Clay Mathematics Proceedings
Volume 8, 2009

The arithmetic of elliptic curves over imaginary quadratic fields and Stark-Heegner points

Matthew Greenberg

Abstract. Heegner points are crucial to our understanding of the arithmetic of elliptic curves over $\mathbb{Q}$ as well as over totally real fields. In this note, we describe a conjectural construction due to Trifković of analogues of Heegner points for elliptic curves defined over imaginary quadratic fields. We expect these points to enrich our understanding of the arithmetic of such curves.

1. Introduction

A large proportion of research into the arithmetic of elliptic curves is devoted to the understanding of *Mordell-Weil groups* — groups of points on elliptic curves rational over number fields. Many questions regarding the structure of Mordell-Weil groups, most famously the conjecture of Birch and Swinnerton-Dyer (BSD), remain open. Much of what we *do* know about these groups (e.g. BSD for elliptic curves over $\mathbb{Q}$ of analytic rank at most one) is due to the existence of a systematic construction of points — so-called *Heegner points* — of Mordell-Weil groups in towers of number fields. In appropriate situations, these Heegner points govern the behaviour of Mordell-Weil groups in a very strong way.

Heegner points on an elliptic curve E are, by definition, the images of CM points under *modular parametrizations* of E: dominant morphisms from modular or Shimura curves to E. In particular, for Heegner points to exist, E needs to admit a modular parametrization in the first place, a condition only reasonable to expect in any kind of generality if E can be defined over a totally real field. Due to the absolutely crucial role played by Heegner points in the study of Mordell-Weil groups, it is extremely natural to desire a generalization of the Heegner point construction to elliptic curves which do not necessarily admit modular parametrizations. In this article, we present such a generalization, due to Trifković [**Tri06**], in the case of elliptic curves defined over imaginary quadratic fields.

Trifković's work is based on Darmon's construction of *Stark-Heegner points* on elliptic curves defined over $\mathbb{Q}$ — analogues of Heegner points which are conjectured

2000 *Mathematics Subject Classification.* Primary 11G05, Secondary 11F11, 11F67, 11G40.
Key words and phrases. elliptic curves, modular forms, imaginary quadratic fields, Stark-Heegner points.

to be rational over ring class fields of real quadratic fields. Although Darmon's construction makes essential use of the modular forms attached to elliptic curves over $\mathbb{Q}$, the modular parametrizations are not explicitly involved.[1] It is this characteristic which raises the prospect of generalizing the Stark-Heegner point construction to base fields other than totally real ones where, although modular parametrizations are not expected to be available, the elliptic curves in question are still expected to be "modular."

The central role played by rational points in the arithmetic of elliptic curves is summed up beautifully by the following lines from the abstract of [**BMSW07**]:

> "Rational points on elliptic curves are the gems of arithmetic: they are, to Diophantine geometry, what units in rings of integers are to algebraic number theory, what algebraic cycles are to algebraic geometry. A rational point in just the right context, at one place in the theory, can inhibit and control — thanks to the ideas of Kolyvagin — the existence of rational points and other mathematical structures elsewhere."

This article is divided into three main parts. First, we will define modular forms and modular symbols relative to an imaginary quadratic base field and state some fundamental results concerning these. Armed with these notions, we will describe Trifković's Stark-Heegner point construction and state his conjectures concerning their algebricity. In the last part, we shall discuss issues related to the computation of these points in practice.

The author would like to sincerely thank the anonymous referee for numerous insightful suggestions which led to significant improvements in this article.

2. Modular forms for imaginary quadratic fields

2.1. Upper half-space. In addition to [**Tri06**], some good references for this section are [**Byg98, Cre84, Cre, CW94, Lin05**]. Reference [**Byg98**] in particular is extremely detailed and contains a wealth of background material. Let F be an imaginary quadratic field of discriminant D with maximal order $\mathcal{O}_F$, and assume that $\mathcal{O}_F$ is a principal ideal domain. Fix an ideal $\mathcal{N}$ of $\mathcal{O}_F$. In analogy with the classical situation, define

$$\mathcal{H} = \mathrm{GL}_2(\mathbb{C})/\mathbb{C}^* \cdot \mathrm{SU}_2$$

and call $\mathcal{H}$ the *upper half-space*. The group $\mathrm{GL}_2(\mathbb{C})$ admits a decomposition $\mathrm{GL}_2(\mathbb{C}) = BKZ$, where

$$B = \left\{ \begin{pmatrix} t & z \\ 0 & 1 \end{pmatrix} : \begin{array}{c} z \in \mathbb{C} \\ t \in \mathbb{R}_{>0} \end{array} \right\}, \quad K = \mathrm{SU}_2, \quad \text{and} \quad Z = \mathbb{C}^*,$$

mirroring the analogous decomposition of $\mathrm{GL}_2^+(\mathbb{R})$ where

$$B = \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} : \begin{array}{c} x \in \mathbb{R} \\ y \in \mathbb{R}_{>0} \end{array} \right\}, \quad K = \mathrm{SO}_2, \quad \text{and} \quad Z = \mathbb{R}^*,$$

