FINDING INTEGRAL POINTS ON ELLIPTIC CURVES OVER IMAGINARY QUADRATIC FIELDS

AASHRAYA JHA

Abstract. We determine the quadratic Chabauty set for integral points on elliptic curves of rank 2 defined over imaginary quadratic fields using quadratic Chabauty. This builds on the work of Bianchi [Bia20] and Balakrishnan et al. [BBBM21]. We give the first instance of the implementation of anticyclotomic heights for curves which are not base changes, along with an implementation of a certain sieve for elliptic curves introduced by Balakrishnan et al. [BBM17] and used by Bianchi [Bia20] to determine integral points of rank 2. We give the first example of the determination of the integral points of an elliptic curve of rank 2 defined over an imaginary quadratic field, which is not a base change via quadratic Chabauty.

Contents

1. Introduction

Let K be a number field with O_K its ring of integers. Let C/K be a smooth, projective, and geometrically irreducible curve, henceforth called a *nice curve*. Let $\mathcal{U}/O_K$ be an affine scheme with projective closure $\mathcal{C}$ such that $\mathcal{C} \times \operatorname{Spec} K \cong C$. Let g be the genus of C. In 1929, Siegel [Sie14]

Date: November 2, 2023.

showed that the set $\mathcal{U}(O_K)$ is finite if $g \geq 1$. For $g \geq 2$, this was superseded by Faltings's theorem in 1983 [Fal83], which shows $C(K)$ is finite for $g \geq 2$.

Neither of these proofs can be made effective; that is, we can not use them to explicitly determine the sets $C(K)$ or $\mathcal{U}(O_K)$. There has been significant progress in determining the sets $\mathcal{U}(O_K)$ and $C(K)$ via p-adic methods of Chabauty and Coleman. Let J be the Jacobian of C and r be the rank of $J(K)$. In his paper [Cha41], Chabauty showed the set $C(K)$ is finite if $r < g$.

We give a heuristic explaining why we might expect this when $K = \mathbb{Q}$. We first pick a prime of good reduction, say p.

We can identify C as a subvariety of J via the Abel-Jacobi map $\iota : C \hookrightarrow J$. If we have $r \leq g-1$, then the closure $\overline{J(K)} \subseteq J(\mathbb{Q}_p)$ has dimension at most r (as an analytic variety over $\mathbb{Q}_p$), and the curve $C_{\mathbb{Q}_p}$ has dimension 1. Since $r+1 \leq g$, we expect the intersection $\overline{J(K)} \cap C_{\mathbb{Q}_p}$ to be finite.

Chabauty constructs functions that vanish on this intersection, which Coleman [Col85] later identified as p-adic (Coleman) integrals of holomorphic differential forms. The method of Chabauty-Coleman relies on the image of the map

$$\log : J(\mathbb{Q}) \otimes \mathbb{Q}_p \to H^0(X_{\mathbb{Q}_p}, \Omega^1)^\vee \tag{1}$$

having positive codimension, which is used to write down abelian integrals vanishing at the rational points.

Kim's work [Kim09] gave rise to the *non-abelian* Chabauty program, which aims to remove the restriction of $r < g$. Kim's method considers unipotent quotients of the $\mathbb{Q}_p$-étale fundamental group of C and looks at the Selmer schemes attached to these quotients. In [Kim10] and its appendix [BKK11], the authors show that a certain p-adic locally analytic function is constant on integral points of elliptic curves with Tamagawa product 1. This p-adic function is a linear combination of an iterated Coleman integral and the square of an abelian Coleman integral.

Let p be a prime of good reduction. We let

$$h \colon C(\mathbb{Q}) \to \mathbb{Q}_p$$

denote the global height of Coleman and Gross [CG89], and for finite places v of K, we let

$$h_v : C(\mathbb{Q}_v) \to \mathbb{Q}_p$$

denote the local heights of Coleman and Gross. We have $h = \sum_v h_v|_{C(\mathbb{Q})}$. In [BB15], the authors extend the function $h - h_p$ to a locally analytic function on $C(\mathbb{Q}_p)$, and show that this function is a scalar multiple of the Coleman function in [Kim10] and [BKK11] . In [BBM16], the authors further extend this approach to hyperelliptic curves. Let C be a hyperelliptic curve defined by $y^2 - f(x)$ where f has degree $2g+1$, and let

$$\mathcal{U} := \operatorname{Spec} \mathbb{Z}[x,y]/(y^2 - f(x))).$$

They prove the following theorem regarding integral points on hyperelliptic curves.

Theorem 1.1. [BBM16, Theorem 3.1] *Suppose that $r = g$ and that the log map in* (1) *is an isomorphism. Then there exists an explicitly computable finite set $T \subset \mathbb{Q}_p$ and an explicitly computable non-constant Coleman function $\rho : \mathcal{U}(\mathbb{Z}_p) \to \mathbb{Q}_p$ such that $\rho(\mathcal{U}(\mathbb{Z})) \subseteq T$.*

We would like to extend this method to curves over more general number fields K. Based on an idea of Wetherell, Siksek [Sik13] looks at the restriction of scalars of $V := \operatorname{Res}^K_{\mathbb{Q}} C$ and $A := \operatorname{Res}^K_{\mathbb{Q}} J$. He exploits the fact $C(K) = V(\mathbb{Q})$ and that

$$V(\mathbb{Q}) \subseteq V(\mathbb{Q}_p) \cap \overline{A(\mathbb{Q})} \subseteq A(\mathbb{Q}_p). \tag{2}$$

Let $B := V(\mathbb{Q}_p) \cap \overline{A(\mathbb{Q})}$. If $r \leq d(g-1)$, one expects B to be finite due to reasons of dimension.

Remark 1.2. Siksek [Sik13] provides a statement that he thinks is **possibly correct**. Let $L \subseteq K$ be a subfield and let D/L be a nice curve such there is an isomorphism $D \times_{\operatorname{Spec} L} \operatorname{Spec} K \cong C$. Let J^D be the Jacobian of D and let r_D be the rank of $J^D(L)$. Then if for all $L \subseteq K$ and all D/L if

$$r_D \leq [L : \mathbb{Q}](g-1), \tag{3}$$

then B is finite. Dogra [Dog23] shows this statement is not true; he constructs a hyperelliptic genus 3 curve for which the the set B is infinite even though it satisfies (3) for each such D/L. On the other hand, he shows if (3) holds and further if J does not share a component with any of its conjugates over $\overline{\mathbb{Q}}$, we have finiteness of the set B.

In the paper [BBBM21], the authors exploit the idea of using Weil restrictions and multiple p-adic height functions to give a quadratic Chabauty method over number fields. They consider the map

$$\log : J(K) \otimes \mathbb{Q}_p \to (\operatorname{Res}^K_{\mathbb{Q}} J)(\mathbb{Q}) \otimes \mathbb{Q}_p \to \operatorname{Lie}(\operatorname{Res}^K_{\mathbb{Q}}(J))_{\mathbb{Q}_p}. \tag{4}$$

Let p be a prime which splits completely in K. For $1 \leq i \leq m$, let $\psi_i : K \hookrightarrow \mathbb{Q}_p$ denote all the embeddings of K into $\mathbb{Q}_p$. Let

$$O_K \otimes \mathbb{Z}_p = \prod_{i=1}^{m} O_K \otimes_{\psi_i} \mathbb{Z}_p \text{ and } \mathcal{U}(O_K \otimes \mathbb{Z}_p) := \prod_{i=1}^{m} \mathcal{U}(O_K \otimes_{\psi_i} \mathbb{Z}_p).$$

Also let $\psi : \mathcal{U}(O_K) \hookrightarrow \mathcal{U}(O_K \otimes \mathbb{Z}_p)$ denote the natural embedding induced by the ψ_i for $1 \leq i \leq m$. We refer the reader to Section 2.1 for the definition of p-adic idèle class characters. They prove the following theorem:

Theorem 1.3 ([BBBM21]). *Let p be a prime such that $\mathcal{U}$ has good reduction at all primes above p, and let χ be a p-adic idèle class character. Suppose the map in* (4) *is injective. Then there exists an explicitly computable finite set $T^\chi \subset \mathbb{Q}_p$ and an explicitly computable non-constant locally analytic function $\rho^\chi : \mathcal{U}(O_K \otimes \mathbb{Z}_p) \to \mathbb{Q}_p$, both dependent on χ, such that $\rho^\chi(\psi(\mathcal{U}(O_K))) \subseteq T^\chi$.*

For practical applications, computing the set of integral points via this method has been limited to quadratic number fields for curves defined over $\mathbb{Q}$. Some of the difficult steps in extending this method to higher degree number fields include finding the generators of (a finite-index subgroup of) the Mordell–Weil group $J(K)$ when the curve is defined over a larger degree number field, implementing Coleman integration and computing heights over field extensions of $\mathbb{Q}_p$.

We review examples that have been computed in the literature thus far. In [BBBM21], the authors compute the set of $\mathbb{Z}[\zeta_3]$-points of a genus 2 curve defined over $\mathbb{Q}$. The *quadratic Chabauty set* is the set of is the preimage of T^χ under ρ^χ as χ ranges over linearly independent idèle class characters. In particular, it is a set of p-adic points in $\mathcal{U}(O_K \otimes \mathbb{Z}_p)$. The authors of [BBBM21] compute finite quadratic Chabauty sets, which are supersets of the O_K-points, of two elliptic curves where K is $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{3})$. To find these sets, they use the *cyclotomic height* and a relation among the linear forms given by abelian Coleman integrals.

We note that the Mordell–Weil sieve cannot be applied to get rid of auxiliary p-adic points which are zeroes of Coleman functions on elliptic curves, since the sieve crucially relies on the fact that the curve embeds as proper subvariety of its Jacobian and consequently the map

$$C_{\mathbb{F}_q}(\mathbb{F}_q) \to J_{\mathbb{F}_q}(\mathbb{F}_q)$$

is not surjective.

