Stark-Heegner points over real quadratic fields

H. Darmon

September 9, 2007

Acknowledgements: This research was partially supported by grants from NSERC and FCAR, and was carried out while the author was a member of CICMA. The article itself was written during a stay at the Mathematical Sciences Research Institute in Berkeley. It is a pleasure to thank Massimo Bertolini for the stimulating collaboration which inspired this work.

Abstract: Motivated by the conjectures of "Mazur-Tate-Teitelbaum type" formulated in [BD1] and by the main result of [BD3], we describe a conjectural construction of a global point $P_K \in E(K)$, where E is a (modular) elliptic curve over $\mathbf{Q}$ of prime conductor p, and K is a real quadratic field satisfying suitable conditions. The point P_K is constructed by applying the Tate p-adic uniformization of E to an explicit expression involving geodesic cycles on the modular curve $X_0(p)$. These geodesic cycles are a natural generalization of the modular symbols of Birch and Manin, and interpolate the special values of the Hasse-Weil L-function of E/K twisted by certain abelian characters of K. In the analogy between Heegner points and circular units, the point P_K is analogous to a Stark unit, since it has a purely conjectural definition in terms of special values of L-functions, but no natural "independent" construction of it seems to be known. We call the conjectural point P_K a "Stark-Heegner point" to emphasize this analogy.

The conjectures of section 4 are inspired by the main result of [BD3], in which the real quadratic field is replaced by an imaginary quadratic field. The methods of [BD3], which rely crucially on the theory of complex multiplication and on the Cerednik-Drinfeld theory of p-adic uniformization of Shimura curves, do not seem to extend to the real quadratic situation. One must therefore content oneself with numerical evidence for the conjectures. This evidence is summarized in the last section.

1 Some motivation: Pell's equation

Mention of the so-called Pell's equation

$$x^2 - Dy^2 = 1 \qquad (D \in \mathbf{Z}, \quad D > 0)$$

can already be found in a 7th century manuscript of the Indian mathematician and astronomer Brahmagupta. (Cf. [We], I.IX.) In spite of its venerable age, Pell's equation has lost none of its fascination, and continues to be a wellspring for the most profound questions in number theory.

Here are three methods for tackling Pell's equation, arranged in increasing order of sophistication and generality:

1. The continued fraction method ([We], [HW])
Appearing in manuscripts of Jayadeva and Bhāskara dating back to the 11th and 12th centuries (and rediscovered independently much later by Fermat), it is one of the great contributions of Indian mathematics and civilization ([We], I.IX).

2. The circular unit method ([Ma], [Was])
Suppose for simplicity that $D \equiv 1 \pmod 4$ is square-free, and let $\chi_D(n) = \left(\frac{n}{D}\right)$ be the quadratic Dirichlet character. The following theorem of Gauss, intimately connected with quadratic reciprocity, is the basis for the circular unit method.

Theorem 1.1 *Every quadratic field is contained in a cyclotomic field generated by roots of unity. More precisely, the quadratic field $\mathbf{Q}(\sqrt{D})$ is contained in $\mathbf{Q}(\zeta_D)$, where ζ_D is a primitive D-th root of unity, and the homomorphism of Galois theory*

$$Gal(\mathbf{Q}(\zeta_D)/\mathbf{Q}) = (\mathbf{Z}/D\mathbf{Z})^\times \longrightarrow Gal(\mathbf{Q}(\sqrt{D})/\mathbf{Q}) = \pm 1$$

is identified with the Dirichlet character χ_D.

The importance of theorem 1.1 (for our discussion) lies in the fact that the cyclotomic field $\mathbf{Q}(\zeta_D)$ is equipped with certain natural units, the so-called *circular units*. These are algebraic integers of the form $(1 - \zeta_D^a)$ if D is not prime, and of the form $\frac{1-\zeta_D^a}{1-\zeta_D}$ if D is prime, with $a \in (\mathbf{Z}/D\mathbf{Z})^\times$. In particular, theorem 1.1 implies that the expression

$$u_D = \prod_{a=1}^{D} (1 - \zeta_D^a)^{\chi_D(a)}$$

is an element of norm 1 in the quadratic field $\mathbf{Q}(\sqrt{D})$, and in fact, in its ring of integers. This unit u_D can be used to write down an explicit solution to Pell's equation in terms of values of trigonometric functions evaluated at rational arguments.

The circular unit method appears less efficient than the continued fraction approach. Its main interest is theoretical and aesthetic (cf. the introduction of [Ma]), and also lies in its *greater generality*. For theorem 1.1 has a natural generalization, the Kronecker-Weber Theorem:

Theorem 1.2 *If K is any abelian extension of the rationals, then it is contained in a cyclotomic field $\mathbf{Q}(\zeta)$ generated by a root of unity ζ.*

Thanks to this theorem, one can construct a subgroup of the unit group of K, when K is any abelian extension of $\mathbf{Q}$, by taking the norms of circular units to K. It turns out that this subgroup is always of finite index. So the circular unit method for solving Pell's equation generalizes to a procedure for finding the unit group of an arbitrary *abelian* extension of the rationals.

3. The L-function method ([Ta], [St])
Let

$$\zeta_K(s) = \sum_{\mathcal{A}} \mathbf{N}(\mathcal{A})^{-s}, \qquad (\mathrm{Re}(s) > 1)$$

where the sum is taken over all the integral ideals of K, be the Dedekind zeta-function of the real quadratic field K. It can be shown that this function has a meromorphic continuation to the entire complex plane, and a functional equation relating its values at s and $1 - s$. The third method is based on the analytic class number formula of Dirichlet, which we state here for the special case of $\zeta_K(s)$.

Theorem 1.3 *The zeta-function $\zeta_K(s)$ has a simple zero at $s = 0$, and*

$$\zeta_K'(0) = 2h \log |u|,$$

where h is the class number of K and u is a fundamental unit in the real quadratic field K.

In particular, the expression

$$e^{\zeta_K'(0)}$$

yields a unit of K, and hence a (non-trivial) solution to Pell's equation.

From a practical and computational point of view, this third method turns out to be not very different from the second. Indeed, theorem 1.1 implies that $\zeta_K(s) = \zeta(s)L(s, \chi_D)$, and one has (cf. [Ta])

$$\zeta'_K(0) = \zeta(0)L'(0, \chi_D) = \log(\prod_{a=1}^{D}(1 - \zeta_D^a)^{\chi_D(a)}), \tag{1}$$

so that $e^{\zeta'_K(0)} = u_D^2$, where u_D is the unit constructed from circular units following the second method.

What is important here is the change in point of view: the analytic class number formula of theorem 1.3 generalizes to an *arbitrary* number field K. In particular, when $\zeta_K(0) = 0$, the identity

$$\zeta'_K(0) = \log|u|,$$

for *some* unit u of K (not necessarily non-trivial!) continues to hold. When $\zeta_K(s)$ has a simple zero at $s = 0$, this identity gives an analytic construction of a non-trivial unit in K from special values of the Dedekind zeta-function.

Unfortunately, the only number fields for which ζ_K has a simple zero at $s = 0$ are the fields with exactly two infinite places, i.e., the real quadratic fields, the cubic fields with one real and one complex place, and the quartic fields with two complex places. This class does not even include the abelian extensions covered by the second method.

To make the method more flexible, one can enlarge the class of L-functions to include the Artin L-functions associated to irreducible representations of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. More precisely, let $\tilde{K}$ be the Galois closure of K, let G denote its Galois group, and let $H = \mathrm{Gal}(\tilde{K}/K) \subset G$. Finally, let $\rho = \mathrm{Ind}_H^G(\mathbf{1})$ be the induced representation. Then the Dedekind zeta-function $\zeta_K(s)$ is equal to the Artin L-function $L(s, \rho)$, which factorizes as a product of Artin L-series:

$$\zeta_K(s) = L(s, \rho) = \prod_i L(s, \rho_i)^{m_i}.$$

where $\sum_i m_i\rho_i$ is the decomposition of ρ as a direct sum of irreducible representations. Stark has conjectured ([St], see also [Ta]) that the leading terms of each of the factors on the right can be written down explicitely in terms of arithmetic invariants attached to K. In particular, when $L(0, \rho_i) = 0$, the first derivative $L'(0, \rho_i)$ should be expressed as an explicit combination of

logarithms of units of K. In this way, one can hope to recover a unit of K from the values of $L'(0, \rho_i)$ when they are non-zero.