Projecting onto the B-coordinate, we have an identification

$$\mathcal{H} \cong \{(z, t) : z \in \mathbb{C},\, t \in \mathbb{R}_{>0}\}.$$

[1] S. Dasgupta [**Das05**] has shown how to explicitly lift the Stark-Heegner points on E to an appropriate modular Jacobian.

The action of $\mathrm{GL}_2(\mathbb{C})$ on $\mathcal{H}$ takes the form

$$(2.1)\qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix}(z,t) = \frac{1}{|cz+d|^2+|ct|^2}\big((az+b)\overline{(cz+d)}+a\bar{c}t, |ad-bc|t\big)$$

The upper half-space $\mathcal{H}$ is equipped with a $\mathrm{GL}_2(\mathbb{C})$-invariant Euclidean metric given by

$$ds^2 = \frac{dzd\bar{z}+dt^2}{t^2}.$$

Let $\mathcal{H}^*$ be the disjoint union of $\mathcal{H}$ with $\mathbb{P}^1(F)$. (Note that, although this is not reflected in the notation, the set $\mathcal{H}^*$ depends on the field F.) Extend the topology of $\mathcal{H}$ to $\mathcal{H}^*$ by declaring sets of the form

$$U_h = \{(z,t)\in\mathcal{H} : t > h\}\cup\{\infty\},$$

as well as their translates by elements of $\mathrm{GL}_2(F)$, to be open. The action of

$$\Gamma_0(\mathcal{N}) := \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in \mathrm{GL}_2(\mathcal{O}_F) : c\in\mathcal{N}\right\}.$$

extends naturally to $\mathcal{H}^*$, so we may consider the quotient

$$X_0(\mathcal{N}) := \Gamma_0(\mathcal{N})\backslash\mathcal{H}^*.$$

We assume that $\Gamma_0(\mathcal{N})$ has no elements of finite order, in which case $X_0(\mathcal{N})$ is a smooth 3-manifold. (See [**Kur78**] for details on dealing with the situation where $\Gamma_0(\mathcal{N})$ contains elements of finite order.) The points $\Gamma_0(\mathcal{N})\backslash\mathbb{P}^1(F)$ are called the *cusps* of $X_0(\mathcal{N})$.

2.2. Modular forms on the upper half space.

Definition 2.1. A *modular form of weight 2 for* $\Gamma_0(\mathcal{N})$ is a $\Gamma_0(\mathcal{N})$-invariant harmonic differential form on $\mathcal{H}$. If it descends to a harmonic differential form on $X_0(\mathcal{N})$, then we call it a *cusp form*.

We denote the set of modular (resp. cusp) forms of weight two for $\Gamma_0(\mathcal{N})$ by $\mathcal{M}_2(\mathcal{N})$ (resp. $\mathcal{S}_2(\mathcal{N})$). Consider the basis of smooth differential 1-forms on $\mathcal{H}$ given by

$$\omega = (\omega_1,\omega_2,\omega_3)^t = (-dz/t, dt/t, d\bar{z}/t)^t.$$

and let $f=(f_1,f_2,f_3)^t$ be a vector of smooth functions on $\mathcal{H}$.

Lemma 2.2.

(1) *The differential form* $f\cdot\omega$ *is* $\Gamma_0(\mathcal{N})$*-invariant if and only if*

$$f(z,t) = (f|\gamma)(z,t) := J(\gamma,(z,t))f(\gamma(z,t))$$

for all $\gamma\in\Gamma_0(\mathcal{N})$*, where*

$$J(\gamma,(z,t)) = \frac{1}{|r|^2+|s|^2}\begin{pmatrix} r^2\Delta & -2rs\Delta & s^2\Delta \\ r\bar{s} & |r|^2-|s|^2 & -\bar{r}s \\ \overline{s^2\Delta} & \overline{2rs\Delta} & \overline{r^2\Delta}\end{pmatrix},$$

$$\Delta = \det\gamma,\quad r=\overline{cz+d}\quad s=\bar{c}t.$$

(2) *The differential form $f \cdot \omega$ is harmonic if and only if the following partial differential equations are satisfied:*

