

Computing Heegner points arising from Shimura curve parametrizations

Matthew Greenberg

ABSTRACT. Let E be an elliptic curve defined over \mathbb{Q} or over a real quadratic field which is uniformized by the Jacobian of a Shimura curve X . We discuss a p -adic analytic algorithm for computing certain *Heegner points* on E – images under the above uniformization of degree zero CM-divisors on X .

1. Heegner points

1.1. Modular parametrizations. Let E/\mathbb{Q} be an elliptic curve of conductor N . By the modularity theorem of Wiles et. al., we have a holomorphic *modular parametrization*

$$\Phi_N : X_0(N)(\mathbb{C}) \longrightarrow E(\mathbb{C}),$$

where the Riemann surface $X_0(N)(\mathbb{C})$ is the quotient of the extended complex upper half-plane \mathcal{H} by the standard congruence subgroup $\Gamma_0(N)$ of level N . Assume that $\Phi_N(\infty)$ is the zero element of $E(\mathbb{C})$. Let $P \in X_0(N)(\mathbb{C})$ and let $\tau \in \mathcal{H}$ be any lift of P . Then

$$(1.1) \quad \Phi_N(P) = W \left(\int_{\infty}^{\tau} 2\pi i f_E(z) dz \right) = W \left(\sum_{n \geq 1} \frac{a_n(f_E)}{n} e^{2\pi i n \tau} \right)$$

where W is the Weierstrass parametrization of E , $f_E \in \mathcal{S}_2(N)$ is the normalized newform attached to E and $a_n(f_E)$ is the n -th Fourier coefficient of f_E .

1.2. CM-points. For the purposes of this talk, a *quadratic order* (resp. an *imaginary quadratic order*) \mathcal{O} is a subring of a quadratic number field (resp. an imaginary quadratic number field) K such that $K = \mathbb{Q}\mathcal{O}$.

The Riemann surface $X_0(N)(\mathbb{C})$ may be identified with the complex-valued points of a curve $X_0(N)$ defined over \mathbb{Q} . This curve is in fact a moduli space — $X_0(N)$ classifies isogenies $P = (A \rightarrow A')$ of elliptic curves whose kernel is cyclic of order N . We will call a point $P \in X_0(N)(\mathbb{C})$ a *CM-point*, and say that P has CM

2000 *Mathematics Subject Classification.* Primary 11G05, Secondary 11F11, 11F85, 11G15, 11G18.

Key words and phrases. elliptic curves, modular forms, Heegner points, Shimura curves, p -adic uniformization.

by the quadratic order \mathcal{O} , if both A and A' have CM by \mathcal{O} . In this case, the theory of complex multiplication says that

$$P \in X_0(N)(H_{\mathcal{O}}), \quad \text{where } H_{\mathcal{O}} = \text{ring class field attached to } \mathcal{O}.$$

1.3. The classical Heegner hypothesis. Let $\mathcal{O} \subset K$ be an imaginary quadratic order of discriminant prime to N .

LEMMA 1.1 ([Dar04, Proposition 3.8]). *The following are equivalent:*

- (1) *There exists a point on $X_0(N)$ with CM by \mathcal{O} .*
- (2) *All primes ℓ dividing N split in K .*

Conditions (1) and (2) are known as the *Heegner hypothesis*. Thus, when the Heegner hypothesis is satisfied, the above construction yields a systematic supply of algebraic points on E defined over specific class fields of K . Due to the importance of Heegner points to the arithmetic theory of elliptic curves (see [Dar] or [Dar04, Chapter 3]), it is natural to desire an analogous construction of algebraic points defined over class fields of imaginary quadratic fields which do not necessarily satisfy this stringent hypothesis, as well as methods to compute such points in practice. Such a generalization requires admitting uniformizations of E by certain *Shimura curves*.

