Algebra &
Number
Theory

Volume 14
2020
No. 9

Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture

Francesca Bianchi

msp

ALGEBRA AND NUMBER THEORY 14:9 (2020)
https://doi.org/10.2140/ant.2020.14.2369

Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture

Francesca Bianchi

We explore a number of problems related to the quadratic Chabauty method for determining integral points on hyperbolic curves. We remove the assumption of semistability in the description of the quadratic Chabauty sets $\mathcal{X}(\mathbb{Z}_p)_2$ containing the integral points $\mathcal{X}(\mathbb{Z})$ of an elliptic curve of rank at most 1. Motivated by a conjecture of Kim, we then investigate theoretically and computationally the set-theoretic difference $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$. We also consider some algorithmic questions arising from Balakrishnan and Dogra's explicit quadratic Chabauty for the rational points of a genus-two bielliptic curve. As an example, we provide a new solution to a problem of Diophantus which was first solved by Wetherell.

Computationally, the main difference from the previous approach to quadratic Chabauty is the use of the p-adic sigma function in place of a double Coleman integral.

1. Introduction

Let (E, O) be an elliptic curve over $\mathbb{Q}$ and fix an odd prime p of good reduction. Denote by $\mathcal{E}$ the minimal regular model of E and by $\mathcal{X}$ the complement of the origin in $\mathcal{E}$.

When E has Mordell–Weil rank 1 and the Tamagawa number of $E/\mathbb{Q}$ is trivial at all primes, Kim [2010a] described an explicit locally analytic function on $\mathcal{X}(\mathbb{Z}_p)$ which vanishes on the set $\mathcal{X}(\mathbb{Z})$ of global integral points.

Subsequently, Balakrishnan, Dan-Cohen, Kim and Wewers [Balakrishnan et al. 2018] generalised the result to arbitrary semistable elliptic curves of rank 1 and gave a similar p-adic characterisation of $\mathcal{X}(\mathbb{Z})$ when E is semistable and has rank 0.

The discussion fits into Kim's nonabelian Chabauty programme as introduced in [Kim 2005; 2009]. In particular, Kim constructed a sequence of subsets of p-adic points

$$\mathcal{X}(\mathbb{Z}_p) \supset \mathcal{X}(\mathbb{Z}_p)_1 \supset \mathcal{X}(\mathbb{Z}_p)_2 \supset \cdots \supset \mathcal{X}(\mathbb{Z}).$$

The p-adic locally analytic functions from [Balakrishnan et al. 2018] are essentially those that define $\mathcal{X}(\mathbb{Z}_p)_2$, the set of *cohomologically global points of level* 2, in the larger $\mathcal{X}(\mathbb{Z}_p)$.

The subscript n in $\mathcal{X}(\mathbb{Z}_p)_n$ indicates a particular quotient U_n of the unipotent p-adic étale fundamental group U of $\mathcal{X}_{\overline{\mathbb{Q}}}$ (at a tangential base point). The set $\mathcal{X}(\mathbb{Z}_p)_n$ is then defined in terms of certain "unipotent Kummer maps" from $\mathcal{X}(\mathbb{Z})$ and $\mathcal{X}(\mathbb{Z}_q)$, at every prime q, to global and local cohomology sets with

MSC2010: primary 11D45; secondary 11G50, 11Y50, 14H52.
Keywords: quadratic Chabauty, p-adic heights, integral points on hyperbolic curves.

U_n-coefficients, respectively, in a way that generalises to objects with nonabelian étale fundamental group the role played by $\mathbb{Q}_p$-Selmer groups in our understanding of rational points on abelian varieties.

Despite its abstract cohomological definition, the set $\mathcal{X}(\mathbb{Z}_p)_n$ is believed to be computable in practice [Balakrishnan et al. 2018] as a union of intersections of zero loci of locally analytic functions defined in terms of iterated p-adic integrals. Unfortunately, such a characterisation is yet to be provided for $n \geq 3$.

Nevertheless, the explicit description of $\mathcal{X}(\mathbb{Z}_p)_2$ in the rank 0 semistable case given in [Balakrishnan et al. 2018] was already sufficient to collect some computational evidence for the following special case of a conjecture of Kim (see [Balakrishnan et al. 2018, §3.1]).

