$\mathbb{Q}(\sqrt{-3})$ -Integral Points on a Mordell Curve

Francesca Bianchi^(✉)

Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence,
University of Groningen, Groningen, The Netherlands
`francesca.bianchi@rug.nl`

Abstract. We use an extension of quadratic Chabauty to number fields, recently developed by the author with Balakrishnan, Besser and Müller, combined with a sieving technique, to determine the integral points over $\mathbb{Q}(\sqrt{-3})$ on the Mordell curve $y^2 = x^3 - 4$.

Keywords: Elliptic curves · Quadratic Chabauty · Integral points

1 Introduction

Let E be an elliptic curve over a number field K , described by a Weierstrass equation

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathcal{O}_K, \quad (1)$$

where $\mathcal{O}_K$ is the ring of integers of K . By the set of (K -)integral points on E we mean the subset of solutions (x, y) to (1) with $x, y \in \mathcal{O}_K$. Such a set is finite by Siegel's Theorem [19].

Assume for now that $K = \mathbb{Q}$. Different solutions to the problem of effectively determining the set of integral points for a fixed elliptic curve have been given. The most notable include reducing the problem to solving some Thue equations, and using elliptic logarithms. See [24] for an overview.

An alternative more recent approach to an effective version of Siegel's Theorem for elliptic curves comes from a very special instance of Kim's non-abelian Chabauty programme. At present, explicit versions of this are known only for elliptic curves of Mordell–Weil rank at most 1 [5, 6, 11, 16] and can be understood in terms of the theory of p -adic heights and formal group logarithms, where p is some fixed prime. Algorithmically, this method, often referred to as “quadratic Chabauty” in the literature, outputs a finite set of (approximations of) p -adic points on E , containing the integral points. When the rank is equal to one, this set typically also contains some points that we cannot *recognise* as rational, or even as algebraic. In order to determine the integral points, we need to be able to *prove* that such points are not p -adic approximations of rational points.

Unfortunately, there is no known method to achieve this, which might place this approach at a disadvantage compared to the previously mentioned ones. However, the idea of using p -adic heights and linear $\mathbb{Q}_p$ -valued functionals on $E(\mathbb{Q})$ and $E(\mathbb{Q}_p)$ to study the integral points turned out to be amenable to extensions to some curves of higher genus [2, 3], where the Mordell–Weil sieve is an effective tool used to address the problem of eliminating spurious p -adic points.

Generalisations to higher genus curves are very interesting from a Diophantine point of view. Nevertheless, we are left with the somewhat unsatisfactory impression that most quadratic Chabauty computations for integral points on elliptic curves appearing in the literature are carried out more as a “proof of concept” than as an actual way to determine integral points (but see [3, Appendix A] and [10, Appendix 4.A] for some examples of full computations of integral points).

In recent work with Balakrishnan, Besser and Müller [1], using restriction of scalars, we extended these explicit quadratic Chabauty techniques for integral points on elliptic curves, and, more generally, odd degree hyperelliptic curves, to arbitrary number fields. Combined with the Mordell–Weil sieve, the method successfully determined the integral points over an imaginary quadratic field on a genus 2 curve, as well as the rational points over some quadratic fields on some genus 2 bielliptic curves. Once again, though, examples of quadratic Chabauty computations for elliptic curves over number fields were also presented, but not turned into a provable determination of the set of integral points.

In this note we use the techniques of [1] to determine the set of $\mathbb{Q}(\sqrt{-3})$ -integral points on the Mordell curve

$$E: y^2 = x^3 - 4. \quad (2)$$

The goal is twofold. First, we want to show that quadratic Chabauty can indeed be a tool to determine the set of integral points on an elliptic curve (even over number fields), and that it is not only a test case for more general techniques that apply to higher genus curves. In order to achieve this, we need to substitute the Mordell–Weil sieve step with an analogous sieve for elliptic curves: we do this by extending to number fields the technique of [3, Appendix A]. Secondly, presenting this particular computation allows us to overcome a lot of the technicalities and notational complexity of [1], while still conveying the general strategy.

A few words about our choices of curve and field. The techniques for the computation of integral points of elliptic curves over $\mathbb{Q}$ were extended to arbitrary number fields by Smart and Stephens [23]. However, it appears that they are currently implemented in **Magma** [12] only over totally real fields; hence the choice of an imaginary quadratic field. In order to get rid of presumed non-integral points in the quadratic Chabauty computation, it is convenient to compare quadratic Chabauty outputs at different primes. For our choice of curve, there are two prime numbers, namely $p_1 = 7$ and $p_2 = 13$, which satisfy $\#E(\mathbb{F}_{p_i}) \equiv 0 \pmod{p_j}$ for $i \neq j$, making the comparison of the respective quadratic Chabauty outputs easier. In fact, this was used in [3, Appendix A] to compute the integral points

over $\mathbb{Q}$, since E has rank 1 over $\mathbb{Q}$ and hence “classical” quadratic Chabauty is applicable. Finally, E attains rank 2 over $\mathbb{Q}(\sqrt{-3})$, both p_1 and p_2 split in $\mathbb{Q}(\sqrt{-3})$, and the latter is also the field of complex multiplication of E , making it a nice example to which our techniques can be applied.