$$\begin{aligned} \frac{\partial f_1}{\partial \bar{z}} + \frac{\partial f_3}{\partial z} &= 0 \\ \frac{\partial f_2}{\partial z} + \frac{\partial f_1}{\partial t} - t^{-1} f_1 &= 0 \\ \frac{\partial f_2}{\partial \bar{z}} - \frac{\partial f_3}{\partial t} + t^{-1} f_3 &= 0 \\ \frac{t}{2}\frac{\partial f_2}{\partial t} - f_2 - 2t\frac{\partial f_1}{\partial \bar{z}} &= 0 \end{aligned}$$

If $f \cdot \omega$ is a modular (resp. cusp) form, then we shall call f a modular (resp. cusp) form too.

2.3. Fourier expansions and cusp forms. Suppose that f satisfies $f|\gamma = f$ for all $\gamma \in \Gamma_0(\mathcal{N})$. This implies that $J(\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right), (z,t))$ is the identity matrix for all $\alpha \in \mathcal{O}_F$, so for each fixed t, the function $f_i(z,t)$ is periodic with respect to the lattice $\mathcal{O}_F \subset \mathbb{C}$. Let $g(z)$ be any function with this property and let

$$\psi : \mathbb{C} \longrightarrow S^1, \quad \psi(z) = e^{2\pi i (z+\bar{z})}$$

be the standard unitary character of the additive group of $\mathbb{C}$. Then g admits a Fourier expansion of the form

$$g(z) = \sum_{\chi} b_g(\chi)\chi(z),$$

where χ varies over the unitary characters of $\mathbb{C}$ which are trivial on $\mathcal{O}_F$. But each of these characters has the form

$$z \mapsto \psi(\alpha z) \quad \text{for some} \quad \alpha \in \mathfrak{d}_F^{-1} = \frac{1}{\sqrt{D}}\mathcal{O}_F.$$

Thus, the expansion of g takes the form

$$g(z) = \sum_{\alpha \in \mathcal{O}_F} c_g(\alpha)\psi\left(\frac{\alpha z}{\sqrt{D}}\right).$$

It follows that for each $\alpha \in \mathcal{O}_F$ there is a vector-valued function

$$c_f(\alpha, t) = (c_1(\alpha,t), c_2(\alpha,t), c_3(\alpha,t))$$

of t such that

$$f(z,t) = \sum_{\alpha \in \mathcal{O}_F} c_f(\alpha,t)\psi\left(\frac{\alpha z}{\sqrt{D}}\right).$$

One may verify that if $\varepsilon \in \mathcal{O}_F^*$ and $\gamma = \left(\begin{smallmatrix} \varepsilon & 0 \\ 0 & 1 \end{smallmatrix}\right)$, then $c_{f|\gamma}(\alpha,t) = c_f(\varepsilon\alpha, t)$. Therefore, as $f|\gamma = \gamma$, we have $c_f(\varepsilon\alpha,t) = c_f(\alpha,t)$ for all $\varepsilon \in \mathcal{O}_F^*$ and all $\alpha \in \mathcal{O}$. Consequently, recalling that we assume $\mathcal{O}_F$ to be a PID, we may rewrite the above sum as a sum over ideals of $\mathcal{O}_F$:

$$f(z,t) = c_f(0,t) + \sum_{0 \subsetneq (\alpha) \subset \mathcal{O}_F} c_f(\alpha,t) \sum_{\varepsilon \in \mathcal{O}_F^*} \psi\left(\frac{\varepsilon \alpha z}{\sqrt{D}}\right).$$

LEMMA 2.3. *If $c_{f|\gamma}(0,t) = 0$ for each $\gamma \in \mathrm{GL}_2(\mathcal{O}_F)$, then f is a cusp form on $\Gamma_0(\mathcal{N})$.*

The harmonicity of $f \cdot \omega$ implies that the components of $c_f(\alpha, t)$ are of a special form.

Definition 2.4. For $i = 0, 1$, let $K_i(t)$ denote the solution to the differential equation

$$\frac{d^2 K_i}{dt^2} + \frac{1}{t}\frac{dK_i}{dt} - \left(1 + \frac{1}{t^{2i}}\right) K_i = 0$$

which decreases rapidly at infinity (see [**Byg98**, Ch. 4]). The functions K_i are called *Bessel functions*.

