Contemporary Mathematics

# Rational points on rank 2 genus 2 bielliptic curves in the LMFDB

Francesca Bianchi and Oana Padurariu

Abstract. Building on work of Balakrishnan, Dogra, and of the first author, we provide some improvements to the explicit quadratic Chabauty method to compute rational points on genus 2 bielliptic curves over $\mathbb{Q}$, whose Jacobians have Mordell–Weil rank equal to 2. We complement this with a precision analysis to guarantee correct outputs. Together with the Mordell–Weil sieve, this bielliptic quadratic Chabauty method is then the main tool that we use to compute the rational points on the 411 locally solvable curves from the LMFDB which satisfy the aforementioned conditions.

## 1. Introduction

Let $X$ be a smooth, projective, geometrically integral curve over the field of rational numbers; let $g$ be its genus, and let $r$ be the Mordell–Weil rank of its Jacobian $J$ over $\mathbb{Q}$. In this article we compute the set of rational points on all such $X$ in the LMFDB [LMF22] - and, in particular, in the database of genus 2 curves computed by Booker, Sijsling, Sutherland, Voight and Yasaki [BSS+16] - which satisfy the following conditions:

(i) $g = 2$;
(ii) $r = 2$;
(iii) $X$ is bielliptic over $\mathbb{Q}$.

For some of these curves, there exists a place $v$ of $\mathbb{Q}$ for which $X(\mathbb{Q}_v) = \emptyset$, so the set of rational points $X(\mathbb{Q})$ is trivially empty. After discarding these, we are left with 411 curves that satisfy (i)–(iii) and are everywhere locally solvable. Our main contribution, which made the computation of the rational points on these curves possible, is an improvement of the explicit quadratic Chabauty approach specific to curves satisfying (i)–(iii) and a `SageMath` [Sag22] implementation of the resulting method (available at [BPb]). We now explain how the assumptions (i)–(iii) place our problem into the more general context of computing rational points on curves.

First of all, since we are assuming (i) that the genus of $X$ is greater than 1, the set of rational points $X(\mathbb{Q})$ is finite by Faltings' theorem [Fal83, Fal84]. Without any further assumption on $X$, there is no practical algorithm that is guaranteed to provably output all the finitely many points in $X(\mathbb{Q})$.

If $r < g$ (and $g$ is small, as in our case), a combination of the Chabauty–Coleman method [Cha41, Col85a] and the Mordell–Weil sieve [Sch99, BS10a] is

2020 *Mathematics Subject Classification.* Primary 14G05, 11G30, 11S80, 11Y50, 11G50.

likely to be successful. Let $p$ be a prime of good reduction for $X$. The core idea of the Chabauty–Coleman method is that the $p$-adic closure of $J(\mathbb{Q})$ inside the $p$-adic manifold $J(\mathbb{Q}_p)$ has codimension at least $\max\{g-r,0\}$, and hence positive codimension if $r < g$. Pulling back to $X$ via $X \to J$, $x \mapsto [\deg D \cdot x - D]$ for a $\mathbb{Q}$-rational divisor $D$ of positive degree, this allows one to write down a locally analytic function $\tilde{\rho}_0 \colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$ which vanishes on $X(\mathbb{Q})$. The zero set $A_0$ of $\tilde{\rho}_0$ is finite and contains $X(\mathbb{Q})$; the Mordell–Weil sieve can then often be used to extract from $A_0$ the set $X(\mathbb{Q})$. An implementation of this method for $g = 2$ is available in `Magma` [**BCP97**].

When $r \geq g$, the Chabauty–Coleman method is, in general, not applicable and computing $X(\mathbb{Q})$ is often a harder problem. Our geometric assumption (iii) comes in to simplify the task. Recall that a curve is bielliptic if it has a degree 2 map to an elliptic curve. We will further require that the map is defined over the base field of the curve. Then a bielliptic genus 2 curve over $\mathbb{Q}$ admits a model of the form

$$y^2 = a_6x^6 + a_4x^4 + a_2x^2 + a_0, \qquad a_i \in \mathbb{Z},$$

and its Jacobian is isogenous to $E_1 \times E_2$, where $E_1$ and $E_2$ are elliptic curves given by the following Weierstrass equations:

$$E_1 \colon y^2 = x^3 + a_4x^2 + a_2a_6x + a_0a_6^2$$
$$E_2 \colon y^2 = x^3 + a_2x^2 + a_4a_0x + a_6a_0^2$$

(see [**FK91**, **Kuh88**]). If one of $E_1$ and $E_2$ has Mordell–Weil rank 0 over $\mathbb{Q}$, we can easily compute the set $X(\mathbb{Q})$; the more interesting case is when each of $E_1$ and $E_2$ has positive rank.

For example, $X_w/\mathbb{Q}\colon y^2 = x^6+x^2+1$ is a bielliptic genus 2 curve, whose elliptic quotients each have rank 1 (so the rank of the Jacobian of $X_w$ is 2). It turns out that the determination of $X_w(\mathbb{Q})$ is equivalent to solving Problem 17 of book VI of Diophantus' Arithmetica. Wetherell [**Wet97**] observed that, in this case, one could exploit the isogeny $E_1 \times E_2 \sim \mathrm{Jac}(X_w)$ to reduce the problem of computing $X_w(\mathbb{Q})$ to that of computing the rational points on two genus 3 curves, for which the method of Chabauty–Coleman is applicable. By carrying this out explicitly, he solved Diophantus' problem, many centuries after it had been formulated.

Flynn and Wetherell [**FW99**] recast Wetherell's solution to Diophantus' problem as a special case of a strategy that can be applied to compute the rational points on arbitrary bielliptic genus 2 curves whose corresponding elliptic curve quotients each have rank equal to 1. Furthermore, they replaced the Chabauty–Coleman computations of Wetherell with computations on elliptic curves over number fields. These have hope of being successful only if the rank of such elliptic curves is strictly less than the number field degree, condition which is not always satisfied (see the example at the end of [**FW99**]). They called the resulting elliptic curve computations "elliptic curve Chabauty"; an extension of the genus 2 bielliptic method of Flynn–Wetherell to curves covering elliptic curves (possibly over some extension of $\mathbb{Q}$) is due to Bruin [**Bru03**]. It would be interesting to investigate for how many of the curves in our database the computation of rational points is algorithmically possible using elliptic curve Chabauty. We have not attempted this, but mention in this respect that Hast [**Has22**] has recently implemented a method to compute rational points on genus 2 curves with a rational Weierstrass point, which combines descent and elliptic curve Chabauty. The resulting algorithm was run on a large

**26 Jun 2023 23:11:48 PDT**
**230105-Padurariu Version 2 - Submitted to LuCaNT**

database of curves, 21 of which also belong to our database. For 15 of these 21 the computation was not successful (see [Has]), due to current algorithmic limitations of `Magma` [BCP97], for instance in the computation of Mordell–Weil ranks of elliptic curves over non-trivial extensions of $\mathbb{Q}$. This does not allow one to conclude whether in some of these cases there could be an actual theoretical obstruction to the method, nor whether other versions of elliptic curve Chabauty (e.g. Flynn–Wetherell's) would be successful on a subset of these curves. For a discussion of elliptic curve Chabauty for hyperelliptic curves and some of its limitations, see also the proof of [BGX21, Proposition 2].

In a different direction, Kim's program [Kim05, Kim09] aims to construct, for an arbitrary $X/\mathbb{Q}$, locally analytic functions $\tilde{\rho}\colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$ vanishing on the set $X(\mathbb{Q})$ by replacing the Jacobian in the method of Chabauty–Coleman with suitable Selmer varieties. Balakrishnan and Dogra [BD18] made one level of Kim's program explicit for curves satisfying $r < g + \rho - 1$, where $\rho$ is the rank of the Néron–Severi group of $J$ over $\mathbb{Q}$. The resulting method is known as "quadratic Chabauty", and the locally analytic function $\tilde{\rho}$ in this case is defined using quadratic forms constructed from $p$-adic heights.

Remark 1.1. Here by "quadratic Chabauty" we always mean, unless otherwise specified, quadratic Chabauty for rational points. A simpler variant of quadratic Chabauty can be used to determine the integral points of elliptic and hyperelliptic curves whose genus is equal to the rank of the Jacobian, and was developed prior to the work of Balakrishan–Dogra. See [Kim10, BKK11, BB15] for elliptic curves and [BBM16, BBM17] for hyperelliptic curves.

In particular, the quadratic Chabauty method is applicable to curves satisfying (i)–(iii), provided that $E_1$ and $E_2$ each have rank 1; in fact, these are perhaps the simplest class of curves for which Chabauty's method is not applicable, but quadratic Chabauty is. Not surprisingly, the first explicit examples of quadratic Chabauty in the literature are genus 2 bielliptic curves [BD18, §§8.3,8.4]. By now, Balakrishnan–Dogra's quadratic Chabauty has also been successfully applied to many modular curves of arithmetic interest, using the techniques and algorithms of [BDM+19, BDM+21].

The bielliptic genus 2 case still remains interesting, since it can be understood independently of the $p$-adic Hodge theory techniques that are normally involved in quadratic Chabauty. In this case, the locally analytic function $\tilde{\rho}$ is defined using abelian integrals and $p$-adic heights on the two elliptic curves $E_1$ and $E_2$; in fact, quadratic Chabauty for the *rational* points of $X$ is, essentially, a combination of quadratic Chabauty for the *integral* points of $E_1$ and $E_2$ (see Remark 1.1). After Balakrishnan–Dogra's first examples of explicit quadratic Chabauty on a bielliptic curve [BD18], the first author [Bia20] made some steps in the method more algorithmic and used this to provide further examples; an extension of this to number fields is given in [BBBM21].

In this article, we propose a simplification of the quadratic Chabauty function used in the computations of [BD18, Bia20, BBBM21]: see Theorem 2.4 and Remark 2.5. One of the resulting improvements is that, unlike in [BD18, Bia20], we can work with one function $\tilde{\rho}$ on the whole of $X(\mathbb{Q}_p)$, rather than having to consider different functions on two affine patches covering $X(\mathbb{Q}_p)$. This makes the computations less involved, and some of the algorithmic assumptions of [BD18, Bia20] unnecessary. We give an elementary proof that the set of rational points is contained

**26 Jun 2023 23:11:48 PDT**
**230105-Padurariu Version 2 - Submitted to LuCaNT**

in

$$A = \{z \in X(\mathbb{Q}_p) : \tilde{\rho}(z) \in \Omega\},$$

where $\Omega$ is a finite subset of $\mathbb{Q}_p$ which we can describe explicitly in terms of our equations for $X$, $E_1$, $E_2$ and the reduction type of $E_1$ and $E_2$ at the primes of bad reduction. The proof relies on properties of global and local $p$-adic heights on elliptic curves. In particular, we use Mazur–Tate $p$-adic heights [**MT83**, **MT91**, **MST06**, **Har08**].

As a result, it is possible to run the algorithm on a database containing hundreds of curves, such as ours. To support our computations, we provide a precision analysis. The function $\tilde{\rho}$ is, locally, given by a power series $f(t) \in \mathbb{Q}_p[[t]]$, where $t$ is a local parameter. In order to compute the finite set of $p$-adic points $z$ satisfying $\tilde{\rho}(z) \in \Omega$, we need to have information about the $p$-adic valuation of the coefficients of $f(t)$. We derive lower bounds for these valuations in Section 3, where we also explain how to use this to compute the set $A$, up to some $p$-adic precision.

Finally, the set $A$ will in general be larger than $X(\mathbb{Q})$. To complete our determination of the set $X(\mathbb{Q})$, we apply the Mordell–Weil sieve as in [**BBM17**] to exclude points in $A$ from belonging to $X(\mathbb{Q})$, until we are left only with points in $A$ that we can recognise as points in $X(\mathbb{Q})$. This normally requires computing the set $A$ for more than one prime $p$. See Section 4 (in particular, §4.3) for a description of a version of the Mordell–Weil sieve that is suitable to our setting, and that is based on [**BBM17**]. For this step in our computations we use the code of Balakrishnan–Dogra–Müller–Tuitman–Vonk, available at [**BDM$^+$**].

For most of the curves in our database, we apply quadratic Chabauty together with the Mordell–Weil sieve to compute $X(\mathbb{Q})$. For a minority of curves (59 of them), one of the two elliptic curves has rank 0, so we can instead compute the rational points in a much more straightforward way by considering the preimages of the $\mathbb{Q}$-rational points on the rank 0 elliptic curve quotient. Finally, for two curves, we suspected that $X(\mathbb{Q}) = \emptyset$, and we proved this using a sieve (without a preliminary quadratic Chabauty computation). See Section 4 for the various steps in our computation.

