

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 algebraicity. 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

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

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

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

Projecting onto the B -coordinate, we have an identification

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

¹S. 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

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

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 *cuspidal form*.

We denote the set of modular (resp. cuspidal) 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

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

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