SHADOW LINES IN THE ARITHMETIC OF ELLIPTIC CURVES

J. S. BALAKRISHNAN, M. ÇIPERIANI, J. LANG, B. MIRZA, AND R. NEWTON

ABSTRACT. Let $E/\mathbb{Q}$ be an elliptic curve and p a rational prime of good ordinary reduction. For every imaginary quadratic field $K/\mathbb{Q}$ satisfying the Heegner hypothesis for E we have a corresponding line in $E(K) \otimes \mathbb{Q}_p$, known as a shadow line. When $E/\mathbb{Q}$ has analytic rank 2 and E/K has analytic rank 3, shadow lines are expected to lie in $E(\mathbb{Q}) \otimes \mathbb{Q}_p$. If, in addition, p splits in $K/\mathbb{Q}$, then shadow lines can be determined using the anticyclotomic p-adic height pairing. We develop an algorithm to compute anticyclotomic p-adic heights which we then use to provide an algorithm to compute shadow lines. We conclude by illustrating these algorithms in a collection of examples.

INTRODUCTION

Fix an elliptic curve $E/\mathbb{Q}$ of analytic rank 2 and an odd prime p of good ordinary reduction. Assume that the p-primary part of the Tate-Shafarevich group of $E/\mathbb{Q}$ is finite. Let K be an imaginary quadratic field such that the analytic rank of E/K is 3 and the Heegner hypothesis holds for E, i.e., all primes dividing the conductor of $E/\mathbb{Q}$ split in K. We are interested in computing the subspace of $E(K) \otimes \mathbb{Q}_p$ generated by the anticyclotomic universal norms. To define this space, let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K and K_n denote the subfield of K_∞ whose Galois group over K is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. The module of *universal norms* is defined by

$$\mathcal{U} = \bigcap_{n \geq 0} N_{K_n/K}(E(K_n) \otimes \mathbb{Z}_p),$$

where $N_{K_n/K}$ is the norm map induced by the map $E(K_n) \to E(K)$ given by $P \mapsto \sum_{\sigma \in \mathrm{Gal}(K_n/K)} P^\sigma$.

Consider

$$L_K := \mathcal{U} \otimes \mathbb{Q}_p \subseteq E(K) \otimes \mathbb{Q}_p.$$

By work of Cornut [Co02], and Vatsal [Va03] our assumptions on the analytic ranks of $E/\mathbb{Q}$ and E/K together with the assumed finiteness of the p-primary part of the Tate-Shafarevich group of $E/\mathbb{Q}$ imply that $\dim L_K \geq 1$. Bertolini [Be95] showed that $\dim L_K = 1$ under certain conditions on the prime p. Wiles and Çiperiani [ÇW08], [Çi09] have shown that Bertolini's result is valid whenever $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q})$ is not solvable; here E_p denotes the full p-torsion of E and $\mathbb{Q}(E_p)$ is its field of definition. The 1-dimensional $\mathbb{Q}_p$-vector space L_K is known as the *shadow line* associated to the triple (E, K, p).

Complex conjugation acts on $E(K) \otimes \mathbb{Q}_p$, and we consider its two eigenspaces $E(K)^+ \otimes \mathbb{Q}_p$ and $E(K)^- \otimes \mathbb{Q}_p$. Observe that $E(K)^+ \otimes \mathbb{Q}_p = E(\mathbb{Q}) \otimes \mathbb{Q}_p$. By work of Skinner-Urban [SU14], Nekovář [Ne01], Gross-Zagier [GZ], and Kolyvagin [Ko90] we know that

$$\dim E(K)^+ \otimes \mathbb{Q}_p \geq 2 \quad \text{and} \quad \dim E(K)^- \otimes \mathbb{Q}_p = 1.$$

Then by the Sign Conjecture [MR03] we expect that

$$L_K \subseteq E(\mathbb{Q}) \otimes \mathbb{Q}_p.$$

Our main motivating question is the following:

Question (Mazur, Rubin). *As K varies, we presumably get different shadow lines L_K – what are these lines, and how are they distributed in $E(\mathbb{Q}) \otimes \mathbb{Q}_p$?*

In order to gather data about this question one can add the assumption that p splits in $K/\mathbb{Q}$ and then make use of the *anticyclotomic p-adic height pairing* on $E(K) \otimes \mathbb{Q}_p$. It is known that $\mathcal{U}$ is contained in the kernel of this pairing [MT83]. In fact, in our situation we expect that $\mathcal{U}$ equals the kernel of the anticyclotomic p-adic height pairing. Indeed we have $\dim E(K)^- \otimes \mathbb{Q}_p = 1$ and the weak Birch and Swinnerton-Dyer Conjecture for $E/\mathbb{Q}$ predicts that $\dim E(\mathbb{Q}) \otimes \mathbb{Q}_p = 2$ from which the statement about $\mathcal{U}$ follows by the properties of the anticyclotomic p-adic height pairing and its expected non-triviality. (This is discussed in §3 in further detail.) Thus computing the anticyclotomic p-adic height pairing allows us to determine the shadow line L_K.

Let $\Gamma(K)$ be the Galois group of the maximal $\mathbb{Z}_p$-power extension of K, and let $I(K) = \Gamma(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Identifying $\Gamma(K)$ with an appropriate quotient of the idele class group of K, Mazur, Stein, and Tate [MST06, §2.6] gave an explicit description of the universal p-adic height pairing

$$(\, ,) : E(K) \times E(K) \to I(K).$$

One obtains various $\mathbb{Q}_p$-valued height pairings on E by composing this universal pairing with $\mathbb{Q}_p$-linear maps $I(K) \to \mathbb{Q}_p$. The kernel of such a (non-zero) $\mathbb{Q}_p$-linear map corresponds to a $\mathbb{Z}_p$-extension of K.

In particular, the anticyclotomic $\mathbb{Z}_p$-extension of K corresponds to a $\mathbb{Q}_p$-linear map $\rho : I(K) \to \mathbb{Q}_p$ such that $\rho \circ c = -\rho$, where c denotes complex conjugation. The resulting anticyclotomic p-adic height pairing is denoted by $(\, ,)_\rho$. One key step of our work is an explicit description of the map ρ, see §1. As in [MST06], for $P \in E(K)$ we define the anticyclotomic p-adic height of P to be $h_\rho(P) = -\frac{1}{2}(P, P)_\rho$. Mazur, Stein, and Tate [MST06, §2.9] provide the following formula[1] for the anticyclotomic p-adic height of a point $P \in E(K)$:

$$h_\rho(P) = \rho_\pi(\sigma_\pi(P)) - \rho_\pi(\sigma_\pi(P^c)) + \sum_{w \nmid p\infty} \rho_w(d_w(P)),$$

where π is one of the prime divisors of p in K and the remaining notation is defined in §2. An algorithm for computing σ_π was given in [MST06]. Using our explicit description of ρ, in §2 we find a computationally feasible way of determining the contribution of finite primes w which do not divide p. This enables us to compute anticyclotomic p-adic height pairings.

We then proceed with a general discussion of shadow lines and their identification in $E(\mathbb{Q}) \otimes \mathbb{Q}_p$, see §3. In §4 we present the algorithms that we use to compute anticyclotomic p-adic heights and shadow lines. We conclude by displaying in §5 two examples of the computation of shadow lines L_K on the elliptic curve "389.a1" with the prime $p = 5$ and listing the results of several additional shadow line computations.

1. Anticyclotomic character

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$ in which p splits as $p\mathcal{O}_K = \pi\pi^c$, where c denotes complex conjugation on K. Let $\mathbb{A}^\times$ be the group of ideles of K. We also use c to denote the involution of $\mathbb{A}^\times$ induced by complex conjugation on K. For any finite place v of K, denote by K_v the completion of K at v, $\mathcal{O}_v$ the ring of integers of K_v, and μ_v the group of roots of unity in $\mathcal{O}_v$. Let $\Gamma(K)$ be the Galois group of the maximal $\mathbb{Z}_p$-power extension of K. As in [MST06], we consider the idele class $\mathbb{Q}_p$-vector space $I(K) = \Gamma(K) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. By class field theory $\Gamma(K)$ is a quotient of $J' := \mathbb{A}^\times / \overline{K^\times \mathbb{C}^\times \prod_{w \nmid p} \mathcal{O}_w^\times}$ by its finite torsion subgroup T, see the proof of Theorem 13.4 in [Wa97]. The bar in the definition of J'

---

[1]The formula appearing in [MST06, §2.9] contains a sign error which is corrected here.

denotes closure in the idelic topology, and the subgroup T is the kernel of the N-th power map on J' where N is the order of the finite group

$$\mathbb{A}^\times / \overline{K^\times \mathbb{C}^\times \prod_{w \nmid p} \mathcal{O}_w^\times (1 + \pi \mathcal{O}_\pi)(1 + \pi^c \mathcal{O}_{\pi^c})}.$$

Thus we have

$$I(K) = J'/T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p. \tag{1}$$

We shall use this idelic description of $\Gamma(K)$ in what follows.