2. Shimura-Heegner points

2.1. Shimura curve parametrizations (over \mathbb{Q}). Assume that N is square-free and let $N = N^+N^-$ be a factorization of N such that N^- has an even number of prime factors. Let C be the unique quaternion algebra over \mathbb{Q} ramified precisely at N^- . (For basic definitions related to quaternion algebras, see [Voi, §1.2] or the comprehensive [Vig80].) Fix an identification ι_{∞} of $C \otimes_{\mathbb{Q}} \mathbb{R}$ with $M_2(\mathbb{R})$. Let S be an Eichler order in C of level N^+ and set

$$\Gamma^C(S) = \{\iota_{\infty}(s) : s \in S, \det \iota_{\infty}(s) = 1\} / \{\pm 1\} \subset \mathrm{PSL}_2(\mathbb{R}).$$

The group $\Gamma^C(S)$ acts discontinuously on \mathcal{H} with quotient denoted $X^C(S)(\mathbb{C})$.

EXAMPLE 2.1. If $N^- = 1$, then $C \cong M_2(\mathbb{Q})$ and S may be taken to be

$$R_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : N^+ \text{ divides } c \right\}.$$

In this case, the group $\Gamma^C(S)$ is the usual congruence subgroup $\Gamma_0(N)$. It is known that $X^C(S)(\mathbb{C})$ is compact if and only if $N^- \neq 1$.

EXAMPLE 2.2. Suppose $p \equiv 3 \pmod{4}$, $N^+ = 1$ and $N^- = 2p$. Then the quaternion algebra C is that which Voight denotes $\left(\frac{-1, p}{\mathbb{Q}}\right)$ in [Voi]. The Eichler order S is simply a maximal order in C and is unique up to conjugation by C^* .

A space of modular forms $\mathcal{S}_2(\Gamma^C(S))$, complete with Hecke action, can be defined as in the classical case $N^- = 1$. By the modularity of E and the Jacquet-Langlands correspondence, there exists an eigenform $g_E \in \mathcal{S}_2(\Gamma^C(S))$ with system of Hecke eigenvalues $\{a_p(g_E)\} = \{a_p(E)\}$, as well as a map

$$\Phi_{N^+, N^-} : \mathrm{Div}^0 \mathcal{H} \rightarrow \mathrm{Jac} X^C(S)(\mathbb{C}) \rightarrow E(\mathbb{C})$$

given by

$$(\tau') - (\tau) \mapsto W\left(\int_{\tau}^{\tau'} g_E(z) dz\right),$$

where W is the Weierstrass parametrization of $E(\mathbb{C})$. If $N^- = 1$, then we are in the situation of §1.1 and Φ_{N^+, N^-} is induced by the map Φ_N .

2.2. CM-points.

THEOREM 2.3 (Shimura). *$X^C(S)(\mathbb{C})$ is the set of complex points of a curve $X^C(S)$ defined over \mathbb{Q} . This curve classifies abelian surfaces with “level N^+ -structure” whose endomorphism rings contain S .*

(For a discussion of this moduli problem, see [Zha01, Chapter 1].)

Let $\mathcal{O} \subset K$ be an imaginary quadratic order. We say a point P in $X^C(S)(\mathbb{C})$ has *CM by \mathcal{O}* if it corresponds to an abelian surface whose endomorphism ring contains \mathcal{O} as a subring commuting with S . Let $\text{CM}(\mathcal{O})$ denote the set of such points P . The map from $\text{Jac } X^C(S)(\mathbb{C})$ to $E(\mathbb{C})$ induced by Φ_{N^+, N^-} is also defined over \mathbb{Q} , so

$$\Phi_{N^+, N^-}(\text{Div}^0 \text{CM}(\mathcal{O})) \subset E(H_{\mathcal{O}}).$$

We will call these points on E *Shimura-Heegner points*.

2.3. The Shimura-Heegner hypothesis. Let $\mathcal{O} \subset K$ an imaginary quadratic order whose discriminant is prime to N .

LEMMA 2.4. *The following are equivalent*

- (1) *The set $\text{CM}(\mathcal{O})$ is nonempty.*
- (2) *All primes ℓ dividing N^+ (resp. N^-) are split (resp. inert) in K .*

Call conditions (1) and (2) are the *Shimura-Heegner hypothesis*. If the Shimura-Heegner hypothesis is satisfied for the maximal order \mathcal{O} of K , call (N^+, N^-, K) a *Shimura-Heegner triple*. (This is not standard terminology and is in force in this paragraph only.) For a given imaginary quadratic field K of discriminant prime to N , there exists a factorization $N = N^+ N^-$ such that (N^+, N^-, K) is a Shimura-Heegner triple if and only if the sign in the functional equation of $L(E/K, s)$ is -1 . Thus, we have a Heegner-point type construction available exactly when the Birch and Swinnerton-Dyer conjecture predicts that the rank of $E(K)$ is positive for reasons of parity.