Conjecture 1.1 (Kim, 2012). *For sufficiently large n, we have*

$$\mathcal{X}(\mathbb{Z}_p)_n = \mathcal{X}(\mathbb{Z}).$$

Indeed, the authors of [loc. cit.] verified the equality

$$\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z})$$

for the prime $p = 5$ and for all the 256 semistable elliptic curves of rank 0 for which they computed $\mathcal{X}(\mathbb{Z}_p)_2$. An additional test that was performed by the same authors was that of fixing $\mathcal{X}$ and varying the prime p: once again, no point in $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$ was found. No other study of the difference $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$ appears in the literature, hence motivating the following two questions:

Question 1.2. Does there exist any elliptic curve of rank 0 for which $\mathcal{X}(\mathbb{Z}_p)_2$ contains at least one point which is not in $\mathcal{X}(\mathbb{Z})$?

Question 1.3. What geometric or algebraic properties should a point in $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$ satisfy?

One goal of the present paper is to give answers to these questions, with the idea that elliptic curves should serve as a test case for a conjecture that is in fact formulated by Kim in much greater generality than how we stated it here, and that as such would have striking applications if it were to hold. Indeed, $\mathcal{X}$ could be replaced by a suitable $\mathbb{Z}$-model $\mathcal{C}$ of any hyperbolic curve over $\mathbb{Q}$ with good reduction at p. In particular, the conjecture would give an effective approach towards finding the set of rational points on a curve of genus $g \geq 2$.

In the elliptic curve case, the conjecture might not have direct Diophantine interest, in the sense that there already exist algorithms for the computation of integral points on elliptic curves [Smart 1994; Pethő et al. 1999; Stroeker and Tzanakis 1994], and the rank 0 and 1 instances which we will explore are particularly well understood. However, the known explicit versions of nonabelian Chabauty for curves of higher genus (cf. [Balakrishnan et al. 2016; 2019a; Balakrishnan and Dogra 2018]) all generalise the explicit description of $\mathcal{X}(\mathbb{Z}_p)_2$ for elliptic curves of rank at most 1. Therefore, a conceptual understanding of the zero sets of the p-adic equations defining $\mathcal{X}(\mathbb{Z}_p)_2$ is essential to hope to achieve something similar in more complicated settings.

In general, even finiteness of $\mathcal{C}(\mathbb{Z}_p)_n$ for n large enough is only conjectural (but see [Kim 2010b; Coates and Kim 2010; Ellenberg and Hast 2017; Balakrishnan and Dogra 2018] for results in this direction, and

[Kim 2009] for a proof assuming the Bloch–Kato conjecture). If $g \geq 2$ and, for a given n, $\mathcal{C}(\mathbb{Z}_p)_n$ is finite and explicitly computable to arbitrary p-adic precision, then the Mordell–Weil sieve could be used to try to provably extrapolate $\mathcal{C}(\mathbb{Z})$ from $\mathcal{C}(\mathbb{Z}_p)_n$. However, the Mordell–Weil sieve is not guaranteed to terminate. Thus, finiteness of $\mathcal{C}(\mathbb{Z}_p)_n$ would not be sufficient to imply an effective version of Faltings's theorem.

Suppose now that $\mathcal{C}(\mathbb{Z}_p)_n$ is finite for n sufficiently large. One reason for expecting that the inclusion $\mathcal{C}(\mathbb{Z}) \subset \mathcal{C}(\mathbb{Z}_p)_n$ should eventually become sharp is explained in [Balakrishnan et al. 2018, §1.8]: assuming some well known motivic conjectures, the number of algebraically independent locally analytic functions vanishing on $\mathcal{C}(\mathbb{Z}_p)_n$ is strictly increasing in n (for $n \gg 0$). See also [Balakrishnan et al. 2018, §1, §3.4] for the philosophy behind Conjecture 1.1 (in its general form) and for its relationship with the conjectural finiteness of the Tate–Shafarevich group and with Grothendieck's section conjecture.

For an elliptic curve of rank 1, finiteness of $\mathcal{X}(\mathbb{Z}_p)_n$ can only hold at level $n \geq 2$. On the other hand, for a rank 0 elliptic curve, $\mathcal{X}(\mathbb{Z}_p)_1$ is finite and there are two independent equations defining $\mathcal{X}(\mathbb{Z}_p)_2$ (see Theorem 1.6 below), hence justifying why Question 1.2 had proved itself arduous. We show, however, that the answer to the question is negative. More precisely, we prove the following two theorems (see also Theorem 4.10).