Definition 1.1 (Anticyclotomic p-adic idele class character)**.** *An* anticyclotomic p-adic idele class character *is a continuous homomorphism*

$$\rho : \mathbb{A}^\times / K^\times \to \mathbb{Z}_p$$

such that $\rho \circ c = -\rho$.

Lemma 1.2. *Every p-adic idele class character*

$$\rho : \mathbb{A}^\times / K^\times \to \mathbb{Z}_p$$

factors via the natural projection

$$\mathbb{A}^\times / K^\times \twoheadrightarrow \mathbb{A}^\times / \left(K^\times \mathbb{C}^\times \prod_{w \nmid p} \mathcal{O}_w^\times \prod_{v \mid p} \mu_v \right).$$

Proof. This is an immediate consequence of the fact that $\mathbb{Z}_p$ is a torsion-free pro-p group. $\square$

The aim of this section is to define a non-trivial anticyclotomic p-adic idele class character. By the identification (1), such a character will give rise to a $\mathbb{Q}_p$-linear map $I(K) \to \mathbb{Q}_p$ which cuts out the anticyclotomic $\mathbb{Z}_p$-extension of K.

1.1. **The class number one case.** We now explicitly construct an anticyclotomic p-adic idele class character ρ in the case when the class number of K is 1.

Recall our assumption that p splits in $K/\mathbb{Q}$ as $p\mathcal{O}_K = \pi\pi^c$ and let

$$U_\pi = 1 + \pi\mathcal{O}_\pi \quad \text{and} \quad U_{\pi^c} = 1 + \pi^c \mathcal{O}_{\pi^c}.$$

Define a continuous homomorphism

$$\varphi : \mathbb{A}^\times \to U_\pi \times U_{\pi^c}$$

as follows. Let $(x_v)_v \in \mathbb{A}^\times$. Under our assumption that K has class number 1, we can find $\alpha \in K^\times$ such that

$$\alpha x_v \in \mathcal{O}_v^\times \quad \text{for all finite } v.$$

Indeed, the ideal $\mathfrak{a}_v$ corresponding to the place v is principal, say generated by $\varpi_v \in \mathcal{O}_K$. Then take $\alpha = \prod_v \varpi_v^{-\mathrm{ord}_v(x_v)}$, where the product is taken over all finite places v of K. We define

$$\varphi((x_v)_v) = ((\alpha x_\pi)^{p-1}, (\alpha x_{\pi^c})^{p-1}). \tag{2}$$

Note that since p is split in K we have $\mathcal{O}_\pi^\times \cong \mathbb{Z}_p^\times \cong \mu_{p-1} \times U_\pi$, and similarly for π^c. To see that φ is independent of the choice of α, we note that any other choice $\alpha' \in K^\times$ differs from α by an element of $\mathcal{O}_K^\times$. Since K is an imaginary quadratic field, $\mathcal{O}_K^\times$ consists entirely of roots of unity. In particular, under the embedding $K \hookrightarrow K_\pi$ we see that $\mathcal{O}_K^\times \hookrightarrow \mu_{p-1}$. Thus, any ambiguity about α is killed when we raise α to the $(p-1)$-power. Therefore, φ is well-defined. The continuity of φ is easily verified.

Proposition 1.3. *Suppose that K has class number 1. Then the map φ defined in* (2) *induces an isomorphism of topological groups*

$$\mathbb{A}^\times / \Big(K^\times \mathbb{C}^\times \prod_{w\nmid p} \mathcal{O}_w^\times \prod_{v|p} \mu_v \Big) \to U_\pi \times U_{\pi^c}.$$

Proof. For $v \in \{\pi, \pi^c\}$, the p-adic logarithm gives an isomorphism $U_v \cong 1 + p\mathbb{Z}_p \to p\mathbb{Z}_p$. Hence, raising to the power $(p-1)$ is an automorphism on U_v for $v \in \{\pi, \pi^c\}$ and consequently φ is surjective. It is easy to see that $K^\times \mathbb{C}^\times \prod_{w\nmid p} \mathcal{O}_w^\times \subset \ker \varphi$. Since $\mu_v \cong \mathbb{F}_p^\times$ for $v \in \{\pi, \pi^c\}$, we have $\prod_{v|p} \mu_v \subset \ker \varphi$. We claim that $\ker \varphi = K^\times \mathbb{C}^\times \prod_{w\nmid p} \mathcal{O}_w^\times \prod_{v|p} \mu_v$. Let $(x_v)_v \in \ker \varphi$ and let $\alpha \in K^\times$ be such that $\alpha x_v \in \mathcal{O}_v^\times$ for all finite v. It suffices to show that $(\alpha x_v)_v \in \mathbb{C}^\times \prod_{w\nmid p} \mathcal{O}_w^\times \prod_{v|p} \mu_v$. This is clear: since $(x_v)_v \in \ker \varphi$, we have $\alpha x_v \in \mu_v$ for $v \in \{\pi, \pi^c\}$.

Finally, since φ is a continuous open map, it follows that φ induces the desired homeomorphism.   □

By Lemma 1.2 we have reduced the problem of constructing an anticyclotomic p-adic idele class character to the problem of constructing a character

$$(3) \qquad\qquad \chi : U_\pi \times U_{\pi^c} \to \mathbb{Z}_p$$

satisfying $\chi \circ c = -\chi$. Note that this last condition implies that $\chi(x,y) = \chi(x/y^c, 1)$. Explicitly:

$$(4) \qquad \chi(x,y) = -\chi \circ c(x,y) = -\chi(y^c, x^c) = -\chi(y^c, 1) - \chi(1, x^c) = -\chi(y^c, 1) + \chi(x, 1) = \chi(x/y^c, 1).$$

In other words, χ factors via the surjection

$$f_\pi : U_\pi \times U_{\pi^c} \twoheadrightarrow U_\pi$$
$$(x, y) \mapsto x/y^c.$$

Therefore, it is enough to define a character $U_\pi \to \mathbb{Z}_p$. Fixing an isomorphism of valued fields $\psi : K_\pi \to \mathbb{Q}_p$ gives an identification $U_\pi \cong 1 + p\mathbb{Z}_p$. Now, up to scaling, there is only one choice of character, namely $\log_p : 1 + p\mathbb{Z}_p \to p\mathbb{Z}_p$. We write $\log_p$ for the unique group homomorphism $\log_p : \mathbb{Q}_p^\times \to (\mathbb{Q}_p, +)$ with $\log_p(p) = 0$ extending $\log_p : 1 + p\mathbb{Z}_p \to p\mathbb{Z}_p$. The extension to $\mathbb{Z}_p^\times$ of the map $\log_p$ is explicitly given by

$$\log_p(u) = \frac{1}{p-1} \log_p(u^{p-1}).$$

We choose the normalization $\rho = \frac{1}{p(p-1)} \log_p \circ \psi \circ f_\pi \circ \varphi$. We summarize our construction of the anticyclotomic p-adic idele class character ρ in the following proposition.

Proposition 1.4. *Suppose that K has class number 1. Fix a choice of isomorphism $\psi : K_\pi \to \mathbb{Q}_p$. Consider the map $\rho : \mathbb{A}^\times / K^\times \to \mathbb{Z}_p$ such that*

$$\rho((x_v)_v) = \frac{1}{p} \log_p \circ \psi \left(\frac{\alpha x_\pi}{\alpha^c x_{\pi^c}^c} \right)$$

where $\alpha \in K^\times$ is such that $\alpha x_v \in \mathcal{O}_v^\times$ for all finite v. Then ρ is the unique (up to scaling) non-trivial anticyclotomic p-adic idele class character.