When K is abelian over $\mathbf{Q}$, the Artin L-series that appear in the factorization of $\zeta_K(s)$ are attached to one-dimensional characters of K, and are equal to Dirichlet L-series $L(s, \chi)$ by theorem 1.2 (Kronecker Weber). An explicit evaluation (cf. [Ta]) shows that when $L(0, \chi) = 0$, the derivative $L'(0, \chi)$ is expressed in terms of the circular units of the second method, by a formula which directly generalizes equation (1).

In general, if an irreducible representation ρ is not one-dimensional, it cuts out a non-abelian extension $K(\rho)$ of $\mathbf{Q}$, and Stark's conjecture provides a more general framework (albeit one which is *conjectural* in general) for finding units in $K(\rho)$ when $L(s, \rho)$ has a simple zero at $s = 0$. For a recent example where Stark's conjecture is used to compute the units in specific ray class fields of certain totally real cubic fields, see [DST].

2 Elliptic curves over Q

Let $E/\mathbf{Q}$ be an elliptic curve over the rationals of conductor N, given by the projective equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3. \tag{2}$$

By the Mordell-Weil theorem, the Mordell-Weil group $E(\mathbf{Q})$ is a finitely generated abelian group,

$$E(\mathbf{Q}) \simeq \mathbf{Z}^r \oplus T,$$

where T is the finite torsion subgroup of $E(\mathbf{Q})$. As has been known for a long time (see for example [Ma]), there is a resonance between Pell's equation and the study of rational points on elliptic curves. In particular, each of the three methods outlined in section 1 for tackling Pell's equation has an analogue in the realm of elliptic curves.

1. The method of descent ([Si1], [Ca])
When Fermat, unaware of the Indian contributions, rediscovered the continued fraction method for solving Pell's equation, he viewed it as a "positive" application of his general method of descent, which he had used until then only to prove that certain Diophantine equations had no solutions. Unlike the continued fraction method, the descent method for computing $E(\mathbf{Q})$ is

not known to give an algorithm in general for finding $E(\mathbf{Q})$, i.e., to always terminate. Such a statement would follow if one knew that the Shafarevich-Tate group $Ш(E/\mathbf{Q})$ (or, even just $Ш(E/\mathbf{Q}) \otimes \mathbf{Z}_\ell$, for some prime ℓ which can be effectively determined) is finite.

2. The Heegner point method ([El], [Gr1], [Za])

If N is a positive integer, let $X_0(N)$ denote the *modular curve* which is the (coarse) moduli space of elliptic curves equipped with a rational subgroup of order N. This curve admits a model over the rationals.

The Heegner point method relies crucially on Wiles' theorem, formerly known as the Shimura-Taniyama conjecture. We state it here in a strong form which follows from combining the works of [Wi], [TW], and [Di].

Theorem 2.1 *Suppose that E is an elliptic curve over the rationals, having semistable reduction at 3 and 5. Then E is modular, i.e., there is a non-constant morphism*

$$\phi_E : X_0(N) \longrightarrow E$$

defined over $\mathbf{Q}$.

Remarks:

1. The reader should note the direct analogy between theorem 2.1 and the more classical theorem 1.1. The latter is intimately connect with abelian reciprocity laws, while the former is a manifestation of a (non-abelian) reciprocity law for $\mathbf{GL_2}$.
2. Theorem 2.1 is in fact somewhat weaker than the original conjecture, which is formulated without the technical assumption of semi-stability at 3 and 5. For the rest of this paper, we will assume that E satisfies the conclusion of theorem 2.1.
3. It is customary to normalize ϕ_E so that it sends the cusp $i\infty$ on $X_0(N)$ to the identity on E, and so that the map $\phi_{E*} : J_0(N) \longrightarrow E$ induced on jacobians by covariant functoriality has connected kernel. This can always be achieved, possibly after replacing E by a curve in the same rational isogeny class.

In the same way that the cyclotomic fields $\mathbf{Q}(\zeta_D)$ are equipped with circular units, the modular curves are endowed with an explicit set of algebraic points, the so-called Heegner points. More precisely, let K be an imaginary quadratic field satisfying

$$\text{All primes } \ell | N \text{ are split in } K/\mathbf{Q}. \tag{3}$$

Let $\mathcal{O}_K$ be the ring of integers of K, and let A be an elliptic curve satisfying $\mathrm{End}(A) \simeq \mathcal{O}_K$. (One says that A has *complex multiplication* by $\mathcal{O}_K$.) By the theory of complex multiplication, the curve A can be defined over the Hilbert class field H of K. The technical assumption (3) implies that A has a cyclic subgroup C of order N which is also defined over H. The pair (A, C) gives rise to a point $\alpha_H \in X_0(N)(H)$. Let $P_H = \phi_E(\alpha_H) \in E(H)$, where ϕ_E is the modular parametrization of theorem 2.1. Let $P_K := \mathrm{trace}_{H/K}(P_H)$ be the trace of P_H to $E(K)$.

Unlike the solution to Pell's equation constructed from circular units, the point P_K may be trivial, so that the Heegner point method for finding a rational point in $E(K)$ does not always succeed. But (just like with circular units, cf. equation (1)), the non-triviality of the point P_K can be related to the non-vanishing of certain L-function values. More precisely, let $L(E/K, s)$ be the Hasse-Weil L-function of E over K. Thanks to theorem 2.1, it is known to have an analytic continuation and a functional equation relating its values at s and $2 - s$. (For $L(E/\mathbf{Q}, s)$, this follows from Hecke's theory. For $L(E/K, s)$, it can be proved either by exploiting the factorization $L(E/K, s) = L(E/\mathbf{Q}, s)L(E^{(K)}/\mathbf{Q}, s)$, where $E^{(K)}$ is the twist of E over K, or by using Rankin's method, as in [GZ].)

The sign in this functional equation can be written down explicitly as a product of local signs. Assumption (3) forces the sign in the functional equation of $L(E/K, s)$ to be -1, so that $L(E/K, 1) = 0$ (cf. [GZ], p. 71). Let $\Omega_{E/K} := \int_{E(\mathbf{C})} \omega \wedge i\bar{\omega}/\sqrt{d_K}$, where ω is a Néron differential on $E/\mathbf{Q}$ and d_K is the discriminant of K. The following result of Gross and Zagier [GZ] can be viewed as an elliptic curve analogue of equation (1).

Theorem 2.2 *There is an explicit non-zero rational number $\alpha \in \mathbf{Q}^\times$ such that*

$$L'(E/K, 1) = \alpha \Omega_{E/K} \langle P_K, P_K \rangle,$$

where $\langle\ ,\ \rangle$ is the Néron-Tate canonical height on $E(K)$. In particular, the point P_K is of infinite order if and only if $L'(E/K, 1) \neq 0$.

A result of Kolyvagin shows that if P_K is of infinite order, then $E(K)$ has rank one. Conversely, it is expected (and it follows from the Birch and Swinnerton-Dyer conjecture) that the Heegner point method works precisely in this "rank one" situation.

3. The L-function method?

By analogy with the zeta-function method for solving Pell's equation, one might ask for a method of computing a rational point in $E(\mathbf{Q})$ from the special values of the Hasse-Weil L-function $L(E/\mathbf{Q}, s)$. The analogue of Dirichlet's analytic class number formula in this context is the Birch and Swinnerton-Dyer conjecture, which relates the arithmetic behaviour of $E/\mathbf{Q}$ to the analytic properties of $L(E/\mathbf{Q}, s)$ in the neighbourhood of $s = 1$. Recall that r is the rank of the Mordell-Weil group $E(\mathbf{Q})$, and that T is its finite torsion subgroup.

Conjecture 2.3 *The Hasse-Weil L-function $L(E/\mathbf{Q}, s)$ vanishes to order r at $s = 1$, and*

$$L^{(r)}(E/\mathbf{Q}, s) = \#Ш(E/\mathbf{Q}) \left(\det\left(\langle P_i, P_j\rangle\right)_{1\le i,j\le r}\right) \#T^{-2} \left(\int_{E(\mathbf{R})} \omega\right) \prod_p m_p,$$

where $Ш(E/\mathbf{Q})$ is the (conjecturally finite) Shafarevich-Tate group of $E/\mathbf{Q}$, the points $P_1, \ldots, P_r$ are a basis for $E(\mathbf{Q})$ modulo torsion, $\langle\ ,\ \rangle$ is the Néron-Tate canonical height, ω is the Néron differential on E, and m_p is the number of connected components in the Néron model of $E/\mathbf{Q}_p$.

