	$A(D)$	D	$a(D)$	$A(D)$
5	2	4	184	−2	4	409	−2	4	593	−2	4	793	2	4
8	−2	4	201	2	4	413	−8	64	601	0	0	796	0	0
12	−2	4	204	2	4	417	−2	4	604	2	4	808	−6	36
28	2	4	205	−2	4	421	4	16	609	0	0	813	6	36
29	2	4	209	0	0	424	2	4	620	6	36	824	−6	36
33	2	4	217	−2	4	429	−2	4	629	−4	16	829	−4	16
37	4	16	220	2	4	433	2	4	632	12	144	844	0	0
61	−2	4	233	0	0	437	−12	144	636	−2	4	849	2	4
65	−2	4	237	0	0	449	−2	4	641	2	4	856	−4	16
69	2	4	241	0	0	456	4	16	652	6	36	865	0	0
73	−2	4	248	−2	4	457	2	4	653	−8	64	872	6	36
76	0	0	249	2	4	460	2	4	664	2	4	888	4	16
77	−6	36	257	−2	4	469	2	4	665	4	16	889	2	4
85	−2	4	265	2	4	472	0	0	673	2	4	892	2	4
88	2	4	277	2	4	476	6	36	677	8	64	893	−4	16
89	2	4	280	4	16	481	0	0	696	4	16	897	−2	4
93	6	36	284	4	16	485	−2	4	716	−2	4	905	0	0
104	2	4	285	−4	16	492	−2	4	717	−12	144	908	8	64
105	0	0	309	2	4	493	6	36	721	−2	4	921	−2	4
113	4	16	313	2	4	501	−2	4	733	8	64	929	0	0
120	0	0	321	0	0	505	2	4	749	0	0	933	2	4
136	−2	4	328	−2	4	521	−2	4	753	2	4	937	2	4
137	4	16	329	0	0	524	0	0	757	4	16	940	4	16
141	−4	16	349	2	4	536	2	4	760	0	0	949	−2	4
149	0	0	364	2	4	545	2	4	761	0	0	953	−2	4
156	2	4	373	−4	16	553	−4	16	764	4	16	965	2	4
157	−4	16	376	0	0	561	2	4	773	18	324	973	2	4
161	2	4	377	6	36	577	2	4	776	−2	4	985	0	0
168	−4	16	381	2	4	581	−2	4	777	−4	16	988	8	64
177	−4	16	389	0	0	589	0	0	781	−4	16	997	−2	4

TABLE 9. Traces of Stark-Heegner points on $43A$, with $D \leq 1000$.

D	$a(D)$	$A(D)$	D	$a(D)$	$A(D)$	D	$a(D)$	$A(D)$	D	$a(D)$	$A(D)$	D	$a(D)$	$A(D)$
8	2	4	181	0	0	389	−4	16	593	−2	4	821	4	16
17	−2	4	185	−2	4	397	−2	4	604	−2	4	824	8	64
21	2	4	193	0	0	401	0	0	616	−2	4	844	0	0
24	0	0	201	2	4	409	0	0	617	−4	16	856	0	0
28	−2	4	204	−4	16	417	−6	36	620	8	64	860	0	0
29	−2	4	209	2	4	421	2	4	633	0	0	861	−2	4
33	2	4	213	−4	16	429	2	4	636	4	16	865	4	16
37	2	4	220	2	4	433	−4	16	641	−4	16	872	−6	36
40	−2	4	221	2	4	437	−6	36	645	−4	16	877	0	0
44	2	4	233	−2	4	444	0	0	653	0	0	885	2	4
53	−4	16	236	−2	4	445	0	0	661	2	4	889	−2	4
69	2	4	237	−6	36	453	−2	4	664	−4	16	892	2	4
85	2	4	265	0	0	456	0	0	665	−6	36	897	−6	36
89	0	0	268	−2	4	457	2	4	669	2	4	904	−2	4
92	2	4	273	2	4	460	−2	4	673	2	4	905	4	16
93	0	0	277	−2	4	465	0	0	677	12	144	908	−6	36
101	2	4	281	4	16	481	2	4	681	2	4	913	0	0
104	−2	4	284	0	0	505	−2	4	689	0	0	917	−2	4
105	−2	4	312	−4	16	509	2	4	697	2	4	921	2	4
120	−4	16	313	0	0	517	0	0	701	0	0	933	−2	4
124	0	0	316	2	4	520	−2	4	709	2	4	941	−6	36
129	0	0	328	−2	4	521	2	4	721	2	4	952	0	0
133	2	4	329	−4	16	541	0	0	749	0	0	953	−10	100
140	2	4	337	−4	16	556	−2	4	753	−4	16	965	12	144
145	2	4	345	2	4	557	−4	16	760	0	0	969	0	0
152	−4	16	348	4	16	572	6	36	761	2	4	984	0	0
157	2	4	349	2	4	573	2	4	764	2	4	993	−2	4
165	2	4	364	2	4	577	2	4	769	−2	4	997	−2	4
172	4	16	373	6	36	581	0	0	776	4	16			
173	4	16	376	0	0	584	−2	4	785	−2	4			
177	2	4	377	2	4	589	−4	16	817	0	0			

TABLE 10. Traces of Stark-Heegner points on $61A$, with $D \leq 1000$.

where $E^{(D)}$ is the twist of E by $\mathbb{Q}(\sqrt{D})$. Suppose that $E(\mathbb{Q})$ has rank 1 and is generated by P. The Birch and Swinnerton-Dyer conjecture predicts that

$$L'(E/\mathbb{Q},1) = \Omega_+ h(P) \# \underline{III}(E/\mathbb{Q}). \qquad (4\text{–}2)$$