In summary, we have the following. Consider the set of genus 2 curves defined over $\mathbb{Q}$ from [**BSS$^+$16**] (available at [**LMF22**]) which have points everywhere locally, are bielliptic over $\mathbb{Q}$, and whose Jacobians have rank 2 over $\mathbb{Q}$. To this set add the quotient of the Shimura curve $X_0(10, 19)$ by the Atkin-Lehner involution $w_{190}$ and the curve $y^2 = x^6 + 6x^5 + 39x^4 + 52x^3 + 39x^2 + 6x + 1$ (see Remark 1.4 below). Let $\Delta$ be the resulting database of 413 curves.

THEOREM 1.2. *The number of rational points of each curve in the database $\Delta$ is listed in [**BPa**].*

REMARK 1.3. For two of the curves in the database $\Delta$, the full set of rational points had been determined prior to our work, and is listed on [**LMF22**]. These curves are:

- The quotient of the modular curve $X_0(129)$ by the group generated by the Atkin-Lehner involutions $w_3$ and $w_{43}$ (with LMFDB label 5547.b.16641.1). The rational points for this curve were determined using 2-cover descent by Bars–González–Xarles [**BGX21**], as well as using geometric quadratic Chabauty by Edixhoven–Lido [**EL21**].

**26 Jun 2023 23:11:48 PDT**
**230105-Padurariu Version 2 - Submitted to LuCaNT**

- The quotient of the modular curve $X_0(91)$ by its Fricke involution $w_{91}$ (with LMFDB label 8281.a.8281.1). The $\mathbb{Q}(i)$-rational points on this curve were computed using quadratic Chabauty over number fields by Balakrishnan–Besser–Müller and the first author [BBBM21].

Our computations for these curves confirm the results of [BGX21,EL21,BBBM21].

Remark 1.4. The computation of the rational points of the following curves in $\Delta$ is relevant to prior work:

- $X_0(10,19)/\langle w_{190}\rangle$: [PS23, §3.1];
- $y^2 = x^6 + 6x^5 + 39x^4 + 52x^3 + 39x^2 + 6x + 1$: [LR22, Theorem 1 and Remark following];
- $X_0(166)^*$ (with LMFDB label 13778.a.27556.1): [ACKP22, §2.4].

This paper is accompanied by our code on GitHub [BPb,BPa]. While the code for bielliptic quadratic Chabauty is an upgrade of the code pertaining to [Bia20], is written in `SageMath` [Sag22] and is available at [BPb], for the Mordell–Weil sieve computations we make extensive use of the `Magma` [BCP97] code available at [BDM$^+$]; the resulting implementation, as well as the results of our computations, can be found at [BPa].

**Acknowledgements.** It is a pleasure to thank Jennifer Balakrishnan, Céline Maistret and Steffen Müller for helpful discussions. We thank Jennifer Balakrishnan for proposing to us this project, based on a suggestion of Andrew Sutherland. We are grateful to Daniel Hast for private communication about [Has22], and to David Roe for answering our questions about the LMFDB. We thank Jennifer Balakrishnan, Barinder Banwait, Raymond van Bommel, and Steffen Müller for useful comments on an earlier version of the paper. We also thank the three anonymous referees for their helpful comments and suggestions. The first author is supported by an NWO Vidi grant. The second author is supported by NSF grant DMS-1945452 and Simons Foundation grant #550023.

**1.1. Notation.** Given a prime $q$, we denote by $\mathrm{ord}_q$ the $q$-adic valuation on $\mathbb{Q}_q$, normalised to be surjective onto $\mathbb{Z}$, and by $|\cdot|_q$ the standard absolute value on $\mathbb{Q}_q$, as well as its extension to $\overline{\mathbb{Q}_q}$.

## 2. Quadratic Chabauty for genus 2 bielliptic curves

Let $X/\mathbb{Q}$ be a non-singular genus 2 curve given by an equation of the form

$$X\colon y^2 = F(x) = a_6x^6 + a_4x^4 + a_2x^2 + a_0, \qquad a_i \in \mathbb{Z} \tag{2.1}$$

and consider the elliptic curves

$$E_1\colon y^2 = x^3 + a_4x^2 + a_2a_6x + a_0a_6^2 \tag{2.2}$$

$$E_2\colon y^2 = x^3 + a_2x^2 + a_4a_0x + a_6a_0^2. \tag{2.3}$$

There are degree 2 maps $\varphi_i\colon X \to E_i$ given on affine points by

$$\varphi_1(x,y) = (a_6x^2, a_6y), \qquad \varphi_2(x,y) = (a_0x^{-2}, a_0yx^{-3}). \tag{2.4}$$

We denote by $\infty^{\pm}$ the two points at infinity in $X(\mathbb{Q}(\sqrt{a_6}))$ and by $\infty$ the point at infinity of an elliptic curve.

Our goal is that of computing $X(\mathbb{Q})$ under some assumptions on the ranks of $E_1$ and $E_2$. Since $\varphi_i(X(\mathbb{Q})) \subseteq E_i(\mathbb{Q})$, the task is easy if one of the two elliptic

curves is of rank 0 over $\mathbb{Q}$. The first interesting case arises when each of $E_1$ and $E_2$ has rank 1 over $\mathbb{Q}$, and this is precisely the situation that we want to consider here. So let us assume that

$$\operatorname{rank}(E_1(\mathbb{Q})) = \operatorname{rank}(E_2(\mathbb{Q})) = 1,$$

and let us fix a prime $p$ of good reduction for the model of $X$ given by (2.1) (and hence also for (2.2) and (2.3)).

The strategy comprises two steps: first we compute a finite $p$-adic approximation of $X(\mathbb{Q})$ inside $X(\mathbb{Q}_p)$ (quadratic Chabauty), and secondly we refine our approximation and extract the set $X(\mathbb{Q})$ (Mordell–Weil sieve). Up until and including Section 3, our focus will be on the quadratic Chabauty part of the method, which is due to Balakrishnan–Dogra [**BD18**].

Some further examples and algorithmic observations and modifications to quadratic Chabauty for genus 2 bielliptic curves were part of the first author's article [**Bia20**]. Our starting point is the code [**Bia**] provided with the latter article, which uses local $p$-adic height functions on $E_1$ and $E_2$ defined in terms of sigma functions [**MT91**,**MST06**,**Har08**] (differently from [**BD18**], which uses Coleman–Gross $p$-adic heights [**CG89**]).

We will need these to define a non-constant locally analytic function $\tilde{\rho}\colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$ and a finite set $\Omega \subset \mathbb{Q}_p$ such that $\tilde{\rho}(X(\mathbb{Q})) \subseteq \Omega$; we further require that $\tilde{\rho}$ and $\Omega$ are computable, at least up to some desired $p$-adic precision. The set

$$\{z \in X(\mathbb{Q}_p) : \tilde{\rho}(z) \in \Omega\}, \tag{2.5}$$

computed to some $p$-adic precision, is our approximation of $X(\mathbb{Q})$.

The main novelty compared to [**BD18**, **Bia20**] is that, by keeping track of logarithmic singularities, we are able to work with a simpler function $\tilde{\rho}$: see Remark 2.5 below.

Let us now introduce what we need to define $\tilde{\rho}$ and $\Omega$. For now, we may assume more generally that $p$ is an odd prime. Further conditions on $p$ will be introduced only when needed.

First, we let $\log\colon \mathbb{Z}_p^\times \to \mathbb{Q}_p$ be the $p$-adic logarithm. It is possible to extend log to a function $\mathbb{Q}_p^\times \to \mathbb{Q}_p$ by choosing a value for $\log(p)$. It is customary (and natural in our situation [**BBBM21**, Remark 2.1]) to choose the Iwasawa branch, namely the one for which $\log(p) = 0$. Some of the summands of $\tilde{\rho}$ depend on this choice, so we fix this choice of branch. Note, however, that overall our $\tilde{\rho}$ will be branch-independent.

Next, we consider the $p$-adic logarithm on an elliptic curve (we will eventually want to apply this to $E_1$ and $E_2$). Let $E$ be an elliptic curve over $\mathbb{Q}_p$ given by the Weierstrass equation

$$E\colon y^2 = x^3 + A_2x^2 + A_4x + A_6, \qquad A_i \in \mathbb{Z}_p,$$

with point at infinity $\infty \in E(\mathbb{Q}_p)$. The $p$-adic logarithm $\operatorname{Log}\colon E(\mathbb{Q}_p) \to \mathbb{Q}_p$ is the abelian group homomorphism defined as follows. For $P \in E(\mathbb{Q}_p)$, we let

$$\operatorname{Log}(P) = \int_\infty^P \omega, \qquad \text{where } \omega = \frac{dx}{2y},$$

and the integral is first defined by formal anti-differentiation in the formal group and then extended to $E(\mathbb{Q}_p)$ by insisting that the resulting function be a homomorphism. The map Log induces a homomorphism $E(\mathbb{Q}_p) \to H^0(E_{\mathbb{Q}_p}, \Omega^1)^\vee$, which is

the $p$-adic Lie group logarithm [Bou98, III, §7.6]. By [Col85b, Theorem 2.8], if $E$ has good reduction, Log coincides with the Coleman integral of $\omega$ between $\infty$ and $P$. We will not use this, but we will use that if $P_1, P_2 \in E(\mathbb{Q}_p)$ reduce to the same point modulo $p$, then

$$\mathrm{Log}(P_1) - \mathrm{Log}(P_2) = \int_{P_2}^{P_1} \omega,$$

where the latter integral can also be computed by formal anti-differentiation of a local expansion of $\omega$. Since $\omega$ is holomorphic, Log is locally analytic, i.e. it can be expressed locally by a convergent power series (see §3.3 for more details). Moreover, Log vanishes at $P \in E(\mathbb{Q}_p)$ if and only if $P \in E(\mathbb{Q}_p)_{\mathrm{tors}}$ (see e.g. [Sil09, IV, Theorem 6.4 (b)], or, more generally, [Col85b, Proposition 3.1]). In summary, $\mathrm{Log}\colon E(\mathbb{Q}_p) \to \mathbb{Q}_p$ is a locally analytic group homomorphism, whose kernel is $E(\mathbb{Q}_p)_{\mathrm{tors}}$.

Finally, the most technical ingredient that we need is the theory of $p$-adic heights on elliptic curves. The appearance of $p$-adic heights in the definition of $\tilde{\rho}$ partly justifies the adjective "quadratic" in the name of the method. Assume now that our elliptic curve is defined over $\mathbb{Q}$:

$$E\colon y^2 = x^3 + A_2x^2 + A_4x + A_6, \qquad A_i \in \mathbb{Z}$$

and has good reduction at $p$. Fix a constant $c \in \mathbb{Q}_p$, or, equivalently, a differential $\eta$ of the form $\eta = (x+c)\frac{dx}{2y}$. Note that the class of $\eta$ spans a one-dimensional subspace of $H^1_{\mathrm{dR}}(E/\mathbb{Q}_p)$ complementary to the space of holomorphic forms, and conversely every such subspace is spanned by the class of a differential of that form.

There are several theories of $p$-adic heights in the literature, although many comparison results are now known. Here we use the same height as in [Bia20]. This is essentially the one of Mazur–Stein–Tate [MST06] (at least when the reduction is ordinary and we pick the above subspace to be the unit root eigenspace of Frobenius, as we will do in Section 3), but we further consider its decomposition into a sum of $p$-adic local Néron functions at every prime $q$

$$\lambda_q\colon E(\mathbb{Q}_q) \setminus \{\infty\} \to \mathbb{Q}_p$$

as in [Bia20, §2A, 4A]. At the primes different from our working prime $p$, these are obtained from real-valued Néron functions with respect to the divisor $2(\infty)$ [Sil94, Chapter VI] by replacing the real logarithm with the $p$-adic one, and therefore satisfy similar properties. At the prime $p$, the local height $\lambda_p$ depends on the choice of $c$; in the formal group of $E$ at $p$, it also depends on the branch of the $p$-adic logarithm.

The properties of these local height functions that we need for the main theorem are listed in Propositions 2.1 and 2.2, and more details on $\lambda_p$ are also provided in the precision analysis (§3.4). Roughly, the local function $\lambda_q$ is well-behaved on the subset of $E(\mathbb{Q}_q)$ consisting of points with coordinates in $\mathbb{Z}_q$, where by "well-behaved" we mean that it has finite image if $q \neq p$ and is locally analytic if $q = p$. In the subset of $E(\mathbb{Q}_q)$ consisting of points reducing to $\infty$, the function $\lambda_q$ has a logarithmic term if $q = p$ and takes infinitely many values if $q \neq p$. When we consider the problem of computing $X(\mathbb{Q})$, we are able to control this unboundedness by using both maps $\varphi_1$ and $\varphi_2$ defined in (2.4) (see Theorem 2.4 (b)).

Proposition 2.1.