The code to perform quadratic Chabauty for an elliptic curve over $\mathbb{Q}$ base-changed to an imaginary quadratic field, as well as for the sieving routines of this example, is available at [9].

2 Quadratic Chabauty for $E/\mathbb{Q}(\sqrt{-3})$

Let K be a number field of degree d and let $\mathbb{A}_{K,f}^\times$ be the group of finite ideles of K ; let p be an odd prime, unramified in K . For ease of exposition, we assume that K has class number 1 and for every prime $\mathfrak{q}$ of K we fix a generator $\xi_{\mathfrak{q}}$ for $\mathfrak{q}$. Furthermore, we let $|\cdot|_{\mathfrak{q}}$ be the absolute value on $K_{\mathfrak{q}}$, normalised so that $|q|_{\mathfrak{q}} = q^{-1}$, if q is the rational prime below $\mathfrak{q}$. Thus $|\xi_{\mathfrak{q}}| = q^{-1/r_{\mathfrak{q}}}$, for some positive integer $r_{\mathfrak{q}}$ which divides the degree $n_{\mathfrak{q}}$ of the extension $K_{\mathfrak{q}}/\mathbb{Q}_{\mathfrak{q}}$.

An idele class character is a continuous homomorphism

$$\chi = \sum_{\mathfrak{q}} \chi_{\mathfrak{q}} : \mathbb{A}_{K,f}^\times / K^\times \rightarrow \mathbb{Q}_p^\times.$$

In principle, the idele class character χ is determined by the value, at each prime $\mathfrak{q}$, of $\chi_{\mathfrak{q}}$ on $\xi_{\mathfrak{q}}$ and on the units $\mathcal{O}_{\mathfrak{q}}^\times$ of the ring of integers of $K_{\mathfrak{q}}$. However, the incompatibility between the $\mathfrak{q}$ -adic and p -adic topology for $\mathfrak{q} \neq p$ and the required vanishing of χ on $K^\times$ have two strong consequences:

- The restrictions of $\chi_{\mathfrak{p}}$ to $\mathcal{O}_{\mathfrak{p}}^\times$ at the primes $\mathfrak{p} \mid p$ uniquely determine χ . Indeed, $\chi_{\mathfrak{q}}$ vanishes on $\mathcal{O}_{\mathfrak{q}}^\times$ if $\mathfrak{q} \nmid p$, and for every prime $\mathfrak{q}$ we have the formula

$$\chi_{\mathfrak{q}}(\xi_{\mathfrak{q}}) = - \sum_{\substack{\mathfrak{p} \mid p \\ \mathfrak{p} \neq \mathfrak{q}}} \chi_{\mathfrak{p}}(\xi_{\mathfrak{q}}). \quad (3)$$

- Each fundamental unit for K imposes an additional constraint on the characters $\chi_{\mathfrak{p}}$. In particular, the idele class characters for K form a $\mathbb{Q}_p^\times$ -vector space V of dimension greater than or equal to $d - \text{rank}(\mathcal{O}_K^\times)$.

Computing a basis for V amounts to doing some linear algebra.

Example 1. In our situation of interest, K is an imaginary quadratic field, in which p splits, say $p = \mathfrak{p}_1 \mathfrak{p}_2$, and we may fix isomorphisms $K_{\mathfrak{p}_i} \simeq \mathbb{Q}_p$. Then V is spanned by two characters: the *cyclotomic* character χ^{cyc} and the *anticyclotomic* character χ^{anti} . The cyclotomic character is the unique character satisfying

$$\chi_{\mathfrak{p}_i}^{\text{cyc}}(x) = \log(x) \quad \text{for all } x \in \mathcal{O}_{\mathfrak{p}_i}^\times,$$

where $\log: \mathbb{Z}_p^\times \rightarrow \mathbb{Q}_p$ is the p -adic logarithm, and we view x as an element of $\mathbb{Z}_p^\times$ via our fixed isomorphism. The anticyclotomic character (depending on our choice of ordering of the primes above p) is determined by

$$\chi_{\mathfrak{p}_1}^{\text{anti}}(x) = \log(x) \quad \text{for all } x \in \mathcal{O}_{\mathfrak{p}_1}^\times; \quad \chi_{\mathfrak{p}_2}^{\text{anti}}(x) = -\log(x) \quad \text{for all } x \in \mathcal{O}_{\mathfrak{p}_2}^\times.$$

The p -adic logarithm comes in the picture because we are considering homomorphisms from the multiplicative $\mathcal{O}_{\mathfrak{p}_i}^\times$ to the additive $\mathbb{Q}_p$.

Formula (3) gives

$$\chi_q^{\text{cyc}}(q) = r_q \chi_q^{\text{cyc}}(\xi_q) = -n_q \log(q) \quad \text{for all } q \neq p; \quad (4)$$

$$\chi_q^{\text{anti}}(q) = r_q \chi_q^{\text{cyc}}(\xi_q) = 0 \quad \text{for all } q \neq p \text{ such that } n_q = 2. \quad (5)$$

Let E/K now be an elliptic curve with good reduction at all primes above p , described by an equation of the form (2), which, for simplicity, we further assume to be minimal at all primes. Let S be the set of primes of bad reduction for E , and for each prime $\mathfrak{q}$ of K , let c_q be the Tamagawa number of E at $\mathfrak{q}$ (cf. [18, Theorem 4.11]).