Gajović and Müller [GM23b] compute the $\mathbb{Z}[\sqrt{7}]$-points of a hyperelliptic curve which is not a base change using *linear quadratic Chabauty.* Their method applies to a hyperelliptic curve in the form

$$y^2 = f(x),$$

where the degree of f is even and f is monic. This complements the work in [BBBM21], where the authors provide a method when the degree is odd. We remark the linear quadratic Chabauty method of Gajović and Müller uses an innovation in [GM23a] to compute p-adic heights of hyperelliptic curves. Based on the work of [BB12], they provide an algorithm which cleverly uses the degree 0 divisor above infinity to compute heights on hyperelliptic curves, which is significantly faster if $\deg(f)$ is odd.

Bianchi [Bia20] looks at the Mordell curve with LMFDB label 20736.1-CMd1 and minimal Weierstrass equation

$$y^2 = x^3 - 4$$

base changed to $\mathbb{Q}(\zeta_3)$, and uses the theory of Mazur-Stein-Tate [MST06] heights on elliptic curves. This heavily relies on the p-adic sigma function developed by Mazur and Tate [MT91]. On computeing the quadratic Chabauty locus, she then employs a sieve that exploits the size of the set of mod 7 and mod 13 points of E. This allowed her to determine all the $\mathbb{Z}[\zeta_3]$ points of this Mordell curve.

In this paper, we give a method to compute the integral points of rank 2 elliptic curves over imaginary quadratic fields which are *not* base changes. We follow the strategy proposed by Bianchi in [Bia20]. Some of the simplifications both in the quadratic Chabauty method and the application of the sieve are lost when one works with a curve that is not a base change. Our work gives the first instance of a calculation of the *anticyclotomic* height of an elliptic curve, which is not a base change from $\mathbb{Q}$, see Proposition 2.14 and Algorithm 1. We also present the first example where the integral points of an elliptic curve over an imaginary quadratic field which is not a base change of an elliptic curve over $\mathbb{Z}$ have been determined via the method of quadratic Chabauty.

The most common algorithms for computing the set of integral points on elliptic curves are based on the study of elliptic logarithms. The implementation in Magma is based on an algorithm of Stroeker and Tzanakis [ST94] which uses linear (group) relations between integral points and the generators of the free component of the Mordell–Weil group transformed into a linear form in elliptic logarithms. This was extended to number fields in the work of Smart and Stephens [SS97]. This implementation seems to be only available for elliptic curves defined over totally real fields. Sage currently has no implementation for computing the set of integral points over number fields apart from the rationals. We thus give a method to determine integral points for elliptic curves over imaginary quadratic fields.

We can use our quadratic Chabauty method to prove the following result:

Theorem 1.4. *Let $O_K = \mathbb{Z}[\zeta_3]$ with fraction field K. Consider the scheme $\mathcal{U}_1/O_K$ cut out by the Weierstrass equation*

$$y^2 + (\zeta_3 + 2)y = x^3 + (-\zeta_3 - 2)x^2 + (\zeta_3 + 1)x.$$

This curve has LMFDB label 134689.3-CMa1 Then

$$\mathcal{U}_1(O_K) =\{(-3 : -8\zeta_3 - 4), (-3 : 7\zeta_3 + 2), (4\zeta_3 + 4 : -8\zeta_3 - 4), (0 : 0), (0 : -\zeta_3 - 2), (\zeta_3 + 1 : 0),$$
$$(\zeta_3 + 1 : -\zeta_3 - 2)(4\zeta_3 + 4 : 7\zeta_3 + 2), (1 : 0), (1 : -\zeta_3 - 2), (-3\zeta_3 + 1 : -8\zeta_3 - 4), (-3\zeta_3 + 1 : 7\zeta_3 + 2)\}.$$

Remark 1.5. The data in the LMFDB is presented in terms of the algebraic integers $a = \zeta_6$. Hence the equations on LMFDB are obtained by replacing ζ_3 above with $a - 1$.

The paper is organised as follows. We look at the theory of heights as formulated by Mazur, Stein, and Tate [MST06] in Section 2. We outline the strategy to determine the quadratic Chabauty sets for a given elliptic curve in Section 3. We then look at a sieve to eliminate spurious p-adic points in Section 4. Finally, we compute explicit examples in Section 5.

While we can determine the quadratic Chabauty set for elliptic curves over imaginary quadratic fields of class number 1, this method is not very effective in determining the set of integral points. The major stumbling block is the sieve we use. To use the sieve, we need the curve to have trivial torsion, and we need the cardinalities of reductions at two split primes to satisfy a particular condition; see Condition 4.1. Unfortunately, this condition is not satisfied too often, and when it is satisfied, the sieve often does not end up eliminating all mock integral points. For example, we found 3528 curves over $\mathbb{Q}(\zeta_3)$ of rank 2, trivial torsion, which were not base changes. Of these, only 36 satisfied Condition 4.1. Amongst these curves, the sieve described in Section 4 only managed to eliminate all mock integral points in one case. Thus, developing a better sieving algorithm for p-adic points of elliptic curves would help improve this method significantly.

The code used in this paper is available on Github [Jha24].

Acknowledgements

We would like to thank Jennifer Balakrishnan for her constant support during this project and all the helpful comments on the write-up. We would also like to thank Alex Best, Alex Betts, Netan Dogra and Steffen Müller for illuminating conversations. We are grateful for support from the Simons Foundation as part of the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation #550023 and NSF grant DMS-1945452.

Notation

K	A number field,
O_K	The ring of integers of K,
$\mathfrak{p}, \mathfrak{q}, v$	Finite places of K,
K_v	The completion of K along a place v,
$\psi_i : K \hookrightarrow \mathbb{Q}_p$	Embeddings of K into $\mathbb{Q}_p$ for completely split primes p.
$O_K \otimes \mathbb{Z}_p \coloneqq \prod_{i=1}^{m} O_K \otimes_{\psi_i} \mathbb{Z}_p$	The product of tensor products given by all embeddings.
$A_K^\times$	The group of idèles of a number field.
E/K	An elliptic curve over K,
$E_{K_v} \coloneqq E \times_{\operatorname{Spec} K} \operatorname{Spec} K_v$	The base change of E to K_v,
$\mathcal{E}/O_K$	An integral model of E, often the minimal Weierstrass model,
$\mathcal{U}/O_K \coloneqq \mathcal{E} \setminus \{\mathcal{O}\}$	$\mathcal{E}$ minus the identity section
$E_{\mathbb{F}_\mathfrak{p}} \coloneqq \mathcal{E} \times O_K/\mathfrak{p}$	The reduction of E at $\mathfrak{p}$.

Remark 1.6. For a rational prime p which splits completely in K and for a prime $\mathfrak{p}_i \mid p$ of K, we will also use ψ_i to denote the isomorphism

$$\psi_i \colon K_{\mathfrak{p}_i} \to \mathbb{Q}_p$$

which extends the embedding $\psi_i \colon K \hookrightarrow \mathbb{Q}_p$.

Remark 1.7. We set

$$\psi \colon K \to \prod_{\mathfrak{p}|p} K_{\mathfrak{p}},\, x \mapsto \prod \psi_i(x),$$

to be the diagonal embedding of K into its completions at places above p.

2. Computing non-Archimedean heights on elliptic curves

A fundamental tool used in quadratic Chabauty is the theory of p-adic heights. In this section, after recalling some basic properties of heights, we will focus on the computational aspects of p-adic heights of elliptic curves over imaginary quadratic fields.

We shall use the definition of p-adic heights from [MT83] and [MST06].

In [MT83] the authors define height parings valued in various abelian groups for abelian varieties defined over various fields, but we stick to the case where E is an elliptic curve over a number field K, and our height pairing is valued in $\mathbb{Q}_p$, for some rational prime p. Given an (admissible) idèle class character [1]

$$\chi : \mathbb{A}_K^\times / K^\times \to \mathbb{Q}_p$$

they show there exists a "canonical" pairing

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

which is symmetric and bilinear and therefore is a height pairing. This height satisfies some nice functorial properties, see [MT83, Section 4].

In [MST06], the authors give explicit formulas for the canonical pairings described in [MT83] as a sum of local pairings and an algorithm to compute these pairings. David Harvey [Har08] provides a more efficient algorithm to calculate the height associated to the cyclotomic character for elliptic curves defined over $\mathbb{Q}$, which we modify to obtain cyclotomic heights in the number field case.

The main inputs in computing p-adic heights on elliptic curves are idèle class characters, the p-adic sigma function introduced in [MT91], and denominators of the x-coordinate of given points. We say more about these in the upcoming subsections.

Simplifying Assumption. We assume henceforth K has class number 1 for ease of exposition and to speed up computations.

2.1. Idèle class characters.

Definition 2.1. An idèle class character

$$\chi = \sum_v \chi_v : \mathbb{A}_K^\times / K^\times \to \mathbb{Q}_p$$

is a *continuous* homomorphism that decomposes as a sum of local characters χ_v. ◇

Below are some properties of idèle class characters:

- For any prime $\mathfrak{q} \nmid p$ we have $\chi_{\mathfrak{q}}(O_{\mathfrak{q}}^\times) = 0$ because of continuity. So if $\pi_{\mathfrak{q}}$ is a uniformiser in $K_{\mathfrak{q}}$, then $\chi_{\mathfrak{q}}$ is completely determined by $\chi_{\mathfrak{q}}(\pi_{\mathfrak{q}})$.

[1] See Definition 2.1

- For any $\mathfrak{p} \mid p$, there is a $\mathbb{Q}_p$ -linear map $t_{\mathfrak{p}}^{\chi}$ such that we can decompose the local height as follows

$$\begin{tikzcd}
O_{\mathfrak{p}}^{\times} \arrow[rr, "\chi_{\mathfrak{p}}"] \arrow[dr, "\log_{\mathfrak{p}}"'] & & \mathbb{Q}_p \\
& K_{\mathfrak{p}} \arrow[ur, "t_{\mathfrak{p}}^{\chi}"'] &
\end{tikzcd} \tag{5}$$

  because $\chi_{\mathfrak{p}}$ take values in the torsion free group $(\mathbb{Q}_p, +)$ where $t_{\mathfrak{p}}^{\chi}$ is a $\mathbb{Q}_p$-linear map.

If a continuous idèle class character χ is ramified at $\mathfrak{p}$, that is, if the local character $\chi_{\mathfrak{p}}$ does not vanish on $O_{\mathfrak{p}}^{\times}$, then we can extend $\log_{\mathfrak{p}} : K_{\mathfrak{p}}^{\times} \to K_{\mathfrak{p}}$ in such a way that the diagram (5) remains commutative.