Set

$$K(t) = \left(-\frac{i}{2}K_1(t), K_0(t), \frac{i}{2}K_1(t)\right).$$

It can be shown that for each $\alpha \in \mathcal{O}_F$ there is a constant $c_f(\alpha)$ such that

$$c_f(\alpha, t) = c_f(\alpha) t^2 K\left(\frac{4\pi|\alpha|t}{\sqrt{|D|}}\right),$$

so the Fourier expansion of f takes the form

$$f(z, t) = \sum_{\alpha \in \mathcal{O}_F} c_f(\alpha) t^2 K\left(\frac{4\pi|\alpha|t}{\sqrt{|D|}}\right) \psi\left(\frac{\alpha z}{\sqrt{D}}\right).$$

2.4. Hecke operators. The vector space $\mathcal{M}_2(\mathcal{N})$ admits an action of certain Hecke operators. Let λ (resp. π) be a prime element of $\mathcal{O}_F$ prime to (resp. dividing) $\mathcal{N}$. Then operators T_λ and U_π are defined by the "usual" formulas:

$$\begin{aligned} f|T_\lambda &= \sum_{\alpha \bmod \lambda} f\Big| \begin{pmatrix} 1 & \alpha \\ 0 & \lambda \end{pmatrix} + f\Big| \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}, \\ f|U_\pi &= \sum_{\alpha \bmod \pi} f\Big| \begin{pmatrix} 1 & \alpha \\ 0 & \pi \end{pmatrix}. \end{aligned}$$

The effect of the Hecke operators on Fourier coefficients is given by the familiar formulas:

$$\begin{aligned} c_{f|T_\lambda}(\alpha) &= \begin{cases} c_f(\lambda\alpha) + \mathrm{Norm}(\lambda) c_f(\alpha/\lambda) & \text{if } \lambda | \alpha, \\ c_f(\lambda\alpha) & \text{if } \lambda \nmid \alpha \end{cases}, \\ c_{f|U_\pi}(\alpha) &= c_f(\pi\alpha). \end{aligned}$$

It follows that the operators T_λ and U_π depend only on the ideals (λ) and (π), respectively.

The Hecke operators generate a commutative subalgebra of $\mathrm{End}\,\mathcal{M}_2(\mathcal{N})$ which preserves $\mathcal{S}_2(\mathcal{N})$. If $f \in \mathcal{S}_2(\mathcal{N})$ is an eigenform for all the Hecke operators and is normalized so that $c_f(1) = 1$, then $f|T_\lambda = c_f(\lambda) f$ and $f|U_\pi = c_f(\pi) f$. A notion of newform may be defined, and an Atkin-Lehner theory developed, in a manner analogous to that employed in the classical case (i.e. over $\mathbb{Q}$).

2.5. L-functions and Shimura-Taniyama. Let $f \in \mathcal{S}_2(\mathcal{N})$ be a normalized newform and define

$$L(f,s) = \sum_{(0)\subsetneq \mathfrak{a} \subset \mathcal{O}_F} c_f(\mathfrak{a})\,\mathrm{Norm}(\mathfrak{a})^{-s},$$

where the sum is over nonzero ideals of $\mathcal{O}_F$.

THEOREM 2.5. *The series defining $L(f,s)$ converges in the right half-plane $\Re s > 3/2$. It admits an Euler product, analytic continuation to the whole complex plane, and satisfies a functional equation relating its values at s and $2-s$.*

The analogue of the Shimura-Taniyama conjecture in this context is:

CONJECTURE 2.6. *There is a one-to-one correspondence between normalized cuspidal newforms $f \in \mathcal{S}_2(\mathcal{N})$ with rational Hecke-eigenvalues and isogeny classes of elliptic curves $E_{/F}$ which do not have complex multiplication by an order in F. If f corresponds to E, then*

$$L(f,s) = L(E,s).$$

REMARK 2.7. If case that E has CM by an order in F, then E corresponds to an Eisensein series on $\Gamma_0(\mathcal{N})$ rather than to a cusp form.

REMARK 2.8. In the classical case (i.e. over $\mathbb{Q}$), the Eichler-Shimura construction attaches both a Galois representation and an elliptic curve to a newform g. In many cases, Richard Taylor has succeeded in constructing Galois representations attached to modular forms over imaginary quadratic fields by relating them to *holomorphic* Siegel modular forms. This allows him to use algebro-geometric methods to locate the desired Galois representations in the ℓ-adic cohomology of these varieties. His construction does not, however, give a construction of an elliptic curve associated to the form g. If one has a prospective elliptic curve E in mind, though, one can use the Faltings-Serre method to show that the Galois representation attached to g is that arising from the Galois action on the Tate module of E.