2.4. Elliptic curves over real quadratic fields. The phenomenon of elliptic curves being parametrized by Shimura curves generalizes to certain elliptic curves defined over totally real fields. For simplicity, let F be a real quadratic field with infinite places σ_1 and σ_2 , and let \mathfrak{p} be a finite prime of F . (The much more mysterious case of imaginary quadratic base fields will be discussed in [Gre].) Let C be the quaternion F -algebra ramified at \mathfrak{p} and σ_1 and let S be a maximal order of C . Fix an isomorphism

$$\iota_{\sigma_2} : C \otimes_{\sigma_2} \mathbb{R} \rightarrow M_2(\mathbb{R}),$$

and let

$$\Gamma^C(S) = \{\iota_{\sigma_2}(s) : s \in S, \det \iota_{\sigma_2}(s) = 1\} / \{\pm 1\} \subset \text{PSL}_2(\mathbb{R}).$$

As before, $\Gamma^C(S)$ acts discontinuously on \mathcal{H} . The quotient $\Gamma \backslash \mathcal{H}$ is a compact Riemann surface which admits a description as the complex points of a Shimura curve X , as well as a corresponding CM-theory.

Let $f \in \mathcal{S}_2(\mathfrak{p})$ be a Hilbert modular newform with rational Hecke eigenvalues. Then the Jacquet-Langlands correspondence together with an Eichler-Shimura construction implies the existence of an elliptic curve E/F parametrized by the Jacobian variety J of X whose L -function matches that of f . Again, we want to compute the images on E of degree zero CM divisors on J , which we also call Shimura-Heegner points.

3. Computing Heegner and Shimura-Heegner points

The classical Heegner points may be efficiently computed using formula (1.1). The quantities $a_n(f_E)$ can be computed using the formula

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

(where p is a prime and \tilde{E} is the reduction of E modulo p) in conjunction with the Euler product for $L(f_E, s)$. For details and a complexity analysis, see [Elk94].

The following questions remain: How do we efficiently compute Φ_{N^+, N^-} , and hence Shimura-Heegner points, when $N^- \neq 1$? The computability of the modular parametrization Φ_N of (1.1) relies on the Fourier expansion of f_E . When $N^- \neq 1$, such an expansion is not available. How about when E is defined over a real quadratic field?

In his article in this volume [Voi], John Voight discussed efficient methods for computing CM-points on certain Shimura curves. Unfortunately (for our purposes), the curves that he discussed were all of genus zero, and hence cannot parametrize elliptic curves.

N. Elkies [Elk98] has also developed methods for performing these computations in certain cases using archimedean analysis and explicit presentations of the groups $\Gamma^C(S)$. His methods are in fact related to those of Voight.

We present an approach based on p -adic analysis. Our main tools are the Cherednik-Drinfeld theorem, p -adic integration and the theory of rigid-analytic automorphic forms on definite quaternion algebras.

4. p -adic integration and uniformization

4.1. The Cherednik-Drinfeld interchange of invariants. Let E/\mathbb{Q} be an elliptic curve of conductor $N = N^+N^-$ and suppose that p is a prime dividing N^- . (In particular, $N^- \neq 1$.) Let B be the quaternion algebra ramified at the primes dividing N^-/p , together with the place at infinity. (We interchange the roles of the places p and infinity — hence the title of this subsection.) Let R be an Eichler \mathbb{Z} -order in B of level N^+p .

EXAMPLE 4.1. In the situation of Example 2.2, B is the algebra of Hamilton's quaternions, denoted $\left(\frac{-1, -1}{\mathbb{Q}}\right)$ in [Voi].