Proof. Let $\alpha \in K^\times$ be such that $\alpha x_v \in \mathcal{O}_v^\times$ for all finite v. By our earlier discussion and the definition of the extension of $\log_p$ to $\mathbb{Z}_p^\times$, we have

$$\begin{aligned} \rho((x_v)_v) &= \frac{1}{p(p-1)} \log_p \circ \psi \left(\frac{(\alpha x_\pi)^{p-1}}{(\alpha^c x_{\pi^c}^c)^{p-1}} \right) \\ &= \frac{1}{p} \log_p \circ \psi \left(\frac{\alpha x_\pi}{\alpha^c x_{\pi^c}^c} \right). \end{aligned}$$

□

1.2. **The general case.** There is a simple generalization of the construction of ρ to the case when the class number of K may be greater than one. Let h be the class number of K. We can no longer define the homomorphism φ of (2) on the whole of $\mathbb{A}^\times$ because $\mathcal{O}_K$ is no longer assumed to be a principal ideal domain. However, we can define

$$\varphi_h : (\mathbb{A}^\times)^h \to U_\pi \times U_{\pi^c}$$

in a similar way, as follows. Let $\mathfrak{a}_v$ be the ideal of K corresponding to the place v. Then $\mathfrak{a}_v^h$ is principal, say generated by $\varpi_v \in \mathcal{O}_K$. For $(x_v)_v \in \mathbb{A}^\times$ we set $\alpha(v) = \varpi_v^{-\mathrm{ord}_v(x_v)}$. Then $\alpha(v)x_v^h \in \mathcal{O}_v^\times$ and $\alpha(v) \in \mathcal{O}_w^\times$ for all $w \neq v$. Note that $\alpha(v) = 1$ for all but finitely many v. Set $\alpha = \prod_v \alpha(v)$ and observe that $\alpha x_v^h \in \mathcal{O}_v^\times$ for all v. Then we define φ_h by

(5) $$\varphi_h((x_v)_v^h) = ((\alpha x_\pi^h)^{p-1}, (\alpha x_{\pi^c}^h)^{p-1}).$$

Fix an isomorphism $\psi : K_\pi \to \mathbb{Q}_p$. As before, we can now use the p-adic logarithm to define an anticyclotomic character $\rho : (\mathbb{A}^\times)^h \to \mathbb{Z}_p$ by setting

$$\rho = \frac{1}{p(p-1)} \log_p \circ \psi \circ f_\pi \circ \varphi_h.$$

We extend the definition of ρ to the whole of $\mathbb{A}^\times$ by setting $\rho((x_v)_v) = \frac{1}{h}\rho((x_v)_v^h)$.

As in Proposition 1.4, we now summarize our construction of the anticyclotomic p-adic idele class character in this more general setting.

Proposition 1.5. *Let h be the class number of K. Fix a choice of isomorphism $\psi : K_\pi \to \mathbb{Q}_p$. Consider the map $\rho : \mathbb{A}^\times/K^\times \to \frac{1}{h}\mathbb{Z}_p$ such that*

$$\rho((x_v)_v) = \frac{1}{hp} \log_p \circ \psi \left(\frac{\alpha x_\pi^h}{\alpha^c x_{\pi^c}^{ch}} \right)$$

where $\alpha \in K^\times$ is such that $\alpha x_v^h \in \mathcal{O}_v^\times$ for all finite v. Then ρ is the unique (up to scaling) non-trivial anticyclotomic p-adic idele class character.

Remark 1.6. *Note that $\rho : \mathbb{A}^\times/K^\times \to \frac{1}{h}\mathbb{Z}_p$, so if $p \mid h$ then ρ is not strictly an anticyclotomic idele class character in the sense of Definition 1.1. However, the choice of scaling of ρ is of no great importance since our purpose is to use ρ to define an anticyclotomic height pairing on $E(K)$ and compute the kernel of this pairing.*

Remark 1.7. *The ideal $\prod_v \mathfrak{a}_v^{-h\,\mathrm{ord}_v(x_v)}$ is principal and a generator of this ideal is the element $\alpha \in K$ that we use when evaluating the character ρ defined in Proposition 1.5.*

2. Anticyclotomic p-adic height pairing

We wish to compute the anticyclotomic p-adic height h_ρ using our explicit description of the anticyclotomic idele class character ρ given in Proposition 1.5. For any finite prime w of K, the natural inclusion $K_w^\times \hookrightarrow \mathbb{A}^\times$ induces a map $\iota_w : K_w^\times \to I(K)$, and we write $\rho_w = \rho \circ \iota_w$. For every finite place w of K and every non-zero point $P \in E(K)$ we can find $d_w(P) \in \mathcal{O}_w$ and $a_w(P), b_w(P) \in \mathcal{O}_w$, each relatively prime to $d_w(P)$, such that

(6) $$(\iota_w(x(P)), \iota_w(y(P))) = \left(\frac{a_w(P)}{d_w(P)^2}, \frac{b_w(P)}{d_w(P)^3} \right).$$

We refer to $d_w(P)$ as a *local denominator* of P at w. The existence of $d_w(P)$ follows from the Weierstrass equation for E and the fact that $\mathcal{O}_w$ is a principal ideal domain. Finally, we let σ_π denote the π-adic σ-function of E.

Given a non-torsion point $P \in E(K)$ such that
- P reduces to 0 modulo primes dividing p, and

- P reduces to the connected component of all special fibers of the Neron model of E,

we can compute its anticyclotomic p-adic height using the following formula[2] [MST06, §2.9] :

$$(7) \qquad h_\rho(P) = \rho_\pi(\sigma_\pi(P)) - \rho_\pi(\sigma_\pi(P^c)) + \sum_{w \nmid p\infty} \rho_w(d_w(P)).$$

In the following lemmas, we make some observations which simplify the computation of $h_\rho(P)$.

Lemma 2.1. *Let w be a finite prime such that $w \nmid p$. Let $x_w \in K_w^\times$. Then $\rho_w(x_w)$ only depends on $\mathrm{ord}_w(x_w)$. In particular, if $x_w \in \mathcal{O}_w^\times$, then $\rho_w(x_w) = 0$.*

Proof. This follows immediately from Lemma 1.2. Alternatively, note that the auxiliary element α used in the definition of ρ only depends on the valuation of x_w. □

Lemma 2.2. *Let w be a finite prime of K. Then $\rho_{w^c} = -\rho_w \circ c$. In particular, if $w = w^c$, then $\rho_w = 0$.*

Proof. This is an immediate consequence of the relations $\rho \circ c = -\rho$ and $c \circ \iota_{\lambda^c} = \iota_\lambda \circ c$. □

Lemma 2.2 allows us to write the formula (7) for the anticyclotomic p-adic height as follows:

$$(8) \qquad h_\rho(P) = \rho_\pi\left(\frac{\sigma_\pi(P)}{\sigma_\pi(P^c)}\right) + \sum_{\substack{\ell = \lambda\lambda^c \\ \ell \neq p}} \rho_\lambda\left(\frac{d_\lambda(P)}{d_{\lambda^c}(P)^c}\right).$$

Remark 2.3. *In order to implement an algorithm for calculating the anticyclotomic p-adic height h_ρ, we must determine a finite set of primes which includes all the split primes $\ell = \lambda\lambda^c \nmid p$ for which $\rho_\lambda\left(\frac{d_\lambda(P)}{d_{\lambda^c}(P)^c}\right) \neq 0$. Let k_λ be the residue field of K at λ and set $\mathcal{D}(P) = \prod_{\lambda \nmid p\infty}(\#k_\lambda)^{\mathrm{ord}_\lambda(d_\lambda(P))}$. It turns out that $\mathcal{D}(P)$ can be computed easily from the leading coefficient of the minimal polynomial of the x-coordinate of P [BÇS, Proposition 4.2]. Observe that $\rho_\lambda\left(\frac{d_\lambda(P)}{d_{\lambda^c}(P)^c}\right) \neq 0$ implies that $\mathrm{ord}_\lambda(d_\lambda(P)) \neq 0$ or $\mathrm{ord}_{\lambda^c}(d_{\lambda^c}(P)) \neq 0$. Hence, the only primes $\ell \neq p$ which contribute to the sum in (8) are those that are split in $K/\mathbb{Q}$ and divide $\mathcal{D}(P)$. However, in the examples that we have attempted, factoring $\mathcal{D}(P)$ is difficult due to its size.*

We now package together the contribution to the anticyclotomic p-adic height coming from primes not dividing p. Consider the ideal $x(P)\mathcal{O}_K$ and denote by $\delta(P) \subset \mathcal{O}_K$ its denominator ideal. Observe that by (6) we know that all prime factors of $\delta(P)$ appear with even powers. Fix $\mathbf{d}_h(P) \in \mathcal{O}_K$ as follows:

$$(9) \qquad \mathbf{d}_h(P)\mathcal{O}_K = \prod_{\mathfrak{q}} \mathfrak{q}^{h\,\mathrm{ord}_\mathfrak{q}(\delta(P))/2}$$

where h is the class number of K, and the product is over all prime ideals $\mathfrak{q}$ in $\mathcal{O}_K$.

Proposition 2.4. *Let $P \in E(K)$ be a non-torsion point which reduces to 0 modulo primes dividing p, and to the connected component of all special fibers of the Neron model of E. Then the anticyclotomic p-adic height of P is*

$$h_\rho(P) = \frac{1}{p}\log_p\left(\psi\left(\frac{\sigma_\pi(P)}{\sigma_\pi(P^c)}\right)\right) + \frac{1}{hp}\log_p\left(\psi\left(\frac{\mathbf{d}_h(P)^c}{\mathbf{d}_h(P)}\right)\right),$$

where $\psi : K_\pi \to \mathbb{Q}_p$ is the fixed isomorphism.

Proof. By (7) we have

$$(10) \qquad h_\rho(P) = \rho_\pi\left(\frac{\sigma_\pi(P)}{\sigma_\pi(P^c)}\right) + \sum_{w \nmid p\infty} \rho_w(d_w(P)).$$

---

[2] The formula appearing in [MST06, §2.9] contains a sign error which is corrected here.