If none of the primes above p is in S , by work of Bernardi [7], Mazur–Tate [17], Coleman–Gross [14] and others, to every idele class character $\chi \in V$ we can attach a quadratic function

$$h_p^\chi: E(K) \rightarrow \mathbb{Q}_p \quad \text{by} \quad h_p^\chi(P) = \begin{cases} (\prod_{\mathfrak{q} \in S} c_q)^{-1} \chi(\iota(P)) & \text{if } P \neq O, \\ 0 & \text{otherwise,} \end{cases}$$

for some suitably chosen $\iota(P) \in \mathbb{A}_{K,f}^\times$, which is independent of χ and whose $\mathfrak{p}$ -adic component at a prime $\mathfrak{p} \mid p$ depends on the choice of a subspace of $H_{\text{dR}}^1(E/K_{\mathfrak{p}})$, complementary to the space of holomorphic forms.

We call h_p^χ the (*global*) p -adic height attached to χ , where we should not forget, however, that we have made some preliminary choices that are not reflected in our notation.

More generally, at every prime $\mathfrak{q}$, given $P_q \in E(K_q) \setminus \{O\}$, there exists $\iota_q(P_q) \in K_q^\times$ and a *local* p -adic height function

$$\lambda_q^\chi: E(K_q) \setminus \{O\} \rightarrow \mathbb{Q}_p, \quad \lambda_q^\chi(P_q) = c_q^{-1} \chi_q(\iota_q(P_q)),$$

so that $\iota(P)_q = \iota_q(P)(\prod_{\mathfrak{r} \in S \setminus \mathfrak{q}} c_{\mathfrak{r}})$ and hence

$$h_p^\chi(P) = \sum_{\mathfrak{q}} \lambda_q^\chi(P) \quad \text{if } P \in E(K) \setminus \{O\}.$$

The failure of each λ_q^χ to be a quadratic function is absorbed into the vanishing of χ on $K^\times$, i.e. we have

$$h_p^\chi(mP) = m^2 h_p^\chi(P) \quad \text{for every } m \in \mathbb{Z} \text{ and } P \in E(K). \quad (6)$$

We do not go into the details here of how to define $\iota_q(P_q)$. We just note that the definition of h_p^χ mimics Néron’s definition of the real canonical height (for which see, for instance, [21, Chapter VI]), and we record the following properties.

Proposition 1. 1. At a prime $\mathfrak{p} \mid p$, the function $\lambda_{\mathfrak{p}}^{\chi}$ restricts to a locally analytic function on $E(\mathcal{O}_{\mathfrak{p}})$, whose power series expansion in a local coordinate t in each residue disc¹ can be computed up to any desired $\mathfrak{p}$ -adic and t -adic precision.

2. At a prime $\mathfrak{q} \nmid p$, $\iota_{\mathfrak{q}}(P)$ is independent of p . We have
 – If P reduces to a non-singular point modulo $\mathfrak{q}$, then

$$\iota_{\mathfrak{q}}(P) = \max\{1, |x(P)|_{\mathfrak{q}}\}^{-c_{\mathfrak{q}}}.$$

- If P reduces to a singular point, then $\iota_{\mathfrak{q}}(P)^{r_{\mathfrak{q}}} \in W_{\mathfrak{q}}$, where $W_{\mathfrak{q}} \subset \mathbb{Q}^{\times}$ is a finite set which can be deduced from knowledge of the Tamagawa number and Kodaira symbol of E at $\mathfrak{q}$.

Corollary 1. Let S be the set of primes of K at which E has bad reduction. For every $\mathfrak{q} \in S$, there exists a finite set $T_{\mathfrak{q}} \subset \mathbb{Q}^{\times}$ such that for every $P \in E(\mathcal{O}_K)$ there exists $t_{\mathfrak{q}} \in T_{\mathfrak{q}}$ with

$$h_p^{\chi}(P) = \sum_{\mathfrak{p} \mid p} \lambda_{\mathfrak{p}}^{\chi}(P) + \sum_{\mathfrak{q} \in S} c_{\mathfrak{q}}^{-1} r_{\mathfrak{q}}^{-1} \chi_{\mathfrak{q}}(t_{\mathfrak{q}}).$$

Moreover, $T_{\mathfrak{q}}$ and $t_{\mathfrak{q}}$ are independent of p and χ .

Corollary 1 and Eq. (6) are the key ingredients for our method. In fact, a point $P \in E(\mathcal{O}_K)$ carries global information by its being a point in $E(K)$. This is encoded in (6), but alone would not suffice to give it a finite characterisation inside $\prod_{\mathfrak{p} \mid p} E(K_{\mathfrak{p}})$, since $E(K)$ could be infinite. Thus, we also need to exploit the local information that it carries by its being integral at every prime and this is where Corollary 1 comes into play.