(a) *The local Néron function $\lambda_p$ is locally analytic away from the residue disc of the point at infinity.*
(b) *Let $t = -\frac{x}{y}$. Then, the expansion of $\lambda_p$ in the disc of $\infty$ in terms of $t$ is of the form $-2\log(t) + O(t)$.*

PROOF. See [Bia20] and §3.4. □

PROPOSITION 2.2. *Let $q \neq p$.*

(a) *If $P \in E(\mathbb{Q}_q)$ reduces to a non-singular point modulo $q$, then*
$$\lambda_q(P) = \log(\max\{1, |x(P)|_q\}).$$
(b) *Let $W_q^E$ be the set of values attained by $\lambda_q$ on points in $E(\mathbb{Q}_q)$ of the form $(x, y)$ with $x, y \in \mathbb{Z}_q$. Then $W_q^E$ is finite, explicitly computable, and $\{0\}$ for all but finitely many $q$ (in particular, $W_q^E \subseteq \{0\}$ at all primes of good reduction for the given model for $E$).*

PROOF. For part (a), see [Bia20, Lemma 2.1]. For part (b), see [Bia20, Lemma 6.4], which as stated seems to be specific to $E_i$, but holds more generally. It provides an explicit description of $W_q^E$. □

For a global point $P \in E(\mathbb{Q})$, the global $p$-adic height is then

$$h_p(P) = \begin{cases} \sum_q \lambda_q(P) & \text{if } P \neq \infty, \\ 0 & \text{otherwise.} \end{cases} \tag{2.6}$$

By Proposition 2.2, this is well-defined, as all but finitely many of the $\lambda_q(P)$ are equal to 0, for a given $P$. The crucial property satisfied by $h_p$ that we need is the following:

$$h_p(mP) = m^2 h_p(P), \qquad \text{for all } m \in \mathbb{Z}, P \in E(\mathbb{Q}). \tag{2.7}$$

We are now ready to introduce the quadratic Chabauty function $\tilde{\rho}$ mentioned above, and the set $\Omega$. See Remark 2.5 for an explanation of how this differs from the explicit quadratic Chabauty function used in [BD18, Bia20] (and in the generalisation to number fields of [BBBM21]).

For a prime $q$, let
$$Z_q = X(\mathbb{Q}_q) \setminus \{P : x(P) \in \{0, \infty\}\}.$$

REMARK 2.3. We explain the notation in Part (c) of the following theorem. The finite sets $W_q^{E_i} \subset \mathbb{Q}_p$ are defined in Proposition 2.2. Given $A, B \subset \mathbb{Q}_p$ and $a \in \mathbb{Q}_p$, we write:
$$A + B = \{a + b : a \in A, b \in B\}, \qquad -A = \{-a : a \in A\}, \qquad a + B = \{a\} + B.$$

THEOREM 2.4. *Suppose that each of $E_1$ and $E_2$ has rank 1 over $\mathbb{Q}$, and let $p$ be a prime of good reduction for the equation (2.1) for $X$. For each $i \in \{1, 2\}$, fix a choice of subspace of $H^1_{\mathrm{dR}}(E_i/\mathbb{Q}_p)$ complementary to the space of holomorphic forms, and consider the corresponding global height $h_p$ and local Néron functions $\lambda_q$, at every $q$. Let $P_i \in E_i(\mathbb{Q})$ be a point of infinite order and let*
$$\alpha_i = \frac{h_p(P_i)}{\mathrm{Log}^2(P_i)}.$$
*Then:*

(a) *The constant $\alpha_i$ is independent of the choice of $P_i$.*

(b) *The function* $\rho\colon Z_p \to \mathbb{Q}_p$ *given by*

$$\rho(z) = \lambda_p(\varphi_1(z)) - \lambda_p(\varphi_2(z)) - 2\log(x(z)) - \alpha_1 \operatorname{Log}^2(\varphi_1(z)) + \alpha_2 \operatorname{Log}^2(\varphi_2(z))$$

*can be continued to a locally analytic function* $\tilde{\rho}\colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$.

(c) *For a prime* $q \neq p$, *let*

$$\Omega_q = (-W_q^{E_1} + W_q^{E_2} + \{-n\log q : -\operatorname{ord}_q(a_6) \leq n \leq \operatorname{ord}_q(a_0) \text{ and } n \equiv 0 \bmod 2\}) \cup (\log|a_0|_q - W_q^{E_1}) \cup (-\log|a_6|_q + W_q^{E_2}).$$

*and set*

$$\Omega = \left\{ \sum_{q \text{ bad}} w_q : w_q \in \Omega_q \right\},$$

*where the sum runs over all primes at which* $X$ *has bad reduction. Then* $\Omega$ *is finite and*

$$\tilde{\rho}(X(\mathbb{Q})) \subseteq \Omega.$$

Remark 2.5. By Proposition 2.1 (b), $\lambda_p(\varphi_1(z))$ has a logarithmic term around points at infinity, $\lambda_p(\varphi_2(z))$ has a logarithmic term around points with zero $x$-coordinate. The term $\log(x(z))$ also has a logarithmic term around each of these points. To make up for this, in [**BD18**, Corollary 8.1] and [**Bia20**, Proposition 6.5] one considered two different affine patches covering $X(\mathbb{Q}_p)$, and correspondingly applied suitable translations on the elliptic curves to move away from these problematic discs. What we propose to do here instead is to discard the logarithmic terms at once, since these overall cancel out.

Moreover, unlike in [**BD18**, Corollary 8.1] and [**Bia20**, Proposition 6.5], we do not assume that $a_6 = 1$. Similarly to [**Bia20**], we give here an elementary proof of the resulting quadratic Chabauty criterion, which does not require any $p$-adic Hodge theory. As a result, we obtain the explicit description of $\Omega$ provided in the theorem statement. Using results in [**BD18**], a smaller $\Omega$ may sometimes be chosen if there are some primes $q$ at which $X$ has bad but potentially good reduction: see Proposion 2.6 below.

Proof of Theorem 2.4.

(a) First note that $\alpha_i$ is well-defined since Log vanishes on torsion points only. The independence of $\alpha_i$ on the choice of $P_i$ is a standard argument in quadratic Chabauty methods. Namely, first note that since Log is a homomorphism, its square satisfies

$$\operatorname{Log}^2(mP) = m^2 \operatorname{Log}^2(P) \qquad \text{for all } m \in \mathbb{Z} \quad \text{and} \quad P \in E(\mathbb{Q}).$$

Since $\operatorname{Log}^2$ is also non-degenerate and $\operatorname{rank}(E_i(\mathbb{Q})) = 1$, any other function $E(\mathbb{Q}) \to \mathbb{Q}_p$ that transforms quadratically with respect to multiplication by $m$ on the elliptic curve must be a scalar multiple of $\operatorname{Log}^2$. This is in particular the case for $h_p$, in view of (2.7).

(b) Each term in $\rho$ is locally analytic, with the following exceptions: the function $\lambda_p(\varphi_1(z))$ has a logarithmic term in residue discs of points with $x(z) = \infty$, the function $\lambda_p(\varphi_2(z))$ has a logarithmic term in residue discs of points with $x(z) = 0$, and $\log(x(z))$ has a logarithmic term in residue discs of points with $x(z) \in \{0, \infty\}$. Using Proposition 2.1 (b), we see that, overall, the logarithmic terms add up to 0. For more details, see the proof of part (c) or Section 3.

(c) First note that $\Omega$ is finite, since $\Omega_q$ is finite and there are finitely many primes of bad reduction for $X$. Also note that

$$\Omega \supseteq \Omega' := \left\{ \sum_{q \neq p} w_q : w_q \in \Omega_q \right\},$$

since $\Omega_q \subseteq \{0\}$ if $q$ is a prime of good reduction (by Proposition 2.2 (b), the fact that the primes dividing $a_0$ or $a_6$ are of bad reduction for the given equation for $X$, and that the primes of good reduction for $X$ are of good reduction for the equations (2.2) and (2.3) as well). Therefore, it suffices to show that $\tilde{\rho}(X(\mathbb{Q})) \subseteq \Omega'$.

Let us first assume that $z \in X(\mathbb{Q}) \cap Z_p$. Then, by (2.6) and part (a),

$$\tilde{\rho}(z) = \rho(z) = \sum_{q \neq p} \left( -\lambda_q(\varphi_1(z)) + \lambda_q(\varphi_2(z)) + 2 \log |x(z)|_q \right).$$

For $z_q \in Z_q$, define

$$w_q(z_q) = -\lambda_q(\varphi_1(z_q)) + \lambda_q(\varphi_2(z_q)) + 2 \log |x(z_q)|_q.$$

Thus, for $z$ as above, we have

$$\rho(z) \in \Omega'' := \left\{ \sum_{q \neq p} w_q(z_q) : (z_q) \in \prod_{q \neq p} Z_q \right\}.$$

The following case distinction (which uses Proposition 2.2) shows that $\Omega'' \subseteq \Omega'$:

(1) If $-\operatorname{ord}_q(a_6) \leq 2 \operatorname{ord}_q(x(z_q)) \leq \operatorname{ord}_q(a_0)$, both $\varphi_1(z_q)$ and $\varphi_2(z_q)$ are integral and

$$w_q(z_q) \in -W_q^{E_1} + W_q^{E_2} + \{-n \log q : -\operatorname{ord}_q(a_6) \leq n \leq \operatorname{ord}_q(a_0) \text{ and } n \equiv 0 \bmod 2\}.$$

(2) If $2 \operatorname{ord}_q(x(z_q)) > \operatorname{ord}_q(a_0)$, then $\varphi_1(z_q)$ is integral, $\varphi_2(z_q)$ is not. We have

$$w_q(z_q) \in -W_q^{E_1} + \log |a_0 x(z_q)^{-2}|_q + 2 \log |x(z_q)|_q = -W_q^{E_1} + \log |a_0|_q.$$

(3) If $2 \operatorname{ord}_q(x(z_q)) < -\operatorname{ord}_q(a_6)$, then $\varphi_2(z_q)$ is integral, while $\varphi_1(z_q)$ is not. We have

$$w_q(z_q) \in W_q^{E_2} - \log |a_6 x(z_q)^2|_q + 2 \log |x(z_q)|_q = -\log |a_6|_q + W_q^{E_2}.$$

Finally we need to compute $\tilde{\rho}(z)$ for $z \in X(\mathbb{Q})$, $x(z) \in \{0, \infty\}$ (if such a point exists).

If $z \in X(\mathbb{Q})$ with $x(z) = 0$, then

$$\lambda_p(\varphi_1(z)) - \alpha_1 \operatorname{Log}^2(\varphi_1(z)) + \alpha_2 \operatorname{Log}^2(\varphi_2(z)) = -\sum_{q \neq p} \lambda_q(\varphi_1(z)) \in \left\{ \sum_{q \text{ bad}} w_q : w_q \in -W_q^{E_1} \right\},$$

since $\varphi_1(z)$ is an integral point and $\varphi_2(z)$ is the point at infinity. The remaining summands in $\rho$ are not individually well-defined at $z$ and we circumvent this issue as explained in part (b), by expanding around $z$. For instance, a parametrisation of the disc containing $z$ is given by

$$z(t) = (x(t), y(t)) = (t, \sqrt{a_0} + O(t)),$$

where $\sqrt{a_0}$ is a suitably chosen square root of $a_0$. Thus,

$$\varphi_2(x(t), y(t)) = (a_0 t^{-2}, a_0 \sqrt{a_0} t^{-3} + O(t^{-2}))$$

and so, by Proposition 2.1 (b),

$$-\lambda_p\circ\varphi_2(z(t))-2\log\circ x(z(t)) = 2\log\left(\frac{1}{\sqrt{a_0}}t+O(t^2)\right)-2\log(t) = -\log(a_0)+O(t).$$

We conclude that, if $a_0$ is a square in $\mathbb{Q}$, then

$$\tilde{\rho}(0,\sqrt{a_0}) = -\sum_{q\neq p}\lambda_q\circ\varphi_1(0,\sqrt{a_0})-\log(a_0) = \sum_{q\neq p}(-\lambda_q\circ\varphi_1(0,\sqrt{a_0})+\log|a_0|_q)\in\Omega.$$

Similarly, if $z=\infty^{\pm}\in X(\mathbb{Q})$, then $\varphi_2(z)$ is an integral point on $E_2$ and $\varphi_1(z)$ is the point at infinity on $E_1$. Thus,

$$-\lambda_p(\varphi_2(z))-\alpha_1\operatorname{Log}^2(\varphi_1(z))+\alpha_2\operatorname{Log}^2(\varphi_2(z)) = \sum_{q\neq p}\lambda_q(\varphi_2(z))\in\left\{\sum_{q\text{ bad}}w_q : w_q\in W_q^{E_2}\right\}.$$

As for the remaining term $\lambda_p(\varphi_1(z))-2\log(x(z))$, we have the following. A parametrisation around $z$ is given by

$$z(t)=(x(t),y(t))=(t^{-1},\sqrt{a_6}t^{-3}+O(t^{-2})).$$

Hence

$$\varphi_1(z(t))=(a_6t^{-2},a_6\sqrt{a_6}t^{-3}+O(t^{-2})).$$

By Proposition 2.1 (b),

$$\lambda_p\circ\varphi_1(z(t))-2\log\circ x(z(t)) = -2\log\left(-\frac{1}{\sqrt{a_6}}t+O(t^2)\right)-2\log(t^{-1}) = \log(a_6)+O(t).$$

So if $a_6$ is a square in $\mathbb{Q}$, then

$$\rho(\infty^{\pm}) = \sum_{q\neq p}(\lambda_q\circ\varphi_2(\infty^{\pm})-\log|a_6|_q)\in\Omega.$$

□

As in the proof of Theorem 2.4, for $z_q\in Z_q$, let

$$w_q(z_q) = -\lambda_q(\varphi_1(z_q))+\lambda_q(\varphi_2(z_q))+2\log|x(z_q)|_q.$$

Otherwise, if $z_q\in X(\mathbb{Q}_q)\setminus Z_q$, we set

$$w_q(z_q) = \begin{cases}-\lambda_q(\varphi_1(z_q))+\log|a_0|_q & \text{if } x(z_q)=0\\ \lambda_q(\varphi_2(z_q))-\log|a_6|_q & \text{if } x(z_q)=\infty.\end{cases}$$

PROPOSITION 2.6. *If $q$ is a prime of potential good reduction for $X$, then $w_q$ is constant on $X(\mathbb{Q}_q)$. Therefore, in Theorem 2.4 we may replace $\Omega_q$ with $\{w_q(z_q)\}$, where $z_q$ is any point in $X(\mathbb{Q}_q)$.*

PROOF. On $Z_q$, this follows from [BD18, Lemma 5.4] and a computation analogous to that of [BD18, Lemma 7.7] (where $X$ is assumed monic). We extend to $z_q\notin Z_q$ using continuity properties of local heights. □

As a first step for the determination of $X(\mathbb{Q})$, we would like to be able to compute the set

$$A=\{z\in X(\mathbb{Q}_p):\tilde{\rho}(z)\in\Omega\}\supseteq X(\mathbb{Q}).$$

In the next section we explain how to do so up to some finite $p$-adic precision.