Combining (4–1) and (4–2) with Conjecture 4.1 leads to the following:

Conjecture 4.3. *Let s^2 be the cardinality of the Shafarevich-Tate group of $E/\mathbb{Q}$, where $s \geq 0$.*

Let K be a real quadratic field of discriminant D. If the rank of $E(\mathbb{Q})$ is not equal to one, then P_K is torsion. Otherwise,

$$P_K = s \cdot a(D) \cdot P,$$

where P is a generator for $E(\mathbb{Q})$ and $a(D)$ is an integer satisfying

$$a(D)^2 = A(D) := \sqrt{D} \cdot L(E^{(D)},1)/\Omega_+. \qquad (4\text{–}3)$$

The elliptic curve $E : y^2 - y = x^3 - x$ of conductor $N = 37$ is equal to $X_0(37)^+$ and hence satisfies all the assumptions made in the above conjecture.

Furthermore $E(\mathbb{Q}) = \langle P \rangle$ is infinite cyclic with $P = (0,0)$. For all real quadratic K of discriminant $D \leq 1000$, the points P_K were calculated to 4 significant 37-adic digits, as well as the integer $a(D)$ defined as the smallest integer (in absolute value) satisfying the relation

$$P_K = a(D)(0,0),$$

to this calculated accuracy. Table 8 summarises the values of $a(D)$ that were obtained in this range.

The integer $A(D)$ was computed by calculating the special value of $L(E^{(D)},1)$ numerically, and it can be verified that in all cases relation (4–3) holds. Tables 9 and 10 provide similar data, with the points P_K calculated to an accuracy of 43^{-4} and 61^{-3} respectively, leading to the same kind of experimental confirmation for Conjecture 4.3 on the elliptic curves $43A$ and $61A$ treated in Section 3.2.

Remark 4.4. It would be interesting to understand more about the nature of the numbers $a(D)$. Are they the Fourier coefficients of a modular form of half-integral weight?

Remark 4.5. Note that the coefficients $a(D)$ in Tables 8, 9 and 10 are all even. The authors are unable to prove that the Stark-Heegner point P_K is always an integer multiple, not to mention an *even* integer multiple, of the generator P. But it does follow from the Birch and Swinnerton-Dyer conjecture that $A(D)$ is even.

REFERENCES

[Bertolini and Darmon 2001] M. Bertolini and H. Darmon, *The p-adic L-functions of modular elliptic curves*, in *Mathematics Unlimited—2001 and Beyond*, Engquist, Schmid, eds., pp. 109–170, Berlin: Springer Verlag, 2001.

[Breuil et al. 2001] C. Breuil. B. Conrad, F. Diamond and R. Taylor. "On the modularity of elliptic curves over Q." *J. of the AMS* **14** (2001), 843–939.

[Cohen 94] H. Cohen. *A course in computational algebraic number theory.* Graduate Texts in Mathematics, 138, Springer-Verlag, New York, 1994.

[Cremona 97] J. E Cremona. *Algorithms for modular elliptic curves.* Second edition. Cambridge University Press, Cambridge, UK, 1997.

[Darmon 98] H. Darmon. "Stark-Heegner points over real quadratic fields." Number theory (Tiruchirapalli, 1996), pp. 41–69, In *Contemp. Math.*, 210, Amer. Math. Soc., Providence, RI, 1998.

[Darmon 02] H. Darmon, "Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications", *Ann. of Math.* **154** (2001), 589–639.

[de Shalit 95] E. de Shalit. "p-adic periods and modular symbols of elliptic curves of prime conductor." *Invent. Math.* **121**:2 (1995), 225–255.

[Edixhoven 91] B. Edixhoven. "On the Manin constants of modular elliptic curves." In *Arithmetic algebraic geometry (Texel, 1989)*, pp. 25–39, Progr. Math., 89, Birkhäuser Boston, Boston, MA, 1991.

[Greenberg and Stevens 93] R. Greenberg and G. Stevens. "p-adic L-functions and p-adic periods of modular forms." *Invent. Math.* **111**:2 (1993), 407–447.

[Gross and Zagier 86] B.H. Gross, D.B. Zagier. "Heegner points and derivatives of L-series." *Invent. Math.* **84**:2 (1986), 225–320.

[Mazur and Tate 87] B. Mazur and J. Tate. "Refined conjectures of the 'Birch and Swinnerton-Dyer type'." *Duke Math. J.* **54**:2 (1987), 711–750.

[Mazur et al. 86] B. Mazur, J. Tate, and J. Teitelbaum. "On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer." *Invent. Math.* **84**:1 (1986), 1–48.

[Silverman 86] J.H. Silverman. *The arithmetic of elliptic curves.* Corrected reprint of the 1986 original. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.

[Taylor and Wiles 95] R. Taylor, A. Wiles, "Ring theoretic properties of certain Hecke algebras," *Ann. of Math. (2)* **141**:3 (1995), 553–572.

[Wiles 95] A. Wiles, "Modular elliptic curves and Fermat's Last Theorem." *Ann. of Math. (2)* **141**:3 (1995), 443–551.

[Zagier 85] D. Zagier. *Modular points, modular curves, modular surfaces and modular forms.* Workshop Bonn 1984 (Bonn, 1984), Lecture Notes in Math., 1111, pp. 225–248, Springer Verlag, Berlin, 1985.

Henri Darmon, Department of Mathematics, McGill University, Montreal, Quebec, Canada H3A 2K6
(darmon@math.mcgill.ca)

Peter Green, Department of Mathematics, Harvard University, Cambridge, MA 02138
(green@math.harvard.edu)

Received March 28, 2001; accepted in revised form January 11, 2002.