In order to use (6) effectively, we need to express the p -adic height h_p^{χ} as the restriction of a locally analytic function $\prod_{\mathfrak{p} \mid p} E(K_{\mathfrak{p}}) \rightarrow \mathbb{Q}_p$. This is where we are forced to impose some conditions on the rank of $E(K)$. We will focus now on our example of interest; see [1] for the general treatment of the quadratic Chabauty steps. The sieving method that we describe is an extension to number fields of [3, Appendix A]; while for the moment we restrict the exposition to this example, the method would apply more generally: see Sect. 3.

Example 2. Let E be the curve over $K = \mathbb{Q}(\sqrt{-3})$ defined by (2). Let

$$E^{-3}: y^2 = x^3 + 108 \tag{7}$$

be the quadratic twist of E by -3 . By computing generators for $E(\mathbb{Q})$ and $E^{-3}(\mathbb{Q})$ with SageMath [25], we deduce that

$$E(K) = \langle Q, R \rangle \simeq \mathbb{Z}^2,$$

¹ A residue disc is a fibre of the reduction map $E(K_{\mathfrak{p}}) \rightarrow E(\mathbb{F}_{\mathfrak{p}})$ where $\mathbb{F}_{\mathfrak{p}}$ is the residue field of $K_{\mathfrak{p}}$.

where

$$Q = (2, 2), \quad R = (-\sqrt{-3} + 1, 2\sqrt{-3}).$$

The set of primes at which E/K has bad reduction is

$$S = \{(2), (\sqrt{-3})\}, \quad \text{with } c_{(2)} = 4, \quad c_{(\sqrt{-3})} = 3.$$

Let $p \in \{7, 13\}$. The prime p splits completely in K and we are in the situation of Example 1, so we have two global p -adic heights

$$h_p^{\text{cyc}} := h_p^{\chi^{\text{cyc}}}, h_p^{\text{anti}} := h_p^{\chi^{\text{anti}}} : E(K) \rightarrow \mathbb{Q}_p,$$

where we have chosen the local heights at $\mathfrak{p}_i$ to be the ones of Mazur–Tate (which coincide with Bernardi’s in this case). For $i \in \{1, 2\}$, we may also consider

$$f_i : E(K) \hookrightarrow E(K_{\mathfrak{p}_i}) \xrightarrow{\text{Log}_i} \mathbb{Q}_p,$$

where Log_i is the unique homomorphism of abelian groups which restricts to the formal group logarithm (composed with $K_{\mathfrak{p}_i} \simeq \mathbb{Q}_p$) on the formal group. By construction, the functions Log_1 and Log_2 are locally analytic, and Lemma 6.4 of [1] shows that f_1 and f_2 (or, more precisely, their extensions to $E(K) \otimes \mathbb{Q}_p$) are linearly independent. Since the rank of $E(K)$ is 2 by (2), it follows that any $\mathbb{Q}_p$ -valued quadratic function on it must be a $\mathbb{Q}_p$ -linear combination of

$$f_1^2, \quad f_1 f_2, \quad f_2^2.$$

In particular, there exist $\alpha_i^{\text{cyc}}, \alpha_i^{\text{anti}} \in \mathbb{Q}_p$ such that

$$h_p^{\text{cyc}} = \alpha_1^{\text{cyc}} f_1^2 + \alpha_2^{\text{cyc}} f_1 f_2 + \alpha_3^{\text{cyc}} f_2^2, \quad h_p^{\text{anti}} = \alpha_1^{\text{anti}} f_1^2 + \alpha_2^{\text{anti}} f_1 f_2 + \alpha_3^{\text{anti}} f_2^2. \quad (8)$$

Properties of the cyclotomic and anticyclotomic characters show that $\alpha_1^{\text{cyc}} = \alpha_3^{\text{cyc}}$; $\alpha_1^{\text{anti}} = -\alpha_3^{\text{anti}}$ and $\alpha_2^{\text{anti}} = 0$ (cf. [1, §6.2]). Furthermore, since h_p^{χ} is invariant under any automorphism of E/K (while f_1^2 and f_2^2 are only invariant under ± 1), in this case all the constants are identically zero, except for α_2^{cyc} , which is non-zero by [8]. We can compute it up to our desired precision, by comparing the values of the p -adic height and of $f_1 f_2$ on any point of infinite order of $E(K)$.

To make (8) sensitive to the difference between K -rational and K -integral points, we use Corollary 1. By work of Cremona–Prickett–Siksek [15] (see also [11, Proposition 2.4]), we may take

$$T_{(2)} = \{1, 2^4\}, \quad T_{(\sqrt{-3})} = \{1, 3^2\}.$$

Consider the locally analytic functions

$$\rho_p^{\text{cyc}} : E(\mathcal{O}_{\mathfrak{p}_1}) \times E(\mathcal{O}_{\mathfrak{p}_2}) \rightarrow \mathbb{Q}_p, \quad \rho_p^{\text{anti}} : E(\mathcal{O}_{\mathfrak{p}_1}) \times E(\mathcal{O}_{\mathfrak{p}_2}) \rightarrow \mathbb{Q}_p,$$

defined by

$$\rho_p^*(P_1, P_2) = \lambda_{\mathfrak{p}_1}^*(P_1) + \lambda_{\mathfrak{p}_2}^*(P_2) - \alpha_2^* \text{Log}_1(P_1) \text{Log}_2(P_2).$$