## 3. Precision analysis

**3.1. Preliminaries.** Let $p$ be a prime of good reduction for the model of $X$ given by $y^2 = F(x) = a_6x^6 + a_4x^4 + a_2x^2 + a_0$, and hence for the given models for $E_1$ and $E_2$. In particular, $p \nmid a_0a_6$.

In Theorem 2.4, we considered the locally analytic function $\tilde{\rho}\colon X(\mathbb{Q}_p) \to \mathbb{Q}_p$ obtained by extending $\rho\colon Z_p \to \mathbb{Q}_p$ defined by

$$\rho(z) = \lambda_p(\varphi_1(z)) - \lambda_p(\varphi_2(z)) - 2\log(x(z)) - \alpha_1 \operatorname{Log}^2(\varphi_1(z)) + \alpha_2 \operatorname{Log}^2(\varphi_2(z)). \tag{3.1}$$

Since $\tilde{\rho}$ is locally analytic, it can be expanded in each residue disc $D$ of $X(\mathbb{Q}_p)$ as a power series in $\mathbb{Q}_p[[t]]$, where $t$ is a local coordinate at a fixed $z \in D$ (that is, $t$ is a uniformiser at $z$ that reduces to a uniformiser for $\overline{z} \in X(\mathbb{F}_p)$). Our goal here is to find lower bounds for the $p$-adic valuation of the coefficients of these series, which will allow us to deduce information about the solutions to $\tilde{\rho}(z) - w$, for $w \in \Omega$, in the disc $D$.

For a similar precision analysis in the simpler setting of the classical method of Chabauty and Coleman, see also [**BBCF+19**, Section 3].

Given a residue disc $D$ in $X(\mathbb{Q}_p)$, there are two choices to make. First, we need to pick a point $z \in D$ and, secondly, we need to pick a local coordinate at $z$. Let $\overline{z} \in X(\mathbb{F}_p)$ be the image of $D$ under reduction.

We proceed as follows:

(i) if $\overline{z}$ is affine with $y(\overline{z}) \neq 0$, we take $z \in X(\mathbb{Q}_p)$ to be the unique point satisfying $x(z) \in \mathbb{Z}$, $0 \leq x(z) \leq p-1$, $\overline{x(z)} = x(\overline{z})$ and $\overline{y(z)} = y(\overline{z})$. As for the local coordinate, we take $t = x - x(z)$. Note that then $y(t) \in \mathbb{Z}_p[[t]]$ is the unique solution to $y(t)^2 = F(x(t))$ such that $y(0) = y(z)$.

(ii) if $\overline{z}$ is Weierstrass (i.e. $y(\overline{z}) = 0$), we take $z \in X(\mathbb{Q}_p)$ to be the unique Weierstrass point in the disc. As for the local coordinate, choose $t = y$. Then $x(t) \in \mathbb{Z}_p[[t]]$ is the unique solution to $F(x(t)) = y(t)^2$ such that $x(0) = x(z)$.

(iii) if $\overline{z}$ is a point at infinity, we take $z \in X(\mathbb{Q}_p)$ to be the unique point at infinity in the disc. For the local coordinate, take $t = x^{-1}$. Then $y(t) = \sqrt{a_6}t^{-3} + O(t^{-2})$, for a suitable choice of $\sqrt{a_6}$.

Remark 3.1. The existence of such a point $z \in X(\mathbb{Q}_p)$ and such a parametrisation in (i) – (iii) is guaranteed by the good reduction assumption and by Hensel's lemma.

We analyse each term in (3.1) separately and then draw conclusions at the end. In fact, for the terms that involve images of $z$ under $\varphi_1$ or $\varphi_2$ (all of them, except for $\log(x(z))$), as a preliminary step we ignore that these come from points on $X$ and analyse the corresponding terms on a generic elliptic curve. Note that, as we already saw in the proof of Theorem 2.4, in the disc of a point at infinity or a point with $x$-coordinate reducing to 0 modulo $p$, not every term is individually expressible as a power series.

Recall that log denotes our chosen branch of the $p$-adic logarithm. We will write $\log_p$ for the real logarithm with respect to base $p$.

We start with an auxiliary lemma.

Lemma 3.2. *Let* $f(T) = \sum_{n=0}^{\infty} B_nT^n \in \mathbb{Q}_p[[T]]$ *with*

$$\operatorname{ord}_p(B_n) \geq -\operatorname{ord}_p(n) + \alpha(n) \qquad \text{for all } n \geq 1,$$

*where $\alpha(n)$ is a (not necessarily strictly) decreasing function of $n$. Let $g(t) = \sum_{i=1}^{\infty} b_i t^i$ for some $b_i \in \mathbb{Z}_p$. Then*

$$f(g(t)) = B_0 + \sum_{n=1}^{\infty} C_n t^n,$$

*with* $\mathrm{ord}_p(C_n) \geq -\mathrm{ord}_p(n) + \alpha(n)$ *for all* $n \geq 1$.

Proof. For $n \geq 1$, we have

$$\begin{aligned} C_n &= \sum_{m=1}^{n} B_m \cdot \left( \text{coefficient of } t^n \text{ in } \left( \sum_{i=1}^{n} b_i t^i \right)^m \right) \\ &= \sum_{m=1}^{n} B_m \cdot \left( \text{coefficient of } t^n \text{ in } \left( \sum_{i_1+\cdots+i_n=m} \binom{m}{i_1, \ldots, i_n} \prod_{k=1}^{n} (b_k t^k)^{i_k} \right) \right). \end{aligned}$$

Thus,

$$\mathrm{ord}_p(C_n) \geq \min \left\{ \mathrm{ord}_p \binom{m}{i_1, \ldots, i_n} + \mathrm{ord}_p(B_m) \right\}.$$

where the minimum is taken over all $m \leq n$ and $i_1, \ldots, i_n \geq 0$ satisfying $\sum_{k=1}^{n} i_k = m$ and $\sum_{k=1}^{n} k i_k = n$.

For such $i_1, \ldots, i_n$, there must exist $k \in \{1, \ldots, n\}$ for which $\mathrm{ord}_p(i_k) \leq \mathrm{ord}_p(n)$. Then we have

$$\binom{m}{i_1, \ldots, i_n} = \frac{m}{i_k} \binom{m-1}{i_1, \ldots, i_{k-1}, i_k - 1, i_{k+1}, \ldots, i_n}.$$

Therefore,

$$\begin{aligned} \mathrm{ord}_p(C_n) &\geq \min_{m \leq n} \{ \mathrm{ord}_p(m) - \mathrm{ord}_p(n) + \mathrm{ord}_p(B_m) \} \\ &\geq \min_{m \leq n} \{ -\mathrm{ord}_p(n) + \alpha(m) \} \geq -\mathrm{ord}_p(n) + \alpha(n), \end{aligned}$$

since $\alpha$ is a decreasing function. □

Remark 3.3. In the special case where $f(T) = \log(1+T)$ (so $\alpha(n) = 0$ for all $n$), one could recover the same precision estimate in a more straightforward way:

$$f(g(t)) = \log(1 + g(t)) = \int \frac{g'(t)}{1 + g(t)} dt.$$

### 3.2. Precision of $\log(x(t))$-term.

Lemma 3.4. *Let $D$ be a residue disc of $X(\mathbb{Q}_p)$ and choose $z \in D$ and a local coordinate at $z$ as in §3.1.*

*(1) If $z \in \{\infty^{\pm}\}$, then $\log(x(t)) = -\log(t)$;*
*(2) If $x(z) = 0$, then $\log(x(t)) = \log(t)$;*
*(3) Otherwise,*

$$\log(x(t)) = \sum_{n=0}^{\infty} C_n t^n \in \mathbb{Q}_p[[t]],$$

*with* $\mathrm{ord}_p(C_0) \geq 1$ *and* $\mathrm{ord}_p(C_n) \geq -\mathrm{ord}_p(n)$ *for all* $n \geq 1$.

PROOF. The first two cases are trivial. For the remaining case, we have

$$x(t) = \alpha\left(1 + \sum_{i=1}^{\infty} b_i t^i\right), \qquad \text{for some } b_i \in \mathbb{Z}_p, \alpha \in \mathbb{Z}_p^\times.$$

Therefore,

$$\log(x(t)) = \log(\alpha) + \log\left(1 + \sum_{i=1}^{\infty} b_i t^i\right) = \log(\alpha) + O(t),$$

which shows the claim on the constant term. In order to bound the valuation of the other terms, we apply Lemma 3.2 to $f(T) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} T^n$ and $g(t) = \sum_{i=1}^{\infty} b_i t^i$. □

**3.3. Precision of Log-terms.** Let $E$ be an elliptic curve over $\mathbb{Q}_p$ given by the Weierstrass equation

$$E : y^2 = x^3 + A_2 x^2 + A_4 x + A_6, \qquad A_i \in \mathbb{Z}_p.$$

Recall that, for $P \in E(\mathbb{Q}_p)$, we have

$$\mathrm{Log}(P) = \int_{\infty}^{P} \omega, \qquad \text{where } \omega = \frac{dx}{2y},$$

and the integral is first defined by formal anti-differentiation in the formal group of $E$ at $p$ and then extended to $E(\mathbb{Q}_p)$ by linearity.

In order to obtain the expansion of Log in a local coordinate $T$ for a residue disc, we may break up the path of integration: given $P_0 \in E(\mathbb{Q}_p)$ reducing to $P$ modulo $p$ and with $T(P_0) = 0$, we have

$$\mathrm{Log}(P) = \mathrm{Log}(P_0) + \int_{P_0}^{P} \omega,$$

where the latter integral can be computed by expanding $\omega$ as a power series in $T$, formally integrating and evaluating at $T(P)$.

LEMMA 3.5. *Let $T$ be a local coordinate for an arbitrary point $P_0$ in a residue disc of $E(\mathbb{Q}_p)$. Then*

$$\mathrm{Log}^2(P(T)) = \sum_{n=0}^{\infty} C_n T^n,$$

*where* $\mathrm{ord}_p(C_0), \mathrm{ord}_p(C_1) \geq 0$ *and* $\mathrm{ord}_p(C_n) \geq -\lfloor \log_p(n-1) \rfloor - \mathrm{ord}_p(n)$ *for* $n \geq 2$. *Moreover, if* $p \nmid \#E(\mathbb{F}_p)$, *then* $\mathrm{ord}_p(C_0) \geq 2$ *and* $\mathrm{ord}_p(C_1) \geq 1$.