Since B is split at p , we may choose an isomorphism

$$\iota_p : B_p := B \otimes_{\mathbb{Q}} \mathbb{Q}_p \longrightarrow M_2(\mathbb{Q}_p)$$

such that ι_p induces an isomorphism of $R_p := R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ with

$$R_0(p\mathbb{Z}_p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}_p) : p \text{ divides } c \right\}.$$

4.2. The p -adic uniformization theorem.

DEFINITION 4.2 (Multiplicative integral). Let

- \mathcal{B}_n be the standard decomposition of $\mathbb{P}^1(\mathbb{Q}_p)$ into $p^n + p^{n-1}$ balls of radius p^{-n} ,
- μ be a \mathbb{Z} -valued measure on $\mathbb{P}^1(\mathbb{Q}_p)$, and
- f be a continuous, nonvanishing function on $\mathbb{P}^1(\mathbb{Q}_p)$.

Define

$$\int_{\mathbb{P}^1(\mathbb{Q}_p)} f(x) d\mu(x) = \lim_{n \rightarrow \infty} \prod_{U \in \mathcal{B}_n} f(t_U)^{\mu(U)},$$

where t_U is any point of U .

In his lecture on p -adic uniformization [Dar], Darmon constructs a \mathbb{Z} -valued distribution μ_E on $\mathbb{P}^1(\mathbb{Q}_p)$ (i.e. a finitely additive, \mathbb{Z} -valued function on the compact-open subsets of $\mathbb{P}^1(\mathbb{Q}_p)$) which is invariant under the group $R[1/p]_1^*$ of units in $R[1/p]$ of reduced norm 1. (The group B_p^* acts via ι_p on the projective line $\mathbb{P}^1(\mathbb{Q}_p)$ and hence on its compact-open subsets.) Let

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

be the p -adic upper half-plane and let

$$\text{Tate} : \mathbb{C}_p^* \rightarrow E(\mathbb{C}_p)$$

be the Tate parametrization of E .

THEOREM 4.3 (p -adic uniformization of E).

- (1) (Cherednik-Drinfeld) There is a canonical surjective map

$$\text{CD} : \mathcal{H}_p \longrightarrow X^C(S)(\mathbb{C}_p).$$

- (2) (Bertolini-Darmon) The map CD satisfies

$$\Phi_{N^+, N^-}((\text{CD}(\tau')) - (\text{CD}(\tau))) = \text{Tate} \left(\int_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{x - \tau'}{x - \tau} \right) d\mu_E(x) \right).$$

Furthermore, one may explicitly describe $\text{CD}^{-1}(\text{CM}(\mathcal{O})) \subset \mathcal{H}_p$.

4.3. Some details. In this subsection, we briefly indicate how the map CD is constructed and we identify the set $\text{CD}^{-1}(\text{CM}(\mathcal{O})) \subset \mathcal{H}_p$. Let

$$\Gamma^B(R[1/p]) = \{\iota_p(r) : r \in R[1/p], \det \iota_p(r) = 1\} / \{\pm 1\} \subset \text{PSL}_2(\mathbb{Q}_p).$$

The group $\Gamma^B(R[1/p])$ acts discontinuously on \mathcal{H}_p and the quotient $\Gamma^B(R[1/p]) \backslash \mathcal{H}_p$, has the structure of a rigid-analytic curve. To prove (1) of Theorem 4.3, Cherednik and Drinfeld show that there is a canonical rigid-analytic isomorphism

$$\text{CD} : \Gamma^B(R[1/p]) \backslash \mathcal{H}_p \longrightarrow X^C(S)_{\mathbb{C}_p}.$$

Let $\mathcal{O} \subset K$ be an imaginary quadratic order satisfying the Shimura-Heegner hypothesis. Call an embedding ψ of $\mathcal{O}[1/p]$ into $R[1/p]$ *optimal* if it does not extend to an embedding of a larger $\mathbb{Z}[1/p]$ -order in K and denote by $\mathcal{E}_p(\mathcal{O})$ the set of all such optimal embeddings. The Shimura-Heegner hypothesis guarantees that $\mathcal{E}_p(\mathcal{O})$ is nonempty. For each $\psi \in \mathcal{E}_p(\mathcal{O})$, the group $\mathcal{O}[1/p]^*$ acts on \mathcal{H}_p via the composite $\iota_p \circ \psi$ with a unique fixed point $\tau_\psi \in \mathcal{H}_p$ satisfying

$$\alpha \begin{pmatrix} \tau_\psi \\ 1 \end{pmatrix} = \psi(\alpha) \begin{pmatrix} \tau_\psi \\ 1 \end{pmatrix}$$

for all $\alpha \in \mathcal{O}[1/p]^*$. Let $\mathcal{H}_p(\mathcal{O})$ be the set of all such τ_ψ . It can be shown (see [BD96]) that

$$\mathcal{H}_p(\mathcal{O}) = \text{CD}^{-1}(\text{CM}(\mathcal{O})).$$

Set

$$(4.1) \quad J(\tau, \tau') = \int_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{x - \tau'}{x - \tau} \right) d\mu_E(x).$$