By Corollary 1 and (4)-(5), for every $P \in E(\mathcal{O}_K)$, there exists $t_{(2)} \in T_{(2)}$ and $t_{(\sqrt{-3})} \in T_{(\sqrt{-3})}$ such that

$$\rho_p^{\text{cyc}}(\psi_p(P)) - \frac{1}{2} \log t_{(2)} - \frac{1}{3} \log t_{(\sqrt{-3})} = 0 = \rho_p^{\text{anti}}(\psi_p(P)),$$

where $\psi_p: E(\mathcal{O}_K) \hookrightarrow E(\mathcal{O}_{\mathfrak{p}_1}) \times E(\mathcal{O}_{\mathfrak{p}_2})$ is the map induced by the completion maps. The strategy is then as follows.

1. Fix a positive integer B and compute²

$$E(\mathcal{O}_K)_{\text{known}} = \{nQ + mR : |n|, |m| \leq B \text{ and } nQ + mR \in E(\mathcal{O}_K)\}.$$

By picking B sufficiently large, we might expect that $E(\mathcal{O}_K)_{\text{known}} = E(\mathcal{O}_K)$ and the following steps try to prove the equality.

2. Fix $(t_{(2)}, t_{(\sqrt{-3})}) \in T_{(2)} \times T_{(\sqrt{-3})}$.
3. Let $p = 7$. Compute, modulo some fixed p -adic precision, all $(P_1, P_2) \in E(\mathcal{O}_{\mathfrak{p}_1}) \times E(\mathcal{O}_{\mathfrak{p}_2})$ such that

$$\rho_7^{\text{cyc}}(P_1, P_2) - \frac{1}{2} \log t_{(2)} - \frac{1}{3} \log t_{(\sqrt{-3})} = 0 = \rho_7^{\text{anti}}(P_1, P_2). \quad (9)$$

If $\varphi \in \text{Aut}(E/K)$ with induced $\varphi_i \in \text{Aut}(E/K_{\mathfrak{p}_i})$, then $(\varphi_1(P_1), \varphi_2(P_2))$ is a solution to (9) if (P_1, P_2) is. Furthermore, if (P_1, P_2) is a solution, then so is (P_2, P_1) where we are abusing notation, in view of the isomorphisms $K_{\mathfrak{p}_1} \simeq \mathbb{Q}_p \simeq K_{\mathfrak{p}_2}$.

4. For every (P_1, P_2) computed in step 3, check if there exists $P \in E(\mathcal{O}_K)_{\text{known}}$ with $\psi_7(P) \equiv (P_1, P_2)$. If such P does not exist, suppose there exists $T \in E(\mathcal{O}_K) \setminus E(\mathcal{O}_K)_{\text{known}}$ with $\psi_7(T) = (P_1, P_2)$. Then $T = nQ + mR$ for some $n, m \in \mathbb{Z}$ satisfying

$$\begin{pmatrix} n \\ m \end{pmatrix} = \begin{pmatrix} f_1(Q) & f_1(R) \\ f_2(Q) & f_2(R) \end{pmatrix}^{-1} \begin{pmatrix} \text{Log}_1(P_1) \\ \text{Log}_2(P_2) \end{pmatrix} \pmod{7}.$$

Furthermore we can compute

$$\begin{pmatrix} n \\ m \end{pmatrix} \pmod{13},$$

by considering the images of P_1, P_2, Q, R in $E(\mathbb{F}_{\mathfrak{p}_1})$ and $E(\mathbb{F}_{\mathfrak{p}_2})$, since $\#E(\mathbb{F}_{\mathfrak{p}_i}) = \#E(\mathbb{F}_7) = 13$. (Note that it is straightforward to verify that there can be at most one such possibility).

5. The solution set of

$$\rho_{13}^{\text{cyc}}(P_1, P_2) - \frac{1}{2} \log t_{(2)} - \frac{1}{3} \log t_{(\sqrt{-3})} = 0 = \rho_{13}^{\text{anti}}(P_1, P_2)$$

² This step could be skipped; assuming this computation just simplifies the exposition of the other steps.

must contain $\psi_{13}(T)$. Since $\#E(\mathbb{F}_{13}) = 3 \cdot 7$, we can, similarly to steps 3 and 4, deduce another list of possibilities for the pair

$$\binom{n}{m} \bmod 13, \quad \binom{n}{m} \bmod 7.$$

If none of these pairs matches the one of step 4, then we have shown that (P_1, P_2) is not in the image of ψ_7 .

6. We repeat steps 3–5 for each element of $T_{(2)} \times T_{(\sqrt{-3})}$.

Remark 1. The computations of the zero sets in steps 3 and 5 are carried out locally, i.e. for every pair $(\overline{P_1}, \overline{P_2}) \in E(\mathbb{F}_{p_1}) \times E(\mathbb{F}_{p_2})$, we can give a two-variable parametrisation of the points in $E(K_{p_1}) \times E(K_{p_2})$ reducing to $(\overline{P_1}, \overline{P_2})$. The task is then reduced to computing zero sets of systems of two-variable equations in two variables. This can be done either naively, or, when the hypotheses apply, using a two-variable version of Hensel’s lemma [1, Appendix A]. For the strategy to give a provable determination of the integral points, it is necessary to verify that the approximations of the zeros corresponding to points in $E(\mathcal{O}_K)$ lift to unique zeros. It is on the other hand not necessary in general to show that the other zeros lift uniquely.