PROOF. We are interested in finding lower bounds for the valuation of the coefficients of

$$\mathrm{Log}^2(P(T)) = \mathrm{Log}^2(P_0) + 2\,\mathrm{Log}(P_0) \int_{P_0}^{P(T)} \omega(T) + \left(\int_{P_0}^{P(T)} \omega(T)\right)^2.$$

Since $\omega$ is holomorphic and non-vanishing and $T$ reduces to a uniformiser modulo $p$, we have

$$\omega(T) = f(T)dT \qquad \text{for some } f(T) \in \mathbb{Z}_p[[T]]^\times.$$

Therefore,

$$\int_{P_0}^{P(T)} \omega(T) = c_0 T + \frac{c_1}{2} T^2 + \frac{c_2}{3} T^3 + \cdots, \qquad \text{for some} \quad c_i \in \mathbb{Z}_p, c_0 \in \mathbb{Z}_p^\times. \tag{3.2}$$

Let $m > 0$ be the smallest integer such that $mP_0$ belongs to the disc at infinity. Since $m$ is a divisor of $\#E(\mathbb{F}_p)$, by the Hasse bound [Sil09, V, Theorem 1.1] we know that $0 \leq \mathrm{ord}_p(m) \leq 1$. We have

$$\mathrm{Log}(P_0) = \frac{\mathrm{Log}(mP_0)}{m}.$$

Now, by (3.2) with $P_0 = \infty$ we see that $\mathrm{ord}_p(\mathrm{Log}(mP_0)) \geq 1$ and hence, by the above considerations on the valuation of $m$, $\mathrm{ord}_p(\mathrm{Log}(P_0)) \geq 1 - \mathrm{ord}_p(\#E(\mathbb{F}_p)) \geq 0$. The statements about the constant and linear coefficient follow.

By (3.2), the $n$-th coefficient in the $T$-expansion of the integral of $\omega(T)$ has valuation at least $-\mathrm{ord}_p(n)$. As for

$$\left(\int_{P_0}^{P(T)} \omega(T)\right)^2 = \left(c_0 T + \frac{c_1}{2}T^2 + \frac{c_2}{3}T^3 + \cdots\right)^2 = \sum_{n=2}^{\infty} \alpha_n T^n$$

we have

$$\mathrm{ord}_p(\alpha_n) \geq \min_{\substack{i+j=n \\ i,j\geq 1}} \mathrm{ord}_p\left(\frac{1}{ij}\right) \geq -\lfloor \log_p(n-1) \rfloor - \mathrm{ord}_p(n),$$

since $\mathrm{ord}_p(i), \mathrm{ord}_p(j) \leq \lfloor \log_p(n-1) \rfloor$, but also $\min\{\mathrm{ord}_p(i), \mathrm{ord}_p(j)\} \leq \mathrm{ord}_p(n)$. □

**3.4. Precision of $\lambda_p$-terms.** Let $E$ be as in §3.3. We are ultimately interested in applying the considerations of this subsection to the case where $E$ is $E_1$ or $E_2$. To simplify our task (or, in fact, to obtain better bounds; see below), we make the following

Assumption 1. The prime $p$ is of ordinary reduction for $E_1$ and $E_2$.

Thus we assume here that $p$ is a prime of good ordinary reduction for $E$, so we can and shall work with the canonical local height at $p$. This is defined in terms of the canonical $p$-adic sigma function[1]

$$\sigma_p(T) = T + O(T^2) \in \mathbb{Z}_p[[T]]$$

of Mazur–Tate [MT91], as follows. We view $\sigma_p$ as a function on points of $E(\mathbb{Q}_p)$ in the formal group $E_f$ by setting

$$\sigma_p(P) := \sigma_p\left(-\frac{x(P)}{y(P)}\right), \qquad \text{for } P \in E_f(\mathbb{Q}_p).$$

If $P \in E_f(\mathbb{Q}_p) \setminus \{O\}$, its canonical local height at $p$ is then given by

$$\lambda_p(P) = -2\log(\sigma_p(P)). \tag{3.3}$$

Note that, in this case, $\lambda_p(P)$ depends on the choice of a branch of the $p$-adic logarithm and general theory on heights suggests that we should choose the branch of the logarithm which is trivial at $p$ (cf. [BBBM21, Remark 2.1]). In practice, for our applications to computing $\tilde{\rho}$ this will not matter, in view of the global cancellation of the logarithmic terms.

[1] If we do not assume that $p$ is of ordinary reduction for $E$, we can replace the Mazur–Tate $p$-adic sigma function with some other $p$-adic sigma function $\sigma_p'(T) = T + O(T^2) \in \mathbb{Q}_p[[T]]$; for example, Bernardi's [Ber81]. The precision bounds then need to be modified appropriately, since $\sigma_p'(T)$ does not, in general, have $p$-adically integral coefficients.

26 Jun 2023 23:11:48 PDT
230105-Padurariu Version 2 - Submitted to LuCaNT

If $P$ is non-torsion and does not reduce to the point at infinity, then let $m$ be a positive integer such that $mP \in E_f(\mathbb{Q}_p)$. If we choose the smallest such $m$, then $m$ divides $\#E(\mathbb{F}_p)$. We define

$$\lambda_p(P) = -\frac{2}{m^2} \log\left(\frac{\sigma_p(mP)}{\phi_m(P)}\right), \tag{3.4}$$

where $\phi_m \in \mathbb{Z}[A_2, A_4, A_6][x, y]$ is the $m$-th division polynomial [Sil09, Exercise 3.7]. This is characterised uniquely up to multiplication by $\pm 1$ by the following properties:

- $\mathrm{div}(\phi_m) = \sum_{Q \in E[m]} (Q) - m^2(\infty)$;
- $\phi_m^2$ is a polynomial in $x$ only with leading term $m^2 x^{m^2-1}$ and coefficients in $\mathbb{Z}[A_2, A_4, A_6]$.

The value $\lambda_p(P)$ for $P \notin E_f(\mathbb{Q}_p)$ as above is independent of the branch of the $p$-adic logarithm and the definition can be extended to torsion points by continuity.

We want to study $\lambda_p$ as a function on a residue disc. By (3.3), if $T$ is a local coordinate at the point at infinity, $\lambda_p$ can be expressed in terms of $T$ as $-2\log(f(T))$ where $f(T) \in T\mathbb{Z}_p[[T]]^\times$. Thus, the analysis can be obtained by applying Lemma 3.2 and is similar to §3.2. We postpone it until we also understand the argument of the logarithm in (3.4) as a power series.

So let $P(T)$ be the parametrisation of a disc on an elliptic curve not reducing to the point at infinity modulo $p$ and let $m$ such that $mP(T)$ reduces to infinity for all $T \in p\mathbb{Z}_p$.

LEMMA 3.6. *With the above assumptions, we have*

$$\frac{\sigma_p(mP(T))}{\phi_m(P(T))} = c_0 + O(T) \in \mathbb{Z}_p[[T]] \qquad \text{with } c_0 \in \mathbb{Z}_p^\times.$$

PROOF. Since $\phi_m(P(T)) \in \mathbb{Z}_p[[T]]$, by the $p$-adic Weierstrass preparation theorem we may factor it as

$$p^n F(T) u(T)$$

where $n$ is an integer, $u(T) \in \mathbb{Z}_p[[T]]^\times$ is a unit power series and $F(T)$ is a distinguished polynomial. In particular, the zeros in $\overline{\mathbb{Q}_p}$ of $F(T)$ all have positive valuation, and hence correspond to $m$-torsion points in the disc of $P(T)$ (since $P(T)$ converges on $|T|_p < 1$).

Now we turn our attention to $\sigma_p(mP(T))$. First note that $mP(T)$ may be viewed as a point of $E$ over $\mathrm{Frac}(\mathbb{Z}_p[[T]])$ (since $x(T), y(T) \in \mathbb{Z}_p[[T]]$). Thus, we may use the $p$-adic Weierstrass preparation theorem to study

$$\tau = -\frac{x(mP(T))}{y(mP(T))} \in \mathrm{Frac}(\mathbb{Z}_p[[T]]).$$

We would like to show that $\tau \in \mathbb{Z}_p[[T]]$ with constant term divisible by $p$. Since $\tau$ has no poles for $|T|_p < 1$, we must have $\tau \in \mathbb{Q} \cdot \mathbb{Z}_p[[T]]$. For every $|T_0|_p < 1$, we have $|\tau(T_0)|_p < 1$; hence picking $T_0$ with $|T_0|_p$ close enough to 1 shows that $\tau \in \mathbb{Z}_p[[T]]$. Indeed, write $\tau = \alpha g(T)$, where $\alpha = p^k$ and $g(T) = \sum_{i=0}^\infty c_i T^i \in \mathbb{Z}_p[[T]] \setminus p\mathbb{Z}_p[[T]]$. Let $r$ be minimal such that $\mathrm{ord}_p(c_r) = 0$. Then, for every $T_0$ with $|T_0|_p < 1$ and for every $i > r$

$$|c_i T_0^i|_p \leq |T_0^i|_p < |T_0^r|_p = |c_r T_0^r|_p.$$

Furthermore, if $|T_0|_p > |c_i|_p^{1/(r-i)}$ for all $i < r$, then for all $i < r$ we have

$$|c_i T_0^i|_p < |T_0|_p^r = |c_r T_0^r|_p;$$

hence, $|g(T_0)|_p = |T_0^r|_p$. If $k < 0$, we may pick $T_0$ that further satisfies $|T_0^r|_p > |\alpha^{-1}|_p$, which gives

$$|\tau(T_0)|_p = |\alpha T_0^r|_p > 1,$$

a contradiction. Finally, since $\tau(0) \in p\mathbb{Z}_p$, we have the claim on the constant term.

So $\sigma_p(mP(T)) \in \mathbb{Z}_p[[T]]$; it has simple zeros in the open unit disc precisely at the $m$-torsion points in the disc $P(T)$. Comparing with $\phi_m(P(T))$, we get that

$$\frac{\sigma_p(mP(T))}{\phi_m(P(T))} \in \mathbb{Q} \cdot \mathbb{Z}_p[[T]].$$

Moreover this quotient is non-vanishing on $|T|_p < 1$, hence in fact it is, up to multiplication by $p^k$ for some $k \in \mathbb{Z}$, a unit power series. This implies that at a given $T_0$ in the open unit disc, the valuation of the quotient is $-k$. But picking $T_0 \in p\mathbb{Z}_p$ such that $mP(T_0) \neq \infty$, we have that $\operatorname{ord}_p(\phi_m(P(T_0))) = \operatorname{ord}_p(d(mP(T_0))) = \operatorname{ord}_p(T(mP(T_0))) = \operatorname{ord}_p(\sigma(mP(T_0)))$, hence $k = 0$. Here $d$ denotes the square-root of the denominator of the $x$-coordinate and the first equality holds true because $p$ is a prime of good reduction (see e.g. [**Wut04**, Proposition 1]). □

COROLLARY 3.7. *Let $T$ be a local coordinate at a point $P \in E(\mathbb{Q}_p)$, which we assume either at infinity or not in the disc of infinity and let $m$ be the order of the reduction of $P$ modulo $p$. Then*

$$\lambda_p(P(T)) = -2\delta \log(T) + \sum_{n=0}^{\infty} C_n T^n,$$

*where $\delta = 1$ if $P$ is the point at infinity and 0 otherwise, and $\operatorname{ord}_p(C_0) \geq 1 - 2\operatorname{ord}_p(m)$, $\operatorname{ord}_p(C_n) \geq -\operatorname{ord}_p(n) - 2\operatorname{ord}_p(m)$ for $n \geq 1$.*

PROOF. In view of Lemma 3.6 and the considerations preceding it, the corollary follows by Lemma 3.2, similarly to the proof of Lemma 3.4. □

REMARK 3.8. While we found it convenient to work out precision estimates for $\lambda_p$ using multiplication-by-$m$ on $E/\operatorname{Frac}(\mathbb{Z}_p[[t]])$, we found it computationally more convenient to use the following formula for $\lambda_p(P(T))$. Let $E_2(E,\omega)$ be the value of the weight two Katz Eisenstein series [**Kat73**, **Kat76**] at the pair $(E,\omega)$ and let

$$c = \frac{4A_2 - E_2(E,\omega)}{12} \in \mathbb{Q}_p, \qquad \eta = (x+c)\frac{dx}{2y}.$$

Then, setting $P_0 = P(0)$, we have

$$\lambda_p(P(t)) = \lambda_p(P_0) + 2\int_{P_0}^{P(t)} \omega_0\eta + 2\int_{\infty}^{P_0} \eta \cdot \int_{P_0}^{P(t)} \omega. \tag{3.5}$$

The integrals involving $P(t)$ are all formal integrals; the remaining integral of $\eta$ is a Coleman integral of a differential of the second kind and can be computed using division polynomials (or the Coleman integration algorithm of [**BBK10**]); we omit details, but formula (3.5) can be derived from [**BBM16**, (4.1)] invoking suitable height comparison results.

If $p \geq 5$, we can compute $E_2(E,\omega)$ and $\lambda_p(P_0)$ using an algorithm of Harvey [**Har08**], which builds on one by Mazur–Stein–Tate [**MST06**] and is implemented

in `SageMath` [Sag22]. If $p = 3$, we use an algorithm of Balakrishnan [Bal16], available at [Bal].

**3.5. Precision of $\tilde{\rho}$.** We can now use the considerations of §§3.2, 3.3, 3.4 to deduce lower bounds for the $p$-adic valuation of the coefficients of the expansion of $\tilde{\rho}(z)$ in a residue disc.