Let $P = (x, y) \in E(K)$. Since P reduces to the identity modulo π and π^c, we have

$$\mathrm{ord}_\pi(x) = -2e_\pi, \quad \mathrm{ord}_\pi(y) = -3e_\pi,$$
$$\mathrm{ord}_{\pi^c}(x) = -2e_{\pi^c}, \quad \mathrm{ord}_{\pi^c}(y) = -3e_{\pi^c},$$

for positive integers e_π and e_{π^c}. Since the p-adic σ function has the form $\sigma(t) = t + \cdots \in t\mathbb{Z}_p[[t]]$, we see that

$$\mathrm{ord}_\pi(\sigma_\pi(P)) = \mathrm{ord}_\pi\left(\sigma_\pi\left(\frac{-x}{y}\right)\right) = \mathrm{ord}_\pi\left(\frac{-x}{y}\right) = e_\pi$$

and similarly

$$\mathrm{ord}_\pi(\sigma_\pi(P^c)) = \mathrm{ord}_\pi\left(\frac{-x^c}{y^c}\right) = \mathrm{ord}_{\pi^c}\left(\frac{-x}{y}\right) = e_{\pi^c}.$$

Thus,

$$(11) \qquad \mathrm{ord}_\pi\left(\frac{\sigma_\pi(P)}{\sigma_\pi(P^c)}\right) = e_\pi - e_{\pi^c}.$$

Let $\alpha \in K^\times$ generate the principal ideal π^h. By (11) and the definition of the anticyclotomic p-adic idele class character, we have

$$
\begin{aligned}
\rho_\pi\left(\frac{\sigma_\pi(P)}{\sigma_\pi(P^c)}\right) &= \frac{1}{hp}\log_p \circ \psi\left(\frac{\alpha^{e_{\pi^c} - e_\pi}\sigma_\pi(P)^h}{(\alpha^c)^{e_{\pi^c} - e_\pi}\sigma_\pi(P^c)^h}\right) \\
&= \frac{1}{p}\log_p\left(\psi\left(\frac{\sigma_\pi(P)}{\sigma_\pi(P^c)}\right)\right) + \frac{1}{hp}\log_p\left(\psi\left(\frac{\alpha}{\alpha^c}\right)^{e_{\pi^c} - e_\pi}\right).
\end{aligned}
$$

Now it remains to show that

$$(12) \qquad \sum_{w \nmid p\infty} \rho_w(d_w(P)) = \frac{1}{hp}\log_p\left(\psi\left(\frac{\mathbf{d}_h(P)^c}{\mathbf{d}_h(P)}\right)\right) - \frac{1}{hp}\log_p\left(\psi\left(\frac{\alpha}{\alpha^c}\right)^{e_{\pi^c} - e_\pi}\right).$$

By the definition of ρ, we have

$$(13) \qquad \sum_{w \nmid p\infty} \rho_w(d_w(P)) = \frac{1}{h}\sum_{w \nmid p\infty} \rho_w(d_w(P)^h).$$

Since $\mathrm{ord}_w(d_w(P)^h) = \mathrm{ord}_w(\mathbf{d}_h(P))$, Lemma 2.1 gives $\rho_w(d_w(P)^h) = \rho_w(\mathbf{d}_h(P))$ for every $w \nmid p\infty$. Substituting this into (13) gives

$$
\begin{aligned}
\sum_{w \nmid p\infty} \rho_w(d_w(P)) &= \frac{1}{h}\sum_{w \nmid p\infty} \rho_w(\mathbf{d}_h(P)) \\
&= \frac{1}{h}\sum_{w \nmid p\infty} \rho \circ \iota_w(\mathbf{d}_h(P)) \\
&= \frac{1}{h}\rho\left(\prod_{w \nmid p\infty} \iota_w(\mathbf{d}_h(P))\right).
\end{aligned}
$$

Now $\prod_{w \nmid p\infty} \iota_w(\mathbf{d}_h(P))$ is the idele with entry $\mathbf{d}_h(P)$ at every place $w \nmid p\infty$ and entry 1 at all other places. Define $\beta \in \mathcal{O}_K$ by $\mathbf{d}_h(P) = \alpha^{e_\pi}(\alpha^c)^{e_{\pi^c}}\beta$. Thus, by Proposition 1.5 and Remark 1.7, we get

$$
\begin{aligned}
\frac{1}{h}\rho\left(\prod_{w \nmid p\infty} \iota_w(\mathbf{d}_h(P))\right) &= \frac{1}{hp}\log_p\left(\psi\left(\frac{\beta^c}{\beta}\right)\right) \\
&= \frac{1}{hp}\log_p\left(\psi\left(\frac{\mathbf{d}_h(P)^c}{\mathbf{d}_h(P)}\right)\right) - \frac{1}{hp}\log_p\left(\psi\left(\frac{\alpha}{\alpha^c}\right)^{e_{\pi^c} - e_\pi}\right)
\end{aligned}
$$

as required. This concludes the proof.   □

In [MST06], the authors describe the "universal" p-adic height pairing $(P, Q) \in I(K)$ of two points $P, Q \in E(K)$. Composition of the universal height pairing with any $\mathbb{Q}_p$-linear map $\rho : I(K) \to \mathbb{Q}_p$ gives rise to a canonical symmetric bilinear pairing

$$(\, , \,)_\rho : E(K) \times E(K) \to \mathbb{Q}_p$$

called the ρ-*height pairing*. The ρ-height of a point $P \in E(K)$ is defined to be $-\frac{1}{2}(P, P)_\rho$.

Henceforth, we fix ρ to be the anticyclotomic p-adic idele class character defined in §1. The corresponding ρ-height pairing is referred to as the *anticyclotomic p-adic height pairing*, and it is denoted as follows:

$$\langle \, , \, \rangle = (\, , \,)_\rho : E(K) \times E(K) \to \mathbb{Q}_p$$

Observe that

$$\langle P, Q \rangle = h_\rho(P) + h_\rho(Q) - h_\rho(P + Q).$$

Let $E(K)^+$ and $E(K)^-$ denote the $+1$-eigenspace and the -1-eigenspace, respectively, for the action of complex conjugation on $E(K)$. Since σ_π is an odd function, using (8) we see that the anticyclotomic height satisfies

$$h_\rho(P) = 0 \quad \text{ for all } P \in E(K)^+ \cup E(K)^-.$$

Therefore, the anticyclotomic p-adic height pairing satisfies

(14) $$\langle E(K)^+, E(K)^+ \rangle = \langle E(K)^-, E(K)^- \rangle = 0.$$

Consequently, if $P \in E(K)^+$ and $Q \in E(K)^-$, then

(15) $$\begin{aligned} \langle P, Q \rangle &= h_\rho(P) + h_\rho(Q) - h_\rho(P + Q) \\ &= -\frac{1}{2}\langle P, P \rangle - \frac{1}{2}\langle Q, Q \rangle - h_\rho(P + Q) \\ &= -h_\rho(P + Q). \end{aligned}$$

3. The shadow line

Let E be an elliptic curve defined over $\mathbb{Q}$ and p an odd prime of good ordinary reduction. Fix an imaginary quadratic extension $K/\mathbb{Q}$ satisfying the Heegner hypothesis for $E/\mathbb{Q}$ (i.e., all primes dividing the conductor of $E/\mathbb{Q}$ split in K). Consider the anticyclotomic $\mathbb{Z}_p$-extension K_∞ of K. Let K_n denote the subfield of K_∞ whose Galois group over K is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. The module of *universal norms* for this $\mathbb{Z}_p$-extension is defined as follows:

$$\mathcal{U} := \bigcap_{n \geq 0} N_{K_n/K}(E(K_n) \otimes \mathbb{Z}_p) \subseteq E(K) \otimes \mathbb{Z}_p,$$

where $N_{K_n/K}$ is the norm map induced by the map $E(K_n) \to E(K)$ given by $P \mapsto \sum_{\sigma \in \mathrm{Gal}(K_n/K)} P^\sigma$.

By work of Cornut [Co02] and Vatsal [Va03] we know that for n large enough, we have a non-torsion Heegner point in $E(K_n)$. Since p is a prime of good ordinary reduction, the trace down to K_{n-1} of the Heegner points defined over K_n is related to Heegner points defined over K_{n-1}, see [BÇS, §2] for further details. Due to this relation among Heegner points defined over the different layers of K_∞, if the p-primary part of the Tate-Shafarevich group of E/K is finite then these points give rise to non-trivial universal norms. Hence, if the p-primary part of the Tate-Shafarevich group of E/K is finite then $\mathcal{U}$ is non-trivial whenever the Heegner hypothesis holds. By [Be95], [ÇW08], and [Çi09] we know that if $\mathrm{Gal}(\mathbb{Q}(E_p)/\mathbb{Q})$ is not solvable then $\mathcal{U} \simeq \mathbb{Z}_p$.