By statement (2) of Theorem 4.3, the points $\text{Tate}(J(\tau, \tau'))$ for $\tau, \tau' \in \mathcal{H}_p(\mathcal{O})$ are Shimura-Heegner points on E defined over the ring class field $H_{\mathcal{O}}$ attached to \mathcal{O} . Slightly more generally, we are interested in the image of an arbitrary element $\mathfrak{d} \in \text{Div}^0 \mathcal{H}_p(\mathcal{O})$ in $E(H_{\mathcal{O}})$. Suppose \mathfrak{d} has the form

$$\mathfrak{d} = \sum_{i=1}^n ((\tau'_i) - (\tau_i)).$$

For later use, we introduce the notation

$$\int_{\mathfrak{d}} \omega_{\mu_E} = \prod_{i=1}^n J(\tau_i, \tau'_i).$$

Thus we have

$$\Phi_{N^+, N^-}(\mathfrak{d}) = \text{Tate} \left(\int_{\mathfrak{d}} \omega_{\mu_E} \right).$$

Not only can we describe the Shimura-Heegner points analytically, but also the action of $\text{Gal } H_{\mathcal{O}}/K$ on them: One can show (see [Gro87, §3.2]) that the class group $\text{Pic } \mathcal{O}$ acts freely on the set $\mathcal{H}_p(\mathcal{O})$. Let

$$\text{rec} : \text{Pic } \mathcal{O} \longrightarrow \text{Gal } H_{\mathcal{O}}/K.$$

be the map induced by the reciprocity homomorphism of class field theory.

THEOREM 4.4 (Shimura's reciprocity law). *Let $\tau, \tau' \in \mathcal{H}_p(\mathcal{O})$. Then for all $\alpha \in \text{Pic } \mathcal{O}$, we have*

$$\Phi_{N^+, N^-}((\tau'^{\alpha}) - (\tau^{\alpha})) = \Phi_{N^+, N^-}((\tau') - (\tau))^{\text{rec } \alpha}.$$

We utilize Shimura's reciprocity extensively in performing our computations.

Summing up this section, we have seen that to compute Shimura-Heegner points p -adically, it suffices to be able to compute p -adic integrals of the form (4.1).

5. Computing p -adic integrals

5.1. The naive approach. It is natural to attempt to evaluate $J(\tau, \tau')$ from the definition, i.e. by evaluating the ‘‘Riemann products’’ defining the multiplicative integral (see Definition 4.2). One can show that we do not lose generality by assuming that the reductions of the points τ and τ' lie in $\mathbb{P}^1(\overline{\mathbb{F}}_p) - \mathbb{P}^1(\mathbb{F}_p)$, and for the rest of the talk we shall work under this assumption. In this case, it is not hard to show that

$$J(\tau, \tau') \equiv^* \prod_{U \in \mathcal{B}_N} \left(\frac{t_U - \tau'}{t_U - \tau} \right)^{\mu(U)} \pmod{p^N},$$

where $x \equiv^* y \pmod{p^N}$ means $x/y - 1 \equiv 0 \pmod{p^N}$. Unfortunately, the size of \mathcal{B}_N is $p^N + p^{N-1} - 1$ — exponential in N . Thus, the naive approach does not facilitate the calculation of (4.1) to high accuracy.

5.2. Outline of the method. In this subsection, we give a sketch of our alternate method for computing (4.1), and hence Shimura-Heegner points. For complete details, see [Gre06].