Remark 2.2. An idèle class character χ is admissible in the sense of [MT83] if the chosen abelian variety A has good, ordinary reduction at places v where χ_v is ramified, i.e. $\chi_v(O_v^{\times}) \neq 0$. If χ is admissible, then we can associate a pairing on $A(K) \times A(K)$.

Example 2.3. *If $K = \mathbb{Q}$, the unique idèle class character up to scalar multiplication is the cyclotomic character $\chi := \chi_{\mathbb{Q}}^{cyc}$. If $x = (x_q)_q \in \mathbb{A}_{\mathbb{Q}}^{\times}$ then, $\chi_{\mathbb{Q}}^{\mathrm{cyc}}(x) = \log_p(x_p) - \sum_{q \neq p} \log_p(q^{v_q(x_q)})$, where v_q denotes the q-adic valuation for $\mathbb{Q}_q^{\times}$. We choose $\log_p$ to be the Iwasawa branch of the* log *function, that is $\log_p(p) = 0$. We note that $\chi(\mathbb{Q}^{\times}) = 0$, so χ factors through the idèle class group $\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times}$.*

Example 2.4. *For general K, let $\mathrm{Nm}_{K/\mathbb{Q}} : \mathbb{A}_K^{\times} \to \mathbb{A}_{\mathbb{Q}}^{\times}$ be induced by the usual norm function. The cyclotomic idèle class character is defined as $\chi_K^{\mathrm{cyc}} := \chi_{\mathbb{Q}}^{\mathrm{cyc}} \circ \mathrm{Nm}_{K/\mathbb{Q}}$*

Remark 2.5. The character χ_K^{cyc} is called 'cyclotomic' because it corresponds to the Galois character which cuts out the cyclotomic $\mathbb{Z}_p$-extension via the identification of p-adic Hecke characters with p-adic continuous Galois characters by class field theory.

Example 2.6. *Suppose K is an imaginary quadratic field. An anticyclotomic p-adic idèle class character is a continuous homomorphism*

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

such that $\chi \circ c = -\chi$. where c is the map induced on $\mathbb{A}_K$ by complex conjugation.

Remark 2.7. By class field theory, the anticyclotomic character cuts out the anticyclotomic $\mathbb{Z}_p$-extension.

Lemma 2.8. [BÇL$^+$16, Proposition 1.4] *Let K be an imaginary quadratic field and let K have class number* 1. *Let p be a prime which splits in K and let $pO_K = \mathfrak{p}_1\mathfrak{p}_2$. Also let $\psi_1 : K_{\mathfrak{p}_1} \to \mathbb{Q}_p$ and $\psi_2 : K_{\mathfrak{p}_2} \to \mathbb{Q}_p$ be isomorphisms induced by the inclusion of K. Consider the map*

$$\begin{aligned} \chi : \mathbb{A}_K^{\times}/K^{\times} &\to \mathbb{Q}_p \\ (x_v)_v &\mapsto \log_p(\psi_1(\alpha) \cdot x_{\mathfrak{p}_1}) - \log_p(\psi_2(\alpha) \cdot x_{\mathfrak{p}_2}) \end{aligned}$$

where $\alpha \in K^{\times}$ is any element such that $\alpha x_v \in O_v^{\times}$ for all finite v. Then χ is the unique (up to scaling) non-trivial anticyclotomic p-adic idèle class character.

Proof. We refer the reader to [BÇL+16, Section 1] for a proof, noting that the if c is the involution on A_K induced by complex conjugation, then $\psi_2(\alpha) = \psi_1(\alpha^c)$ for $\alpha \in K$. We note complex conjugation acts in the following manner (see for example [Neu13, Section V1.2])

$$\begin{aligned} c : \mathbb{A}_K^\times \to & \mathbb{A}_K^\times \\ (x_v)_v \mapsto & (c(x_{v_c})). \end{aligned}$$

So, at the two places above p, complex conjugation acts by switching them. ■

The restriction to class number one above is not essential, as there is an explicit formula (albeit more complicated) for class number not one. In this paper we look at number fields that have class number one, so will restrict our attention to this case.

Lemma 2.9. [BBBM21, Corollary 2.4] *Let K have $2r_2$ complex places. Then the continuous idèle class characters of K form a $\mathbb{Q}_p$-vector space V_K of dimension $\geq r_2 + 1$. If Leopoldt's conjecture* [Leo62] *holds for K, then we have $\dim_{\mathbb{Q}_p} V_K = r_2 + 1$. In particular, this holds if $K/\mathbb{Q}$ is an abelian extension.*

For an imaginary quadratic field, the cyclotomic and anticyclotomic characters described above span the space of continuous idèle class characters.

2.2. **p-adic sigma function.** In their 1991 paper [MT91], Mazur and Tate introduce the notion of p-adic sigma function, which we will recall in this section.

Let R be a complete discrete valuation ring with uniformiser π and residue field $k = R/\pi R$ of characteristic $p > 0$. Let K be the field of fractions of R. Let E/K be an elliptic curve over K. Let E^f the formal group of E. We suppose that E is ordinary, i.e.

$$E^f_{\overline{k}} \cong \left(\mathbb{G}^f_m\right)_{\overline{k}}.$$

In that case there is a good p-adic analog of the classical Weierstrass sigma function if p is odd, and of its square if $p = 2$. In [MT91], the authors give 11 different characterisations of the p-adic sigma function, but we will present the one which is amenable to calculations. Let

$$x(t) = \frac{1}{t^2} + \cdots \in R((t))$$

be the formal Laurent series that expresses x in terms of the local parameter $t = -x/y$ at infinity.

Theorem 2.10 ([MST06, Theorem 1.3])**.** *There is exactly one odd function $\sigma(t) = t + \cdots \in tR[[t]]$ and constant $c \in R$ that together satisfy the differential equation*

$$x(t) + c = -\frac{d}{\omega}\left(\frac{1}{\sigma}\frac{d\sigma}{\omega}\right) \tag{6}$$

where ω is the invariant differential $dx/(2y + a_1x + a_3)$ associated with our chosen Weierstrass equation for E.

An algorithm to compute the p-adic sigma function is given in [MST06]. A more efficient algorithm to calculate it was given by David Harvey in [Har08]. This is the implementation we use. The implementation in SageMath [The23] is for elliptic curves defined over the rationals. We modify the algorithm to use it for elliptic curves defined over (imaginary) quadratic extensions at split primes.

Remark 2.11. If $m \in \mathbb{Z}$, and $Q \in E^f(\overline{R})$, then [MT91, Theorem 3.1] states that

$$\sigma(mQ) = \sigma(Q)^{m^2} f_m(Q).$$

where f_m is the mth division polynomial relative to ω. Now taking log, we see

$$\log(\sigma(mQ)) = m^2 \log(\sigma(Q)) + \log(f_m(Q))$$

Informally, we say that, up to a correction term that the function $\log \sigma$ is quadratic.

2.3. **Denominator.** For any point $P = (x, y) \in E_v(K_v)$ which reduces to a non-singular point, for any finite place v, we can find a_v, b_v, d_v which generate O_v, unique up to scaling by an element of $O_v^\times$ such that

$$x = \frac{a_v}{d_v^2}, y = \frac{b_v}{d_v^3}$$

since O_v is a unique factorisation domain.

Let π_v be a uniformiser of O_v. Let val_v be the valuation on K_v. In [MST06], the authors define $\tilde{\sigma}_v(P) = \pi_v^{\mathrm{val}_v(d_v)}$ for $v \nmid p$. We note that $\tilde{\sigma}_v$ can be defined at places where the reduction *is not* good and ordinary, whereas σ_v, the v-adic sigma function of E_v cannot be defined at such places.

In [MST06], the authors say that $\tilde{\sigma}_v$ is a serviceable replacement for σ_v in the following sense. The v-adic valuation of $\tilde{\sigma}_v$ is the same as the v-adic valuation of the v-adic sigma function. Since $\chi : \mathbb{A}_K^\times / K^\times \to \mathbb{Q}_p$ is unramified at $v \nmid p$ and consequently χ_v is sensitive only to the v-adic valuation of the input, this is an appropriate replacement for the sigma function.

Note that for a global point $P = (x, y) \in E(K)$, we get points $P_v \in E(K_v)$ for all places v. In this case, Wuthrich [Wut04b, Proposition 2] shows that on a finite index subgroup $E^\circ(K)$ of $E(K)$ we have a choice of a global denominator $d(P) \in O_K$ along with $a(P), b(P) \in O_K$ such that

$$x = \frac{a(P)}{d(P)^2}, y = \frac{b(P)}{d(P)^3},$$

and $a(P), b(P), d(P)$ are pairwise coprime. Consequently $d_v = d(P)$ in K_v up to $O_v^\times$ for all v.

Remark 2.12. In fact in Wuthrich's thesis [Wut04a, Proposition IV.3], he shows that for a point P in $E^\circ(K)$, we have $d(mP) = d(P)^{m^2} f_m(P)$. Comparing this to Remark 2.11, we see the function

$$h(P) := \log(\sigma(P)) - \log(d(P))$$

satisfies $h(mP) = m^2 h(P)$ for $P \in E^\circ(K)$. Since the class group is trivial, $E^\circ(K)$ is precisely the subgroup of points that reduce to a non-singular point for all places v.

2.4. **Computing heights for imaginary quadratic Fields.** In this section, we outline how one obtains heights from idèle class characters, denominators and p-adic sigma functions. We then give explicit formulas for the cyclotomic and anti-cyclotomic heights.

For $\mathfrak{p} \mid p$, let $\sigma_\mathfrak{p}$ be the sigma function attached to the elliptic curve $E_{K_\mathfrak{p}}$. Let $\mathcal{E}$ denote the minimal Weierstrass model. Note $\sigma_\mathfrak{p}$ defines a function on the kernel of reduction $E^1_\mathfrak{p} := \ker(\mathcal{E}(K_\mathfrak{p}) \to \mathcal{E}(k_\mathfrak{p}))$ to $\mathbb{Z}_p$. Indeed, if $P = (x, y) \in E^1_\mathfrak{p}$ and $t = -x/y$ then $\mathrm{val}_v(t) \geq 1$, and so $\sigma_\mathfrak{p}(P) := \sigma_\mathfrak{p}(t)$ is a well-defined element of $O_{K_\mathfrak{p}}$. If $m = \#\mathcal{E}(k_\mathfrak{p})$, then any $P \in E(K)$, $mP \in E^1_\mathfrak{p}$.