Theorem 1.4. *There exist infinitely many rank* 0 *elliptic curves for which*

$$\mathcal{X}(\mathbb{Z}) \subsetneq \mathcal{X}(\mathbb{Z}_p)_2$$

for infinitely many good primes p.

Theorem 1.5. *There exists exactly one rank* 0 *elliptic curve of conductor at most* 30000 *for which*

$$\mathcal{X}(\mathbb{Z}) \subsetneq \mathcal{X}(\mathbb{Z}_p)_2$$

for all primes p of good (*ordinary and supersingular*) *reduction. This is the curve 8712.u5* [LMFDB 2019].

When we analyse these results in conjunction with Question 1.3, it will become apparent that they should not be considered as negative evidence for Conjecture 1.1. We will return below to discussing Theorems 1.4, 1.5 and answers to Question 1.3 in the context of the methods we develop in order to prove them. For the reader's convenience, let us first digress to write down the equations defining $\mathcal{X}(\mathbb{Z}_p)_2$. In fact, the very first goal of this article is to extend the explicit description of $\mathcal{X}(\mathbb{Z}_p)_2$ to an arbitrary elliptic curve of rank 0 and at the same time correct a slight imprecision in the analogous statement in the semistable case [Balakrishnan et al. 2018, Theorem 1.12] (see Remark 2.6).

Before stating the theorem, we introduce some additional notation, which is convenient to maintain similar to [Balakrishnan et al. 2018]. Let $\mathcal{E}$ be described by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

and let S be the set of primes at which E has bad reduction.

For each $q \in S$, define the set $W_q \subset \mathbb{Q}_p$ as follows. If the Tamagawa number at q is 1, let

$$W_q = \{0\};$$

in all other cases,

$$W_q = \begin{cases} W_q^{\text{bad}} & \text{if } q = 2 \text{ and } E \text{ is split multiplicative at } q, \\ W_q^{\text{bad}} \cup \{0\} & \text{otherwise,} \end{cases}$$

where W_q^{bad} is the finite subset of $\mathbb{Q}_p$ described in Table 1 (with $F = \mathbb{Q}$ and $v = (q_v) = (q)$); in particular, W_q^{bad} only depends on the reduction type of E at q. Let

$$W = \prod_{q \in S} W_q$$

and, if $w \in W$, write $\|w\| = \sum_{q \in S} w_q$. Let b be the integral tangent vector at the origin which is dual to $\omega(O)$, where

$$\omega = \frac{dx}{2y + a_1 x + a_3}$$

and let $\eta = x\omega$. Furthermore, for $z \in \mathcal{X}(\mathbb{Z}_p)$ write

$$\operatorname{Log}(z) = \int_b^z \omega \quad \text{and} \quad D_2(z) = \int_b^z \omega\eta,$$

where the integrals are Coleman integrals.

Theorem 1.6. *Suppose that E has rank 0 and the p-primary part of the Tate–Shafarevich group is finite.*

(1) *If, for at least one of $q \in \{2, 3\}$, the reduction of E at q is good and $\bar{E}(\mathbb{F}_q) = \{O\}$, or if E has split multiplicative reduction of Kodaira type I_1 at 2, then*

$$\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z}) = \varnothing.$$

(2) *Otherwise,*

$$\mathcal{X}(\mathbb{Z}_p)_2 = \bigcup_{w \in W} \phi(w),$$

where

$$\phi(w) = \{z \in \mathcal{X}(\mathbb{Z}_p) : \operatorname{Log}(z) = 0, 2D_2(z) + \|w\| = 0\}.$$

We also remove the assumption of semistable reduction in the rank 1 case [Balakrishnan et al. 2018, Proposition 5.12]. Assume E has good ordinary[1] reduction at p. Let $\boldsymbol{E}_2$ be the Katz p-adic weight 2 Eisenstein series [Katz 1976] and let

$$C = \frac{a_1^2 + 4a_2 - \boldsymbol{E}_2(E, \omega)}{12}. \tag{2}$$

[1] Although not explicitly stated in [Balakrishnan et al. 2018], their statement also holds only when p is ordinary. However, a similar result holds in the supersingular case; see Remark 2.8.

Let $h_p : E(\mathbb{Q}) \to \mathbb{Q}_p$ be $(-2p)$ times the p-adic height of [Mazur et al. 2006] and define

$$c = \frac{h_p(z_0)}{\operatorname{Log}(z_0)^2}$$

for a nontorsion point $z_0 \in E(\mathbb{Q})$.