First, we observe that the Teichmüller representative of $J(\tau, \tau')$ is the same as that of

$$\prod_{a=0}^{p-1} \left(\frac{a - \tau'}{a - \tau} \right)^{\mu(a+p\mathbb{Z}_p)},$$

an easily computed quantity. Consequently, it is sufficient to compute $\log J(\tau, \tau')$, where “log” denotes the (standard) branch of the p -adic logarithm satisfying $\log p = 0$.

For simplicity, we assume that there is some $i \in R[1/p]_1^*$ such that $\iota_p(i) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. This is easy to arrange if B is the algebra of Hamilton’s quaternions, for instance. Write

$$\log J(\tau, \tau') = \sum_{a \in \mathbb{P}^1(\mathbb{F}_p)} \log J_a(\tau, \tau'), \quad \text{where}$$

$$J_a(\tau, \tau') = \int_{\mathbf{b}_a} \left(\frac{x - \tau'}{x - \tau} \right) d\mu_E(x),$$

and \mathbf{b}_a is the standard residue disk around a . Let

$$J_\infty(\tau) = \int_{\mathbf{b}_0} (1 + \tau x) d\mu_E(x),$$

$$J_a(\tau) = \int_{\mathbf{b}_a} (x - \tau) d\mu_E(x), \quad 0 \leq a \leq p - 1.$$

Then for each $a \in \mathbb{P}^1(\mathbb{F}_p)$, we have

$$J_a(\tau, \tau') = J_a(\tau')/J_a(\tau).$$

(To prove the above for $a = \infty$, we use the above assumption on the existence of i .)

Straightforward manipulations (see [DP06, §1.3]) show that the expansions

$$(5.1) \quad \log J_\infty(\tau) = \sum_{n \geq 1} \frac{(-1)^n}{n} \tau^n \omega(0, n),$$

$$(5.2) \quad \log J_a(\tau) = \sum_{n \geq 1} \frac{1}{n(a - \tau)^n} \omega(a, n), \quad 0 \leq a \leq p - 1.$$

are valid, where (following the notation of [DP06]),

$$\omega(a, n) = \int_{\mathbf{b}_a} (x - a)^n d\mu_E(x), \quad 0 \leq a \leq p - 1.$$

Let

$$(5.3) \quad M' = \max\{n : \text{ord}_p(p^n/n) < M\}, \quad M'' = M + \left\lfloor \frac{\log M'}{\log p} \right\rfloor.$$

Examining formulas (5.1), (5.2), and (5.3), it is easy to deduce the following:

PROPOSITION 5.1. *To compute $\log J(\tau, \tau')$ to a precision of p^{-M} , it suffices to compute the data*

$$(5.4) \quad \omega(a, n) \pmod{p^{M''}}, \quad 0 \leq a \leq p - 1, \quad 0 \leq n \leq M'.$$

THEOREM 5.2. *The data (5.4) may be computed in $O(M^3 p^3 \log M)$ operations on integers of size on the order of p^M .*

Theorem 5.2 is proved in detail in [Gre06, Proposition 7]. The idea is to relate the moments $\omega(a, n)$ to certain automorphic forms on the definite quaternion algebra B . We show that the data (5.4) is encoded in a natural way in an automorphic form $\Phi^{M''}$ taking values in a module of “approximate distributions” on \mathbb{Z}_p . $\Phi^{M''}$ is characterized by a finite amount of data and can be represented nicely on a computer. The form $\Phi^{M''}$ is the M'' -th term in a sequence of approximations Φ_n . The transition from the n -th approximation Φ_n to the $(n+1)$ -st Φ_{n+1} proceeds by an application of the Hecke operator U_p , a process which can be carried out algorithmically. Each of the M'' required applications of the U_p operator requires $O(M^2 p^3 \log M)$ operations on elements of $\mathbb{Z}/p^{M''}\mathbb{Z}$. The running-time estimate of Theorem 5.2 follows from the fact that $M'' \approx M$.