Consider

$$L_K := \mathcal{U} \otimes \mathbb{Q}_p.$$

If the p-primary part of the Tate-Shafarevich group of E/K is finite then L_K is a line in the vector space $E(K) \otimes \mathbb{Q}_p$ known as the *shadow line* associated to the triple (E, K, p). The space $E(K) \otimes \mathbb{Q}_p$ splits as the direct sum of two eigenspaces under the action of complex conjugation

$$E(K) \otimes \mathbb{Q}_p = E(K)^+ \otimes \mathbb{Q}_p \oplus E(K)^- \otimes \mathbb{Q}_p.$$

Observe that

$$E(K)^+ \otimes \mathbb{Q}_p = E(\mathbb{Q}) \otimes \mathbb{Q}_p \quad \text{and} \quad E(K)^- \otimes \mathbb{Q}_p \simeq E^K(\mathbb{Q}) \otimes \mathbb{Q}_p,$$

where E^K denotes the quadratic twist of E with respect to K. Since the module $\mathcal{U}$ is fixed by complex conjugation, the shadow line L_K lies in one of the eigenspaces:

$$L_K \subseteq E(\mathbb{Q}) \otimes \mathbb{Q}_p \quad \text{or} \quad L_K \subseteq E(K)^- \otimes \mathbb{Q}_p.$$

The assumption of the Heegner hypothesis forces the analytic rank of E/K to be odd, and hence the dimension of $E(K) \otimes \mathbb{Q}_p$ is odd by the Parity Conjecture [Ne01] and our assumption of the finiteness of the p-primary part of the Tate-Shafarevich group of E/K. Hence, $\dim E(K)^- \otimes \mathbb{Q}_p \neq \dim E(\mathbb{Q}) \otimes \mathbb{Q}_p$. The Sign Conjecture states that L_K is expected to lie in the eigenspace of higher dimension [MR03].

Our main motivating question is the following:

Question 3.1 (Mazur, Rubin). *Consider an elliptic curve $E/\mathbb{Q}$ of positive even analytic rank r, an imaginary quadratic field K such that E/K has analytic rank $r + 1$, and a prime p of good ordinary reduction such that the p-primary part of the Tate-Shafarevich group of $E/\mathbb{Q}$ is finite. By the Sign Conjecture, we expect L_K to lie in $E(\mathbb{Q}) \otimes \mathbb{Q}_p$. As K varies, we presumably get different shadow lines L_K. What are these lines and how are they distributed in $E(\mathbb{Q}) \otimes \mathbb{Q}_p$?*

Note that in the statement of the above question we make use of the following results:

(1) Since $E/\mathbb{Q}$ has positive even analytic rank we know that $\dim E(\mathbb{Q}) \otimes \mathbb{Q}_p \geq 2$ by work of Skinner-Urban [SU14, Theorem 2] and work of Nekovar [Ne01] on the Parity Conjecture.

(2) Since our assumptions on the analytic ranks of $E/\mathbb{Q}$ and E/K imply that the analytic rank of $E^K/\mathbb{Q}$ is 1, by work of Gross-Zagier [GZ] and Kolyvagin [Ko90] we know that

    (a) $\dim E(K)^- \otimes \mathbb{Q}_p = 1$;

    (b) the p-primary part of the Tate-Shafarevich group of $E^K/\mathbb{Q}$ is finite, and hence the finiteness of the p-primary part of the Tate-Shafarevich group of E/K follows from the finiteness of the p-primary part of the Tate-Shafarevich group of $E/\mathbb{Q}$.

Thus by (2b) we know that $L_K \subseteq E(K) \otimes \mathbb{Q}_p$, while (1) and (2a) are the input to the Sign Conjecture.

It is natural to start the study of Question 3.1 by considering elliptic curves $E/\mathbb{Q}$ of analytic rank 2. In this case, assuming that

$$(16) \qquad\qquad\qquad\qquad\qquad \text{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 2,$$

we identify L_K in $E(\mathbb{Q}) \otimes \mathbb{Q}_p$ by making use of the anticyclotomic p-adic height pairing, viewing it as a pairing on $E(K) \otimes \mathbb{Z}_p$. This method forces us to restrict our attention to quadratic fields K where p splits. It is known that $\mathcal{U}$ is contained in the kernel of the anticyclotomic p-adic height pairing [MT83, Proposition 4.5.2]. In fact, in our situation, the properties of this pairing and (16) together with the fact that $\dim E(K)^- \otimes \mathbb{Q}_p = 1$ imply that either $\mathcal{U}$ is the kernel of the pairing or the pairing is trivial. Thus computing the anticyclotomic p-adic height pairing allows us to verify the Sign Conjecture and determine the shadow line L_K.

In order to describe the lines L_K for multiple quadratic fields K, we fix two independent generators P_1, P_2 of $E(\mathbb{Q}) \otimes \mathbb{Q}_p$ (with E given by its reduced minimal model) and compute the slope of $L_K \otimes \mathbb{Q}_p$ in the corresponding coordinate system. For each quadratic field K we compute a non-torsion point $R \in E(K)^-$ (on the reduced minimal model of E). The kernel of the anticyclotomic p-adic height pairing on $E(K) \otimes \mathbb{Z}_p$ is generated by $aP_1 + bP_2$ for $a, b \in \mathbb{Z}_p$ such that $\langle aP_1 + bP_2, R \rangle = 0$. Then by (15) the shadow line $L_K \otimes \mathbb{Q}_p$

in $E(\mathbb{Q}) \otimes \mathbb{Q}_p$ is generated by $h_\rho(P_2 + R)P_1 - h_\rho(P_1 + R)P_2$ and its slope with respect to the coordinate system induced by $\{P_1, P_2\}$ equals

$$-h_\rho(P_1 + R)/h_\rho(P_2 + R).$$

4. Algorithms

Let $E/\mathbb{Q}$ be an elliptic curve of analytic rank 2; see [Br00, Chapter 4] for an algorithm that can provably verify the non-triviality of the second derivative of the L-function. Our aim is to compute shadow lines on the elliptic curve E. In order to do this using the method described in §3 we need to

- verify that $\mathrm{rank}_\mathbb{Z} E(\mathbb{Q}) = 2$, and
- compute two $\mathbb{Z}$-independent points $P_1, P_2 \in E(\mathbb{Q})$.

By work of Kato [Ka04, Theorem 17.4], computing the ℓ-adic analytic rank of $E/\mathbb{Q}$ for any prime ℓ of good ordinary reduction gives an upper bound on $\mathrm{rank}_\mathbb{Z} E(\mathbb{Q})$ (see [SW13, Proposition 10.1]). Using the techniques in [SW13, §3], which have been implemented in Sage, one can compute an upper bound on the ℓ-adic analytic rank using an approximation of the ℓ-adic L-series, thereby obtaining an upper bound on $\mathrm{rank}_\mathbb{Z} E(\mathbb{Q})$. Since the analytic rank of $E/\mathbb{Q}$ is 2, barring the failure of standard conjectures we find that $\mathrm{rank}_\mathbb{Z} E(\mathbb{Q}) \leq 2$. Then using work of Cremona [Cr97, Section 3.5] implemented in Sage, we search for points of bounded height, increasing the height until we find two $\mathbb{Z}$-independent points $P_1, P_2 \in E(\mathbb{Q})$. We have thus computed a basis of $E(\mathbb{Q}) \otimes \mathbb{Q}_p$.

We will now proceed to describe the algorithms that allow us to compute shadow lines on the elliptic curve $E/\mathbb{Q}$.

Algorithm 4.1. *Generator of $E(K)^- \otimes \mathbb{Q}_p$.*

Input:
- *an elliptic curve $E/\mathbb{Q}$ (given by its reduced minimal model) of analytic rank 2,*
- *an odd prime p of good ordinary reduction;*
- *an imaginary quadratic field K such that*
    - *the analytic rank of E/K equals 3, and*
    - *all rational primes dividing the conductor of $E/\mathbb{Q}$ split in K.*

Output: A generator of $E(K)^- \otimes \mathbb{Q}_p$ (given as a point on the reduced minimal model of $E/\mathbb{Q}$).