Theorem 1.7. *Suppose that E has rank* 1 *and that p is a prime of good ordinary reduction.*

(1) *If, for at least one of $q \in \{2, 3\}$, the reduction of E at q is good and $\bar{E}(\mathbb{F}_q) = \{O\}$, or if E has split multiplicative reduction of Kodaira type* I_1 *at* 2, *then*

$$\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z}) = \varnothing.$$

(2) *Otherwise,*

$$\mathcal{X}(\mathbb{Z}) \subset \mathcal{X}(\mathbb{Z}_p)_2' := \bigcup_{w \in W} \psi(w),$$

where

$$\psi(w) = \{z \in \mathcal{X}(\mathbb{Z}_p) : 2D_2(z) + C(\operatorname{Log}(z))^2 + \|w\| = c(\operatorname{Log}(z))^2\}.$$

According to [Balakrishnan et al. 2018], the set $\bigcup_{w \in W} \psi(w)$ should equal $\mathcal{X}(\mathbb{Z}_p)_2$: hence the notation $\mathcal{X}(\mathbb{Z}_p)_2'$. Section 2 is devoted to the proofs of Theorems 1.6 and 1.7.

The equations defining the sets of p-adic points of the two theorems can be given an elementary interpretation as linear relations amongst $\mathbb{Q}_p$-valued quadratic functions on $E(\mathbb{Q})$, dictated by the assumptions on the rank. More precisely, any global p-adic height $E(\mathbb{Q}) \to \mathbb{Q}_p$ (of Bernardi, Coleman–Gross, Mazur–Tate) vanishes identically if the rank is 0, and is a scalar multiple of $\operatorname{Log}^2|_{E(\mathbb{Q})}$ if the rank is 1. To go from here to a p-adic approximation of the global integral points, one invokes the decomposition of the p-adic height on $E(\mathbb{Q}) \setminus \{O\}$ as a sum, over the nonarchimedean primes q, of local p-adic heights $\lambda_q : E(\mathbb{Q}_q) \setminus \{O\} \to \mathbb{Q}_p$. Indeed, the restriction of λ_q to $\mathcal{X}(\mathbb{Z}_q) \supset \mathcal{X}(\mathbb{Z})$ has finite image for all $q \neq p$, zero image for almost all $q \neq p$, and is locally analytic for $q = p$.

This point of view is crucial in our investigation, in Section 3, of what points could arise in $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$ in rank 0. Recall that no example of an elliptic curve of rank 0 and a prime p for which $\mathcal{X}(\mathbb{Z}_p)_2 \supsetneq \mathcal{X}(\mathbb{Z})$ was previously known. A careful study of the Mazur–Tate and Bernardi local p-adic heights allows us to deduce possible obstructions to the sharpness of $\mathcal{X}(\mathbb{Z}_p)_2$, and to give necessary and sufficient conditions for a point in $\mathcal{X}(\mathbb{Z}_p) \setminus \mathcal{X}(\mathbb{Z})$ to belong to $\mathcal{X}(\mathbb{Z}_p)_2$.

First note that a point in $\mathcal{X}(\mathbb{Z}_p)_2$ is algebraic, since it is in the zero set of the abelian logarithm Log. Our sufficient conditions then come from studying how automorphisms of $E/\overline{\mathbb{Q}}$ affect the values of the local p-adic heights at certain algebraic points, and from an analysis of noncyclotomic p-adic heights over nontotally real number fields. A combination of these two phenomena explains the appearance of extra points at level 2 in the family of quadratic twists of the modular curve $X_0(49)$ (see Proposition 3.14). As an application, in Section 3C we prove Theorem 1.4.