For $v \nmid p$, if P reduces to the identity component of the special fibre at v, $\tilde{\sigma}_v(P) = d_v$ as in Section 2.3. As discussed in Remark 2.12, for points in $E^\circ(K)$, a finite index subgroup of $E(K)$, we have a global denominator, $d(P) \in O_K$. This is well defined up to an O_K unit. If n is the least common multiple of the Tamagawa numbers, then for any $P \in E(K)$, we have $nP \in E^\circ(K)$.

Definition 2.13. Let $E(K)_{\text{ht}} \subseteq E(K)$ be the set of non-torsion points P which lie in $E^1_{\mathfrak{p}}$ for all $\mathfrak{p} \mid p$ and reduce to the identity component for $v \nmid p$. This is a finite index subgroup of $E(K)$. $\diamond$

Fix $P \in E(K)_{\text{ht}}$ and an idèle class character χ. For $\mathfrak{p} \mid p$ and $v \nmid p$, we define

$$h^{\chi}_{\mathfrak{p}}(P) \coloneqq \chi_{\mathfrak{p}}((\sigma_{\mathfrak{p}}(P))) \qquad \text{and} \qquad h^{\chi}_{v}(P) \coloneqq \chi_v(\tilde{\sigma}_v(P)).$$

For $P \in E(K)$, let n be such that $nP \in E(K)_{\text{ht}}$. As before, let f_n be the nth division polynomial. For any place v, we extend local heights as follows:

$$h^{\chi}_{v}(P) = \frac{1}{n^2}\left(h^{\chi}_{v}(nP) - \chi_v(f_n(P))\right)$$

This definition does not depend on n; see Remark 2.11 for $v \mid p$ and Remark 2.12 for $v \nmid p$.

Finally, we have a formula for the global height

$$h^{\chi}(P) \coloneqq \sum_{v} h^{\chi}_{v}(P) = \frac{1}{n^2}\sum_{v} h^{\chi}_{v}(nP). \tag{7}$$

We now compute cyclotomic and anti-cyclotomic heights explicitly. We fix K, an imaginary quadratic field and E/K an elliptic curve. Let p be a split prime and write $\mathfrak{p}_1, \mathfrak{p}_2$ for the prime factors of pO_K. Let σ_1, σ_2 be the sigma functions attached to the curves $E_{K_{\mathfrak{p}_1}}$ and $E_{K_{\mathfrak{p}_2}}$ respectively. Fix a non-torsion point P, and choose an n such that $nP \in E(K)_{\text{ht}}$. Let $nP = (x, y)$, and $t = -x/y$. Set $t_i = \psi_i(t)$ for $i = 1, 2$. Also, let d be the denominator of nP as in Section 2.3.

2.4.1. *Cyclotomic Height.* Using (7) and using the formula for the cyclotomic character in Example 2.4, we get

$$h^{\text{cyc}}(P) = \frac{1}{n^2}\left(\log_p\left(\frac{\sigma_1(t_1)}{\sigma_2(t_2)}\right) + \log_p\left(\frac{\psi_1(d)}{\psi_2(d)}\right)\right).$$

2.4.2. *Anticyclotomic Height.* The formula to calculate with the anticyclotomic character is a bit more involved than the formula for the cyclotomic character. We prove a slight generalization of [BÇL+16, Proposition 2.4] and use it to compute the anticyclotomic height. See Remark 2.15 for more details.

Proposition 2.14 (Anticyclotomic Height)**.** *Let $P \in E(K)_{\text{ht}}$ be a non-torsion point. Then, the anticyclotomic p-adic height of P, denoted $h^{\text{anti}}(P)$ is given by the formula*

$$h^{\text{anti}}(P) = \log_p\left(\frac{\sigma_1(t_1)}{\sigma_2(t_2)}\right) - \log_p\left(\frac{\psi_1(d)}{\psi_2(d)}\right)$$

Proof. Let $P = (x, y)$ reduce to the origin modulo $\mathfrak{p}_1, \mathfrak{p}_2$. By considering valuations, we see there exist $e_1, e_2 \in \mathbb{Z}_{\geq 1}$ such that we have $\text{val}_{\mathfrak{p}_i}(x) = -2e_i, \text{val}_{\mathfrak{p}_i}(y) = -3e_i$ for $i = 1, 2$. We get

$$\text{val}_{\mathfrak{p}_i}(t) = \text{val}_{\mathfrak{p}_i}(x) - \text{val}_{\mathfrak{p}_i}(y) = e_i.$$

Furthermore $\text{val}_{\mathfrak{p}_i}(\sigma_i(t_i)) = e_i$ since $\sigma_i(t) \in t + t^2\mathbb{Z}_p[t]$ for $i = 1, 2$. Let $\pi_1, \pi_2 \in O_K$ generate $\mathfrak{p}_1, \mathfrak{p}_2$ respectively. Choosing $\alpha = \pi^{-e_1}$ in Lemma 2.8, we get

$$\chi^{\text{anti}}_{\mathfrak{p}_1}(\sigma_1(P)) = \log_p(\psi_1(\pi_1^{-e_1})) + \log_p(\sigma_1(t_1)) - \log_p\left(\psi_2(\pi_1^{-e_1})\right),$$

and choosing $\alpha = \pi_2^{-e_2}$, we get

$$\chi^{\text{anti}}_{\mathfrak{p}_2}(\sigma_2(P)) = \log_p(\psi_1(\pi_2^{-e_2})) - \log_p(\sigma_2(t_2)) - \log_p\left(\psi_2(\pi_2^{-e_2})\right).$$

Therefore we get

$$h_{\mathfrak{p}_1}^{\mathrm{anti}}(P) + h_{\mathfrak{p}_2}^{\mathrm{anti}}(P) = \log_p\left(\frac{\sigma_1(t_1)}{\sigma_2(t_2)}\right) - \log_p\left(\frac{\log_p(\psi_1(\pi_1^{e_1}\pi_2^{e_2}))}{\log_p(\psi_2(\pi_1^{e_1}\pi_2^{e_2}))}.\right) \tag{8}$$

For local heights away from p we get

$$\sum_{v \nmid p\infty} h_v^{\mathrm{anti}}(P) = \sum_{v \nmid p\infty} \chi_v^{\mathrm{anti}}(d_v(P)) = \sum_{v \nmid p\infty} \chi_v^{\mathrm{anti}}(d(P))$$

by definition of $d(P)$. Choose $\beta \in O_K$ such that $d(P) = \pi_1^{e_1}\pi_2^{e_2}\beta$ and

$$\mathrm{val}_{\mathfrak{p}_1}(\beta) = \mathrm{val}_{\mathfrak{p}_2}(\beta) = 0.$$

Then by Lemma 2.8 we get

$$\begin{aligned}\sum_{v \nmid p\infty} h_v^{\mathrm{anti}}(P) &= \log_p\left(\frac{\psi_1(\beta^{-1})}{\psi_2(\beta^{-1})}\right)\\ &= -\log_p\left(\frac{\psi_1(d(P))}{\psi_2(d(P))}\right) + \log_p\left(\frac{\psi_1(\pi_1^{e_1}\pi_2^{e_2})}{\psi_2(\pi_1^{e_1}\pi_2^{e_2})}\right).\end{aligned} \tag{9}$$

Adding (8) and (9), we get the desired result. ∎

Remark 2.15. Proposition 2.14 is a mild generalization of Proposition 2.4 in [BÇL$^+$16]. There are a few key differences:

(1) Let c denote the action of complex conjugation, which is the same as the non-trivial Galois automorphism of K. Since we are working with E/K, a curve which is not necessarily a base change of one over $\mathbb{Q}$, it is not necessarily the case that if $P = (x, y) \in E(K)$ then $(x^c, y^c) \in E(K)$.

(2) We get two different sigma functions attached to E above p.

We describe an algorithm to compute the cyclotomic and anti-cyclotomic heights.

Algorithm 1 (Computing the Cyclotomic and Anticyclotomic Height)**.** *Input: An affine point $P = (x, y) \in E(K)$.*
Output: The cyclotomic and anticyclotomic heights $h^{\mathrm{cyc}}(P)$ and $h^{\mathrm{anti}}(P)$.

(1) If P is torsion, $h^{\mathrm{cyc}}(P) = h^{\mathrm{anti}}(P) = 0$.

(2) We first compute the least common multiple of the Tamagawa numbers of the elliptic curve. Call this number m.

(3) Given $P \in E(K)$, we find the order of P in $E_{\mathbb{F}_{\mathfrak{p}_i}}$ for $i = 1, 2$. We call these n_1, n_2 and let $n = lcm(n_1, n_2, m)$.

(4) Compute nP, and find a square root of the denominator of the x-coordinate $d(nP)$. Note we can do this since we have chosen K to have class number 1.

(5) Let

$$t = -\frac{x(nP)}{y(nP)},$$

and let $t_1 = \psi_1(t), t_2 = \psi_2(t)$. Compute the sigma functions attached to $E_{K_{\mathfrak{p}_i}}$ and call them σ_i for $i = 1, 2$. Compute

$$s_i := \sigma_i(t_i)$$

for $i = 1, 2$.

(6) *Compute*

$$d_1 = \psi_1(d(nP)), d_2 = \psi_2(d(nP)).$$

(7) *Return the heights:*

$$h^{\text{cyc}}(P) = \frac{1}{n^2}\left(\log_p(s_1) + \log_p(s_2)\right) - \frac{1}{n^2}\left(\log_p(d_1) + \log_p(d_2)\right)$$

and

$$h^{\text{anti}}(P) = \frac{1}{n^2}\left(\log_p(s_1) - \log_p(s_2)\right) - \frac{1}{n^2}\left(\log_p(d_1) - \log_p(d_2)\right)$$

3. Quadratic Chabauty for integral points of elliptic curves

Let K be a quadratic imaginary number field with ring of integers O_K and let E/K be an elliptic curve. As before, let K have class number one. Let $f(x,y)$ be the Weierstrass equation of the minimal Weierstrass model of E, and let

$$\mathcal{U} := \operatorname{Spec} O_K[x,y]/f(x,y).$$

We let $\mathcal{E}$ be the minimal regular resolution of projective closure of $\mathcal{U}$ in $\mathbb{P}^2_{O_K}$. We shall give a method to determine the set $\mathcal{U}(O_K)$, when $E(K)$ has rank 2 and trivial torsion based on the proof of Theorem 1.3. If $E(K)$ has rank 0, one just needs to compute the torsion points of E to determine the set $\mathcal{U}(O_K)$. Since there are finitely many choices for the different groups $E(K)$ can be [Kam92], this can be done relatively easily using division polynomials.