We implement this technique in **SageMath** and run it with $B = 10$. As we vary $t_{(2)}$ and $t_{(\sqrt{-3})}$, this gives 426 solutions to (9) which do not come from points in $E(\mathcal{O}_K)_{\text{known}}$. Out of these 426, there are only 4 up to automorphisms and conjugation which survive our sieve.

We need to show these 4 solutions do not come from points in $E(\mathcal{O}_K)$. We first note that they are p -adically isolated. Then we show that, if one of them did come from a point T in $E(\mathcal{O}_K)$, then, up to automorphism, it would come from a point in $E(\mathbb{Z})$ or a point in $E^{-3}(\mathbb{Z})$ where we take the minimal model (7) (this amounts to showing that in the automorphism class of the solution, there is a point of the form (P_1, P_1) or $(P_1, -P_1)$, where we are using our isomorphisms $K_{p_i} \simeq \mathbb{Q}_p$). At this point, we could invoke existing implementations to compute $E(\mathbb{Z})$ and $E^{-3}(\mathbb{Z})$, to show that all the points in $E(\mathcal{O}_K)$ coming from points in these sets are in $E(\mathcal{O}_K)_{\text{known}}$. Alternatively, we observe that being in the image of $E(\mathbb{Z})$ or $E^{-3}(\mathbb{Z})$ imposes additional constraints on the local heights away from p of P , which allow us to eliminate at once 3 of the automorphisms classes. The remaining one must come from $E^{-3}(\mathbb{Z})$ and hence must be of the form mR . There is some information that we have not used yet: since $3 \mid \#E(\mathbb{F}_{13})$, we also know $m \bmod 3$. In particular, $m \equiv 0 \bmod 3$. But then mR is a multiple of $3R$, which is in the formal group at $(\sqrt{-3})$: thus mR cannot be integral. This shows that

Theorem 1. $E(\mathcal{O}_K) = \{\varphi(P), \varphi(P^c) : P \in G, \varphi \in \text{Aut}(E/K)\}$, where P^c is the Galois conjugate of P and

$$G = \{(2, 2), (5, 11), (-2, 2\sqrt{-3}), (1, \sqrt{-3}), \\ (-122, 778\sqrt{-3}), (3\sqrt{-3} - 5, 4\sqrt{-3} + 18)\}.$$

3 A More General Approach

We end this article with an outline of the strategy that was implicitly used in Example 2, in the hope that this discussion will convince the reader that similar methods could be used to determine the integral points of other elliptic curves over number fields.

Let E be an elliptic curve over an imaginary quadratic field K . Suppose further that existing algorithms - e.g. as implemented in [12] - succeed in the computation of the rank r of $E(K)$. If $r \geq 3$, our methods are not applicable. If $r = 0$, the computation of $E(\mathcal{O}_K)$ is trivial; if $r = 1$, minor modifications to the quadratic Chabauty method over $\mathbb{Q}$ are sufficient [4].

Thus, we may assume that r is exactly equal to 2, and that we can compute generators for the Mordell–Weil group $E(K)$. For simplicity, we further assume that the torsion subgroup of $E(K)$ is trivial. Hence,

$$E(K) = \langle Q, R \rangle$$

for some points of infinite order Q and R . Our goal is the computation of the integral points $E(\mathcal{O}_K)$.

It is reasonable to first compute the integral points up to a certain height bound and we shall denote the resulting set by $E(\mathcal{O}_K)_{\text{known}}$. Indeed, for instance, if Q and R are non-integral at the same prime $\mathfrak{q}$, then $E(\mathcal{O}_K)$ is empty and no further step should be taken (see [22, Chapter VII]).

Let p be an odd prime such that E has good reduction at every $\mathfrak{p} \mid p$. Current restrictions in the implementation of some of the techniques that we need also require us to assume that p is split in K , say $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for distinct primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $\mathcal{O}_K$. We have homomorphisms

$$f_i: E(K) \rightarrow \mathbb{Q}_p,$$

obtained by composing the completion map $E(K) \hookrightarrow E(K_{\mathfrak{p}_i})$ with $\mathfrak{p}_i$ -adic abelian integration and with the isomorphism $K_{\mathfrak{p}_i} \cong \mathbb{Q}_p$. If f_1 and f_2 are linearly independent, then we can carry out quadratic Chabauty for the prime p on E/K . Linear independence is guaranteed by [1, Lemma 6.4] if E is the base-change of an elliptic curve over $\mathbb{Q}$ of rank 1, and we also expect it to hold if E does not descend to $\mathbb{Q}$.