(1) *Let $d \in \mathbb{Z}$ such that $K = \mathbb{Q}(\sqrt{d})$. Compute a short model of E^K, of the form $y^2 = x^3 + ad^2x + bd^3$.*
(2) *Our assumption on the analytic ranks of $E/\mathbb{Q}$ and E/K implies that the analytic rank of $E^K/\mathbb{Q}$ is 1. Compute a non-torsion point[3] of $E^K(\mathbb{Q})$ and denote it (x_0, y_0). Then $(\frac{x_0}{d}, \frac{y_0\sqrt{d}}{d^2})$ is an element of $E(K)$ on the model $y^2 = x^3 + ax + b$.*
(3) *Output the image of $(\frac{x_0}{d}, \frac{y_0\sqrt{d}}{d^2})$ on the reduced minimal model of E.*

Algorithm 4.2. *Computing the anticyclotomic p-adic height associated to (E, K, p).*
Input:
- *elliptic curve $E/\mathbb{Q}$ (given by its reduced minimal model);*
- *an odd prime p of good ordinary reduction;*

---

[3]Note that by [GZ] and [Ko90] the analytic rank of $E^K/\mathbb{Q}$ being 1 implies that the algebraic rank of $E^K/\mathbb{Q}$ is 1 and the Tate-Shafarevich group of $E^K/\mathbb{Q}$ is finite. Furthermore, in this case, computing a non-torsion point in $E^K(\mathbb{Q})$ can be done by choosing an auxiliary imaginary quadratic field F satisfying the Heegner hypothesis for $E^K/\mathbb{Q}$ such that the analytic rank of E^K/F is 1 and computing the corresponding basic Heegner point in $E^K(F)$.

- *an imaginary quadratic field K such that p splits in $K/\mathbb{Q}$;*
- *a non-torsion point $P \in E(K)$.*

Output: The anticyclotomic p-adic height of P.

(1) *Let $p\mathcal{O}_K = \pi\pi^c$. Fix an identification $\psi : K_\pi \simeq \mathbb{Q}_p$. In particular, $v_p(\psi(\pi)) = 1$.*

(2) *Let $m_0 = \operatorname{lcm}\{c_\ell\}$, where ℓ runs through the primes of bad reduction for $E/\mathbb{Q}$ and c_ℓ is the Tamagawa number at ℓ. Compute[4] $R = m_0 P$.*

(3) *Determine the smallest positive integer n such that nR and nR^c reduce to $0 \in E(\mathbb{F}_p)$ modulo π. Note that n is a divisor of $\#E(\mathbb{F}_p)$. Compute $T = nR$.*

(4) *Compute $\mathbf{d}_h(R) \in \mathcal{O}_K$ defined in (9) as a generator of the ideal*

$$\prod_{\mathfrak{q}} \mathfrak{q}^{h \operatorname{ord}_{\mathfrak{q}}(\delta(R))/2}$$

where h is the class number of K, the product is over all prime ideals $\mathfrak{q}$ of $\mathcal{O}_K$, and $\delta(R)$ is the denominator ideal of $x(R)\mathcal{O}_K$.

(5) *Let f_n denote the nth division polynomial associated to E. Compute $\mathbf{d}_h(T) = \mathbf{d}_h(nR) = f_n(R)^h \mathbf{d}_h(R)^{n^2}$. Note that by Step (2) and Proposition 1 of Wuthrich [Wu04] we see that $f_n(R)^h \mathbf{d}_h(R)^{n^2} \in \mathcal{O}_K$ since $\mathbf{d}_h(T)$ is an element of K that is integral at every finite prime.*

(6) *Compute $\sigma_\pi(t) := \sigma_p(t)$ as a formal power series in $t\mathbb{Z}_p[[t]]$ with sufficient precision. This equality holds since our elliptic curve E is defined over $\mathbb{Q}$.*

(7) *We use Proposition 2.4 to determine the anticyclotomic p-adic height of T: compute*

$$
\begin{aligned}
h_\rho(T) &= \frac{1}{p}\log_p\left(\psi\left(\frac{\sigma_\pi(T)}{\sigma_\pi(T^c)}\right)\right) + \frac{1}{hp}\log_p\left(\psi\left(\frac{\mathbf{d}_h(T)^c}{\mathbf{d}_h(T)}\right)\right) \\
&= \frac{1}{p}\log_p\left(\psi\left(\frac{\sigma_p\left(\frac{-x(T)}{y(T)}\right)}{\sigma_p\left(\frac{-x(T)^c}{y(T)^c}\right)}\right)\right) + \frac{1}{hp}\log_p\left(\psi\left(\frac{\mathbf{d}_h(T)^c}{\mathbf{d}_h(T)}\right)\right) \\
&= \frac{1}{p}\log_p\left(\frac{\sigma_p\left(\psi\left(\frac{-x(T)}{y(T)}\right)\right)}{\sigma_p\left(\psi\left(\frac{-x(T)^c}{y(T)^c}\right)\right)}\right) + \frac{1}{hp}\log_p\left(\psi\left(\frac{\mathbf{d}_h(T)^c}{\mathbf{d}_h(T)}\right)\right).
\end{aligned}
$$

(8) *Output the anticyclotomic p-adic height of P: compute[5]*

$$h_\rho(P) = \frac{1}{n^2 m_0^2} h_\rho(T).$$

Algorithm 4.3. *Shadow line attached to (E, K, p).*
Input:

- *an elliptic curve $E/\mathbb{Q}$ (given by its reduced minimal model) of analytic rank 2 such that $\operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 2$;*
- *an odd prime p of good ordinary reduction such that the p-primary part of the Tate-Shafarevich group of $E/\mathbb{Q}$ is finite;*
- *two $\mathbb{Z}$-independent points $P_1, P_2 \in E(\mathbb{Q})$;*
- *an imaginary quadratic field K such that*

---

[4]Note that Step 2 and Step 3 are needed to ensure that the point whose anticyclotomic p-adic height we will compute using formula (7) satisfies the required conditions.

[5]As a consistency check we compute the height of nP and verify that $h_\rho(nP) = \frac{1}{n^2} h_\rho(P)$ for positive integers $n \leq 5$.

  − *the analytic rank of E/K equals 3, and*

  − *p and all rational primes dividing the conductor of $E/\mathbb{Q}$ split in K.*

Output: The slope of the shadow line $L_K \subseteq E(\mathbb{Q}) \otimes \mathbb{Q}_p$ with respect to the coordinate system induced by $\{P_1, P_2\}$.

(1) *Use Algorithm 4.1 to compute a non-torsion point $S \in E(K)^-$. We then have generators P_1, P_2, S of $E(K) \otimes \mathbb{Q}_p$ such that $P_1, P_2 \in E(\mathbb{Q})$ and $S \in E(K)^-$ (given as points on the reduced minimal model of $E/\mathbb{Q}$).*

(2) *Compute $P_1 + S$ and $P_2 + S$.*

(3) *Use Algorithm 4.2 to compute[6] the anticyclotomic p-adic heights: $h_\rho(P_1+S)$ and $h_\rho(P_2+S)$. Finding that at least one of these heights is non-trivial implies that the shadow line associated to (E, K, p) lies in $E(\mathbb{Q}) \otimes \mathbb{Q}_p$, i.e., the Sign Conjecture holds for (E, K, p).*

(4) *The point $h_\rho(P_2 + S)P_1 - h_\rho(P_1 + S)P_2$ is a generator of the shadow line associated to (E, K, p). Output the slope of the shadow line $L_K \subseteq E(\mathbb{Q}) \otimes \mathbb{Q}_p$ with respect to the coordinate system induced by $\{P_1, P_2\}$: compute*
$$-h_\rho(P_1 + S)/h_\rho(P_2 + S) \in \mathbb{Q}_p.$$

5. Examples

Let E be the elliptic curve "389.a1" [L, Elliptic Curve 389.a1] given by the model
$$y^2 + y = x^3 + x^2 - 2x.$$

We know that the analytic rank of $E/\mathbb{Q}$ equals 2 [Br00, §6.1] and $\operatorname{rank}_\mathbb{Z} E(\mathbb{Q}) = 2$, see [Cr97]. In addition, 5 and 7 are good ordinary primes for E. We find two $\mathbb{Z}$-independent points
$$P_1 = (-1, 1), P_2 = (0, 0) \in E(\mathbb{Q}).$$

We will now use the algorithms described in §4 to compute the slopes of two shadow lines on $E(\mathbb{Q}) \otimes \mathbb{Q}_5$ with respect to the coordinate system induced by $\{P_1, P_2\}$.

5.1. **Shadow line attached to** $\left("389.a1", \mathbb{Q}(\sqrt{-11}), 5\right)$**.** The imaginary quadratic field $K = \mathbb{Q}(\sqrt{-11})$ satisfies the Heegner hypothesis for E and the quadratic twist E^K has analytic rank 1. Moreover, the prime 5 splits in K.