6. Sample computations

EXAMPLE 6.1. Let E/\mathbb{Q} be the curve

$$E : y^2 + xy + y = x^3 + x^2 - 70x - 279 \quad (38B2)$$

of conductor $N = 38 = 2 \cdot 19$. Taking $N^- = N$ and $p = 19$ as in Example 4.1, we have that B is the algebra of Hamilton’s quaternions. Consider the maximal order $\mathcal{O} = \mathbb{Z}[\xi] \subset K = \mathbb{Q}(\xi)$, where

$$\xi = \frac{1 + \sqrt{-195}}{2}.$$

Both 2 and 19 are inert in K , so the Shimura-Heegner hypothesis is satisfied. One may compute that

$$\text{Pic } \mathcal{O} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \quad H_{\mathcal{O}} = K(\sqrt{-3}, \sqrt{5})$$

Let χ_1, χ_2, χ_3 be the characters of $\text{Pic } \mathcal{O}$ of exact order 2. Assume these characters are indexed so that the fields corresponding to χ_1, χ_2 , and χ_3 are $K(u)$, $K(v)$, and $K(w)$, respectively, where

$$u = \frac{1 + \sqrt{-15}}{2}, \quad v = \frac{1 + \sqrt{5}}{2}, \quad w = \frac{1 + \sqrt{65}}{2}.$$

We remark that $K(u, v, w)$ is the Hilbert class field of K . Choose an optimal embedding of \mathcal{O} into the maximal order of B and let $\tau \in \mathcal{H}_p(\mathcal{O})$ be its fixed point. Define degree 0 CM divisors

$$\mathfrak{d}_i = \sum_{\alpha \in \text{Pic } \mathcal{O}} \chi_i(\alpha) \tau^\alpha, \quad i = 1, 2, 3.$$

(Note that this makes sense as χ takes values in $\{1, -1\}$.) Define a degree 0 divisor corresponding to the trivial character by

$$\mathfrak{d}_0 = \sum_{\alpha \in \text{Pic } \mathcal{O}} ((3 + 1 - T_3) \tau)^\alpha,$$

where T_3 is the usual Hecke operator. Set

$$P_i = \text{Tate} \left(\int_{\mathfrak{d}_i}^* \omega_{\mu_E} \right), \quad i = 0, 1, 2, 3.$$

We computed 19-adic approximations to the $P_i \in E(K_{19})$ modulo 19^{40} . These approximations were recognized as the global points

$$\begin{aligned} P_0 &= (-4610/39, (-277799\xi + 228034)/1521), \\ P_1 &= (25/12, -94/9u + 265/72), \\ P_2 &= (10, -11v), \\ P_3 &= (1928695/2548, (-2397574904w + 1023044339)/463736). \end{aligned}$$

But how do we recognize 19-adic approximations as points with algebraic coordinates? We represent a generic element $19^a u + 19^b v \xi \in K_{19}$ with $u, v \in \mathbb{Z}_{19}^*$ as the quadruple $(a, u \pmod{19^{40}}, b, v \pmod{19^{40}})$. Thus, to recognize such an approximation as an element of K , it suffices to be able to recognize an approximation to an element of \mathbb{Z}_{19}^* as a rational number. This is accomplished using lattice reduction techniques as in [DP06]. These ideas allowed us to recognize the coordinates of P_0 as elements of K . The coordinates $x(P_1)$ and $y(P_1)$ should be rational over $K(u)$, not over K itself. Let σ be a generator of $\text{Gal } K(u)/K$. Using Shimura reciprocity, we can compute approximations to $x(P_1)^\sigma$ and $y(P_1)^\sigma$ in K_{19} . If $x(P_1) = u + v\sqrt{-15}$ with $u, v \in K$, then

$$u = \frac{1}{2}(x(P_1) + x(P_1)^\sigma), \quad v = \frac{1}{2\sqrt{-15}}(x(P_1) - x(P_1)^\sigma).$$

Fixing an embedding of $K(u)$ into K_{19} , we may compute approximations to u and v as elements of K_{19} and then attempt to recognize them as elements of K as described above. The coordinate $y(P_1)$, as well as the coordinates of P_2 and P_3 , were identified in the same way.

We remark that, for this example, the computation of the data (5.4) to a precision of 40 19-adic digits took approximately one minute.

EXAMPLE 6.2. Let

$$\omega = \frac{1 + \sqrt{5}}{2}, \quad F = \mathbb{Q}(\omega),$$

and consider the elliptic curve

$$E : y^2 + xy + \omega y = x^3 - (\omega + 1)x^2 - (30\omega + 45)x - (11\omega + 117).$$

of conductor $(3 - 5\omega) =: \mathfrak{p}$. (We have $(31) = \mathfrak{p}\bar{\mathfrak{p}}$.) In this case, the definite quaternion algebra B which comes into play is the base change to F of the \mathbb{Q} -algebra of Hamilton's quaternions.