LEMMA 3.9. *Let $z \in X(\mathbb{Q}_p)$ such that $\overline{z}$ is not a ramification point of $\varphi_i$ and let $t$ be a local coordinate at $z$. Let $T_i$ be a local coordinate for $\varphi_i(z)$. Then*

$$T_i(\varphi_i(z(t))) = t \cdot u(t) \qquad \text{for some} \quad u(t) \in \mathbb{Z}_p[[t]]^\times.$$

PROOF. Since $\varphi_i$ is unramified at $z$, we have that $\varphi_i^* T_i$ is a uniformiser for $z$. This applies to $X/\mathbb{Q}_p$, as well as $X/\mathbb{F}_p$, so $\varphi_i^* T_i$ is a local coordinate. □

LEMMA 3.10. *Let $z \in X(\mathbb{Q}_p)$ such that $\overline{z}$ is a ramification point for $\varphi_i$ and let $t$ be a local coordinate at $z$. Let $T_i$ be a local coordinate for $\varphi_i(z)$. Then*

$$T_i(\varphi_i(z(t))) = t^2 \cdot u(t) \qquad \text{for some} \quad u(t) \in \mathbb{Z}_p[[t]]^\times.$$

PROOF. The ramification index of any such point is 2. □

REMARK 3.11. The ramification points of $\varphi_1$ are those satisfying $x = 0$; the ramification points of $\varphi_2$ are the points at infinity.

PROPOSITION 3.12. *Let $t$ be a local coordinate at a point $z \in X(\mathbb{Q}_p)$ as in §3.1 and let*

$$\epsilon = \min\{\mathrm{ord}_p(\alpha_1), -2\,\mathrm{ord}_p(\#E_1(\mathbb{F}_p)), \mathrm{ord}_p(\alpha_2), -2\,\mathrm{ord}_p(\#E_2(\mathbb{F}_p))\}.$$

*Then, under Assumption 1 on ordinarity,*

$$\tilde{\rho}(z(t)) = \sum_{n=0}^{\infty} C_n t^n \in \mathbb{Q}_p[[t]]$$

*with $\mathrm{ord}_p(C_0), \mathrm{ord}_p(C_1) \geq \epsilon$ and, for all $n \geq 2$, $\mathrm{ord}_p(C_n) \geq -\lfloor \log_p(n-1) \rfloor - \mathrm{ord}_p(n) + \epsilon$. Moreover, if $p \nmid \#E_1(\mathbb{F}_p) \cdot \#E_2(\mathbb{F}_p)$, then $\mathrm{ord}_p(C_0) \geq 1 + \epsilon$.*

PROOF. This follows from Lemmas 3.4, 3.5, Corollary 3.7 and Lemmas 3.9, 3.10, in view of Lemma 3.2. □

Let $M \geq 2$ be an integer and let $\tilde{\rho}_M(t) \in \mathbb{Q}_p[t]$ be a polynomial of degree less than $M$ such that

$$\tilde{\rho}_M(t) - \tilde{\rho}(z(t)) = O(t^M).$$

LEMMA 3.13. *Let $N = M - \lfloor \log_p(M-1) \rfloor - \lfloor \log_p(M) \rfloor + \epsilon$. Then*

$$\tilde{\rho}_M(pt) - \tilde{\rho}(z(pt)) = O(p^N).$$

PROOF. Let $n \geq M$. By Proposition 3.12, the coefficient of the term of degree $n$ in $\tilde{\rho}(z(pt))$ has valuation bounded from below by

$$n - \lfloor \log_p(n-1) \rfloor - \mathrm{ord}_p(n) + \epsilon \geq n - \lfloor \log_p(n-1) \rfloor - \lfloor \log_p(n) \rfloor + \epsilon.$$

The right hand side of this inequality is (not necessarily strictly) increasing for $n$ an integer $\geq 2$. □

Let $w \in \Omega$. Let $k$ be the minimal valuation of a coefficient of $\tilde{\rho}_M(pt) - w$. If $k < N$, then $\tilde{\rho}_M(pt) - w$ is non-zero modulo $N$. If $p^{-k}(\tilde{\rho}_M(pt) - w)$ has a zero in $\mathbb{Z}/p^{N-k}\mathbb{Z}$ whose derivative is non-zero modulo $p^{\lceil (N-k)/2 \rceil}$, then by Hensel's lemma it lifts uniquely to a zero of $\tilde{\rho}(z(pt)) - w$ in $\mathbb{Z}_p$ (we use [Con, Theorem 8.2 (1)] to determine to which precision we know the lift).

Furthermore, any zero in $\mathbb{Z}_p$ of $\tilde{\rho}(z(pt))$ reduces modulo $p^{N-k}$ to a zero of $p^{-k}\tilde{\rho}_M(pt)$. When it comes to zeros not corresponding to known rational points, the uniqueness of the lifting is not so important. Indeed, suppose that we found a root modulo $p^{N'}$ that could or could not lift (perhaps not uniquely), and that we suspect does not correspond to a rational point of $X$. Then in the Mordell–Weil sieve step (§§4.2, 4.3) we will try to show that such a root cannot possibly correspond to a point in $X(\mathbb{Q})$.

On the other hand, it is important to show that the zeros corresponding to our known rational points are isolated, so that we can discard such roots at once before the Mordell–Weil sieve step. Because of the extra automorphisms $X$ possesses, we actually expect some of these to be non-simple.

PROPOSITION 3.14. *Let $z \in X(\mathbb{Q})$ such that $x(z) = 0$, or $y(z) = 0$, or $z$ is a point at infinity and let $t$ be the local coordinate at $z$ of §3.1. Let $w \in \Omega$ such that $\tilde{\rho}(z) = w$. Then*

$$\tilde{\rho}(z(t)) - w = t^2 f(t) \qquad \text{for some } f(t) \in \mathbb{Q}_p[[t]].$$

PROOF. The point $z$ is fixed by the hyperelliptic involution or one of the automorphisms $(x, y) \mapsto (-x, y)$ and $(x, y) \mapsto (-x, -y)$. Let $\theta$ be the automorphism fixing $z$. Then $\rho(\theta(z)) = \rho(z)$, since upon noticing that $\varphi_i \circ \theta$ is either the identity or multiplication by $-1$, we see that each of the terms making up $\tilde{\rho}(z)$ is invariant under $\theta$. Now, in view of our choice of $t$, we have $\theta^* t = -t$. Therefore,

$$\tilde{\rho}(z(t)) = \tilde{\rho}(z(-t)),$$

and hence $\tilde{\rho}(z(t))$ has trivial coefficient of $t^{2k+1}$ for all non-negative $k$. Finally since $\tilde{\rho}(0) = w$, the proposition follows. □

Our strategy is then the following:

(i) If $\tilde{\rho}_M(pt) - w = O(t^2)$, then we verify that we are in the situation of Proposition 3.14. We do this by checking that the coefficient of $t^2$ is non-zero, and that $t = 0$ corresponds to a point at infinity, or with vanishing $x$- or $y$-coordinate.

(ii) In the other cases, we check that the recovered roots can be lifted uniquely using Hensel's lemma.

(iii) We return an error if a root does not meet the conditions of (i) or (ii).

## 4. Computations

We now explain how we used the results of Sections 2 and 3 together with the Mordell–Weil sieve to prove Theorem 1.2, that is, to compute the rational points on a database $\Delta$ of genus 2 curves over $\mathbb{Q}$ that have points everywhere locally, are bielliptic and have a rank 2 Jacobian.

We describe three main steps in our implementation. First, we explain in §4.1 how we obtained the dataset $\Delta$, and how we computed, for each curve $X \in \Delta$, various inputs for the quadratic Chabauty and Mordell–Weil sieve computations.

For instance, we need to choose a set of primes with respect to which to apply the quadratic Chabauty technique described in the previous sections. For a given prime, we discussed in Section 3 the theoretical results needed for an implementation of the quadratic Chabauty method. Therefore, we only explain here (§4.2) how to turn the output of this computation into an input for a Mordell–Weil sieve. Finally in §4.3, we explain how to use the Mordell–Weil sieve, and, in particular, its `Magma` [**BCP97**] implementation available at [**BDM+**], to complete the determination of the rational points on $X$.

The remaining §4.4 and §4.5 concern some exceptional curves in our database.

**4.1. Step 1: The database and some preliminary computations.** All the computations of this step were performed in `Magma` [**BCP97**] (see [**BPa**]). Recall that our database contains 413 curves in total, 411 of which belong to the database [**BSS+16**], available on the LMFDB [**LMF22**]. To the present date, the LMFDB contains all 66,158 genus 2 curves over $\mathbb{Q}$ with absolute discriminant at most $10^6$ that have an integral model of the form

$$y^2 + (h_3x^3 + h_2x^2 + h_1x + h_0)y = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

with $h_i \in \{0, 1\}$, and $f_i$ satisfying at least one of the following conditions:

- $|f_i| \leq 90$;
- $|f_i| \leq 2(3.51)^{6-i}$;
- $|f_i| \leq (7.13)^{4-|i-3|}$;
- $\sum_{i=0}^{6} \lceil \log_{10}(|f_i| + 1) \rceil \leq 10$.

From these curves we extracted 411 curves as follows. First, we are interested in curves that are locally solvable, and we can filter the LMFDB search to return such curves only. Secondly, a genus 2 curve $X$ over $\mathbb{Q}$ is bielliptic (over $\mathbb{Q}$) if and only if the $\mathbb{Q}$-automorphism group of $X$ has a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Finally, if $X$ is bielliptic, there exist elliptic curves $E_1$ and $E_2$ such that the Jacobian $J$ of $X$ is (Richelot) isogenous to $E_1 \times E_2$ [**Ric36**, **Ric37**, **CF96**, **Smi05**]; therefore, the Mordell–Weil rank of $J$ is equal to the sum of the ranks $r_1$ and $r_2$ of $E_1$ and $E_2$. We use this to identify the curves with a rank 2 Jacobian.

If $r_1$ or $r_2$ is equal to zero, we may apply elementary methods to determine $X(\mathbb{Q})$. Therefore, we hereafter restrict our attention to the 354 curves $X \in \Delta$ for which $r_1 = r_2 = 1$. For each such $X$, we compute the following data.

*A "bielliptic" model.* The equation for $X$ as given in the LMFDB is of the form $y^2 + f_1(x)y = f_2(x)$, for some $f_1(x), f_2(x) \in \mathbb{Z}[x]$ of degrees at most 3 and 6, respectively. In order to apply Theorem 2.4, we need to find a *bielliptic* model of the form $y^2 = a_6x^6 + a_4x^4 + a_2x^2 + a_0 \in \mathbb{Z}[x]$, or, equivalently, models for $E_1$ and $E_2$ of the form

$$E_1 \colon y^2 = x^3 + a_4x^2 + a_2a_6x + a_0a_6^2,$$
$$E_2 \colon y^2 = x^3 + a_2x^2 + a_4a_0x + a_6a_0^2.$$

Equations for $E_1$ and $E_2$ of this form (though not necessarily integral) are computed internally by `Magma`'s function `RichelotIsogenousSurfaces`. We use this to compute an integral bielliptic model for $X$.

*A candidate list of rational points.* Let $X(\mathbb{Q})_{\text{known}}$ be the set of rational points of $X$ such that the naive height of the $x$-coordinate, with respect to the bielliptic model from above, is less than $10^4$. We compute $X(\mathbb{Q})_{\text{known}}$ using the `Magma`

function `RationalPoints`. The ultimate goal of our computation will be to prove that $X(\mathbb{Q}) = X(\mathbb{Q})_{\text{known}}$.

*Generators of $J(\mathbb{Q})$.* In order to apply Theorem 2.4, we only need to know a point of infinite order on each of $E_1$ and $E_2$. However, for the subsequent Mordell–Weil sieve step, we assume that we know generators for the full Mordell–Weil group $J(\mathbb{Q})$. The `Magma` function `MordellWeilGroupGenus2`, implemented by Stoll, successfully determined these for every curve. We denote by $B_1$ and $B_2$ generators for $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$.

*A set of primes for quadratic Chabauty.* In order to apply Theorem 2.4, we need to pick a prime $p$ of good reduction. In addition, in the precision estimates of §3.4, we assumed that each of $E_1$ and $E_2$ has ordinary reduction at $p$. In general, it is expected that Theorem 2.4 will not suffice by itself to determine $X(\mathbb{Q})$, since it will only return a $p$-adic approximation of a superset of $X(\mathbb{Q})$. The strategy that we will describe in detail in the next steps entails using the Mordell–Weil group $J(\mathbb{Q})$ and reduction maps to $J(\mathbb{F}_\ell)$, for various primes $\ell$, to refine the superset and prove that $X(\mathbb{Q}) = X(\mathbb{Q})_{\text{known}}$. This method is often more likely to succeed if the quadratic Chabauty computation is performed for more than one prime $p$. We therefore compute, for each curve, the three smallest primes $p_1, p_2, p_3$ of good ordinary reduction. See Remark 4.1 for possible improvements in the choice of primes.