In particular, if $L(E/\mathbf{Q}, s)$ has a simple zero at $s = 1$, then conjecture 2.3 predicts that $E(\mathbf{Q})$ has rank 1 and that

$$L'(E/\mathbf{Q}, 1) = \#T^{-2} \left(\int_{E(\mathbf{R})} \omega\right) \prod_p m_p \langle P, P\rangle,$$

where $P = \sqrt{\#Ш(E/\mathbf{Q})}P_0$, and P_0 is a generator for $E(\mathbf{Q})$ modulo torsion. This formula allows one to compute the Néron-Tate canonical height $h(P) = \langle P, P\rangle$ of a point $P \in E(\mathbf{Q})$ from the special value $L'(E/\mathbf{Q}, 1)$.

In [Si2], Silverman explains how the a priori knowledge of $h(P)$ can be used to assist in the calculation of P itself. Silverman's method seems quite efficient computationally – in all likelihood, alot more so than the p-adic methods we are about to describe. Still, there is no simple analytic function, analogous to the exponential in the case of Pell's equation, which would reconstruct the point P directly from $h(P)$. From this point of view the analogy with method 3 of section 1 seems to break down somewhat.

It turns out that the analogy can be pushed in another direction if one replaces the classical L-function by a p-adic avatar. Such a phenomenon

was first discovered by Karl Rubin [Ru] for elliptic curves with complex multiplication. More precisely, if E is such a curve, Rubin showed (building on the formula of Gross-Zagier and on Perrin-Riou's p-adic analogue [PR]) that a global point in $E(\mathbf{Q})$ can be obtained by applying the exponential map in the formal group of $E/\mathbf{Q}_p$ to the first derivative of a certain two-variable p-adic L-function of E (which in this case interpolates the special values of a Hecke L-series with Grossencharacter).

More recently, the article [BD3] described a construction of a global point $P_K \in E(K)$ from the first derivative of a p-adic L-function, in the case when E is a (modular) elliptic curve over $\mathbf{Q}$ having a prime p of multiplicative reduction, and K is a quadratic imaginary field in which p is inert. In this formula, the role of the exponential map is played by the Tate uniformization:

$$\Phi_{\text{Tate}} : K_p^\times \longrightarrow E(K_p),$$

(where $K_p = K \otimes \mathbf{Q}_p$ is the completion of K at p). The next section recalls the formula of [BD3].

3 p-adic L-functions and rational points

Assume as before that E is a (modular) elliptic curve of conductor N. Let K be a quadratic imaginary field of discriminant D relatively prime to N. Furthermore, suppose that

1. The curve E has good or multiplicative reduction at all primes which are inert in $K/\mathbf{Q}$.

2. There is at least one prime, p, which is inert in K and for which E has multiplicative reduction.

3. The sign in the functional equation for $L(E/K, s)$ is -1.

Write $N = N^+N^-p$, where N^+, resp. N^- is divisible only by primes which are split, resp. inert in K. Note that by assumptions 1 and 2, N^- is square-free and not divisible by p.

Let H be the Hilbert class field of K, and let H_n the ring class field of conductor p^n. We write $H_\infty = \bigcup H_n$, and set

$$G_n := \text{Gal}(H_n/H), \quad \tilde{G}_n := \text{Gal}(H_n/K),$$

$$G_\infty := \mathrm{Gal}(H_\infty/H), \quad \tilde{G}_\infty := \mathrm{Gal}(H_\infty/K), \quad \Delta := \mathrm{Gal}(H/K).$$

There is an exact sequence of Galois groups

$$0 \longrightarrow G_\infty \longrightarrow \tilde{G}_\infty \longrightarrow \Delta \longrightarrow 0,$$

and, by class field theory, G_∞ is canonically isomorphic to $K_p^\times/\mathbf{Q}_p^\times$, which can be identified with the group $(K_p)_1^\times$ of elements of norm 1 in $K_p^\times$ (by sending z to $\frac{z}{\bar{z}}$). The completed integral group rings $\mathbf{Z}[\![G_\infty]\!]$ and $\mathbf{Z}[\![\tilde{G}_\infty]\!]$ are defined as the inverse limits of the integral group rings $\mathbf{Z}[G_n]$ and $\mathbf{Z}[\tilde{G}_n]$ under the natural projection maps.

Let

$$\Omega_E := \iint_{E(\mathbf{C})} \omega \wedge i\bar{\omega}$$

be the complex period (or Parshin-Faltings height) of E, where ω is a Néron differential on E. Write d for the discriminant of the order $\mathcal{O}$ of conductor c and u for one half the order of the group of units of $\mathcal{O}$.

Theorem 3.1 *There exists an element $\mathcal{L}_p(E/K) \in \mathbf{Z}[\![\tilde{G}_\infty]\!]$ such that*

$$|\chi(\mathcal{L}_p(E/K))|^2 = \frac{L(E/K,\chi,1)}{\Omega_E}\sqrt{d}\cdot u^2,$$

for all finite order characters χ of $\tilde{G}_\infty$.

Remark. The interpolation property of theorem 3.1 determines $\mathcal{L}_p(E/K)$ uniquely, up to right multiplication by elements in $\tilde{G}_\infty$, if it exists. The existence amounts to a statement of rationality and integrality for the special values $L(E/K,\chi,1)$. The construction of $\mathcal{L}_p(E/K)$, which is based on work of Gross [Gr2] and Daghigh [Dag], is explained in chapter 2 of [BD3].

If χ is the trivial character (or, more generally, any character of $\tilde{G}_\infty$ which is unramified at p, i.e., factors through Δ) then the interpolation property of theorem 3.1 implies that

$$\chi(\mathcal{L}_p(E/K)) = 0. \tag{4}$$

In particular, $\mathcal{L}_p(E/K)$ belongs to the augmentation ideal $\tilde{I}$ of $\mathbf{Z}[\![\tilde{G}_\infty]\!]$. Let $\mathcal{L}'_p(E/K)$ denote the image of $\mathcal{L}_p(E/K)$ in $\tilde{I}/\tilde{I}^2 = \tilde{G}_\infty$. The reader should view $\mathcal{L}'_p(E/K) \in \tilde{G}_\infty$ as the first derivative of $\mathcal{L}_p(E/K)$ evaluated at the central point.

Lemma 3.2 *The element $\mathcal{L}_p'(E/K)$ belongs to $G_\infty \subset \tilde{G}_\infty$.*

Proof: Formula (4) implies that $\mathcal{L}_p(E/K)$ belongs to the kernel of the natural projection $\mathbf{Z}[\![\tilde{G}_\infty]\!] \longrightarrow \mathbf{Z}[\Delta]$. This implies that $\mathcal{L}_p'(E/K)$ belongs to the kernel of the map $\tilde{G}_\infty \longrightarrow \Delta$.

Thanks to lemma 3.2, the element $\mathcal{L}_p'(E/K)$ can (and will) be viewed as an element of $K_p^\times$ of norm 1.

The main formula of [BD3] is:

Theorem 3.3 *The local point $\Phi_{\mathrm{Tate}}(\mathcal{L}_p'(E/K)) \in E(K_p)$ is a global point in $E(K)$.*

Crucial to the proof of theorem 3.3 is the fact that the global point P_K constructed from special values of L-functions has an *alternate construction*. This construction relies on two basic ingredients: the theory of complex multiplication, and the Cerednik-Drinfeld theory of p-adic uniformization of Shimura curves associated to indefinite quaternion algebras.

Before making this more precise, we record the following lemma:

Lemma 3.4 *The integer N^- is the product of an odd number of primes.*

Proof: By page 71 of [GZ], the sign in the functional equation of the complex L-function $L(E/K, s)$ is $(-1)^{\#\{\ell | N^- p\}+1}$. The result follows.