In the case of $E(K)$ being rank one, one can generically find a p-adic linear functional and a height function which vanishes on the integral points of $\mathcal{U}$, as was done in [BBBM21]. The case of rank 2 is the one where one needs to genuinely use the two different height functions to determine the quadratic Chabauty set, and this is the case we shall explore. Let

$$E(K) = \mathbb{Z}\cdot P \oplus \mathbb{Z}\cdot Q.$$

Fix an idèle class character χ. In Theorem 1.3, we have a function ρ^χ for a choice of idèle class character χ, and a set T^χ such that $\rho^\chi(\psi(\mathcal{U}(O_K))) \subseteq T^\chi$. We shall explain how to obtain the function ρ^χ and the set T^χ using the p-adic heights considered in Section 2.

We first recall some preliminaries on Coleman integration.

3.1. **Coleman integration and height functions.**

Let $L/\mathbb{Q}_p$ be a finite extension and let X_{an}/L be a rigid analytic curve. See [Col85, Section 1] for notions on rigid geometry used in the following theorem. See [FVdP12] for a more thorough introduction to rigid geometry.

Theorem 3.1 (Coleman, [Col85, Proposition 2.4, Theorem 2.7])**.** *Let η, ξ be 1-forms on a wide open V of X_{an} and $A, B, C \in V(L)$. Let $a, b \in L$. The definite Coleman integral has the following properties:*

(1) ***Linearity:***

$$\int_A^B (a\eta + b\xi) = a\int_A^B \eta + b\int_A^B \xi.$$

(2) ***Additivity in endpoints:***

$$\int_A^B \xi = \int_C^B \xi + \int_A^C \xi$$

(3) ***Change of variables:*** *If $\varphi : X_{\mathrm{an}} \to X'_{\mathrm{an}}$ is a rigid analytic map then*

$$\int_A^B \varphi^* \xi = \int_{\varphi(A)}^{\varphi(B)} \xi$$

(4) ***Fundamental theorem of calculus:***

$$\int_A^B df = f(B) - f(A)$$

for f a rigid analytic function on X.

We now state an easy consequence of the properties of the Coleman integral, which we will use.

Lemma 3.2 ([Col85, Theorem 2.8])**.** *Let E/L be an elliptic curve and $P_1, P_2 \in E(L)$ be points on the elliptic curve. Let $\omega \in H^0(E, \Omega^1)$ be an invariant differential. Then*

$$\int_{\mathcal{O}}^{P_1+P_2} \omega = \int_{\mathcal{O}}^{P_1} \omega + \int_{\mathcal{O}}^{P_2} \omega$$

We use the implementation of Coleman integration in [BBK10].

Let p be a split prime and write $\mathfrak{p}_1, \mathfrak{p}_2$ for the prime factors of pO_K. Further, we let $\psi_1, \psi_2 : K \hookrightarrow \mathbb{Q}_p$ be the natural embeddings. Let

$$E_{K_{\mathfrak{p}_1}} := E \times_{\psi_1} \operatorname{Spec} \mathbb{Q}_p, \qquad E_{K_{\mathfrak{p}_2}} := E \times_{\psi_2} \operatorname{Spec} \mathbb{Q}_p.$$

Fix $\omega \in H^0(E, \Omega^1)$, a choice of invariant differential, and let $\omega_i = \psi_i^* \omega$ be the pullbacks to $E_{K_{\mathfrak{p}_i}}$ for $i = 1, 2$. For $P_1 \in E_{K_{\mathfrak{p}_1}}(\mathbb{Q}_p), P_2 \in E_{\mathbb{K}_{\mathfrak{p}_2}}(\mathbb{Q}_p)$ we let

$$f_1(P_1) := \int_O^{P_1} \omega_1 \qquad \text{and} \qquad f_2(P_2) := \int_O^{P_2} \omega_2$$

where the integrals are Coleman integrals. In particular for $R \in E(K)$ we let

$$f_1(R) := \int_O^{\psi_1(R)} \omega_1 \qquad \text{and} \qquad f_2(R) := \int_O^{\psi_2(R)} \omega_2.$$

By Lemma 3.2, f_i are linear functions on $E_{K_{\mathfrak{p}_i}}(\mathbb{Q}_p)$ for $i = 1, 2$. Consider

$$\operatorname{Span}_{\mathbb{Q}_p}\{f_1, f_2\} \subseteq (E(K) \otimes \mathbb{Q}_p)^\vee$$

where $(E(K) \otimes \mathbb{Q}_p)^\vee = \operatorname{Hom}_{\mathbb{Q}_p}(E(K) \otimes \mathbb{Q}_p, \mathbb{Q}_p)$.

If f_1, f_2 are linearly independent, this inclusion is an equality (since $E(K)$ has rank 2), and we can use the idea of quadratic Chabauty and restriction of scalars to find the integral points $\mathcal{U}(O_K)$. We now assume the following condition holds:

Condition 3.3. $\operatorname{Span}_{\mathbb{Q}_p}\{f_1, f_2\} = (E(K) \otimes \mathbb{Q}_p)^\vee$.

If Condition 3.3, one can compute a linear combination of f_1 and f_2 which vanishes on the integral points of E via a version of Siksek's method.

Definition 3.4. For $R_1 \in E_{K_{\mathfrak{p}_1}}(\mathbb{Q}_p), R_2 \in E_{K_{\mathfrak{p}_2}}(\mathbb{Q}_p)$, let

$$g_{ij}(R_1, R_2) = \frac{1}{2}(f_i(R_1)f_j(R_2) + f_i(R_1)f_j(R_2))$$

for $1 \leq i \leq j \leq 2$. ◇

Remark 3.5. When Condition 3.3 holds $\mathrm{Span}_{\mathbb{Q}_p}\{g_{11}, g_{12}, g_{22}\}$ is the full space of symmetric $\mathbb{Q}_p$-bilinear forms on $E(K)\otimes\mathbb{Q}_p$. It is essential in computing locally analytic expansions of the functions ρ^χ

3.2. **Finding the quadratic Chabauty sets for elliptic curves.** The global height pairing is bilinear, so if Condition 3.3 holds, it can be expressed as a linear combination

$$h^\chi = \alpha^\chi_{11} g_{11} + \alpha^\chi_{12} g_{12} + \alpha^\chi_{22} g_{22}, \tag{10}$$

where the coefficients $\alpha_{i,j} \in Q_p$. Now we return to sketch an algorithm to find a set $B_p \subseteq E(K\otimes\mathbb{Q}_p)$ which contains the image $\psi_1(\mathcal{U}(O_K)) \times \psi_2(\mathcal{U}(O_K))$. We need the following properties of heights:

(1) For $v \nmid p$, h^χ_v takes only finitely many values on O_K-points. Call this set of values T^χ_v. If v does not divide the discriminant of E, then $T^\chi_v = \{0\}$. This follows from the fact that the local heights of Coleman–Gross [CG89] coincide with the height of Mazur and Tate by work of Balakrishnan and Besser [BB15, Corollary 4.3]. The local heights of Coleman and Gross away from places above p are given by

$$h_v(R) = (R, R)\chi(v)$$

where $(\cdot,\cdot)$ is an intersection pairing. In [BBM17, Lemma 2.4], the authors show the intersection pairing, and hence the local height at $v \nmid p$ only depends on the connected component that R reduces onto in the special fibre. Hence, this set is finite and in fact equal to $\{0\}$ for almost all v.

To compute this set for elliptic curves, we follow the algorithm in [Sil88, Section 5] and use [CPS06, Proposition 6].

(2) The global height h^χ and local height $h^\chi_\mathfrak{p}$ for $\mathfrak{p} \mid p$ can be expressed as locally analytic p-adic functions in each residue disk and computed to desired p-adic and t_1, t_2-adic precision as elements of $\mathbb{Z}_p[[t_1, t_2]]$. For a point P such that mP lies in an appropriate neighbourhood of the identity, we use the identity $h^\chi_\mathfrak{p}(P) = \frac{1}{m^2}\left(h^\chi_\mathfrak{p}(mP) - \chi_{|mfp}(f_m(P))\right)$

To compute analytic expansions of h^χ in all residue disks we first find $\alpha_{11}, \alpha_{12}, \alpha_{22}$ in Equation 10 by plugging in $P, Q, P{+}Q$. Then, we can compute Coleman integrals by finding a local parametre at a fixed point in each disk and using it to compute a tiny integral.

Hence we can compute

$$\rho^\chi := h^\chi - \sum_{\mathfrak{p}|p} h^\chi_\mathfrak{p}$$

as a p-adic analytic function up to desired p-adic precision in each residue disk.

Thus ρ^χ is a p-adic analytic function in two variables, and

$$\rho^\chi(\psi_1(\mathcal{U}(O_K)) \times \psi_2(\mathcal{U}(O_K))) \subseteq T^\chi,$$

where T^χ is determined by the sets T^χ_v above.

For K imaginary quadratic, as discussed in Section 2.1, one has two linearly independent characters χ^{cyc}, the cyclotomic character and χ^{anti} the anticyclotomic character. Let $\overline{\rho} = (\rho^{\mathrm{cyc}}, \rho^{\mathrm{anti}})$. We wish to solve the system of equations $\overline{\rho} = (t_1, t_2)$ for $(t_1, t_2) \in T^{\mathrm{cyc}} \times T^{\mathrm{anti}}$.