We use Algorithm 4.1 to find a non-torsion point $S = (\frac{1}{4}, \frac{1}{8}\sqrt{-11} - \frac{1}{2}) \in E(K)^-$. We now proceed to compute the anticyclotomic p-adic heights of $P_1 + S$ and $P_2 + S$ which are needed to determine the slope of the shadow line associated to the triple $\left("389.a1", \mathbb{Q}(\sqrt{-11}), 5\right)$. We begin by computing
$$A_1 := P_1 + S = \left(-\frac{6}{25}\sqrt{-11} + \frac{27}{25}, -\frac{62}{125}\sqrt{-11} + \frac{29}{125}\right),$$
$$A_2 := P_2 + S = (-2\sqrt{-11}, -4\sqrt{-11} - 12).$$

We carry out the steps of Algorithm 4.2 to compute $h_\rho(A_1)$:

(1) Let $5\mathcal{O}_K = \pi\pi^c$, where $\pi = (\frac{1}{2}\sqrt{-11} + \frac{3}{2})$ and $\pi^c = (-\frac{1}{2}\sqrt{-11} + \frac{3}{2})$. This allows us to fix an identification
$$\psi : K_\pi \to \mathbb{Q}_5$$
that sends
$$\frac{1}{2}\sqrt{-11} + \frac{3}{2} \mapsto 2 \cdot 5 + 5^2 + 3 \cdot 5^3 + 4 \cdot 5^4 + 4 \cdot 5^5 + 3 \cdot 5^7 + 5^8 + 5^9 + O(5^{10}).$$

---

[6]We compute the height of $P_1 + P_2 + S$ as a consistency check.

(2) Since the Tamagawa number at 389 is trivial, i.e., $c_{389} = 1$, we have $m_0 = 1$. Thus $R = A_1$.

(3) We find that $n = 9$ is the smallest multiple of R and R^c such that both points reduce to 0 in $E(\mathcal{O}_K/\pi)$. Set $T = 9R$.

(4) Note that the class number of K is $h = 1$. We find $\mathbf{d}_h(R) = \frac{1}{2}\sqrt{-11} - \frac{3}{2}$.

(5) Let f_9 denote the 9th division polynomial associated to E. We compute

$$\mathbf{d}_h(T) = \mathbf{d}_h(9R)$$
$$= f_9(R)\mathbf{d}_h(R)^{9^2}$$
$$= 242270418622475167540889257109222259344570\sqrt{-11}$$
$$- 1473553998959120341158969425573952631751125.$$

(6) We compute

$$\sigma_\pi(t) := \sigma_5(t)$$
$$= t + \left(4 + 5 + 3 \cdot 5^2 + 5^3 + 2 \cdot 5^4 + 3 \cdot 5^5 + 2 \cdot 5^6 + O(5^8)\right) t^3$$
$$+ \left(3 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 + 2 \cdot 5^5 + 2 \cdot 5^6 + O(5^7)\right) t^4$$
$$+ \left(1 + 5 + 5^2 + 5^3 + 3 \cdot 5^4 + 3 \cdot 5^5 + O(5^6)\right) t^5$$
$$+ \left(4 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 3 \cdot 5^4 + O(5^5)\right) t^6$$
$$+ \left(4 + 3 \cdot 5 + 4 \cdot 5^2 + O(5^4)\right) t^7 + \left(3 + 3 \cdot 5^2 + O(5^3)\right) t^8$$
$$+ \left(3 \cdot 5 + O(5^2)\right) t^9 + \left(2 + O(5)\right) t^{10} + O(t^{11}).$$

(7) We use Proposition 2.4 to determine the anticyclotomic p-adic height of T: we compute

$$h_\rho(T) = \frac{1}{p} \log_p \left(\psi \left(\frac{\sigma_\pi(T)}{\sigma_\pi(T^c)} \right) \right) + \frac{1}{hp} \log_p \left(\psi \left(\frac{\mathbf{d}_h(T)^c}{\mathbf{d}_h(T)} \right) \right)$$
$$= \frac{1}{p} \log_p \left(\frac{\sigma_p \left(\psi \left(\frac{-x(T)}{y(T)} \right) \right)}{\sigma_p \left(\psi \left(\frac{-x(T)^c}{y(T)^c} \right) \right)} \right) + \frac{1}{hp} \log_p \left(\psi \left(\frac{\mathbf{d}_h(T)^c}{\mathbf{d}_h(T)} \right) \right)$$
$$= 3 + 5 + 5^2 + 4 \cdot 5^4 + 3 \cdot 5^5 + 4 \cdot 5^7 + 3 \cdot 5^8 + 5^9 + O(5^{10}).$$

(8) We output the anticyclotomic p-adic height of A_1:

$$h_\rho(A_1) = \frac{1}{9^2} h_\rho(T)$$
$$= 3 + 3 \cdot 5 + 3 \cdot 5^2 + 2 \cdot 5^4 + 4 \cdot 5^5 + 4 \cdot 5^6 + 3 \cdot 5^8 + O(5^{10}).$$

Repeating Steps (1) – (8) for A_2 yields

$$h_\rho(A_2) = 3 + 2 \cdot 5 + 4 \cdot 5^2 + 2 \cdot 5^5 + 5^6 + 4 \cdot 5^7 + 4 \cdot 5^9 + O(5^{10}).$$

As a consistency check, we also compute

$$h_\rho(P_1 + P_2 + S) = 1 + 5 + 3 \cdot 5^2 + 5^3 + 2 \cdot 5^4 + 5^5 + 5^6 + 4 \cdot 5^8 + 4 \cdot 5^9 + O(5^{10}).$$

Observe that, numerically, we have

$$h_\rho(P_1 + P_2 + S) = h_\rho(P_1 + S) + h_\rho(P_2 + S).$$

The slope of the shadow line $L_K \subseteq E(\mathbb{Q}) \otimes \mathbb{Q}_p$ with respect to the coordinate system induced by $\{P_1, P_2\}$ is thus

$$-\frac{h_\rho(P_1 + S)}{h_\rho(P_2 + S)} = 4 + 2 \cdot 5 + 5^2 + 3 \cdot 5^3 + 5^4 + 5^6 + 5^7 + O(5^{10}).$$

5.2. **Shadow line attached to** $\left(\text{``389.}a1\text{''}, \mathbb{Q}(\sqrt{-24}), 5\right)$**.** Consider the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-24})$. Note that K satisfies the Heegner hypothesis for E, the twist E^K has analytic rank 1, and the prime 5 splits in K.

Using Algorithm 4.1 we find a non-torsion point $S = \left(\frac{1}{2}, \frac{1}{8}\sqrt{-24} - \frac{1}{2}\right) \in E(K)^-$. We then compute

$$P_1 + S = \left(-\frac{1}{6}\sqrt{-24} + \frac{1}{3}, -\frac{5}{18}\sqrt{-24} - 1\right)$$

$$P_2 + S = \left(-\frac{1}{2}\sqrt{-24} - 2, -6\right).$$

Many of the steps taken to compute $h_\rho(P_1 + S)$ and $h_\rho(P_2 + S)$ are quite similar to those in §5.1. One notable difference is that in this example the class number h of K is equal to 2. We find that

$$h_\rho(P_1 + S) = 4 + 2 \cdot 5 + 3 \cdot 5^4 + 2 \cdot 5^5 + 4 \cdot 5^6 + 2 \cdot 5^7 + 5^8 + 2 \cdot 5^9 + O(5^{10}),$$

$$h_\rho(P_2 + S) = 1 + 5 + 5^3 + 5^5 + 2 \cdot 5^6 + 4 \cdot 5^7 + 2 \cdot 5^8 + 3 \cdot 5^9 + O(5^{10}).$$

In addition, we compute $h_\rho(P_1 + P_2 + S)$ and verify that

$$h_\rho(P_1 + P_2 + S) = 4 \cdot 5 + 5^3 + 3 \cdot 5^4 + 3 \cdot 5^5 + 5^6 + 2 \cdot 5^7 + 4 \cdot 5^8 + O(5^{10})$$
$$= h_\rho(P_1 + S) + h_\rho(P_2 + S).$$

This gives that the slope of the shadow line $L_K \subseteq E(\mathbb{Q}) \otimes \mathbb{Q}_p$ with respect to the coordinate system induced by $\{P_1, P_2\}$ is

$$-\frac{h_\rho(P_1 + S)}{h_\rho(P_2 + S)} = 1 + 5 + 3 \cdot 5^2 + 3 \cdot 5^5 + 3 \cdot 5^6 + 3 \cdot 5^7 + 2 \cdot 5^8 + 5^9 + O(5^{10}).$$

5.3. **Summary of results of additional computations of shadow lines.** The algorithms developed in §4 enable us to compute shadow lines in many examples which is what is needed to initiate a study of Question 3.1. We will now list some results of additional computations of slopes of shadow lines on the elliptic curve "389.a1". In the following two tables we fix the prime $p = 5, 7$ respectively, and vary the quadratic field.