**4.2. Step 2: Extra points in bielliptic quadratic Chabauty.** In the following discussion we assume that our curve has at least one known $\mathbb{Q}$-rational point $b$. While some modification of this would be applicable in the other case too, we decided to treat curves with no known rational points separately: see §4.4. Our code for this stage of the computation is written in `SageMath` [Sag22] and is available at [BPb].

We perform the bielliptic quadratic Chabauty algorithm on $X$ for the three primes $p_1, p_2, p_3$. Fix $i \in \{1, 2, 3\}$. Using the precision estimates of Section 3, we compute the set

$$A_i = \{z \in X(\mathbb{Q}_{p_i}) : \tilde{\rho}_i(z) \in \Omega_i\},$$

where $\tilde{\rho}_i(z)$ and $\Omega_i$ are the function and set from Theorem 2.4, respectively, for the prime $p_i$. By Theorem 2.4, the set $A_i$ contains $X(\mathbb{Q})$; it may or may not contain other points in $X(\mathbb{Q}_{p_i})$. Let $A_{\text{extra},i}$ be the set of $p_i$-adic points in $A_i$ which have not been recognised as points in $X(\mathbb{Q})_{\text{known}}$. The points in $A_{\text{extra},i}$ are only known modulo $p_i^{m_i}$, for some integer $m_i$ depending on our chosen working precision. If $A_{\text{extra},i} \neq \emptyset$, our strategy to *prove* that the points in $A_{\text{extra},i}$ are not reductions modulo $p_i^{m_i}$ of points in $X(\mathbb{Q})$ is to feed them into the Mordell–Weil sieve (described in §4.3), following the strategy outlined in [BBM17, Sections 5-7]. We describe here the preliminary step (which essentially amounts to applying Section 6 of *loc. cit.* to our setting).

Let $\iota$ be the Abel–Jacobi map on $X(\mathbb{Q})$ with respect to $b$:

$$\iota\colon X(\mathbb{Q}) \hookrightarrow J(\mathbb{Q}), \qquad P \mapsto [P - b].$$

Let $P_i \in A_{\text{extra},i}$ be one of our extra points and assume for the sake of contradiction that $P_i$ corresponds to a point $P \in X(\mathbb{Q})$. Then there exist integers $a_1, a_2 \in \mathbb{Z}$ and a torsion point $T \in J(\mathbb{Q})$ such that

$$\iota(P) = a_1 B_1 + a_2 B_2 + T. \tag{4.1}$$

We can compute $a_1, a_2$ modulo $p_i^{n_i}$, for some $n_i \leq m_i$, by noting that, for each $j \in \{1,2\}$, we have

$$\mathrm{Log}(\varphi_j(P)) - \mathrm{Log}(\varphi_j(b)) = a_1 \,\mathrm{Log}(\varphi_{j,*}(B_1)) + a_2 \,\mathrm{Log}(\varphi_{j,*}(B_2)).$$

Therefore, for every $P_i \in A_{\mathrm{extra},i}$, we obtain at most $\#J(\mathbb{Q})_{\mathrm{tors}}$ possibilities for the image of $\iota(P)$ in $J(\mathbb{Q})/p_i^{n_i}J(\mathbb{Q})$, under our running assumption that $P_i$ corresponds to a point $P \in X(\mathbb{Q})$.

The goal of the sieve is to show that such cosets in $J(\mathbb{Q})/p_i^{n_i}J(\mathbb{Q})$ cannot arise from points in $X(\mathbb{Q})$ by considering reduction maps modulo several primes.

We can consider more than one quadratic Chabauty prime in $\{p_1, p_2, p_3\}$ as follows. Suppose $k \neq i$. Then there must also exist $P_k \in A_{\mathrm{extra},k}$ such that $P$ reduces modulo $p_k^{m_k}$ to $P_k$. Using the Chinese remainder theorem, we then obtain cosets of $p_i^{n_i}p_k^{n_k}J(\mathbb{Q})$ in $J(\mathbb{Q})$ that we want to eliminate in the Mordell–Weil sieve step.

We refine this strategy by noticing that some elements in $A_{\mathrm{extra},k}$ may be ruled out from corresponding to $P$ in the following way. First note that elements of $\Omega_i$ are sums over the bad primes $q$ of $\mathbb{Q}$-rational multiples of $\log_i(q)$, where $\log_i$ is the $p_i$-adic logarithm, and that for $k \neq i$ the set $\Omega_k \subset \mathbb{Q}_{p_k}$ can be obtained from $\Omega_i \subset \mathbb{Q}_{p_i}$ just by replacing each occurrence of $\log_i$ with $\log_k$. Moreover, if $P_i \in A_i$ and $P_k \in A_k$ both correspond to $P \in X(\mathbb{Q})$, we must have

$$\tilde{\rho}_i(P) = \sum_{q \text{ bad}} v_q \log_i(q), \qquad \tilde{\rho}_k(P) = \sum_{q \text{ bad}} v_q \log_k(q),$$

where, for every $q$, the number $v_q$ is rational (the same one for $i$ and $k$). It follows that we only need to compare points in $A_{\mathrm{extra},i}$ and $A_{\mathrm{extra},k}$ corresponding to compatible elements in $\Omega_i$ and $\Omega_k$.

Since $A_i$ is closed under the hyperelliptic involution and the automorphisms $(x,y) \mapsto (-x, \pm y)$ of $X$, for one of the three primes it suffices to compute $A_i$ modulo automorphisms. We do so for $p_1$.

**4.3. Step 3: The Mordell–Weil sieve.** The Mordell–Weil sieve is a powerful tool for obtaining information about the rational points of a curve of genus greater than 1. It first appears in Scharaschkin's Phd thesis [Sch99] as a strategy to prove that a curve has no rational points. However, it can also be used in conjunction with methods such as classical or quadratic Chabauty to determine the set of rational points when we know that this is non-empty. See for instance [Fly04, PSS07, BS08, BS10a] for successful sieving computations. Here we apply to the curve $X$ of §4.2 the technique of [BBM17, Sections 5-7] and the `Magma` implementation thereof available at [BDM+]; see [BPa].

We retain the notation of §4.2. Let $I$ be a subset of $\{1,2,3\}$, and let $M = \prod_{j\in I} p_j^{n_j}$. In §4.2, we reduced the problem of determining $X(\mathbb{Q})$ to that of showing that some subset $C_M$ of the quotient $J(\mathbb{Q})/MJ(\mathbb{Q})$ does not contain the image of a point in $X(\mathbb{Q})$, under the composition of the embedding $\iota$ with the canonical quotient map $\pi\colon J(\mathbb{Q}) \to J(\mathbb{Q})/MJ(\mathbb{Q})$. More generally, by applying the Chinese remainder theorem, we can work with $M = M' \prod_{j\in I} p_j^{n_j}$ for some integer $M'$ coprime to $p_j$ for all $j \in I$.

Let $S$ be a finite set of primes of good reduction for $X$ and consider the commutative diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \xrightarrow{\pi\circ\iota} & J(\mathbb{Q})/MJ(\mathbb{Q}) \\ \downarrow & & \downarrow{\scriptstyle \alpha_S} \\ \displaystyle\prod_{\ell\in S} X(\mathbb{F}_\ell) & \xrightarrow{\beta_S} & \displaystyle\prod_{\ell\in S} J(\mathbb{F}_\ell)/MJ(\mathbb{F}_\ell), \end{array}$$

where the vertical and bottom maps are the natural ones. Because of the commutativity of the diagram, we succeed in determining $X(\mathbb{Q})$ if we can find a set $S$ for which

$$\alpha_S(C_M) \cap \beta_S\left(\prod_{\ell\in S} X(\mathbb{F}_\ell)\right) = \emptyset. \tag{4.2}$$

We use the repository [BDM+] to choose a set $S$ of primes in such a way that (4.2) has some likelihood of holding. The strategy is to pick primes $\ell$ for which the order of $J(\mathbb{F}_\ell)/MJ(\mathbb{F}_\ell)$ is large relative to the number of points in $X(\mathbb{F}_\ell)$ (or relative to its Hasse–Weil approximation $\ell+1$). In particular, we pick primes $\ell \le 10^4$ for which

$$\frac{\#J(\mathbb{F}_\ell)/MJ(\mathbb{F}_\ell)}{\ell+1} > 2.$$

Remark 4.1. We could (but did not) apply a similar strategy in the choice of the primes $p_1, p_2, p_3$. Namely, we could restrict to primes $p$ for which, for some integer $n$, the ratio $\frac{\#J(\mathbb{F}_\ell)/p^nJ(\mathbb{F}_\ell)}{\ell+1}$ is large, for at least one choice of $\ell \le 10^4$. We refer the reader to [BBM17, Section 7] for a discussion on how to simultaneously make optimal choices for the set $S$ and the integer $M$.

Our cosets $C_M$ are naturally partitioned into $\#\Omega_1 = \#\Omega_2 = \#\Omega_3$ subsets (as explained in §4.2). We run a separate sieve for each such subset.

For $M' \in [1,2,4]$, we do the following:

(1) Let $S$ be a suitable set of primes (in the sense above) for $M'p_1^4p_2^4p_3^4$.
(2) For $I \in [\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}]$, run the sieve with respect to $M = M'\prod_{j\in I} p_j^4$ and the set $S$. If (4.2) holds for some $I$, stop.

The reason why we avoid considering $I \in \{\{1\},\{2\},\{3\}\}$ is explained in [BBM17, Section 6].

Of course, even if the sieve does not succeed in eliminating the whole of $C_M$, we should not discard the information on which cosets are sieved out when changing $M$.

If $J(\mathbb{Q})_{\mathrm{tors}}$ is non-trivial, we may also try to take $M'$ to be a divisor of $\#J(\mathbb{Q})_{\mathrm{tors}}$.

For our database, the choices of $n_j = 4$ for each $j \in \{1,2,3\}$ and $M' \in \{1,2,4\} \cup \{\text{divisors of } \#J(\mathbb{Q})_{\mathrm{tors}}\}$ were successful for every curve. If one were to apply the technique to one specific curve (rather than to a database), it might be advisable to make more ad hoc choices.

**4.4. Curves with no known rational points.** In §4.2–4.3, we explained our strategy for determining $X(\mathbb{Q})$ when $X(\mathbb{Q})_{\mathrm{known}} \neq \emptyset$. If $X(\mathbb{Q})_{\mathrm{known}} = \emptyset$, we skip the quadratic Chabauty computations and directly apply a Mordell–Weil sieve to prove that $X(\mathbb{Q}) = \emptyset$. To this end, we implemented [BPa] a simple sieve that

uses only one good prime $\ell$ and the fact that $X$ is bielliptic (cf. [Sik15, Example 8.3]). Let $\varphi = (\varphi_1, \varphi_2)$. Then we have a commutative diagram

$$\begin{array}{ccc} X(\mathbb{Q}) & \xrightarrow{\varphi} & E_1(\mathbb{Q}) \times E_2(\mathbb{Q}) \\ \downarrow{\scriptstyle \mathrm{red}_\ell} & & \downarrow{\scriptstyle \mathrm{red}_\ell} \\ X(\mathbb{F}_\ell) & \xrightarrow{\varphi} & E_1(\mathbb{F}_\ell) \times E_2(\mathbb{F}_\ell), \end{array}$$

where $\mathrm{red}_\ell$ denotes reduction modulo $\ell$. If $\varphi(X(\mathbb{F}_\ell)) \cap \mathrm{red}_\ell(E_1(\mathbb{Q}) \times E_2(\mathbb{Q}))$ is the empty set, we are done.

Our implementation relies on functions in [BS10b] for constructing explicit maps $E_i(\mathbb{F}_p) \xrightarrow{\sim} A_i$, where $A_i$ is an abstract abelian group.

We applied this to two curves in $\Delta$: the ones with LMFDB labels 473256.a.946512.1 and 826672.a.826672.1. We used the prime $\ell = 331$ and $\ell = 181$, respectively. These two curves are examples of violation of the Hasse principle.

Remark 4.2. We could have replaced $J$ with $E_1 \times E_2$ also in the commutative diagram of §4.3. We chose not to do so, since the code [BDM+] was directly applicable. However, the fact that $X$ is bielliptic is implicitly used. Indeed, an important ingredient in §4.3 is the computation of the Mordell–Weil group $J(\mathbb{Q})$. In the bielliptic case, the `Magma` implementation for this uses the isogeny $J \sim E_1 \times E_2$.

**4.5. Sharp quadratic Chabauty computations.** For 6 curves we succeeded in determining the set of rational points using quadratic Chabauty only (i.e. without performing §4.3). This may be of some interest in the context of conjectures on sharpness of more general Chabauty–Kim sets (cf. [BDCKW18, Conjecture 3.1]).