As regards necessary conditions for $\mathcal{X}(\mathbb{Z}_p)_2$ to contain parasite points, we prove a sort of "p-adic height saturation" condition (see the discussion in Section 3D):

Theorem 1.8 (Theorem 3.18). *Let $E/\mathbb{Q}$ and p be as in Theorem 1.6. Suppose that $z \in \mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$. Then z is the localisation of a torsion point P over a number field K and, for each rational prime q, the value $\lambda_{\mathfrak{q}}(P)$ of the local height at $\mathfrak{q}$ of the cyclotomic p-adic height of E/K is independent of the prime $\mathfrak{q} \mid q$ of K.*

We then present in Section 4 the computations of the sets $\mathcal{X}(\mathbb{Z}_p)_2$ for all the elliptic curves over $\mathbb{Q}$ of rank 0 and conductor less than or equal to 30000 and for some choices of p. We propose a slightly different but equivalent way of computing the set $\mathcal{X}(\mathbb{Z}_p)_2$, compared to the one used in [Balakrishnan et al. 2018]. In particular, our method does not rely on general algorithms to compute double Coleman integrals, but rather uses Bernardi's and Mazur and Tate's description of the p-adic height on an elliptic curve to express the double Coleman integrals in terms of p-adic sigma functions.

Our computations (run on SageMath [2017–2019]) suggest that the failure of sharpness of $\mathcal{X}(\mathbb{Z}_p)_2$ is still to be considered a rare phenomenon, which we were always able to explain using the sufficient conditions of Section 3. Extra points become even more exceptional if we allow the prime p to vary. In particular, we prove Theorem 1.5 (see Theorem 4.10).

In future work, it would be interesting to verify whether Conjecture 1.1 holds at level 3 for the curves and primes for which we found $\#\mathcal{X}(\mathbb{Z}_p)_2 > \#\mathcal{X}(\mathbb{Z})$.

When E has rank 1, the set described in Theorem 1.7(2) is generally larger than $\mathcal{X}(\mathbb{Z})$. Naively, this is because $\mathcal{X}(\mathbb{Z}_p)_2'$ is cut out by the vanishing of one function only. In Section 5A, we ask what algebraic points can belong to $\mathcal{X}(\mathbb{Z}_p)_2' \setminus \mathcal{X}(\mathbb{Z})$. In Section 5B we compute $\mathcal{X}(\mathbb{Z}_p)_2'$ for all the 14783 rank 1 elliptic curves of conductor at most 5000; for each curve, we let p be the smallest prime greater than or equal to 5 at which the curve has good ordinary reduction.

Finally, in Section 6 we apply some of our techniques for elliptic curves to the computation of rational points on certain genus 2 curves C over $\mathbb{Q}$. Indeed, when C admits degree 2 maps to two elliptic curves over $\mathbb{Q}$, each of rank 1, Balakrishnan and Dogra [2018] described a $\mathbb{Q}_p$-valued locally analytic function on $C(\mathbb{Q}_p)$ vanishing on $C(\mathbb{Q})$. This is defined using local p-adic heights on each elliptic curve. We explain how one can replace direct computations of double Coleman integrals with computations involving the p-adic sigma function and division polynomials also in this situation. We make the computation explicit for a curve arising from a problem from the *Arithmetica* of Diophantus and use it to give an alternative proof to the one given by Wetherell in his thesis [1997] of the fact that the curve has exactly 8 rational points.

Balakrishnan and Dogra implemented their method numerically in some examples. However, algorithmically, their approach was still based on a case-by-case study. This consideration applies especially to a preliminary step which consists in the computation of two finite subsets of $\mathbb{Q}_p$ (which play the role of the set $\|W\|$ above). By combining results of [Balakrishnan and Dogra 2018] with properties of local p-adic heights on elliptic curves, in Section 6A we offer a more general and applicable numerical approach to the method. For example, we give an algorithm that takes as input a bielliptic curve C whose associated elliptic curves have Mordell–Weil rank 1 together with a good prime p and outputs a finite set of p-adic points containing $C(\mathbb{Q})$ (i.e., we remove the preliminary computation step). In doing so, we also provide a more elementary proof and approach to the explicit result of [Balakrishnan and Dogra 2018].

The code used for the computations in this article is available at [Bianchi 2019].

2. Description of $\mathcal{X}(\mathbb{Z}_p)_2$

2A. ***The p-adic height and its local components.*** Let p be an odd prime and extend the usual p-adic logarithm $\log : 1 + p\mathbb{Z}_p \to \mathbb{Q}_p$ to $\mathbb{Q}_p^\times$ via $\log(p) = 0$.