This can be done using a multivariate Hensel's lemma. We can lift mod p^n solutions using a Newton's method type argument uniquely in disks of small radius under certain conditions satisfied by the Jacobian matrix of partials of $\overline{\rho}$. See, for example [BBBM21, Appendix A]. Since finitely many disks cover $\mathcal{U}(\mathbb{Z}_{\mathfrak{p}_i})$, one gets finitely many $\mathcal{U}(\mathbb{Z}_{\mathfrak{p}_1}) \times \mathcal{U}(\mathbb{Z}_{\mathfrak{p}_2})$-solutions (z_1, z_2) such that $\overline{\rho}(z_1, z_2) = (t_1, t_2)$ for $(t_1, t_2) \in T^{\text{cyc}} \times T^{\text{anti}}$. Some adjustments need to be made when the Jacobian matrix does not satisfy the required criterion, which is also discussed in [BBBM21, Appendix A].

We call the set of solutions obtained above the *quadratic Chabauty set* and denote it $B_p \subseteq \mathcal{U}(O_K \otimes \mathbb{Z}_p)$. We use a version of algdep which relies on the LLL [LLL82] algorithm to recognise O_K-points for p-adic points. We call the set of points which we have not been able to identify as *mock integral points* and use the notation A_p to identify them. We would like to use some sieving method to show that these points are not integral, but unfortunately the Mordell–Weil sieve can not be used for elliptic curves.

We discuss an alternative sieve in Section 4. Here is an overview of the algorithm to be followed to find the set A_p above.

Algorithm 2 (Finding the quadratic Chabauty set for an elliptic curve)**.**
Input: An elliptic curve E/K over an imaginary quadratic field such that $E(K) = Z \cdot P \oplus \mathbb{Z} \cdot \mathbb{Q}$. A prime p which splits in K and E has good, ordinary reduction at both primes above p.

Output: A finite set $B_p \subseteq \mathcal{U}(O_K \otimes \mathbb{Z}_p)$ containing $\sigma(\mathcal{U}(O_K))$ and a set A_p containing mock integral points.

(1) *Find the Mordell–Weil generators of $E(K)$ and let $E(K) = \mathbb{Z} \cdot P \oplus \mathbb{Z} \cdot Q$. To speed up the algorithm, one can optionally fix a positive integer C and compute*

$$E(O_K)_{known} = \{nP + mQ : |n|, |m| \leq C \textit{ and } nQ + mR \in \mathcal{U}(O_K)\}.$$

(2) *Calculate the sets T^{cyc} and T^{anti} by computing the possible values of intersection pairings as in* [CPS06] *and* [Sil88].

(3) *For $\chi = \chi^{\text{cyc}}, \chi = \chi^{\text{anti}}$ find an analytic expansion of $h^\chi - \sum_{\mathfrak{p}|p} h_v^\chi$ in all residue disks. This will be done in two steps.*
   - (a) *Compute the local height at $\mathfrak{p} \mid p$ by using the p-adic sigma function as in Section 2.2.*
   - (b) *Consider the system*

$$\begin{pmatrix} h(P,P) \\ h(P,Q) \\ h(Q,Q) \end{pmatrix} = \begin{pmatrix} g_{11}(P,P) & g_{12}(P,P) & g_{22}(P,P) \\ g_{11}(P,Q) & g_{12}(P,Q) & g_{22}(P,Q) \\ g_{11}(Q,Q) & g_{12}(Q,Q) & g_{22}(Q,Q) \end{pmatrix} \begin{pmatrix} \alpha_{11} \\ \alpha_{12} \\ \alpha_{22} \end{pmatrix}$$

   and solve for $\alpha_{11}, \alpha_{12}, \alpha_{22}$. Using implementations of Coleman integration for the matrix on the right and Algorithm 1 for the heights on the left, we can find $\alpha_{11}, \alpha_{12}, \alpha_{22}$. Hence we can express $h - \sum_{\mathfrak{p}|p} h_v$ as a p-adic power series in two variables.

(4) *Let $\rho^\chi = h^\chi - \sum_{\mathfrak{p}|p} h_{\mathfrak{p}}^\chi$. We solve the system $(\rho^{\chi^{\text{cyc}}}, \rho^{\chi^{\text{anti}}}) = (t_1, t_2)$ for all $(t_1, t_2) \in T^{\text{cyc}} \times T^{\text{anti}}$ using multivariate Hensel's lemma. Pull back solutions to points in $\mathcal{U}(O_K)$. This is the set B_p.*

(5) *We identify elements of B_p which lie in $\mathcal{U}(O_K)$ using p-adic LLL. We let A_p be the complement of the points which are recognised as integral.*

Remark 3.6. The bottleneck in this algorithm is solving the system of p-adic power series. One would like to optimise solving these multivariate series to make this algorithm faster.

In the next section, we discuss a method that shows certain points in A_p are not O_K-points.

4. A sieve for integral points on elliptic curves

As before, let p be a prime which splits in the chosen imaginary quadratic field K. On running the quadratic Chabauty algorithm for an elliptic curve to find integral points, one gets the following output:

$$B_p \coloneqq \left\{(R_1, R_2) \in \mathcal{U}(\mathbb{Z}_{p_1}) \times \mathcal{U}(\mathbb{Z}_{p_2}) : \rho^{\mathrm{cyc}}(R_1, R_2) \in T^{\mathrm{cyc}}, \rho^{\mathrm{anti}}(R_1, R_2) \in T^{\mathrm{anti}}\right\}.$$

We often have p-adic points which are not recognised as algebraic points. For a curve with genus $g \geq 2$, one uses the Mordell–Weil sieve to show auxiliary p-adic points are not algebraic, but this is not applicable in our case.

Instead, we outline a method that first appeared in the appendix of the paper [BBM17]. We first choose two primes p, q for which we run the quadratic Chabauty algorithm. As always, we assume the primes split in the chosen imaginary quadratic field, say $pO_K = \mathfrak{p}_1\mathfrak{p}_2$ and $qO_K = \mathfrak{q}_1\mathfrak{q}_2$. Also assume E has good reduction at $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{q}_1, \mathfrak{q}_2$. The primes must satisfy the following condition:

Condition 4.1. Let $\mathbb{F}_{\mathfrak{p}_i} \coloneqq O_K/\mathfrak{p}_i$, $\mathbb{F}_{\mathfrak{q}_i} \coloneqq O_K/\mathfrak{q}_i$. We require $q \mid \#\mathcal{E}(\mathbb{F}_{\mathfrak{p}_i})$ for at least one of $i = 1, 2$, *and* $p \mid \#\mathcal{E}(\mathbb{F}_{\mathfrak{q}_j})$ for at least one of $j = 1, 2$. This is equivalent to $p \mid \#\mathcal{E}(O_K/q)$ *and* $q \mid \#\mathcal{E}(O_K/p)$ since $\mathcal{E}(O_K/p) = \mathcal{E}(\mathbb{F}_{\mathfrak{p}_1}) \times \mathcal{E}(\mathbb{F}_{\mathfrak{p}_2})$ and $\mathcal{E}(O_K/q) = \mathcal{E}(\mathbb{F}_{\mathfrak{q}_1}) \times \mathcal{E}(\mathbb{F}_{\mathfrak{q}_2})$.

Since we have chosen a curve such that

$$E(K) = \mathbb{Z} \cdot P \oplus \mathbb{Z} \cdot Q,$$

we know any integral point, R can be expressed as

$$R = mP + nQ \tag{11}$$

for some unique integers m, n.

We shall find constraints on the m and n mod p and mod q using Coleman integrals (log information) and using the cardinalities of the reductions at p, q which satisfy Condition 4.1. We discuss this in the upcoming sections. For an abelian group G and a positive integer n, we let G/n denote the quotient G/nG.

4.1. **Reduction information.** Let p, q be rational primes which satisfy Condition 4.1. Consider the following diagram:

$$\begin{tikzcd}
\mathcal{U}(O_K) \arrow[r] \arrow[d] & B_p \arrow[d] \\
\mathcal{E}(O_K) \arrow[r] \arrow[d] & E(K \otimes \mathbb{Q}_p) \arrow[d] \\
\mathcal{E}(O_K)/q \arrow[r, "\mathrm{red}"] & \mathcal{E}(O_K/p)/q.
\end{tikzcd}$$

Figure 1. Reduction data.

Let $\overline{\mathcal{R}}$ denote the image of $\mathcal{R}$ under the map $B_p \to E(K \otimes \mathbb{Q}_p) \to \mathcal{E}(O_K/p)/q$.

Definition 4.2. Let $\mathrm{red}_{\mathcal{R}} \coloneqq \mathrm{red}^{-1}(\overline{\mathcal{R}}) \subset \mathcal{E}(O_K)/q$. We call this set the collection of mod q reduction constraints on a putative integral point corresponding to the p-adic point $\mathcal{R}$. ◇

Since we have fixed generators P, Q, we have an isomorphism $\mathcal{E}(O_K) \cong \mathbb{Z}^2$, and with this choice of basis, we obtain (mod q) constraints on the coordinates m and n of a putative integral point giving rise to $\mathcal{R}$ in this basis.

Remark 4.3. Condition 4.1, the $\mathbb{F}_p$-vector space $\mathcal{E}(O_K/p)/q$ is not isomorphic to $\{0\}$, so we do get meaningful information by considering $\mathrm{red}_{\mathcal{R}}$.

Let $\overline{P}_i, \overline{Q}_i$ for $i = 1, 2$ denote the image of the generators in $E_{\mathbb{F}_{\mathfrak{q}_i}}(\mathbb{F}_q)$ for $i = 1, 2$, and let $\overline{R}_i$ denote the reduction of $\mathcal{R} = (R_1, R_2) \in B_p$. Then we can compute $\mathrm{red}_{\mathcal{R}}$ as

$$\mathrm{red}_{\mathcal{R}} = \left\{(m, n) \mid m, n \in \mathbb{Z}/p, \overline{R}_1 = m\overline{P}_1 + n\overline{Q}_1, \overline{R}_2 = m\overline{P}_2 + n\overline{Q}_2\right\}.$$

If this set is empty, we can immediately discard the point (R_1, R_2) as not coming from a point $R \in \mathcal{E}(O_K)$, by the commutativity of Figure 1. Else we record $\mathrm{red}_{\mathcal{R}}$.