Let B be the indefinite quaternion algebra which is ramified exactly at the primes dividing pN^-. Such a B exists, by Hilbert's reciprocity law and lemma 3.4. Choose a maximal order R in B, and an Eichler order $R(N^+) \subset R$ of level N^+, defined as in [BD3]. Let Γ be the subgroup of $R(N^+)^\times$ of elements of reduced norm 1. By fixing an embedding of $B \otimes \mathbf{R}$ into $M_2(\mathbf{R})$, the group Γ acts on the standard complex upper half plane by Mobius transformations. The complex-analytic quotient $X = \mathcal{H}/\Gamma$ is a complex model for a curve X. Shimura showed that X has a model over $\mathbf{Q}$ by identifying it with a (coarse) moduli space for polarized abelian surfaces with endomorphisms by R and an appropriate level N^+ structure. For details, see [Ro] or [BD1] for example.

The curve X is endowed with a set of *Heegner points* corresponding to quaternionic surfaces A with complex multiplication by the maximal order $\mathcal{O}_K$ of K. (By complex multiplication by $\mathcal{O}_K$, one means that the ring of endomorphisms of A which commute with the quaternionic multiplications and respect the level N^+-structure is isomorphic to $\mathcal{O}_K$.) These points are

defined over the Hilbert class field H of K, and are permuted transitively by the group $\mathrm{Gal}(H/K) \times W$, where W is the group of exponent 2 generated by all the Atkin-Lehner involutions on X (cf. [BD1]). Let $\alpha_1, \ldots, \alpha_h$ ($h = [H : K]$) be a $\mathrm{Gal}(H/K)$-orbit of Heegner points, and let $\alpha'_j = w_{N/p}\alpha_j$, where $w_{N/p}$ is the product of the Atkin-Lehner involutions w_ℓ over all primes $\ell | N/p$. Note that $\alpha'_1, \ldots, \alpha'_h$ is another $\mathrm{Gal}(H/K)$-orbit of Heegner points, so that the effective divisor $(\alpha'_1) + \cdots + (\alpha'_h)$ is K-rational.

The Jacobian J of X is an abelian variety over $\mathbf{Q}$. By a theorem of Jacquet-Langlands [JL], it is isogenous to the quotient of $J_0(N^+N^-p)$ corresponding to cusp forms which are new at N^-p. Hence, the modularity of E (theorem 2.1) implies the existence of a generically surjective map

$$\phi_E : J \longrightarrow E.$$

The degree 0 divisor on X:

$$D = (\alpha_1) + \cdots + (\alpha_h) - (\alpha'_1) - \cdots - (\alpha'_h) \tag{5}$$

is defined over K, and hence gives rise to a canonical "Heegner element" in $J(K)$, which depends on the choice of the α_i only up to the action of the Atkin-Lehner involutions. Let

$$P_K = \phi_E(D) \in E(K)$$

be its image in $E(K)$. Note that P_K depends only up to sign on the choice of the K-rational effective divisor $(\alpha_1) + \cdots + (\alpha_h)$.

The more precise form of theorem 3.3 proved in [BD3] states that the local point $\Phi_{\mathrm{Tate}}(\mathcal{L}'_p(E/K))$ is equal to the global point P_K, up to a sign and a simple fudge factor. The proof exploits a p-adic analytic construction of P_K supplied by the Cerednik-Drinfeld theory of p-adic uniformization of X. For more details, see [BD3].

Again, the formula relating P_K to $\mathcal{L}'_p(E/K)$ is analogous to formula (1) expressing circular units in terms of derivatives of abelian L-series. Circular units (and, in our situation, Heegner points on Shimura curves) lead to examples of what Kolyvagin has called an "Euler system". When they can be constructed, such Euler systems provide powerful insights into the associated L-function values. However, there are many instances where no Euler system is known to exist. The units defined conjecturally from derivatives

of non-abelian Artin L-functions – whose construction would supply a key to the Stark conjectures – are a case in point. Motivated by the discussion in section 1, one might ask whether the (p-adic) L-function methods of the present section suggest (conjectural) constructions of global points on elliptic curves, in situations where there is no (known) Euler system construction. Or, put more succintly: "Are there Stark-Heegner points"?

The remainder of this article describes a fragment of experimental mathematics suggesting that the answer to this question is "yes".

4 A real quadratic analogue

We will restrict ourselves for simplicity to the case where the elliptic curve E has prime conductor $N = p$. This simplifying assumption allows us, in particular, to avoid Shimura curves and formulate our construction entirely within the setting of classical modular curves – a luxury which was not available to us in section 3.

Let K be a real quadratic field in which p is inert. (This corresponds to assumptions 1 and 2 of section 3.) Let $L(E/K, s)$ be the Hasse-Weil L-function for E/K.

Lemma 4.1 *If $N = p$ is inert in K, then the sign in the functional equation for $L(E/K, s)$ is -1.*

In particular, $L(E/K, 1) = 0$, and the conjecture of Birch and Swinnerton-Dyer leads us to expect that $E(K)$ is infinite. We will now describe a conjectural method for constructing a global point $P_K \in E(K)$ (or rather, a p-adic approximation of it) using modular symbols and Tate's p-adic analytic theory. We caution the reader that, just as with all the methods covered previously, we expect that this method yields a non-trivial global point precisely when $E(K)$ has rank 1.

4.1 Modular symbols

Let $\mathcal{O}_K = \mathbf{Z}[\omega]$ be the ring of integers of K. An order in K is a subring of K which is finitely generated as a $\mathbf{Z}$-module. Every order in K is contained in $\mathcal{O}_K$, and is of the form $\mathbf{Z}[c\omega]$, for a (unique) positive integer c, called the *conductor* of the order.

A *lattice* in K is a $\mathbf{Z}$-submodule of K which is free of rank 2. If I is any lattice, the set of elements

$$\mathrm{End}(I) := \{x \in K | xI \subset I\}$$

is an order in $\mathcal{O}_K$, which we also call the *order associated to* I. By abuse of notation, we will sometimes say that a lattice has conductor c if its associated order is of conductor c.

Let c be an integer which is prime to p, and let I be a lattice of conductor cp^n with $n \geq 1$.

Lemma 4.2 *There is a unique sublattice $I_0 \subset I$ contained in I with index p having conductor cp^{n-1}.*

Proof: Let $\mathbf{P}_1(I)$ be the set of all index p sublattices of I. It is in bijection with $\mathbf{P}_1(\mathbf{F}_p)$ and hence has cardinality $p+1$. If $\mathcal{O} = \mathrm{End}(I)$ is the order associated to I, then we have (non-canonical) isomorphisms of groups:

$$(\mathcal{O}/p\mathcal{O})^\times/\mathbf{F}_p^\times \simeq (\mathbf{F}_p[\epsilon]/(\epsilon^2))^\times/\mathbf{F}_p^\times \simeq \mathbf{Z}/p\mathbf{Z}.$$

The first isomorphism sends $a + bcp^n\omega$ $(a, b \in \mathbf{Z})$ to $a + b\epsilon$, and the second isomorphism sends $a + b\epsilon \in \mathbf{F}_p[\epsilon]^\times$ to b/a. The group $(\mathcal{O}/p\mathcal{O})^\times/\mathbf{F}_p^\times$ acts on $\mathbf{P}_1(I)$ in the natural way, and has exactly one fixed point. This fixed point corresponds to the sublattice I_0. The p remaining sublattices have conductor cp^{n+1}.

Choose a real embedding of K, and say that an element of K is positive (resp. negative) if its image by this embedding is positive (resp. negative).

Definition 4.3 *A basis ω_1, ω_2 for $K/\mathbf{Q}$ is called* positive *if*

$$\det \begin{pmatrix} \omega_1 & \omega_2 \\ \bar{\omega}_1 & \bar{\omega}_2 \end{pmatrix} > 0.$$

Now, choose a $\mathbf{Z}$-basis (ω_1, ω_2) for I satisfying

1. ω_1 belongs to I_0.

2. The basis (ω_1, ω_2) is positive.

Note that I_0 is the set of elements in I of the form $a\omega_1 + b\omega_2$ with $p|b$. Let now u be any unit in $\mathcal{O}^\times$ of norm 1. Multiplication by u gives an endomorphism

of I. Since the sublattice I_0 is stable under this endomorphism (indeed, it is stable under multiplication by the order of conductor cp^{n-1}) it follows that the matrix describing the multiplication by u in the basis (ω_1, ω_2) belongs to $\Gamma_0(p)$. Let $m_u(I)$ denote this matrix.