Let E be an elliptic curve over $\mathbb{Q}$ as in Section 1 and assume E has good reduction at p. We will sometimes need to consider the base-change of E to a number field F (whose ring of integers is denoted $\mathcal{O}_F$); thus, we do not restrict the following definitions to $E(\mathbb{Q})$. Let

$$h_p : E(F) \to \mathbb{Q}_p$$

be a cyclotomic[2] p-adic height of Coleman–Gross (see [Coleman and Gross 1989] and [Balakrishnan and Besser 2015]). The use of the indefinite article here is due to the dependence of h_p on a choice that will be made explicit in Section 2A2. The function h_p is quadratic, i.e., satisfies the relation

$$h_p(mP) = m^2 h_p(P) \quad \text{for all } m \in \mathbb{Z} \text{ and } P \in E(F),$$

and is defined as a sum of local heights, one for each nonarchimedean prime of F. In particular, we have[3] $h_p(O) = 0$ and for $P \in E(F) \setminus \{O\}$

$$h_p(P) = \frac{1}{[F : \mathbb{Q}]} \sum_v n_v \lambda_v(P),$$

where the sum is over all finite primes v of F, $n_v = [F_v : \mathbb{Q}_v]$ and

$$\lambda_v : E(F_v) \setminus \{O\} \to \mathbb{Q}_p$$

is a *p-adic local Néron function at v*.

Let q_v be the norm of v and $|\cdot|_v$ be the normalised absolute value corresponding to v. That is, if $x \in F_v^\times$, we have

$$|x|_v = q_v^{-\operatorname{ord}_v(x)/n_v},$$

where the valuation ord_v is such that $\operatorname{ord}_v(F_v^\times) = \mathbb{Z}$.

[2] If the space of continuous idele class characters $\mathbb{A}_F^\times / F^\times \to \mathbb{Q}_p$ has dimension larger than 1, we will see in Section 3B that one can define other types of p-adic heights.

[3] Here we choose to normalise the p-adic height in such a way that it becomes independent of the choice of the field F containing the coordinates of P; note that this is not the case in many other articles, such as [Mazur et al. 2006].

2A1. The p-adic local Néron function at a nonarchimedean prime $v \nmid p$ is equal to the real local Néron function $\widehat{\lambda}_v$ at v with the p-adic logarithm in place of the real one. Thus, any reference that we provide for $\widehat{\lambda}_v$ can be applied also to our setting. For instance, analogously to the real case, for $v \nmid p$, the following properties determine a unique function $\lambda_v : E(F_v) \setminus \{O\} \to \mathbb{Q}_p$:

(i) λ_v is continuous on $E(F_v) \setminus \{O\}$ and bounded on the complement of any neighbourhood of O with respect to the v-adic topology.

(ii) $\lim_{P \to O}(\lambda_v(P) - \log|x(P)|_v)$ exists.

(iii) λ_v satisfies the *quasiparallelogram law*: for all $P, Q \in E(F_v)$ such that $P, Q, P \pm Q \neq O$, we have

$$\lambda_v(P+Q) + \lambda_v(P-Q) = 2\lambda_v(P) + 2\lambda_v(Q) - 2\log|x(P) - x(Q)|_v. \tag{3}$$

Uniqueness follows from topological reasons. For existence, it suffices to show that the p-adic analogue of $\widehat{\lambda}_v$ obtained as described above satisfies (i)–(iii) (see [Silverman 1994, VI, Exercise 6.3]).

We also have

(iv) For all $P \in E(F_v)$ and all $m \geq 1$ with $mP \neq O$,

$$\lambda_v(mP) = m^2\lambda_v(P) - 2\log|f_m(P)|_v,$$

where f_m is the m-th division polynomial of E (see for instance [Silverman 2009, III, Exercise 3.7] for the definition of f_m). We say that λ_v is *quasiquadratic*.

Moreover, uniqueness implies the following key fact:

(v) If ψ is an automorphism of E defined over F_v, then $\lambda_v(\psi(P)) = \lambda_v(P)$ for all $P \in E(F_v)$.

See also [Bernardi 1981] for a more general transformation property under isogeny.

We wish to determine which values λ_v can attain on $\mathcal{X}(\mathcal{O}_v)$, where $\mathcal{O}_v$ is the ring of integers of F_v and $v \nmid p$. For this, it will be convenient to assume that $\mathcal{E}$ is minimal at v. If that is not the case, we can always switch to a minimal equation at v and use the following (see [Cremona et al. 2006, Lemma 4]):

$$\lambda_v = \lambda_v^{\min} + \tfrac{1}{6}\log|\Delta/\Delta^{\min}|_v, \tag{4}$$

where Δ denotes the discriminant and the superscript min has the obvious meaning. See also Remark 3.3.