REMARK 2.9. In [**Tri06**, p. 432], the analogue of the Shimura-Taniyama conjecture is phrased in terms of plusforms. Trifković's plusform condition is always satisfied for the modular forms in this paper since we require them to be invariant with respect to a congruence subgroup of $\mathrm{GL}_2(\mathcal{O}_F)$ whereas Trifković asks only for invariance with respect to a conguence subgroup of $\mathrm{SL}_2(\mathcal{O}_F)$.

3. Modular symbols and mixed period integrals

Let $f \in S_2(\mathcal{N})$ be a Hecke-eigenform where $\mathcal{N} \in \mathcal{O}_F$. Suppose further that $\mathcal{N}$ has the form $\pi\mathcal{M}$, where π is a prime element of $\mathcal{O}_F$ (lying over the rational prime p, say) and $\pi \nmid \mathcal{M}$. Let F_π be the completion of F at the ideal (π) and let $\mathcal{O}_{F,\pi}$ be its ring of integers.

PROPOSITION 3.1 ([**Kur78**]). *There exists a unique positive real number $\Omega_f \in \mathbb{R}$ such that*

$$\left\{\int_r^s f\cdot\omega : r, s \text{ cusps}\right\} = \Omega_f\mathbb{Z}.$$

We call the quantity Ω_f the *period of* f. Using this definition of the period, Darmon's mixed period integral formalism (see [**Dar01**] or [**Dar**]) extends easily to our setting: Let

$$\tilde{\Gamma} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_F[1/\pi]) : c \in \mathcal{M} \right\}.$$

The group $\mathrm{GL}_2(F_\pi)$ acts from the left on $\mathbb{P}^1(F_\pi)$ by fractional linear transformations. We call a subset B of $\mathbb{P}^1(F_\pi)$ a *ball* if it is of the form $\sigma\mathcal{O}_{F,\pi}$ for some $\sigma \in \mathrm{GL}_2(F_\pi)$. By the strong approximation theorem, the group $\tilde{\Gamma}$ acts transitively on the set $\mathcal{B}$ of these balls.

A $\mathbb{Z}$-*valued distribution* on $\mathbb{P}^1(F_\pi)$ is, by definition, a finitely additive, $\mathbb{Z}$-valued function on $\mathcal{B}$. We shall denote the set of such by $\mathcal{D}_{\mathbb{Z}}(\mathbb{P}^1(F_\pi))$. If $\mu \in \mathcal{D}_{\mathbb{Z}}(\mathbb{P}^1(F_\pi))$ and φ is a nonvanishing, continuous, $\mathbb{C}_p$-valued function on $\mathbb{P}^1(F_\pi)$, we define the *multiplicative integral*

$$\times\!\!\!\!\!\!\int_{\mathbb{P}^1(F_\pi)} \varphi(x)d\mu(x) = \lim_{\mathcal{U}} \prod_{U\in\mathcal{U}} \varphi(x_U)^{\mu(U)} \in \mathbb{C}_p^*,$$

where $\mathcal{U}$ varies over increasingly fine covers of $\mathbb{P}^1(F_\pi)$ by pairwise disjoint balls, and x_U is any point in U. (Note that since we are exponentiating by the values of μ, it is essential that μ is $\mathbb{Z}$-valued.)

Let $c_f(\pi) = \pm 1$ be the U_π-eigenvalue of f and define a $\mathcal{D}_{\mathbb{Z}}(\mathbb{P}^1(F_\pi))$-*valued modular symbol*

$$F : \mathbb{P}^1(F) \times \mathbb{P}^1(F) \to \mathcal{D}_{\mathbb{Z}}(\mathbb{P}^1(F_\pi))$$

by the rule

$$F\{r \to s\}(\sigma\mathcal{O}_{F,\pi}) = \frac{c_f(\pi)^{\mathrm{ord}_\pi \det \sigma}}{\Omega_f} \int_r^s (f|\sigma^{-1}) \cdot \omega.$$

That $F\{r \to s\}$ is finitely additive follows from the fact that f is a U_π-eigenform. By Proposition 3.1, the distributions $F\{r \to s\}$ are all $\mathbb{Z}$-valued.