Lemma 4.4 *The matrix $m_u(I)$ is well-defined up to conjugation in $\Gamma_0(p)$.*

Proof: Any two choices of bases for I satisfying the conditions 1 and 2 above differ by an element of $\Gamma_0(p)$.

Two lattices I and J are said to be *equivalent* if there exists an element $\alpha \in K^\times$ of positive norm such that

$$J = \alpha I.$$

Of course, equivalent lattices have the same associated order. Furthermore:

Lemma 4.5 *If I and J are equivalent, then the matrices $m_u(I)$ and $m_u(J)$ are conjugate in $\Gamma_0(p)$.*

Proof: If (ω_1, ω_2) is a basis for I satisfying conditions 1 and 2 above, and $J = \alpha I$, then $(\alpha\omega_1, \alpha\omega_2)$ is a basis for J satisfying the same conditions. Relative to these bases, the matrices expressing the multiplication by u are in fact equal. The lemma follows.

An element of $\Gamma = \Gamma_0(p)$ (well-defined up to conjugation) gives rise in the usual way to a class in the integral homology $H_1(X_0(p), \mathbf{Z})$ which is a quotient (by the torsion and parabolic elements) of the commutator factor group $\Gamma/[\Gamma, \Gamma]$. Let $\mathrm{Pic}(\mathcal{O})$ be the set of equivalence classes of lattices of conductor cp^n. The map m_u sets up an assignment, which we denote by γ_u to emphasize the dependence on u:

$$\gamma_u : \mathrm{Pic}(\mathcal{O}) \longrightarrow H_1(X_0(p), \mathbf{Z}).$$

Definition 4.6 *We call $\gamma_u(I)$ the* modular symbol *attached to the lattice I of conductor cp^n ($n \geq 1$) and to the unit $u \in \mathcal{O}^\times$.*

Remarks:
1. To an equivalence class of lattices I of conductor cp^n one can associate the primitive binary quadratic form of discriminant $\mathrm{Disc}(K)c^2p^{2n}$

$$F(x, y) = \mathrm{norm}(x\omega_1 + y\omega_2)g^{-1} = Ax^2 + Bxy + Cy^2,$$

where ω_1, ω_2 is a basis for I chosen as above and g is the unique rational number such that $A, B, C \in \mathbf{Z}$ and $\gcd(A, B, C) = 1$. Note that $p^2|A$ and $p|B$. The roots of the polynomial $F(X, 1)$ are two elements of $K \subset \mathbf{R}$ which are Galois conjugate. Consider the geodesic in the Poincaré upper half plane which joins these two roots on the real line. This geodesic maps to an infinitely repeating periodic path on $X_0(p)$. If u is a fundamental unit of norm 1 in $\mathcal{O}^\times$, then the element $\gamma_u(I)$ is the basic period in this cycle, viewed as a homology class of $X_0(p)$. For this reason, it is sometimes called the *geodesic cycle* on $X_0(p)$ associated to the binary quadratic form $F(x, y)$.

2. Like the modular symbols of Birch and Manin, the geodesic cycles on $X_0(p)$ encode special values of L-functions. More precisely, they interpolate the special values of $L(E/K, s)$ at $s = 1$, twisted by ring class characters of K of conductor dividing cp^n. They can be used, just as in [MT], to construct "theta-elements" which are adèlic analogues "at finite level" of the more familiar p-adic L-functions. This point of view, which forms the basis for the present article, is developped in [Dar].

3. In the same way that the modular symbols of Birch and Manin are calculated efficiently by computing the continued fraction expansion of certain rational numbers, the geodesic cycles attached to a binary quadratic form can be calculated from the (periodic) continued fraction expansion of certain real quadratic irrationalities.

4.2 The tree associated to a lattice

In this subsection, let I be a sublattice of conductor c prime to p, and let $\mathcal{O} = \mathrm{End}(I)$ be its associated order. Let $\mathcal{T}(I)$ be the graph whose vertices correspond to homothety classes of sublattices of I which are contained in I with index p^n for some n. The edges of $\mathcal{T}(I)$ join vertices which correspond to lattices which are contained one inside the other with index p.

The graph $\mathcal{T}(I)$ is a homogenous tree of weight $p + 1$, equipped with a distinguished vertex v_0 which corresponds to the homothety class of I. One defines a distance function on $\mathcal{T}(I)$ in the natural way. If v is a vertex of $\mathcal{T}(I)$ corresponding to a lattice I_v, then the order $\mathrm{End}(I_v)$ has conductor cp^m, where m is the distance from v_0 to v. The vertex v is then said to be of *level* m.

Let

$$G_m = (\mathcal{O}_K \otimes \mathbf{Z}/p^m\mathbf{Z})^\times/(\mathbf{Z}/p^m\mathbf{Z})^\times = (\mathcal{O}_K \otimes \mathbf{Z}/p^m\mathbf{Z})^\times_1,$$

where the isomorphism between these two descriptions sends z to $\frac{z}{\bar{z}}$. The group

$$G_\infty = K_p^\times/\mathbf{Q}_p^\times = (\mathcal{O}_K \otimes \mathbf{Z}_p)^\times/\mathbf{Z}_p^\times \simeq K_{p,1}^\times = \lim_{\leftarrow} G_n$$

acts naturally on $\mathcal{T}(I)$, leaving v_0 fixed and permuting transitively the vertices of a given level m. The isotropy group of a vertex of level m is the group of elements which are congruent to a scalar modulo p^m, and hence, G_m acts simply transitively on the set of vertices of level m.

Let

$$u = a + b\omega \in \mathcal{O}^\times$$

be a unit of norm 1 in $\mathcal{O}^\times$, and let n be the largest integer such that $p^n|b$. The modular symbol γ_u defined in the previous section gives rise to a function (which we denote also by γ_u by abuse of notation) on the set of all vertices of $\mathcal{T}(I)$ satisfying

$$0 < \text{level}(v) \leq n.$$

Extending the domain of definition of γ_u slightly, we define $\gamma_u(v_0) := 0$.

Let v be any vertex of level $m < n$, and let $v_1, \ldots, v_p$ be the p vertices of level $m+1$ which are adjacent to it. Recall the Atkin-Lehner involution w_p which acts on $X_0(p)$ and hence on the homology $H_1(X_0(p), \mathbf{Z})$.

Lemma 4.7 *The function γ_u satisfies the relation*

$$\gamma_u(v_1) + \cdots + \gamma_u(v_p) = -w_p\gamma_u(v).$$

Proof: The homology class

$$\gamma_u(v_1) + \cdots + \gamma_u(v_p) + w_p\gamma_u(v)$$

is in the image of the map $H_1(X_0(1), \mathbf{Z}) \longrightarrow H_1(X_0(p), \mathbf{Z})$ induced by the natural degeneracy maps $X_0(p) \longrightarrow X_0(1)$. Since $H_1(X_0(1), \mathbf{Z}) = 0$, the lemma follows.

4.3 The element $\mathcal{L}'_p(I)$

In this section, let I be again a (fixed) lattice of conductor prime to p, and $\mathcal{O}$ its associated order. Let

$$u = a + b\omega \in \mathcal{O}^\times$$

be the fundamental unit of norm 1 in $\mathcal{O}^\times$, and let n be the largest integer such that $p^n|b$.

Let $v_0, v_1, \ldots, v_n$ be a sequence of vertices of level $0, 1, \ldots, n$ such that v_m is adjacent to v_{m+1}, and let

$$\mathcal{L}_{p,m}(I) := \sum_{\sigma \in G_m} (-w_p)^m \gamma_u(\sigma v_m) \cdot \sigma^{-1} \in H_1(X_0(p), \mathbf{Z}) \otimes \mathbf{Z}[G_m].$$

This element is analogous to the theta-elements introduced in [MT]. It is closely related to the special values of the partial L-function

$$L(f, I, s) = \sum_n a_n(f) r_I(n) n^{-s},$$

at $s = 1$ twisted by ring class characters of conductor p^n. Here, f is a cusp form of weight 2 on $\Gamma_0(p)$, $a_n(f)$ is its n-th Fourier coefficient, and $r_I(n)$ is the number of lattices of norm n which are equivalent to I. For more details, see for example [GKZ] or [Ko].