The curves, together with the relevant primes used for quadratic Chabauty, are listed in the following table.

| LMFDB label | Bielliptic model | Prime(s) | $\#X(\mathbb{Q})$ |
|---|---|---|---|
| 99856.b.99856.1 | $y^2 = x^6 + 22x^4 - 19x^2 + 4$ | $p_1 = 3$ | 8 |
| 322624.b.322624.1 | $y^2 = x^6 - 2x^4 - 7x^2 + 4$ | $p_1 = 3$ | 8 |
| 614656.a.614656.1 | $y^2 = x^6 - 83x^4 + 19x^2 - 1$ | $p_1 = 3$ | 6 |
| 571536.a.571536.1 | $y^2 = x^6 - 12x^4 + 36x^2 - 4$ | $p_1 = 5$ | 2 |
| 274576.a.274576.1 | $y^2 = x^6 - 4x^4 - 4x^2 - 4$ | $p_1 = 3, p_2 = 7$ | 2 |
| 489648.a.489648.1 | $y^2 = -3x^6 + 4x^4 + 4x^2 - 4$ | $p_1 = 5$ | 4 |

In particular, for the first four listed curves, the set $A_{\mathrm{extra},1}$ is empty (cf. §4.2). For 274576.a.274576.1, neither $A_{\mathrm{extra},1}$, nor $A_{\mathrm{extra},2}$ is empty; however, there exists no pair $(\omega_1, \omega_2) \in \Omega_1 \times \Omega_2$ of compatible elements for which both $A_{\mathrm{extra},1}$ and $A_{\mathrm{extra},2}$ contain a point.

Finally, for 489648.a.489648.1, for each point $P_1$ in the (non-empty) $A_{\mathrm{extra},1}$, we find that at least one of the coefficients $a_1, a_2$ in (4.1) has negative $p_1$-adic valuation, a contradiction to their being integers.

## References

[ACKP22] N. Adžaga, S. Chidambaram, T. Keller, and O. Padurariu, *Rational points on hyperelliptic Atkin-Lehner quotients of modular curves and their coverings*, Research in Number Theory **8** (2022), no. 87. 1.4

[Bal] J. S. Balakrishnan, *SageMath code*, https://github.com/jbalakrishnan/AWS [Online; Accessed 25 August 2022]. 3.8

[Bal16] J. S. Balakrishnan, *On 3-adic heights on elliptic curves*, J. Number Theory **161** (2016), 119–134. 3.8

**26 Jun 2023 23:11:48 PDT**
**230105-Padurariu Version 2 - Submitted to LuCaNT**

[BB15] J. S. Balakrishnan and A. Besser, *Coleman-Gross height pairings and the p-adic sigma function*, J. Reine Angew. Math. **698** (2015), 89–104. 1.1

[BBBM21] J. S. Balakrishnan, A. Besser, F. Bianchi, and J. S. Müller, *Explicit quadratic Chabauty over number fields*, Israel J. Math. **243** (2021), no. 1, 185–232. 1, 1.3, 2, 2, 3.4

[BBCF+19] J. S. Balakrishnan, F. Bianchi, V. Cantoral-Farfán, M. Çiperiani, and A. Etropolski, *Chabauty-Coleman experiments for genus 3 hyperelliptic curves*, Research directions in number theory—Women in Numbers IV, Assoc. Women Math. Ser., vol. 19, Springer, Cham, 2019, pp. 67–90. 3.1

[BBK10] J. S. Balakrishnan, R. W. Bradshaw, and K. S. Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, Algorithmic number theory (ANTS-IX), Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 16–31. 3.8

[BBM16] J. S. Balakrishnan, A. Besser, and J. S. Müller, *Quadratic Chabauty: p-adic heights and integral points on hyperelliptic curves*, J. Reine Angew. Math. **720** (2016), 51–79. 1.1, 3.8

[BBM17] J. S. Balakrishnan, A. Besser, and J. S. Müller, *Computing integral points on hyperelliptic curves using quadratic Chabauty*, Math. Comp. **86** (2017), no. 305, 1403–1434. 1.1, 1, 4.2, 4.3, 4.1, 4.3

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language (Magma V2.26-5)*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265, Computational algebra and number theory (London, 1993). 1, 1, 4, 4.1

[BD18] J. S. Balakrishnan and N. Dogra, *Quadratic Chabauty and rational points, I: p -adic heights*, Duke Math. J. **167** (2018), no. 11, 1981–2038, With an appendix by J. S. Müller. 1, 1, 2, 2, 2, 2.5, 2

[BDCKW18] J. S. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers, *A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves*, Math. Ann. **372** (2018), no. 1-2, 369–428. 4.5

[BDM+] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, *Magma code*, https://github.com/steffenmueller/QCMod [Online; Accessed 15 December 2022]. 1, 1, 4, 4.3, 4.3, 4.2

[BDM+19] ———, *Explicit Chabauty—Kim for the split Cartan modular curve of level 13*, Ann. of Math. **189** (2019), no. 3, 885–944. 1

[BDM+21] ———, *Quadratic Chabauty for modular curves: Algorithms and examples*, arXiv:2101.01862 (2021). 1

[Ber81] D. Bernardi, *Hauteur p-adique sur les courbes elliptiques*, Séminaire de Théorie des Nombres, Paris 1979–80, Progr. Math., vol. 12, Birkhäuser, Boston, Mass., 1981, pp. 1–14. 1

[BGX21] F. Bars, J. González, and X. Xarles, *Hyperelliptic parametrizations of $\mathbb{Q}$ curves*, Ramanujan J. **56** (2021), no. 1, 103–120. 1, 1.3

[Bia] F. Bianchi, *SageMath code*, https://github.com/bianchifrancesca/quadratic_chabauty [Online; Accessed 25 August 2022]. 2

[Bia20] ———, *Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture*, Algebra Number Theory **14** (2020), no. 9, 2369–2416. 1, 1, 2, 2, 2, 2, 2, 2.5

[BKK11] J. S. Balakrishnan, K. S. Kedlaya, and M. Kim, *Appendix and erratum to "Massey products for elliptic curves of rank 1"*, J. Amer. Math. Soc. **24** (2011), no. 1, 281–291. 1.1

[Bou98] N. Bourbaki, *Lie groups and Lie algebras. Chapters 1–3*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1998, Translated from the French, Reprint of the 1989 English translation. 2

[BPa] F. Bianchi and O. Padurariu, *Magma code and rational points database*, https://github.com/oana-adascalitei/MWSieveForDatabase. 1.2, 1, 4.1, 4.3, 4.4

[BPb] ———, *SageMath code*, https://github.com/bianchifrancesca/QC_bielliptic. 1, 1, 4.2

[Bru03] N. Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49. 1

[BS08] N. Bruin and M. Stoll, *Deciding existence of rational points on curves: an experiment*, Experiment. Math. **17** (2008), no. 2, 181–189. 4.3

**26 Jun 2023 23:11:48 PDT**
**230105-Padurariu Version 2 - Submitted to LuCaNT**

[BS10a] ———, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306. 1, 4.3

[BS10b] ———, *'MWSieve-new.m', MAGMA code for Mordell–Weil sieve computation, 2009, electronic appendix to 'The Mordell-Weil sieve: proving non-existence of rational points on curves'*, LMS J. Comput. Math. **13** (2010), 272–306. 4.4

[BSS+16] A. R. Booker, J. Sijsling, A. V. Sutherland, J. Voight, and D. Yasaki, *A database of genus-2 curves over the rational numbers*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 235–254. 1, 1, 4.1

[CF96] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. 4.1

[CG89] R. F. Coleman and B. H. Gross, *p-adic heights on curves*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, Mass., 1989, pp. 73–81. 2

[Cha41] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C.R. Acad. Sci. Paris **212** (1941), 882–885. 1

[Col85a] R. F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. 1

[Col85b] ———, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168. 2

[Con] K. Conrad, *Hensel's lemma*, http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/hensel.pdf [Online; Accessed 11 August 2022]. 3.5

[EL21] B. Edixhoven and G. Lido, *Geometric quadratic Chabauty*, J. Inst. Math. Jussieu (2021), 1–55. 1.3

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. 1

[Fal84] ———, *Erratum: "Finiteness theorems for abelian varieties over number fields"*, Invent. Math. **75** (1984), no. 2, 381. 1

[FK91] G. Frey and E. Kani, *Curves of genus* 2 *covering elliptic curves and an arithmetical application*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., vol. 89, Birkhäuser, Boston, Mass., 1991, pp. 153–176. 1

[Fly04] E. V. Flynn, *The Hasse principle and the Brauer-Manin obstruction for curves*, Manuscripta Math. **115** (2004), no. 4, 437–466. 4.3

[FW99] E. V. Flynn and J. L. Wetherell, *Finding rational points on bielliptic genus 2 curves*, Manuscripta Math. **100** (1999), no. 4, 519–533. 1

[Har08] D. Harvey, *Efficient computation of p-adic heights*, LMS J. Comput. Math. **11** (2008), 40–59. 1, 2, 3.8

[Has] D. R. Hast, *Raw data for the paper "Explicit two-cover descent for genus 2 curves" (2022)*, https://github.com/HastD/twocover-results, [Online; accessed 3 September 2022]. 1

[Has22] ———, *Explicit two-cover descent for genus 2 curves*, Research in Number Theory **8** (2022), no. 67. 1, 1

[Kat73] N. M. Katz, *p-adic properties of modular schemes and modular forms*, Modular Functions of One Variable III, Lecture Notes in Mathematics, vol. 350, Springer, Berlin, 1973, pp. 69–190. 3.8

[Kat76] ———, *p-adic interpolation of real analytic Eisenstein series*, Ann. of Math. (2) **104** (1976), no. 3, 459–571. 3.8

[Kim05] M. Kim, *The motivic fundamental group of* $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ *and the theorem of Siegel*, Invent. Math. **161** (2005), no. 3, 629–656. 1

[Kim09] ———, *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. **45** (2009), no. 1, 89–133. 1

[Kim10] ———, *Massey products for elliptic curves of rank 1*, J. Amer. Math. Soc. **23** (2010), no. 3, 725–747. 1.1

[Kuh88] R. M. Kuhn, *Curves of genus* 2 *with split Jacobian*, Trans. Amer. Math. Soc. **307** (1988), no. 1, 41–49. 1

[LMF22] The LMFDB Collaboration, *The L-functions and modular forms database*, http://www.lmfdb.org, 2022, [Online; accessed 4 July 2022]. 1, 1, 1.3, 4.1

[LR22] X. Lang and J. Rouse, *Rational points on* $x^3 + x^2y^2 + y^3 = k$, arXiv:2205.13442 (2022). 1.4

[MST06] B. Mazur, W. Stein, and J. Tate, *Computation of p-adic heights and log convergence*, Doc. Math. (2006), no. Extra Vol., 577–614. 1, 2, 2, 3.8

[MT83] B. Mazur and J. Tate, *Canonical height pairings via biextensions*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser, Boston, Mass., 1983, pp. 195–237. 1

[MT91] ———, *The p-adic sigma function*, Duke Math. J. **62** (1991), no. 3, 663–688. 1, 2, 3.4

[PS23] O. Padurariu and C. Schembri, *Rational points on Atkin–Lehner quotients of geometrically hyperelliptic Shimura curves*, Expositiones Mathematicae (2023). 1.4

[PSS07] B. Poonen, E. F. Schaefer, and M. Stoll, *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$*, Duke Math. J. **137** (2007), no. 1, 103–158. 4.3

[Ric36] F. J. Richelot, *Essai sur une méthode générale pour déterminer la valeur des intégrales ultra-elliptiques, fondée sur des transformations remarquables de ces transcendantes*, C. R. Acad. Sci. Paris. **2** (1836), 622–627. 4.1

[Ric37] ———, *De transformatione integralium Abelianorum primi ordinis commentatio*, J. Reine Angew. Math. **16** (1837), 221–284. 4.1

[Sag22] Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.6)*, 2022, http://www.sagemath.org. 1, 1, 3.8, 4.2

[Sch99] V. Scharaschkin, *Local-global problems and the Brauer-Manin obstruction*, ProQuest LLC, Ann Arbor, MI, 1999, Thesis (Ph.D.)–University of Michigan. 1, 4.3

[Sik15] S. Siksek, *Chabauty and the Mordell-Weil sieve*, Advances on superelliptic curves and their applications, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 41, IOS, Amsterdam, 2015, pp. 194–224. 4.4

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. 2

[Sil09] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. 2, 3.3, 3.4

[Smi05] B. A. Smith, *Explicit endomorphisms and correspondences*, 2005, Thesis (Ph.D.)–University of Sydney. 4.1

[Wet97] J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, ProQuest LLC, Ann Arbor, MI, 1997, Thesis (Ph.D.)–University of California, Berkeley. 1

[Wut04] C. Wuthrich, *On p-adic heights in families of elliptic curves*, J. London Math. Soc. (2) **70** (2004), no. 1, 23–40. 3.4

Francesca Bianchi
*Email address*: francesca.bianchi.maths@gmail.com

Oana Padurariu
*Current address*: Max Planck Institute for Mathematics, Bonn
*Email address*: oana.padurariu11@gmail.com