Let $\mathcal{H}_\pi$ denote the π-adic upper half-plane $\mathbb{P}^1(\mathbb{C}_p) - \mathbb{P}^1(F_\pi)$. For cusps r, s and points $\tau, \tau' \in \mathcal{H}_\pi$, define the *mixed period integral*

$$\times\!\!\!\!\!\!\int_\tau^{\tau'} \int_r^s f = \times\!\!\!\!\!\!\int_{\mathbb{P}^1(F_p)} \left(\frac{x-\tau'}{x-\tau}\right) dF\{r \to s\}(x) \in \mathbb{C}_p^*.$$

Trifković conjectures that, up to certain π-adic periods, the above mixed period integral map be written as a quotient of two indefinite integrals (defined below). Let $E_{/F}$ be a representative of the isogeny class of elliptic curves associated to f by Conjecture 2.6. Then E has multiplicative reduction over F_π and therefore a Tate uniformization over $\mathbb{C}_p$, where p is the rational prime below π.

Conjecture 3.2. *There exists a lattice* $\Lambda \subset \mathbb{C}_p^*$ *commensurable with the Tate lattice of* E *and a function*

$$\mathcal{H}_\pi \times \mathbb{P}^1(F) \times \mathbb{P}^1(F) \to \mathbb{C}_p, \quad \textit{written} \quad (\tau, r, s) \mapsto \times\!\!\!\!\!\!\int^\tau \int_r^s f, \tag{3.1}$$

such that

(1) $\times\!\!\!\!\!\!\int^{\gamma\tau} \int_{\gamma r}^{\gamma s} f = \times\!\!\!\!\!\!\int^\tau \int_r^s f$ *for all* $\gamma \in \tilde{\Gamma}$ *and all cusps* r, s,

(2) $\times\!\!\!\!\!\!\int^\tau \int_r^s f \times \times\!\!\!\!\!\!\int^\tau \int_s^t f = \times\!\!\!\!\!\!\int^\tau \int_r^t f$ *for all cusps* r, s, t,

(3) $\displaystyle \times\!\!\!\!\!\!\int_{\tau}^{\tau'}\int_{r}^{s} f = \times\!\!\!\!\!\!\int^{\tau'}\int_{r}^{s} f \Big/ \times\!\!\!\!\!\!\int^{\tau}\int_{r}^{s} f$ *in* $\mathbb{C}_p^*/\Lambda$.

Since the Tate lattices of isogenous elliptic curves are commensurable, the above conjecture does not depend on our choice of representative E of the isogeny class of elliptic curves associated to f. We refer to the function in (3.1) as an *indefinite integral*.

4. Stark-Heegner points

Let K/F be a quadratic extension in which (π) is inert and all prime ideals dividing $\mathcal{M}$ are split (this is the analogue of the Heegner hypothesis in our situation) and let $\mathcal{O}$ be a $\mathcal{O}_F[1/\pi]$-order in K of conductor prime to $\mathcal{M}$. Let

$$R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathcal{O}_F) : \mathcal{M} \text{ divides } c \right\}.$$

We say that an embedding $\psi : K \to M_2(F)$ of F-algebras is $(\mathcal{O}, R)$-*optimal* if $\psi(K) \cap R = \psi(\mathcal{O})$. Let $\mathcal{E}(\mathcal{O}, R)$ be the set of such embeddings. The conditions that the primes dividing $\mathcal{M}$ split in K and that the conductor of $\mathcal{O}$ is prime to $\mathcal{M}$ guarantee that $\mathcal{E}(\mathcal{O}, R)$ is nonempty. The group $\tilde{\Gamma}$ of units in R acts naturally on $\mathcal{E}(\mathcal{O}, R)$ by conjugation. Moreover, there is a natural free action of $\operatorname{Pic}\mathcal{O}$ on $\mathcal{E}(\mathcal{O}, R)/\tilde{\Gamma}$ which partitions $\mathcal{E}(\mathcal{O}, R)/\tilde{\Gamma}$ into $2^{\omega(\mathcal{M})}\# \operatorname{Pic}\mathcal{O}$ orbits, where $\omega(\mathcal{M})$ denotes the number of prime factors of $\mathcal{M}$. (For details, see [**Tri06**, §3.2].)

For each $\psi \in \mathcal{E}(\mathcal{O}, R)$, there is a unique $\tau_\psi \in \mathcal{H}_\pi$ such that

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

for all $\alpha \in K^*$. As (π) is inert in K/F, the point τ_ψ actually lies in $\mathcal{H}_\pi$. Note that if ψ and ψ' are $\tilde{\Gamma}$-conjugate, then the corresponding fixed points τ and τ' in $\mathcal{H}_\pi$ are in the same $\tilde{\Gamma}$-orbit.