It follows from lemma 4.7 that the elements $\mathcal{L}_{p,m}(I)$ are compatible under the natural projection maps $\mathbf{Z}[G_m] \longrightarrow \mathbf{Z}[G_{m-1}]$, and that $\mathcal{L}_{p,m}(I)$ belongs to $H_1(X_0(p), \mathbf{Z}) \otimes I_m$, where I_m is the augmentation ideal of $\mathbf{Z}[G_m]$. Let $\mathcal{L}'_{p,m}(I)$ be the image of $\mathcal{L}_{p,m}(I)$ by the natural projection to $H_1(X_0(p), \mathbf{Z}) \otimes (I_m/I_m^2)$. After identifying I_m/I_m^2 with G_m in the usual way, we have:

$$\mathcal{L}'_{p,m}(I) := \sum_{\sigma \in G_m} (-w_p)^m \gamma_u(\sigma v_m) \cdot \sigma^{-1} \in H_1(X_0(p), \mathbf{Z}) \otimes G_m.$$

Since $\mathcal{L}_{p,m}(I)$ depends on the choice of the vertex v_m of level m only up to right multiplication by an element of G_m, and since the induced action of G_m on I_m/I_m^2 is trivial, the elements $\mathcal{L}'_{p,m}(I)$ $(m \leq n)$ do not depend on the choice of the vertex v_m, and they are compatible under the natural projection maps from G_m to G_{m-1}.

To lighten notations, set

$$\mathcal{L}'_p(I) := \mathcal{L}'_{p,n}(I).$$

It is a canonical element in $H_1(X_0(p), \mathbf{Z}) \otimes G_n$ associated to I, well-defined up to a sign and the action of the Atkin-Lehner involution w_p.

Let $H_1(X_0(p), \mathbf{Z})^+ \subset H_1(X_0(p), \mathbf{Z})$ be the subgroup of the homology which is fixed under the action of complex conjugation.

Lemma 4.8 *The element $\mathcal{L}'_p(I)$ belongs to $H_1(X_0(p), \mathbf{Z})^+ \otimes G_n$.*

The proof of this lemma, which we leave to the reader, follows by comparing the action of the Atkin-Lehner involution w_p on the modular symbols with the action of complex conjugation on $H_1(X_0(N), \mathbf{Z})$.

4.4 Local points

Let

$$\mathcal{L}'_p(c) := \sum_I \mathcal{L}'_p(I),$$

where the sum is taken over $\mathrm{Pic}(\mathcal{O})$, the set of equivalence classes of lattices of conductor c.

The basic intuition is that the element $\mathcal{L}'_p(c)$ should encode the position of a special point in $J_0(p)(K)$, analogous to the Heegner divisor of equation (5) except that the role of the imaginary quadratic field is now played by a real quadratic field.

To make this precise, fix now an elliptic curve E of conductor p. Let f be the modular form on $X_0(p)$ which is associated to E by Wiles' theorem, and let w be the sign of the Atkin-Lehner involution w_p acting on f. Let $E^w(K)$ (resp. $E^w(K_p)$) be the subgroup of $E(K)$ (resp. $E(K_p)$) on which complex conjugation acts like w_p. We note the following two properties of $E^w(K)$ and $E^w(K_p)$ (the first global, and the second local):

1. The sign in the functional equation for $L(E/\mathbf{Q}, s)$ is $-w$. Hence, it follows from the Birch and Swinnerton-Dyer conjecture that $E^w(K)$ has odd rank and that $E^{-w}(K)$ has even rank.

2. The curve E has split (resp. non-split) multiplicative reduction at p if and only if $w = -1$ (resp. $w = 1$). In particular, the group $E^w(K_p)$ is contained in the group $E_{ns}(K_p)$ of points having non-singular reduction, and the Tate uniformization Φ_{Tate} induces an isomorphism

$$\Phi_{\mathrm{Tate}} : (K_p^\times)_1 \longrightarrow E^w(K_p).$$

The compact group $(K_p^\times)_1$ is equipped with a canonical filtration

$$(K_p^\times)_1 \supset (K_p^\times)_1^{(1)} \supset (K_p^\times)_1^{(2)} \supset \cdots$$

with the property that $G_n = (K_p^\times)_1/(K_p^\times)_1^{(n)}$. Likewise, the group $E^w(K_p)$ is equipped with the canonical p-adic filtration defined in [Si2]

$$E^w(K_p) \supset E^w(K_p)^{(1)} \supset E^w(K_p)^{(2)} \supset \cdots$$

and the isomorphism between $(K_p^\times)_1$ and $E^w(K_p)$ given by the Tate uniformization respects these filtrations. In particular, by passing to the quotient one has isomorphisms

$$\Phi_{\mathrm{Tate},n} : G_n \longrightarrow E^w(K_p)/E^w(K_p)^{(n)}.$$

Now, let

$$\phi_E : X_0(p) \longrightarrow E$$

be the modular parametrization of theorem 2.1. It induces a surjection on the real homology:

$$\phi_{E*} : H_1(X_0(p), \mathbf{Z})^+ \longrightarrow H_1(E, \mathbf{Z})^+ \simeq \mathbf{Z},$$

and a corresponding map $H_1(X_0(p), \mathbf{Z})^+ \otimes G_n \longrightarrow G_n$, also denoted ϕ_{E*} by abuse of notation.

By lemma 4.8, the element $\mathcal{L}'_p(c)$ belongs to $H_1(X_0(p), \mathbf{Z})^+ \otimes G_n$. Let

$$\mathcal{L}'_p(c, E) := \phi_{E*}(\mathcal{L}'_p(c)) \in G_n.$$

Now, define the local point

$$P_K(c) := \Phi_{\mathrm{Tate},n}(\mathcal{L}'_p(c, E)) \in E^w(K_p)/E^w(K_p)^{(n)}.$$

This point is well-defined as a function of E, K, and c, up to an ambiguity of sign, and can be viewed as an approximation to a point in $E(K_p)$, with a p-adic accuracy of p^{-n}. Let t denote the order of the torsion subgroup of $E(K)$. Suppose that c is square-free and relatively prime to $p\mathrm{Disc}(K)$; let c^+ (resp. c^-) denote the product of the primes which are split (resp. inert) in $K/\mathbf{Q}$.

Conjecture 4.9 *The point $P_K(c)$ is trivial if the rank of $E(K)$ is greater than 1. Otherwise, there is a global point $P \in E(K)$ (not deepending on c) such that:*

$$t \cdot P_K(c) \equiv \pm \prod_{\ell | c^+} (a_\ell - 2) \prod_{\ell | c^-} a_\ell \cdot \sqrt{\#Ш(E/K)} \cdot (P + w\bar{P}) \qquad (mod\ \ E^w(K_p)^{(n)}),$$

where $\bar{P}$ is the complex conjugate point.

Furthermore, if the modular parametrization used to define $P_K(c)$ is a strong parametrization, then P is a generator for $E(K)$ modulo torsion.

Frequently, t is relatively prime to $(p+1)p$. In this case conjecture 4.9 can be written

$$P_K(c) \equiv \pm \prod_{\ell | c^+} (a_\ell - 2) \prod_{\ell | c^-} a_\ell \cdot \sqrt{\#Ш(E/K)} t^{-1} \cdot (P + w\bar{P}) \qquad (\text{mod}\ \ E^w(K_p)^{(n)}),$$

where the inverse of t is taken modulo $(p+1)p^{n-1}$.

Remarks:

1. Conjecture 4.9 predicts that there is a global point $P_K \in E(K)$ such that

$$t \cdot P_K(c) = \pm \prod_{\ell | c^+} (a_\ell - 2) \prod_{\ell | c^-} a_\ell \cdot P_K \qquad (\text{mod } E^w(K_p)^{(n)}), \qquad (6)$$

for all positive integers c which are relatively prime to p. Given any $n \geq 0$, it is possible to find c so that the fundamental unit of norm 1 in the order of conductor c also belongs to the order of conductor p^n. Hence equation (6) defines the point P_K uniquely up to sign, and gives a p-adic recipe for computing it. We call P_K the *Stark-Heegner point* associated to E over the real quadratic field K.