4.2. **Log information.** Recall that we have a map $\psi : E(K) \to E(K \otimes \mathbb{Q}_p), P \mapsto (\psi(P))$ which embeds points diagonally. Let T_1, T_2 denote the tangent spaces of $E(K_{\mathfrak{p}_1})$ and $E(K_{\mathfrak{p}_2})$. For $i = 1, 2$, we had f_1, f_2 in Condition 3.3 as functionals on $H^0(E_{\mathbb{Q}_{\mathfrak{p}_i}}, \Omega^1) \cong T_i^*$. We have a natural log map

$$\begin{aligned} \log : E(K \otimes \mathbb{Q}_p) &\to T_1 \times T_2 \\ (R_1, R_2) &\mapsto (f_1(R_1), f_2(R_2)) \end{aligned}$$

We have the following commutative diagram which encapsulates the objects and maps we have discussed:

$$\begin{tikzcd}
\mathcal{U}(O_K) \arrow[r] \arrow[d] & B_p \arrow[r] & E(K \otimes \mathbb{Q}_p) \arrow[d, "\log"] \\
\mathcal{E}(K) \arrow[rr, "\log|_{\mathcal{E}(K)}"] \arrow[d, "\mathrm{red}"] & & T_1 \times T_2 \\
\mathcal{E}(K)/p & &
\end{tikzcd}$$

FIGURE 2. Log data

Definition 4.4. Let $\log_{\mathcal{R}} \coloneqq \mathrm{red}(\log|^{-1}_{\mathcal{E}(K)}\mathcal{R})) \subseteq \mathcal{E}(K)/p$. We call this set the collection of mod p log constraints on a putative integral point corresponding to the p-adic point $\mathcal{R}$. ◇

Suppose $\mathcal{R} = (R_1, R_2) \in A_p$. To calculate $\log_{\mathcal{R}}$, we solve for m, n in the following equations:

$$\begin{aligned} f_1(R_1) &= mf_1(P) + nf_1(Q) \\ f_2(R_2) &= mf_2(P) + nf_2(Q). \end{aligned} \tag{12}$$

If M is invertible, we let

$$M = \begin{pmatrix} f_1(P_1) & f_1(Q_1) \\ f_2(P_2) & f_2(Q_2) \end{pmatrix},$$

and let

$$\begin{pmatrix} m \\ n \end{pmatrix} = M^{-1} \begin{pmatrix} f_1(R_1) \\ f_2(R_2) \end{pmatrix}, \tag{13}$$

where $m, n \in \mathbb{Q}_p$. If $m, n \notin \mathbb{Z}_p$, then the point (R_1, R_2) is not integral. If $m, n \in \mathbb{Z}_p$, we can take mod p reductions to get $\log_{\mathcal{R}}$. If M is not invertible, then we need to check if (13) has infinitely many solutions or no solutions. If it has no solution, we can discard the point $\mathcal{R}$, else, we reduce mod p and record $\log_{\mathcal{R}}$.

4.3. **Comparing log and reduction information.** For $\mathcal{R} \in B_p$, let $\mathrm{red}_{\mathcal{R}} \times \log_{\mathcal{R}} \subset \mathcal{E}(O_K)/q \times (O_K)/p$ be as in Definition 4.2 and Definition 4.4. Similarly, for $\mathcal{S} \in B_q$, let $\log_{\mathcal{S}} \times \mathrm{red}_{\mathcal{S}} \subset \mathcal{E}(O_K)/q \times \mathcal{E}(O_K)/p$. Let $\mathfrak{S}$ be the union of $\log_{\mathcal{S}} \times \mathrm{red}_{\mathcal{S}}$ for all $\mathcal{S}$ in B_q.

Lemma 4.5. *Assume condition 4.1. Let $\mathcal{R} \in B_p$. If $(\mathrm{red}_R \times \log_R) \cap \mathfrak{S}$ is empty, then $\mathcal{R}$ is not the image of a point in $\mathcal{U}(O_K)$.*

Proof. By the commutativity of Diagrams 1 and 2 , it follows that the image of a global point in $\mathcal{U}(O_K)$ in $\mathcal{E}(K)/q \times \mathcal{E}(K)/p$ must be in the intersection of $(\mathrm{red}_R \times \log_R) \cap \mathfrak{S}$. ■

We now list the steps to carry out the sieve.

Algorithm 3. *Input: Sets $A_p \subseteq \mathcal{E}(O_K \otimes \mathbb{Z}_p)$ and $A_q \subseteq \mathcal{E}(O_K \otimes \mathbb{Z}_q)$.*
Output: Subsets $A'_p \subset A_p$ and $A'_q \subset A_q$, which only contain points which satisfy reduction and log considerations.

(1) *For all $\mathcal{R} \in A_p$, compute* $\mathrm{red}_{\mathcal{R}}$. *Let $R_q = \{\mathrm{red}_{\mathcal{R}} : \mathcal{R} \in A_p\}$. Let R_p be the analogous set for the set A_q.*

(2) *For $\mathcal{R} \in A_p$, calculate* $\log_{\mathcal{R}}$ *as in 4.2. Let $L_p := \{\log_{\mathcal{R}} : \mathcal{R} \in A_p\}$. Similarly, let L_q denote the analogous set for A_q.*

(3) *For each $\mathcal{R}$, compute*

$$(\log_{\mathcal{R}} \times \mathrm{red}_{\mathcal{R}}) \bigcap \left(\bigcup_{\mathcal{S} \in A_q} \mathrm{red}_{\mathcal{S}} \times \log_{\mathcal{S}} \right) \tag{14}$$

If the set in (14) *is empty, then we discard $\mathcal{R}$.*

(4) *If the set in* (14) *is not empty, we record each $\mathcal{S} \in A_q$ such that $(\log_{\mathcal{R}} \times \mathrm{red}_{\mathcal{R}}) \cap (\log_{\mathcal{S}} \times \mathrm{red}_{\mathcal{S}}) \neq \emptyset$. We check for each such $\mathcal{S}$ if the sum of local heights away from q corresponds to the sum of local height away from p computed for $\mathcal{R}$. If they correspond to different local heights, we discard $\mathcal{R}$. Else, we append $\mathcal{R}$ to A'_p.*

(5) *We run through Step 1 to Step 4 for all $\mathcal{R} \in A_p$. This leaves us with a subset $A'_p \subseteq A_p$ of points that satisfy the restrictions obtained from log information and reduction information. We also get a similar set $A'_q \subseteq A_q$.*

5. Examples

Let $K = \mathbb{Q}(\zeta_3)$, and $O_K = \mathbb{Z}[\zeta_3]$.

Example 5.1. *Consider the scheme $\mathcal{U}_1/O_K$ cut out by the Weierstrass equation*

$$y^2 + (\zeta_3 + 2)y = x^3 + (-\zeta_3 - 2)x^2 + (\zeta_3 + 1)x.$$

We let E be the projectivisation of the generic fibre of $\mathcal{U}_1$. Let $pO_K = \mathfrak{p}_1\mathfrak{p}_2$ for $p = 7$ and $qO_K = \mathfrak{q}_1\mathfrak{q}_2$ for $q = 13$. We have the following information about this curve:

(1) *$E(K) = \mathbb{Z} \cdot P \oplus \mathbb{Z} \cdot Q$ where $P = (1, 0), Q = (\zeta_3 + 1, 0)$.*

(2) *$E_{\mathbb{F}_{\mathfrak{p}_1}}(\mathbb{F}_p) \cong \mathbb{Z}/13\mathbb{Z} \cong E_{\mathbb{F}_{\mathfrak{p}_2}}(\mathbb{F}_p)$.*

(3) *$E_{\mathbb{F}_{\mathfrak{q}_1}}(\mathbb{F}_q) \cong \mathbb{Z}/7\mathbb{Z}, E_{\mathbb{F}_{\mathfrak{q}_2}}(\mathbb{F}_q) \cong \mathbb{Z}/19\mathbb{Z}$.*

(4) *The curve has bad reduction at the single prime* $\mathfrak{p} = (-22\zeta_3 - 9)$ *and* $\mathrm{Nm}(\mathfrak{p}) = 367$. *It has Kodaira Symbol II, Tamagawa number* 1. *The discriminant and conductor of the curve are both* $\mathfrak{p}^2$. *For more information about this curve, see the LMFDB page at* `https://www.lmfdb.org/EllipticCurve/2.0.3.1/134689.3/CMa/1`.

(5) *The sets* T^{cyc} *and* T^{anti} *as described in Algorithm 2 are* $\{0\}$ *for* $i = 1, 2$.

We first search for points of small height and get a list of 12 O_K*-points. We wish to certify these are the only points of* $\mathcal{U}_1$.

On finding the quadratic Chabauty sets for $p = 7, q = 13$ *since they satisfy Condition 4.1, we get* $\#A_p = 204, \#A_q = 108$. *On applying the sieve described in Algorithm 3, all the classes are eliminated, that is all the extra* 7*-adic points and* 13*-adic points are eliminated via mod* 7 *and mod* 13 *considerations. Hence we get*

$$\mathcal{U}_1(O_K) = \{(-3 : -8\zeta_3 - 4), (-3 : 7\zeta_3 + 2), (4\zeta_3 + 4 : -8\zeta_3 - 4), (0 : 0), (0 : -\zeta_3 - 2), (\zeta_3 + 1 : 0),$$
$$(\zeta_3 + 1 : -\zeta_3 - 2), (4\zeta_3 + 4 : 7\zeta_3 + 2), (1 : 0), (1 : -\zeta_3 - 2), (-3\zeta_3 + 1 : -8\zeta_3 - 4), (-3\zeta_3 + 1 : 7\zeta_3 + 2)\}.$$

Example 5.2. *Consider the scheme* $\mathcal{U}_2/O_K$ *cut out by the Weierstrass equation*

$$y^2 + (-\zeta_3 + 1)y = x^3 + (\zeta_3 - 1)x^2 - \zeta_3 x$$

More infromation about this curve can be found at This is the Galois-conjugate of the scheme $\mathcal{U}_1$ *in Example 5.1. We have a bijection of* O_K*-points via the non-trivial Galois automorphism of* $\mathbb{Q}(\zeta_3)$*; that is, there is a bijection*

$$\mathcal{U}_1(O_K) \longleftrightarrow \mathcal{U}_2(O_K).$$

Hence we get $\#\mathcal{U}_2(O_K) = 12$.