Fix a generator γ of $\mathcal{O}_K^*$, a cusp r, and a positive integer t such that Λ^t is contained in the Tate lattice of E. To an optimal embedding $\psi \in \mathcal{E}(\mathcal{O}, R)$, we associate the period $J_\psi \in \mathbb{C}_p^*/\Lambda$ defined by

$$J_\psi = \times\!\!\!\!\!\!\int^{\tau_\psi}\int_{r}^{\psi(\gamma)r} f \tag{4.1}$$

and the point

$$P_\psi = \operatorname{Tate}(J_\psi^t) \in E(\mathbb{C}_p).$$

By the $\tilde{\Gamma}$-invariance property of the indefinite integral (property (1) of Conjecture 3.2), the period J_ψ and the point P_ψ depends only on the $\tilde{\Gamma}$-conjugacy class of ψ. We call P_ψ the *Stark-Heegner point* attached to the optimal embedding ψ. Let $H_{\mathcal{O}}$ be the ring class field associated to the order $\mathcal{O}$ and let

$$\operatorname{rec} : \operatorname{Pic}\mathcal{O} \to \operatorname{Gal} H_{\mathcal{O}}/K$$

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

Conjecture 4.1 (Trifković). *The point P_ψ belongs to $E(H_{\mathcal{O}})$. The Galois action on P_ψ is described by*

$$(P_\psi)^{\operatorname{rec}(\mathfrak{a})} = P_{\psi^{\mathfrak{a}}}.$$

We expect the analogues of the formula of Gross-Zagier and the theorem of Kolyvagin to hold in this context: Assuming Conjecture 4.1, we may let

$$P_K = \mathrm{Trace}_{H_{\mathcal{O}}/K} P_\psi = \sum_{\mathfrak{a} \in \mathrm{Pic}\,\mathcal{O}} P_{\psi^{\mathfrak{a}}} \in E(K).$$

Let $\langle \cdot, \cdot \rangle$ denote the canonical height pairing on $E(K)$.

CONJECTURE 4.2. *There is an explicit nonzero fudge factor α such that*

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

In particular, $L'(E/K,1) \neq 0$ if and only if P_K is nontorsion.

CONJECTURE 4.3. *Suppose that the point P_K has infinite order in $E(K)$. Then* $\mathrm{rank}\, E(K) = 1$.

Armed with suitable nonvanishing results for twists of the L-function of E, Conjectures 4.2 and 4.3 should imply BSD for elliptic curves over F of analytic rank at most one. For a sketch of this argument, see [**Dar04**, §3.9].

5. Computing Stark-Heegner points

In the absence of proofs for the above conjectures, some numerical evidence supporting them is most desirable. Trifković provides this in abundance in the case where $\mathcal{O}_F$ is a Euclidean domain and the conductor of E is prime. In order to compute J_ψ in this case, Trifković, following Darmon and Green [**DG02**], begins by producing a candidate for the indefinite integral. Since $\mathcal{O}_F$ is a Euclidean domain, we may use Manin's continued fraction algorithm to write an arbitrary degree zero divisor $(s) - (r)$ on $\mathbb{P}^1(F)$ as

$$(s) - (r) = [(s) - (t_1)] + [(t_1) - (t_2)] + \cdots + [(t_{n-1}) - (t_n)] + [(t_n) - (r)],$$

where each pair in square brackets is a pair of adjacent cusps. (Two elements $(a : b)$ and $(c : d)$ of $\mathbb{P}^1(F)$ are called *adjacent* if $ad - bc = 1$.) Therefore, by the "path-multiplicativity" of the indefinite integral (property (2) of Conjecture 3.2), we may assume that r and s are adjacent cusps. All adjacent pairs of cusps are $\tilde{\Gamma} = \mathrm{PSL}_2(\mathcal{O}_F[1/\pi])$-equivalent. (Note that $\tilde{\Gamma} = \mathrm{PSL}_2(\mathcal{O}_F[1/\pi])$ because the conductor of E is assumed to be prime.) Therefore, by property (1) of Conjecture 3.2, we have reduced the computation of J_ψ to that of integrals of the form

$$\times\!\!\!\!\!\!\int^{\tau}\int_0^{\infty} f.$$

Similar manipulations using the properties of the indefinite integral give the identity

$$\times\!\!\!\!\!\!\int^{\tau}\int_0^{\infty} f = \times\!\!\!\!\!\!\int_{1-\frac{1}{\tau}}^{\tau-1}\int_0^{\infty} f = \times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{x - (\tau - 1)}{x - (1 - 1/\tau)} \right) dF\{0 \to \infty\}(x).$$

Thus, we have reduced the calculation to that of multiplicative integrals of the form

$$\times\!\!\!\!\!\!\int_{\mathbb{P}^1(\mathbb{Q}_p)} \left(\frac{x - \tau}{x - \tau'} \right) d\mu(x),$$

where $\tau, \tau' \in \mathcal{H}_\pi$ and μ is a measure on $\mathbb{P}^1(F_\pi)$. The ideas used in the computation of such integrals are the same as those discussed in [**Gre**].