2. The appearance of the factor

$$\prod_{\ell | c^+} (a_\ell - 2) \prod_{\ell | c^-} a_\ell$$

may seem unnatural. This factor plays the role of a product of Euler factors at the primes ℓ dividing c. By replacing the element $\mathcal{L}_p(c)$ with the "regularized element" $\sum_{d|c} \epsilon(d)\mu(c/d)\mathcal{L}_p(c/d)$, where ϵ is the Dirichlet character

associated to K,and μ is the Mobius function, one would obtain a slightly different construction of a point $P_K(c)$, involving the more natural factor

$$\prod_{\ell|c^+}(\ell+1-a_\ell)\prod_{\ell|c^-}(\ell+1+a_\ell)$$

in the conjecture.

3. *A caveat*: The precise form of conjecture 4.9 was suggested by the analogy with the formula in [BD3], as well as by the numerical experiments of section 5. Note that some of the fudge factors one might expect to find in a Birch and Swinnerton-Dyer type formula, such as the order m_p of the group of connected components of the Néron model of $E/\mathbf{Q}_p$, do not appear in our formula. It would be of interest to formulate a precise conjecture along the lines of conjecture 4.9 for curves of arbitrary conductor, where we expect some of the integers m_ℓ, with $\ell \neq p$, to appear. We felt that our numerical evidence was too scant, and our conceptual understanding too incomplete, to make confident predictions about the precise fudge factors which would appear in general.

5 Experimental evidence

5.1 Experiments with $X_0(11)$

Let E be the elliptic curve $X_0(11)$ with minimal Weierstrass equation

$$y^2+y=x^3-x^2-10x-20.$$

Its Mordell-Weil group over $\mathbf{Q}$ is finite, of order $t=5$. The Atkin-Lehner involution w_{11} acts on E by -1, and hence $w=-1$.

Let $K=\mathbf{Q}(\sqrt{2})$. The prime 11 is inert in this real quadratic field, and the maximal order $\mathcal{O}_K=\mathbf{Z}[\sqrt{2}]$ has class number 1 and fundamental unit equal to $1+\sqrt{2}$.

The Mordell-Weil group of E over K is of rank 1, and is generated (modulo torsion) by the point in $E^w(K)$

$$P=(9/2,\frac{-2+7\sqrt{2}}{4}).$$

Let

$$\Phi_{\mathrm{Tate}} : K_{11}^{\times} \longrightarrow E(K_{11})$$

be the Tate 11-adic uniformization, and let $\tilde{P}$ be a lift of P to the group of units in $\mathcal{O}_{11}^{\times}$. Since

$$\Phi_{\mathrm{Tate}}(40612 + 94673\sqrt{2}) \equiv (9/2, \frac{-2 + 7\sqrt{2}}{4}) \pmod{11^4},$$

it follows that $\tilde{P}$ is equal to $40612 + 94673\sqrt{2}$ for this degree of 11-adic accuracy.

In order to try out the conjectures of the previous section, we need to exploit some non-maximal orders whose fundamental unit $a + b\sqrt{2}$ satisfies $11^n | b$, for some $n > 0$.

For simplicity, we will work only with orders of prime conductor ℓ. One sees directly that, if the fundamental unit $u = a + b\omega$ of $\mathcal{O}$ satisfies $11^n | b$, then necessarily we have either:

1. ℓ is split in $\mathbf{Q}(\sqrt{11})$ and $12 \cdot 11^{n-1}$ divides $\ell - 1$, or
2. ℓ is inert in $\mathbf{Q}(\sqrt{11})$ and $12 \cdot 11^{n-1}$ divides $\ell + 1$.

Here is a small table of the first few primes ℓ satisfying these conditions, together with their narrow class numbers and fundamental units: (Here $u = 1 + \sqrt{2}$ is a fundamental unit of K.)

ℓ	h	Unit	ℓ	h	Unit	ℓ	h	Unit
73	4	u^{36}	347	2	u^{348}	673	4	u^{336}
83	2	u^{84}	433	4	u^{216}	683	6	u^{228}
97	4	u^{48}	467	2	u^{468}	769	4	u^{384}
107	2	u^{108}	491	2	u^{492}	827	6	u^{276}
$*131$	2	u^{132}	563	2	u^{564}	937	4	u^{468}
179	10	u^{36}	587	2	u^{588}	947	2	u^{948}
193	4	u^{96}	601	20	u^{60}	971	2	u^{972}
251	6	u^{84}	$*659$	2	u^{660}	1009	28	u^{72}

Note that in all cases, the fundamental unit of $\mathcal{O}$ listed in the table is a power of u^{12}, and hence belongs to the order of conductor 11 in $\mathbf{Z}[\sqrt{2}]$. Note also that in the two cases marked with a $*$, the fundamental unit is actually a

power of $u^{12\cdot 11}$, and hence belongs to the order of conductor 11^2 of K. In these two cases, the constructions of the previous section will allow us to construct an approximation to a global point in $E^w(\mathcal{O}_K \otimes (\mathbf{Z}/121\mathbf{Z}))$, and not just in $E^w(\mathcal{O}_K \otimes (\mathbf{Z}/11\mathbf{Z}))$.

Suppose first that the 11 divides b exactly. Then conjecture 4.9, assuming that $\#Ш(E/K) = 1$, predicts that

$$\mathcal{L}'_{11}(\ell, E) \equiv \tilde{P}^{\pm 2\frac{\ell+1-a_\ell}{5}} \pmod{11} = \begin{cases} -1 \text{ if } 2 \not| \ell+1-a_\ell, \\ +1 \text{ if } 2|\ell+1-a_\ell. \end{cases}$$

We indeed checked that this was true on the 24 discriminants listed in the table.

For further verifications, we carried out the calculations modulo 11^2 with the orders of conductor 131 and 659. Here, we obtained a canonical element in $(\mathcal{O}/11^2\mathcal{O})^\times$. For example, in the case of $\ell = 131$, there are two narrow ideal classes I_1 and I_2. A calculation shows that

$$\mathcal{L}'_{11}(I_1) = \mathcal{L}'_{11}(I_2) = (120 + 77\sqrt{2}) \otimes \omega,$$

where ω is a real period of E. Hence,

$$\mathcal{L}'_{11}(131, E) \equiv (120 + 77\sqrt{2})^2 \equiv 1 + 88\sqrt{2} \pmod{11^2}.$$

On the other hand, the 131st Fourier coefficient for $X_0(11)$ is $a_{131} = -18$, so that the predicted right hand side on the conjecture is

$$\tilde{P}^{2(131+1-a_{131})/5} \equiv \tilde{P}^{60} \equiv 1 + 88\sqrt{2} \pmod{11^2},$$

confirming the conjecture.

Likewise, in the case of $\ell = 659$, we found that

$$\mathcal{L}'_{11}(659, E) \equiv 1 + 99\sqrt{2} \pmod{11^2},$$

and that the right hand side (noting that $(\ell + 1 - a_\ell)/5 = 130$) is

$$\tilde{P}^{260} \equiv 1 + 99\sqrt{2} \pmod{11^2}.$$

We have performed similar verifications with the orders of conductor 23, 43, and 89, which have the property that if u denotes their fundamental unit, then u^6 belongs to the order of conductor 11^2. Hence, by working with the

modular symbols γ_{u^6} instead of γ_u, one could obtain an approximation to $\tilde{P}^{12(\ell+1-a_\ell)/5}$. The results are listed in the following table:

ℓ	h^+	a_ℓ	$\mathcal{L}'_{11}(\ell, E)^6$	$\tilde{P}^{12(\ell+1-a_\ell)/5}$
23	2	-1	$1+88\sqrt{2}$	$1+88\sqrt{2}$
43	2	-6	$1+55\sqrt{2}$	$1+55\sqrt{2}$
89	4	15	$1+22\sqrt{2}$	$1+22\sqrt{2}$

We could have pushed the calculation further, using primes ℓ for which the fundamental unit of the order of conductor ℓ also belongs to the unit of conductor 11^3. This would give an approximation to the generator of $E(K)$ with an 11-adic accuracy of 11^{-3}, provided that 11 does not divide $\ell+1-a_\ell$. The first prime with this property is $\ell = 727$. Unfortunately, the calculation of $\mathcal{L}'_{11}(727, E)$ with our implementation of the algorithm seemed to require more computer time than we were willing to devote (about 3 hours). It is likely that the algorithm could be improved, and it would be interesting to explore issues of computational efficiency more carefully.