TABLE 1. Slopes of shadow lines for $\left(\text{``389.}a1\text{''}, K, 5\right)$

K	slope
$\mathbb{Q}(\sqrt{-11})$	$4 + 2 \cdot 5 + 5^2 + 3 \cdot 5^3 + 5^4 + 5^6 + 5^7 + O(5^{10})$
$\mathbb{Q}(\sqrt{-19})$	$1 + 4 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^5 + 5^6 + 4 \cdot 5^7 + 3 \cdot 5^8 + 4 \cdot 5^9 + O(5^{10})$
$\mathbb{Q}(\sqrt{-24})$	$1 + 5 + 3 \cdot 5^2 + 3 \cdot 5^5 + 3 \cdot 5^6 + 3 \cdot 5^7 + 2 \cdot 5^8 + 5^9 + O(5^{10})$
$\mathbb{Q}(\sqrt{-59})$	$4 + 5 + 4 \cdot 5^2 + 5^3 + 2 \cdot 5^4 + 2 \cdot 5^5 + 3 \cdot 5^7 + 4 \cdot 5^8 + 2 \cdot 5^9 + O(5^{10})$
$\mathbb{Q}(\sqrt{-79})$	$2 + 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 4 \cdot 5^4 + 4 \cdot 5^5 + 3 \cdot 5^6 + 3 \cdot 5^7 + 3 \cdot 5^8 + 2 \cdot 5^9 + O(5^{10})$
$\mathbb{Q}(\sqrt{-91})$	$4 + 3 \cdot 5 + 5^2 + 5^4 + 2 \cdot 5^5 + 4 \cdot 5^6 + 5^7 + 2 \cdot 5^9 + O(5^{10})$
$\mathbb{Q}(\sqrt{-111})$	$5^{-2} + 4 \cdot 5^{-1} + 4 + 4 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + 4 \cdot 5^4 + 2 \cdot 5^5 + 3 \cdot 5^6 + 5^7 + 2 \cdot 5^8 + 5^9 + O(5^{10})$
$\mathbb{Q}(\sqrt{-119})$	$4 \cdot 5^{-1} + 2 + 2 \cdot 5 + 2 \cdot 5^2 + 4 \cdot 5^3 + 4 \cdot 5^4 + 2 \cdot 5^5 + 5^6 + 4 \cdot 5^7 + 4 \cdot 5^8 + 4 \cdot 5^9 + O(5^{10})$
$\mathbb{Q}(\sqrt{-159})$	$2 \cdot 5 + 4 \cdot 5^4 + 4 \cdot 5^5 + 5^6 + 5^7 + 4 \cdot 5^8 + 5^9 + O(5^{10})$
$\mathbb{Q}(\sqrt{-164})$	$3 + 2 \cdot 5 + 4 \cdot 5^2 + 5^3 + 4 \cdot 5^4 + 3 \cdot 5^5 + 3 \cdot 5^6 + 3 \cdot 5^8 + 4 \cdot 5^9 + O(5^{10})$

TABLE 2. Slopes of shadow lines for $\left(\text{“389.a1”}, K, 7\right)$

K	slope
$\mathbb{Q}(\sqrt{-19})$	$3 + 2 \cdot 7 + 2 \cdot 7^2 + 3 \cdot 7^3 + 7^4 + 7^5 + 4 \cdot 7^7 + 6 \cdot 7^9 + O(7^{10})$
$\mathbb{Q}(\sqrt{-20})$	$1 + 5 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 + 2 \cdot 7^4 + 3 \cdot 7^5 + 3 \cdot 7^6 + 3 \cdot 7^7 + O(7^{10})$
$\mathbb{Q}(\sqrt{-24})$	$1 + 3 \cdot 7 + 3 \cdot 7^2 + 2 \cdot 7^3 + 6 \cdot 7^4 + 2 \cdot 7^5 + 2 \cdot 7^6 + 6 \cdot 7^7 + 2 \cdot 7^8 + O(7^{10})$
$\mathbb{Q}(\sqrt{-52})$	$1 + 5 \cdot 7 + 7^2 + 3 \cdot 7^3 + 3 \cdot 7^4 + 2 \cdot 7^5 + 5 \cdot 7^6 + 3 \cdot 7^9 + O(7^{10})$
$\mathbb{Q}(\sqrt{-55})$	$1 + 7 + 6 \cdot 7^2 + 3 \cdot 7^3 + 5 \cdot 7^4 + 3 \cdot 7^5 + 7^7 + 4 \cdot 7^9 + O(7^{10})$
$\mathbb{Q}(\sqrt{-59})$	$2 + 7 + 3 \cdot 7^2 + 3 \cdot 7^3 + 5 \cdot 7^4 + 5 \cdot 7^5 + 2 \cdot 7^6 + 4 \cdot 7^7 + 7^8 + 6 \cdot 7^9 + O(7^{10})$
$\mathbb{Q}(\sqrt{-68})$	$4 + 4 \cdot 7 + 2 \cdot 7^3 + 5 \cdot 7^4 + 5 \cdot 7^5 + 7^6 + 7^7 + 5 \cdot 7^8 + 5 \cdot 7^9 + O(7^{10})$
$\mathbb{Q}(\sqrt{-87})$	$3 \cdot 7 + 4 \cdot 7^2 + 7^3 + 2 \cdot 7^4 + 2 \cdot 7^5 + 7^6 + 5 \cdot 7^7 + 7^9 + O(7^{10})$
$\mathbb{Q}(\sqrt{-111})$	$7^{-2} + 2 \cdot 7^{-1} + 5 + 2 \cdot 7 + 7^2 + 2 \cdot 7^3 + 6 \cdot 7^4 + 5 \cdot 7^5 + 7^6 + 2 \cdot 7^7 + 2 \cdot 7^9 + O(7^{10})$
$\mathbb{Q}(\sqrt{-143})$	$5 + 5 \cdot 7 + 2 \cdot 7^3 + 4 \cdot 7^4 + 3 \cdot 7^5 + 3 \cdot 7^6 + 2 \cdot 7^7 + 2 \cdot 7^9 + O(7^{10})$

REFERENCES

[BÇS] J. S. Balakrishnan, M. Çiperiani, and W. Stein, *p-adic heights of Heegner points and Λ-adic regulators*, Math. Comp. **84** (2015), no. 292, 923–954.

[Be95] M. Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions*, Compositio Math. 99 (1995), no. 2, 153–182.

[Br00] R.W. Bradshaw, *Provable computation of motivic L-functions*, Thesis (Ph.D.)University of Washington. 2010.

[ÇW08] M. Çiperiani and A. Wiles, *Solvable points on genus one curves*, Duke Math. J. 142 (2008), 381–464.

[Çi09] M. Çiperiani *Tate-Shafarevich groups in anticyclotomic $\mathbb{Z}_p$-extensions at supersingular primes*, Compositio Mathematica 145 (2009), 293–308.

[Co02] C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. 148 (2002), 495–523.

[Cr97] J.E. Cremona, *Algorithms for modular elliptic curves*, Second edition, Cambridge University Press, Cambridge, 1997.

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

[Ka04] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms, Cohomologies p-adiques et application arithmétiques. III*, Astérisque, vol. 295, Société Mathématique de France, Paris, 2004.

[Ko90] V.A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., 87, Birkhauser Boston, Boston, MA, 1990, 435–483.

[L] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, http://www.lmfdb.org, 2014 , [Online; accessed 14 October 2014].

[MR03] B. Mazur and K. Rubin, *Studying the growth of Mordell-Weil*, Doc. Math. 2003, Extra Vol., 585–607.

[MST06] B. Mazur, W. Stein, and J. Tate. *Computation of p-adic heights and log convergence*, Doc. Math. 2006, Extra Vol., 577–614.

[MT83] B. Mazur and J. Tate, *Canonical height pairings via biextensions*, Arithmetic and geometry, Vol. I, 195–237, Progr. Math., 35, Birkhuser Boston, Boston, MA, 1983.

[Ne01] J. Nekovář, *On the parity of ranks of Selmer groups. II*, C. R. Acad. Sci. Paris Ser. I Math. 332 (2001), no. 2, 99–104.

[SU14] C. Skinner and E. Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. 195 (2014), no. 1, 1–277.

[SW13] W. Stein and C. Wuthrich, *Algorithms for the arithmetic of elliptic curves using Iwasawa theory*, Math. Comp. 82 (2013), no. 283, 1757–1792.

[Va03] V. Vatsal, *Special values of anticyclotomic L-functions*, Duke Math. J. 116 (2003), 219–261.

[Wa97] L. C. Washington, *Introduction to cyclotomic fields*, Second edition, Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997.

[Wu04] C. Wuthrich, *On p-adic heights in families of elliptic curves*, J. London Math. Soc. (2) 70 (2004), no. 1, 23–40.

J. S. Balakrishnan, Mathematical Institute, University of Oxford, Woodstock Road, Oxford OX2 6GG, UK
 E-mail address: balakrishnan@maths.ox.ac.uk

M. Çiperiani, Department of Mathematics, The University of Texas at Austin, 1 University Station, C1200 Austin, Texas 78712, USA
 E-mail address: mirela@math.utexas.edu

J. Lang, UCLA Mathematics Department, Box 951555, Los Angeles, CA 90095-1555, USA
 E-mail address: jaclynlang@math.ucla.edu

B. Mirza, Department of Mathematics and Statistics, McGill University, 805 Sherbrooke Street West, Montreal, Quebec, Canada, H3A 0B9
 E-mail address: mirza@math.mcgill.ca

R. Newton, Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany
 E-mail address: rachel@mpim-bonn.mpg.de