We conclude with a numerical example taken from [**Tri06**, §1.3.2]. Let $F = \mathbb{Q}(\alpha)$ where $\alpha = (1+\sqrt{-3})/2$ and consider the elliptic curve

$$E : y^2 + xy = x^3 + (\alpha+1)x^2 + \alpha x.$$

The curve E has prime conductor (π) of norm 73, where $\pi = \alpha + 8$. The Mordell-Weil group $E(F)$ is cyclic of order 6 generated by the point $(-1, 1)$. Let $K = F(\beta)$ where $\beta^2 = 2\alpha + 21$. Then (π) is inert in the quadratic extension K of F. Let ψ be an $(\mathcal{O}_K, M_2(\mathcal{O}_F[1/\pi]))$-optimal embedding of K into $M_2(F)$. As the class number of K is one, we expect the Stark-Heegner point P_ψ to be rational over $K = H_{\mathcal{O}_K}$. An approximation to P_ψ module π^{30} was recognized as the global point $(x, y) \in E(K)$, where

$$\begin{aligned} x &= \frac{1259988}{127165927}\alpha + \frac{126090782}{127165927} \\ y &= \left(\frac{2903147975024}{31646131095439}\alpha + \frac{11037094266063}{31646131095439}\right)\beta \\ &\quad + \frac{629994}{127165927}\alpha + \frac{63045391}{127165927}. \end{aligned}$$

References

[BMSW07] B. Bektemirov, B. Mazur, W. Stein, and M. Watkins, *Average ranks of elliptic curves: tension between data and conjecture*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), no. 2, 233–254 (electronic). MR 2291676

[Byg98] J.S. Bygott, *Modular forms and modular symbols over imaginary quadratic fields*, Ph.D. thesis, University of Exeter, 1998, http://www.warwick.ac.uk/staff/J.E.Cremona/theses/bygott.pdf.

[Cre] J. E. Cremona, *Modular forms and elliptic curves over imaginary quadratic fields*, www.exp-math.uni-essen.de/zahlentheorie/preprints/PS/cremona.ps.

[Cre84] J. E. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Math. **51** (1984), no. 3, 275–324. MR 743014 (85j:11063)

[CW94] J. E. Cremona and E. Whitley, *Periods of cusp forms and elliptic curves over imaginary quadratic fields*, Math. Comp. **62** (1994), no. 205, 407–429. MR 1185241 (94c:11046)

[Dar] H. Darmon, *Rational points on curves*, in this volume.

[Dar01] ———, *Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications*, Ann. of Math. (2) **154** (2001), no. 3, 589–639. MR 1884617 (2003j:11067)

[Dar04] ———, *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)

[Das05] S. Dasgupta, *Stark-Heegner points on modular Jacobians*, Ann. Sci. École Norm. Sup. (4) **38** (2005), no. 3, 427–469. MR 2166341 (2006e:11080)

[DG02] H. Darmon and P. Green, *Elliptic curves and class fields of real quadratic fields: algorithms and evidence*, Experiment. Math. **11** (2002), no. 1, 37–55. MR 1960299 (2004c:11112)

[Gre] M. Greenberg, *Computing Heegner points arising from Shimura curve parametrizations*, in this volume.

[Kur78] P. F. Kurčanov, *The cohomology of discrete groups and Dirichlet series that are related to Jacquet-Langlands cusp forms*, Izv. Akad. Nauk SSSR Ser. Mat. **42** (1978), no. 3, 588–601, English translation in: Math. USSR-Izv. 12 (1978), no. 3, 543–555. MR 503433 (80b:10038)

[Lin05] M. Lingham, *Modular forms and elliptic curves over imaginary quadratic fields*, Ph.D. thesis, University of Nottingham, 2005, http://etheses.nottingham.ac.uk/archive/00000138.

[Tri06] M. Trifković, *Stark-Heegner points on elliptic curves defined over imaginary quadratic fields*, Duke Math. J. **135** (2006), no. 3, 415–453. MR 2272972 (2008d:11064)

Department of Mathematics, McGill University, Montreal, Quebec, Canada
Current address: Max-Planck-Institut für Mathematik, 53111 Bonn, Germany
E-mail address: fmgreenberg@gmail.com