Needless to say, one could in principle construct a global point to an arbitrary level of 11-adic accuracy, by using these conjectures and exploiting primes ℓ for which

1. The fundamental unit in the order of conductor ℓ also belongs to the order of conductor 11^n;

2. 11 does not divide $\ell + 1 - a_\ell$.

It can be shown, using the Chebotarev density theorem, that there are infinitely many primes ℓ with these properties, for any given n. (For instance, with $n = 4$ the smallest prime satisfying the above conditions is $\ell = 2663$.)

5.2 Experiments with $X_0(37)$

In this section, let E be the elliptic curve $X_0(37)^+$ with minimal Weierstrass equation

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

Here the sign of w_{37} is 1, and hence $w = 1$. The Mordell-Weil group $E^w(K) = E(\mathbf{Q})$ is isomorphic to $\mathbf{Z}$ and is generated by the point $P = (0, 0)$.

This time, we varied the real quadratic field, seeking fields whose fundamental unit also belongs to the order of conductor 37. It is likely that there are infinitely many such fields, although proving such a statement appears to be difficult. In the range $D \leq 9,000$, we found 12 such fields with narrow class number 1. (Restricting to fields of narrow class number 1 allowed for some simplication in the calculations, but was not really necessary.)

For each of these fields, we computed the element $\mathcal{L}'_{37}(1, E)$ associated to the maximal order of K. We could verify that

$$\Phi_{\mathrm{Tate}}(\mathcal{L}'_{37}(1, E)) = \pm 2\sqrt{\#Ш(E/K)^?} \cdot (0, 0), \quad \text{in} \quad E(\mathbf{F}_{37}).$$

Here

$$\#Ш(E/K)^? = L(E^K, 1)/\Omega_{E^K},$$

where E^K is the twist of E over K, and Ω_{E^K} is its associated period. Thus, $s^2 = \#Ш(E/K)^?$ is the order of $Ш(E/K)$ that is predicted by the Birch and Swinnerton-Dyer conjecture, at least when it is non-zero. The results are summarized in the table below.

D	$\mathcal{L}'_{37}(1, E)$	$\Phi_{\mathrm{Tate}}(\mathcal{L}'_{37}(1, E))$	s	$2 \cdot s \cdot (0, 0)$
1277	$17 + 13\sqrt{1277}$	$(30, 13)$	12	$(30, 23)$
1609	$28 + 5\sqrt{1609}$	$(2, 2)$	2	$(2, 34)$
1613	$22 + 8\sqrt{1613}$	$(17, 33)$	14	$(17, 33)$
2333	$28 + 15\sqrt{2333}$	$(2, 2)$	2	$(2, 34)$
2437	$4 + 16\sqrt{2437}$	$(15, 31)$	8	$(15, 31)$
4993	$28 + 16\sqrt{4993}$	$(2, 2)$	2	$(2, 34)$
5009	$28 + 23\sqrt{5009}$	$(2, 34)$	2	$(2, 34)$
5869	1	∞	0	∞
7349	$13 + 5\sqrt{7349}$	$(26, 3)$	4	$(26, 3)$
7369	$13 + 18\sqrt{7369}$	$(26, 3)$	4	$(26, 3)$
7793	$4 + 18\sqrt{7793}$	$(15, 5)$	8	$(15, 31)$
8677	$17 + 13\sqrt{8677}$	$(30, 13)$	12	$(30, 23)$

Note that when $D = 5869$, one has $s = 0$, suggesting that the curve E^K has infinite Mordell-Weil group and that $\mathrm{rank}(E(K)) > 1$. In this case, conjecture 4.9 predicts that the points $P_K(c) \in E^w(K_p)/E^w(K_p)^{(n)}$ are trivial for all c, so that the Stark-Heegner point $P_K \in E(K)$ is trivial.

References

[BD1] M. Bertolini and H. Darmon, *Heegner points on Mumford-Tate curves*, CICMA preprint; Invent. Math., to appear.

[BD2] M. Bertolini and H. Darmon (with an appendix by B. Edixhoven) *A rigid analytic Gross-Zagier formula and arithmetic applications*, CICMA preprint; Annals of Math., to appear.

[BD3] M. Bertolini and H. Darmon, *Heegner points, p-adic L-functions and the Cerednik-Drinfeld uniformization*, CICMA preprint; submitted.

[Ca] J.W.S. Cassels, Lectures on elliptic curves, London Mathematical Society Student Texts **24**, Cambridge University Press, Cambridge 1991.

[Dag] H. Daghigh, McGill PhD. Thesis, in progress.

[Dar] H. Darmon, *Heegner points, Heegner cycles, and congruences*, in "Elliptic curves and related topics", CRM proceedings and lecture notes vol. **4**, H. Kisilevsky and M. Ram Murty eds. (1992) pp. 45-60.

[Di] F. Diamond, *On deformation rings and Hecke rings*, to appear in Annals of Math.

[DST] D.S. Dummit, J.W. Sands, and B.A. Tangedal, *Computing Stark units for totally real cubic fields*, preprint.

[El] N. Elkies, *Heegner point computations*, Algorithmic number theory (Ithaca, NY, 1994) 122–133, Lecture Notes in Computer Science **877** Springer, Berlin, 1994.

[Gr1] B.H. Gross, *Heegner points on $X_0(N)$*, in Modular Forms, R.A. Rankin ed., p. 87-107, Ellis Horwood Ltd., 1984.

[Gr2] B.H. Gross, *Heights and the special values of L-series*, Number theory (Montreal, Que., 1985), 115–187, CMS Conf. Proc., **7**, Amer. Math. Soc., Providence, RI, 1987.

[GKZ] B.H.Gross, W.Kohnen, D.Zagier, *Heegner points and derivatives of L-series. II.* Math. Ann. **278** (1987), no. 1-4, 497–562.

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

[HW] G.H. Hardy, E.M. Wright, An introduction to the theory of numbers, fifth ed., the Clarendon Press, Oxford University Press, New York, 1979

[JL] H. Jacquet, R.P. Langlands, *Automorphic forms on* $\mathbf{GL}(\mathbf{2})$, Springer Lecture Notes, **114**, (1970).

[Ko] W. Kohnen, *Modular forms and real quadratic fields.* Automorphic functions and their applications (Khabarovsk, 1988), 126–134, Acad. Sci. USSR, Inst. Appl. Math., Khabarovsk, 1990.

[Ma] B. Mazur, *Modular curves and arithmetic*, Proceedings of the Int. Congress of Math., (1983), Warszawa, pp. 185-209.

[MT] B. Mazur, J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math. J. **54** (1987), no. 2, 711–750.

[MTT] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Inv. Math. **84** 1-48 (1986).

[PR] B. Perrin-Riou, *Points de Heegner et dérivées de fonctions L p-adiques*, Invent. Math. **89** 1987, no. 3, 455-510.

[Ro] D. Roberts, Shimura curves analogous to $X_0(N)$, Harvard PhD. Thesis, 1989.

[Ru] K. Rubin, *p-adic L-functions and rational points on elliptic curves with complex multiplication*, Invent. Math. **107**, 323-350 (1992).

[Si1] J.H. Silverman, The arithmetic of elliptic curves, GTM **106**, Springer-Verlag, New York 1986.

[Si2] J.H. Silverman, *Computing rational points on rank 1 elliptic curves via L-series and canonical heights*, (preprint).

[St] H.M. Stark, *Values of L-functions at $s = 1$, I, II, III*, and *IV*, Advances in Math. **7** (1971), 301–343; **17** (1975), 60–92; **22** (1976), 64–84; **35** (1980), 197–235.

[Ta] J. Tate, Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$. Birkhäuser, Boston, 1984.

[TW] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141**, No. 3, 1995, pp. 553-572.

[Wal] J-L. Waldspurger, *Sur les valeurs de certaines fonctions L automorphes en leur centre de symmétrie*, Compos. Math. **54** (1985) no. 2, 173–242.

[Was] L. Washington, Introduction to Cyclotomic Fields, GTM **83**, Springer-Verlag, 1982.

[We] A. Weil, Number Theory: An approach through history, from Hammurapi to Legendre. Birkhäuser, 1984.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Math. **141**, No. 3, 1995, pp. 443-551.

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