In the belief that the exposition of the quadratic Chabauty computation in Sect. 2 was, when not already in full generality, easily generalisable, we do not elaborate on that further. The upshot is that we can compute a set U_p of points in $E(\mathcal{O}_{\mathfrak{p}_1}) \times E(\mathcal{O}_{\mathfrak{p}_2})$ such that if $P \in E(\mathcal{O}_K) \setminus E(\mathcal{O}_K)_{\text{known}}$ then the image of P under the completion maps lies in U_p . By “computing”, we mean that given a large enough integer n we can find the finite set of approximations modulo³ p^n of the points in U_p . This is provided that we can show that, modulo p^n , there are no points in U_p that have the same reduction as any point in $E(\mathcal{O}_K)_{\text{known}}$. Based on experimental data, we can say that the latter task can generally be addressed

³ Given that $K_{\mathfrak{p}_i} \cong \mathbb{Q}_p$, the phrasing “modulo p^n ” has the obvious meaning.

using the multivariable Hensel's lemma, but occasionally needs support from theoretical arguments [1, Appendix A] (see also Remark 1).

If U_p is empty, we deduce that $E(\mathcal{O}_K) = E(\mathcal{O}_K)_{\text{known}}$. Otherwise, we can try to extrapolate more information from U_p , or compute U_p for more than one choice of p . If the primes are chosen wisely, it is possible to compare the outputs U_p . We explain here a good choice; many others could be possible.

For $i \in \{1, 2\}$, let $k_{\mathfrak{p}_i}$ be the greatest common divisor of the orders in $E(\mathbb{F}_{\mathfrak{p}_i})$ of the reduction of Q and R . Assume that $(P_{\mathfrak{p}_1}, P_{\mathfrak{p}_2}) \in U_p$ is the localisation of a point $P \in E(\mathcal{O}_K) \setminus E(\mathcal{O}_K)_{\text{known}}$. Then there must exist $n, m \in \mathbb{Z}$ such that

$$P = nQ + mR.$$

Using $\mathfrak{p}_i$ -adic abelian integration, we may compute a unique pair $(n_p, m_p) \in (\mathbb{Z}/p\mathbb{Z})^2$ such that

$$(n, m) \equiv (n_p, m_p) \pmod{p}. \quad (10)$$

Furthermore, for every i we can compute a list of possibilities for

$$(n, m) \pmod{k_{\mathfrak{p}_i}}, \quad (11)$$

by considering the images of Q , R and $P_{\mathfrak{p}_i}$ in $E(\mathbb{F}_{\mathfrak{p}_i})$.

If $p \mid k_{\mathfrak{p}_i}$ for at least one i , then (10) and (11) can sometimes be used to rule out points in U_p from being localisations of points in $E(\mathcal{O}_K)$.

If this is not sufficient to prove that no point in U_p can correspond to a point in $E(\mathcal{O}_K)$, or if p is coprime with each $k_{\mathfrak{p}_i}$, then we may look for a split odd prime q of good reduction such that $q \mid k_{\mathfrak{p}_i}$ and $p \mid k_{\mathfrak{q}_j}$ for at least one (i, j) , if $q\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$. If the element $(P_{\mathfrak{p}_1}, P_{\mathfrak{p}_2}) \in U_p$ corresponds to $P \in E(\mathcal{O}_K)$, then P must map to some $(P_{\mathfrak{q}_1}, P_{\mathfrak{q}_2}) \in U_q$ under the $(\mathfrak{q}_1, \mathfrak{q}_2)$ -completion maps. By running through U_q , we obtain a list of possibilities for the pair

$$(n, m) \pmod{q} \quad \text{and} \quad (n, m) \pmod{k_{\mathfrak{q}_j}},$$

which we can compare with (10) and (11).

If this is still not sufficient to show that $E(\mathcal{O}_K) = E(\mathcal{O}_K)_{\text{known}}$, we can look for sequences of primes with similar patterns.

Elliptic curves E over $\mathbb{Q}$ admitting a pair of primes of good reduction (p, q) satisfying $\#E(\mathbb{F}_p) = q$ and $\#E(\mathbb{F}_q) = p$ were studied by Silverman–Stange [20]. Assuming that there are infinitely many primes ℓ for which $\#E(\mathbb{F}_\ell)$ is prime, the authors conjectured that the number of such pairs (p, q) with $p < q$ and $p \leq X$ should grow like a multiple of $X/(\log X)^2$ if E has CM, and of $\sqrt{X}/(\log X)^2$ otherwise. More generally, they considered sequences of primes $(p_1, \dots, p_m)$ of arbitrary length m such that $\#E(\mathbb{F}_{p_i}) = p_{i+1}$, where i is taken modulo m .

This study is relevant for us if our elliptic curve over K is the base-change of an elliptic curve over $\mathbb{Q}$, as the one of Example 2. For more general elliptic curves over number fields, see [13].

Finally, the discussion of this section is readily generalisable to number fields other than imaginary quadratic ones, after deriving the analogue of Example 1 and suitably replacing the condition $r = 2$ (see [1]).

Acknowledgements. The author would like to thank Jennifer Balakrishnan and Stefan Müller for providing feedback on an earlier draft and for useful conversations. She is grateful to the anonymous referees for their comments and suggestions. She is supported by an NWO Vidi grant.