Example 5.3. *Consider the scheme* $\mathcal{U}_3 \subseteq \mathbb{A}^2_{O_K}$ *given by*

$$y^2 + (\zeta_3 + 1)y = x^3 + (-\zeta_3 - 2)x^2 + (\zeta_3 + 1)x + (\zeta_3 + 2)$$

There are at least 24 *points of small height in* $\mathcal{U}_3$, *and we compute a finite superset* $\mathcal{U}_3(\mathbb{Z}_p)_{\mathrm{sieve}} \subseteq \mathcal{U}(O_K \otimes \mathbb{Z}_p)$ *of the integral points. We let* E *be the elliptic curve given by the Weierstrass equation above. For more information about this curve, see the LMFDB page at* `https://www.lmfdb.org/EllipticCurve/2.0.3.1/47089.9/CMa/1`.

Let $pO_K = \mathfrak{p}_1\mathfrak{p}_2$ *for* $p = 13$ *and* $qO_K = \mathfrak{q}_1\mathfrak{q}_2$ *for* $q = 19$. *We have the following information about this curve:*

- $E(K) = \mathbb{Z} \cdot P \oplus \mathbb{Z} \cdot Q$ *where* $P = (-1, -2\zeta_3 - 1), Q = (2\zeta_3 + 2, \zeta_3)$.
- $E_{\mathbb{F}_{\mathfrak{p}_1}}(\mathbb{F}_p) \cong \mathbb{Z}/19\mathbb{Z}, E_{\mathbb{F}_{\mathfrak{p}_2}}(\mathbb{F}_p) \cong \mathbb{Z}/21\mathbb{Z}$.
- $E_{\mathbb{F}_{\mathfrak{q}_1}}(\mathbb{F}_q) \cong \mathbb{Z}/13\mathbb{Z} \cong E_{\mathbb{F}_{\mathfrak{q}_2}}(\mathbb{F}_q)$.
- *The curve has bad reduction at a prime above* 7, $v_1 = (3a - 2)$ *and at a prime above* 31, $v_2 = (6a - 5)$. *Over* v_1, *the Kodaira Symbol is* IV, *with Tamagawa number* 3 *and at* v_2, *the Kodaira symbol is II with Tamagawa number* 2. *The conductor is* $v_1^2 v_2^2$ *and the discriminant is* $v_1^4 v_2^2$.
- *The sets* $T^{\mathrm{cyc}} = \left\{0, -\frac{2}{3}\chi^{\mathrm{cyc}}(v_2)\right\}$ *and* $T^{\mathrm{anti}} = \left\{0, -\frac{2}{3}\chi^{\mathrm{anti}}(v_2)\right\}$ *as described in Algorithm 2. The set* A_p *has cardinality* 672 *while the set* A_q *has cardinality* 216. *Performing the sieve described in Algorithm 3, we have* 24 *points which are not accounted for. So we have a set* $\mathcal{U}_3(\mathbb{Z}_p)_{\mathrm{sieve}}$ *such that*

  $$\mathcal{U}_3(O_K)_{\mathrm{known}} \subseteq \mathcal{U}_3(O_K) \subseteq \mathcal{U}_3(\mathbb{Z}_p)_{\mathrm{sieve}} \subseteq \mathcal{U}(O_K \otimes \mathbb{Z}_p)$$

  such that $\#\mathcal{U}_3(O_K)_{\mathrm{known}} = 24$ *and* $\mathcal{U}_3(\mathbb{Z}_p)_{\mathrm{sieve}} = 48$.

References

[BB12] Jennifer S Balakrishnan and Amnon Besser, *Computing local p-adic height pairings on hyperelliptic curves*, International Mathematics Research Notices **2012** (2012), no. 11, 2405–2444. 4

[BB15] ———, *Coleman-Gross height pairings and the p-adic sigma function*, Journal für die reine und angewandte Mathematik (Crelles Journal) **2015** (2015), no. 698, 89–104. 2, 14

[BBBM21] Jennifer S Balakrishnan, Amnon Besser, Francesca Bianchi, and J Steffen Müller, Israel Journal of Mathematics **243** (2021), no. 1, 185–232. 1, 3, 4, 8, 12, 14, 15

[BBK10] Jennifer S Balakrishnan, Robert W Bradshaw, and Kiran S Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, Algorithmic Number Theory: 9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010. Proceedings 9, Springer, 2010, pp. 16–31. 13

[BBM16] Jennifer S Balakrishnan, Amnon Besser, and J Steffen Müller, *Quadratic Chabauty: p-adic heights and integral points on hyperelliptic curves*, Journal für die reine und angewandte Mathematik (Crelles Journal) **2016** (2016), no. 720, 51–79. 2

[BBM17] Jennifer Balakrishnan, Amnon Besser, and J Müller, *Computing integral points on hyperelliptic curves using quadratic Chabauty*, Mathematics of Computation **86** (2017), no. 305, 1403–1434. 1, 14, 16

[BÇL$^+$16] Jennifer S Balakrishnan, Mirela Çiperiani, Jaclyn Lang, Bahare Mirza, and Rachel Newton, *Shadow lines in the arithmetic of elliptic curves*, Directions in Number Theory: Proceedings of the 2014 WIN3 Workshop, Springer, 2016, pp. 33–55. 7, 8, 10, 11

[Bia20] Francesca Bianchi, *$\mathbb{Q}(\sqrt{-3})$-Integral Points on a Mordell curve*, International Congress on Mathematical Software, Springer, 2020, pp. 39–50. 1, 4

[BKK11] Jennifer Balakrishnan, Kiran Kedlaya, and Minhyong Kim, *Appendix and erratum to "Massey products for elliptic curves of rank 1"*, Journal of the American Mathematical Society **24** (2011), no. 1, 281–291. 2

[CG89] Robert F Coleman and Benedict H Gross, *p-adic Heights on Curves*, Algebraic Number Theory—in honor of K. Iwasawa, vol. 17, Mathematical Society of Japan, 1989, pp. 73–82. 2, 14

[Cha41] Claude Chabauty, *Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieurea la dimension*, CR Acad. Sci. Paris **212** (1941), 1022–1024. 2

[Col85] Robert F Coleman, *Torsion points on curves and p-adic abelian integrals*, Annals of Mathematics **121** (1985), no. 1, 111–168. 2, 12, 13

[CPS06] JE Cremona, Martin Prickett, and Samir Siksek, *Height difference bounds for elliptic curves over number fields*, Journal of Number Theory **116** (2006), no. 1, 42–68. 14, 15

[Dog23] Netan Dogra, *Unlikely intersections and the Chabauty–Kim method over number fields*, Mathematische Annalen (2023), 1–62. 3

[Fal83] Gerd Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inventiones mathematicae **73** (1983), 349–366. 2

[FVdP12] Jean Fresnel and Marius Van der Put, *Rigid analytic geometry and its applications*, vol. 218, Springer Science & Business Media, 2012. 12

[GM23a] Stevan Gajović and J Steffen Müller, *Computing p-adic heights on hyperelliptic curves*, arXiv preprint arXiv:2307.15787 (2023). 4

[GM23b] ———, *Linear quadratic Chabauty*, arXiv preprint arXiv:2307.15781 (2023). 4

[Har08] David Harvey, *Efficient computation of p-adic heights*, LMS Journal of Computation and Mathematics **11** (2008), 40–59. 6, 8

[Jha24] Aashraya Jha, *Github repository for quadratic Chabauty for elliptic curves over imaginary quadratic fields.*, `https://github.com/AashrayaJha/QC_ECIm`, 2024. 5

[Kam92] Sheldon Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Inventiones Mathematicae **109** (1992), 221–229. 12

[Kim09] Minhyong Kim, *The unipotent Albanese map and Selmer varieties for curves*, Publications of the Research Institute for Mathematical Sciences **45** (2009), no. 1, 89–133. 2

[Kim10] ———, *Massey products for elliptic curves of rank 1*, Journal of the American Mathematical Society **23** (2010), no. 3, 725–747. 2

[Leo62] Heinrich-Wolfgang Leopoldt, *Zur Arithmetik in abelschen Zahlkörpern.*, Journal für die reine und angewandte Mathematik **209** (1962), 54–71. 8

[LLL82] Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász, *Factoring polynomials with rational coefficients*, Mathematische annalen **261** (1982), 515–534. 15

[MST06] Barry Mazur, William Stein, and John Tate, *Computation of p-adic heights and log convergence*, Doc. Math (2006), 577–614. 4, 5, 6, 8, 9

[MT83] Barry Mazur and John Tate, *Canonical height pairings via biextensions*, Arithmetic and Geometry: Papers Dedicated to IR Shafarevich on the Occasion of His Sixtieth Birthday Volume I Arithmetic (1983), 195–237. 6, 7

[MT91] B Mazur and J Tate, *The p-adic sigma function*, Duke Mathematical Journal **62** (1991), no. 3, 663. 4, 6, 8, 9

[Neu13] Jürgen Neukirch, *Algebraic number theory*, vol. 322, Springer Science & Business Media, 2013. 8

[Sie14] Carl L Siegel, *Über einige Anwendungen diophantischer Approximationen: Abhandlungen der preußischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse 1929, nr. 1*, Springer, 2014. 1

[Sik13] Samir Siksek, *Explicit Chabauty over number fields*, Algebra & Number Theory **7** (2013), no. 4, 765–793. 2, 3

[Sil88] Joseph H Silverman, *Computing heights on elliptic curves*, Mathematics of computation **51** (1988), no. 183, 339–358. 14, 15

[SS97] Nigel P Smart and NM Stephens, *Integral points on elliptic curves over number fields*, Mathematical Proceedings of the Cambridge Philosophical Society, vol. 122, Cambridge University Press, 1997, pp. 9–16. 4

[ST94] Roel J Stroeker and Nikos Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arithmetica **67** (1994), no. 2, 177–196. 4

[The23] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 10.1)*, 2023, `https://www.sagemath.org`. 8

[Wut04a] Christian Wuthrich, *The fine Selmer group and height pairings*, PhD thesis, `https://www.maths.nottingham.ac.uk/plp/pmzcw/download/phd.pdf` (2004). 9

[Wut04b] Christian Wuthrich, *On p-adic heights in families of elliptic curves*, Journal of the London Mathematical Society **70** (2004), no. 1, 23–40. 9

aashjha@bu.edu, Department of Mathematics and Statistics, 665 Commonwealth Avenue, Boston MA 02215