Consider the CM-field $K = F(\sqrt{2\omega - 15})$ with maximal order \mathcal{O} . $\text{Pic } \mathcal{O} \cong \mathbb{Z}/8\mathbb{Z}$ and thus has a unique character χ of exact order 2 with corresponding field $K(\sqrt{-13\omega + 2})$. Choose a base point $\tau \in \mathcal{H}_p(\mathcal{O})$ and define a divisor

$$\mathfrak{d}_\chi = \sum_{\alpha \in \text{Pic } \mathcal{O}} \chi(\alpha) \tau^\alpha$$

and a point

$$P_\chi = \text{Tate} \left(\int_{\mathfrak{d}_\chi}^* \omega_{\mu_E} \right)$$

associated to χ . (Again, this makes sense as χ takes values in $\{1, -1\}$.)

Using the techniques described above, the point P_χ was recognized as the global point

$$(x, y) \in E(F(\sqrt{-13\omega + 2})), \quad \text{where}$$

$$\begin{aligned}
x &= 1/501689727224078580 \times \\
&\quad (-20489329712955302181\omega + \\
&\quad\quad 1590697243182535465) \\
y &= 1/794580338951539798133856600 \times \\
&\quad (-24307562136394751979713438023\omega \\
&\quad - 52244062542753980406680036861) \\
&\quad \times \sqrt{-13\omega + 2} \\
&\quad + 1/1003379454448157160 \times \\
&\quad (19987639985731223601\omega \\
&\quad - 1590697243182535465).
\end{aligned}$$

Our computations were all carried out using the Magma computer algebra system.

References

- [BD96] M. Bertolini and H. Darmon, *Heegner points on Mumford-Tate curves*, Invent. Math. **126** (1996), no. 3, 413–456. MR 1419003 (97k:11100)
- [Dar] H. Darmon, *Rational points on curves*, in this volume.
- [Dar04] H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, vol. 101, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004. MR 2020572 (2004k:11103)
- [DP06] H. Darmon and R. Pollack, *Efficient calculation of Stark-Heegner points via overconvergent modular symbols*, Israel J. Math. **153** (2006), 319–354. MR 2254648 (2007k:11077)
- [Elk94] N. D. Elkies, *Heegner point computations*, Algorithmic number theory (Ithaca, NY, 1994) (L. M. Adleman and M.-D. Huang, eds.), Lecture Notes in Comput. Sci., vol. 877, Springer, Berlin, 1994, proceedings of ANTS-1, 1994, pp. 122–133. MR 1322717 (96f:11080)
- [Elk98] ———, *Shimura curve computations*, Algorithmic number theory (Portland, OR, 1998) (J.P. Buhler, ed.), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, proceedings of ANTS-3, 1998, pp. 1–47. MR 1726059 (2001a:11099)
- [Gre] M. Greenberg, *The arithmetic of elliptic curves over imaginary quadratic fields and Stark-Heegner points*, in this volume.
- [Gre06] ———, *Heegner point computations via numerical p -adic integration*, Algorithmic number theory (F. Hess, S. Pauli, and M. Pohst, eds.), Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, proceedings of ANTS-7, 2006, pp. 361–376. MR 2282936 (2008a:11069)
- [Gro87] B. H. Gross, *Heights and the special values of L -series*, Number theory (Montreal, Que., 1985) (H. Kisilevsky and J. Labute, eds.), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 115–187. MR 894322 (89c:11082)
- [Vig80] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980. MR 580949 (82i:12016)
- [Voi] J. Voight, *Shimura curve computations*, in this volume.
- [Zha01] S.-W. Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27–147. MR 1826411 (2002g:11081)

DEPARTMENT OF MATHEMATICS, MCGILL UNIVERSITY, MONTREAL, QUEBEC, CANADA
Current address: Max-Planck-Institut für Mathematik, 53111 Bonn, Germany
E-mail address: fmgreenberg@gmail.com