References

1. Balakrishnan, J.S., Besser, A., Bianchi, F., Müller, J.S.: Explicit quadratic Chabauty over number fields. *Isr. J. Math.*, to appear (2019). ([arXiv:1910.04653](https://arxiv.org/abs/1910.04653))
2. Balakrishnan, J.S., Besser, A., Müller, J.S.: Quadratic Chabauty: p -adic heights and integral points on hyperelliptic curves. *J. Reine Angew. Math.* **720**, 51–79 (2016). <https://doi.org/10.1515/crelle-2014-0048>
3. Balakrishnan, J.S., Besser, A., Müller, J.S.: Computing integral points on hyperelliptic curves using quadratic Chabauty. *Math. Comp.* **86**(305), 1403–1434 (2017). <https://doi.org/10.1090/mcom/3130>
4. Balakrishnan, J.S., Dogra, N.: Quadratic Chabauty and rational points, I: p -adic heights. *Duke Math. J.* **167**(11), 1981–2038 (2018). <https://doi.org/10.1215/00127094-2018-0013>. With an appendix by J.S. Müller
5. Balakrishnan, J.S., Kedlaya, K.S., Kim, M.: Appendix and erratum to “Massey products for elliptic curves of rank 1”. *J. Amer. Math. Soc.* **24**(1), 281–291 (2011)
6. Balakrishnan, J.S., Dan-Cohen, I., Kim, M., Wewers, S.: A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves. *Math. Ann.* **372**(1–2), 369–428 (2018). <https://doi.org/10.1007/s00208-018-1684-x>
7. Bernardi, D.: Hauteur p -adique sur les courbes elliptiques, Séminaire de Théorie des Nombres Paris, 1979–80. *Progr. Math.* **12**, 1–14 (1981). Birkhäuser, Boston, Mass
8. Bertrand, D.: Valeurs de fonctions thêta et hauteurs p -adiques, Séminaire de Théorie des Nombres, Paris 1980–81. *Progr. Math.* **22**, 1–12 (1982). Birkhäuser, Boston, Mass
9. Bianchi, F.: SageMath code. https://github.com/bianchifrancesca/QC-elliptic-imaginary-quadratic-rank_2
10. Bianchi, F.: Topics in the theory of p -adic heights on elliptic curves. Ph.D. thesis, University of Oxford (2019)
11. Bianchi, F.: Quadratic Chabauty for (bi)elliptic curves and Kim’s conjecture. *Algebra Number Theory* (2019). to appear ([arXiv:1904.04622](https://arxiv.org/abs/1904.04622))
12. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. *J. Symb. Comput.* **24**(3–4), 235–265 (1997). <https://doi.org/10.1006/jSCO.1996.0125>
13. Brown, J., Heras, D., James, K., Keaton, R., Qian, A.: Amicable pairs and aliquot cycles for elliptic curves over number fields. *Rocky Mt. J. Math.* **46**(6), 1853–1866 (2016). <https://doi.org/10.1216/RMJ-2016-46-6-1853>
14. Coleman, R.F., Gross, B.H.: p -adic heights on curves. In: *Algebraic number theory, Advanced Studies in Pure Mathematics*, vol. 17, pp. 73–81. Academic Press, Boston (1989)
15. Cremona, J.E., Prickett, M., Siksek, S.: Height difference bounds for elliptic curves over number fields. *J. Number Theory* **116**(1), 42–68 (2006). <https://doi.org/10.1016/j.jnt.2005.03.001>
16. Kim, M.: Massey products for elliptic curves of rank 1. *J. Am. Math. Soc.* **23**(3), 725–747 (2010)

17. Mazur, B., Tate, J.: The p -adic sigma function. *Duke Math. J.* **62**(3), 663–688 (1991). <https://doi.org/10.1215/S0012-7094-91-06229-0>
18. Schmitt, S., Zimmer, H.G.: *Elliptic Curves. A Computational Approach*. With an appendix by Attila Pethő, vol. 31 in *de Gruyter Studies in Mathematics*. Walter de Gruyter & Co. (2003). <https://doi.org/10.1515/9783110198010>
19. Siegel, C.: Über einige Anwendungen Diophantischer Approximationen. *Abh. Preus. Acad. Wiss.* **1** (1929). https://doi.org/10.1007/978-88-7642-520-2_2
20. Silverman, J.H., Stange, K.E.: Amicable pairs and aliquot cycles for elliptic curves. *Exp. Math.* **20**(3), 329–357 (2011). <https://doi.org/10.1080/10586458.2011.565253>
21. Silverman, J.: *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, vol. 151. Springer, New York (1994). <https://doi.org/10.1007/978-1-4612-0851-8>
22. Silverman, J.: *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, vol. 106, 2nd edn. Springer, Dordrecht (2009). <https://doi.org/10.1007/978-0-387-09494-6>
23. Smart, N.P., Stephens, N.M.: Integral points on elliptic curves over number fields. In: *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 122, no. 1, pp. 9–16 (1997). <https://doi.org/10.1017/S0305004196001211>
24. Smart, N.P.: *The algorithmic Resolution of Diophantine Equations*. London Mathematical Society Student Texts, vol. 41. Cambridge University Press, Cambridge (1998). <https://doi.org/10.1017/CBO9781107359994>
25. Stein, W., et al.: *Sage Mathematics Software (Version 8.9)*. The Sage Development Team (2019). <http://www.sagemath.org>