So assume for the rest of this subsection that λ_v is computed with respect to a minimal model at the prime v. Denote by $\overline{E}_{ns}(\mathbb{F}_v)$ the group of nonsingular points of the reduction of E modulo v and let

$$E_0(F_v) = \{P \in E(F_v) : \overline{P} \in \overline{E}_{ns}(\mathbb{F}_v)\}.$$

If E has good reduction at v, we may also write $\overline{E}(\mathbb{F}_v)$ for $\overline{E}_{ns}(\mathbb{F}_v)$.

Lemma 2.1. *Suppose $v \nmid p$. Then*

(i) *if $P \in E_0(F_v) \setminus \{O\}$, $\lambda_v(P) = \log(\max\{1, |x(P)|_v\})$;*

(ii) *if $P \notin E_0(F_v)$, $\lambda_v(P)$ depends exclusively on the image of P in $E(F_v)/E_0(F_v)$.*

Proof. See [Silverman 1988] or [Cremona et al. 2006, Proposition 5]. □

Proposition 2.2. *If $v \nmid p$ and $[E(F_v) : E_0(F_v)] = 1$, then*

$$\lambda_v(\mathcal{X}(\mathcal{O}_v)) = \begin{cases} \{0\} & \text{if } \#\bar{E}_{ns}(\mathbb{F}_v) > 1 \\ \varnothing & \text{otherwise.} \end{cases}$$

Proof. By Lemma 2.1(i), $\lambda_v(\mathcal{X}(\mathcal{O}_v)) \subseteq \{0\}$, with equality if and only if $\mathcal{X}(\mathcal{O}_v) \neq \varnothing$. Let

$$E_1(F_v) = \{P \in E(F_v) : \bar{P} = \bar{O}\};$$

in particular, $\mathcal{X}(\mathcal{O}_v) \cap E_1(F_v)$ is empty and every point in $E_0(F_v) \setminus E_1(F_v)$ comes from a point in $\mathcal{X}(\mathcal{O}_v)$. According to [Silverman 2009, VII, Proposition 2.1], the sequence

$$0 \to E_1(F_v) \to E_0(F_v) \to \bar{E}_{ns}(\mathbb{F}_v) \to 0$$

is exact, which proves the proposition. □

We now give an elementary necessary condition for $\#\bar{E}_{ns}(\mathbb{F}_v) = 1$. We show it is also a sufficient condition in all cases except when v is of good reduction.

Lemma 2.3. *The group $\bar{E}_{ns}(\mathbb{F}_v)$ has cardinality at least 2 in all of the following cases:*

(1) *E has additive or nonsplit multiplicative reduction at v.*

(2) *E has good reduction at v and $q_v > 4$.*

(3) *E has split multiplicative reduction at v and $q_v > 2$.*

Conversely, if E has split multiplicative reduction at v and $q_v = 2$, then

$$\#\bar{E}_{ns}(\mathbb{F}_v) = 1.$$

Proof. If E has additive reduction at v, then $\bar{E}_{ns}(\mathbb{F}_v) \cong \mathbb{F}_v^+$ always contains at least two elements. If the reduction is nonsplit multiplicative, then

$$\bar{E}_{ns}(\mathbb{F}_v) \cong \{a \in k^\times : N_{k/\mathbb{F}_v}(a) = 1\},$$

where $[k : \mathbb{F}_v] = 2$ and $N_{k/\mathbb{F}_v}$ is the field norm of $k/\mathbb{F}_v$. Thus, if $q_v > 2$, then the statement is clear; if $q_v = 2$, then k is the splitting field of $x^4 - x$ over $\mathbb{F}_2$ and each element in $k^\times$ has norm 1 over $\mathbb{F}_2$.

When E has good reduction at v and $q_v > 4$, the Hasse bound yields $\#\bar{E}(\mathbb{F}_v) > 1$. Finally, if the reduction is split multiplicative, then $\bar{E}_{ns}(\mathbb{F}_v) \cong \mathbb{F}_v^\times$. □

Proposition 2.4. *If $v \nmid p$ and $[E(F_v) : E_0(F_v)] \neq 1$, then*

$$n_v\lambda_v(\mathcal{X}(\mathcal{O}_v)) = \begin{cases} W_v^{\text{bad}} & \text{if } q_v = 2 \text{ and } E \text{ is split multiplicative at } v, \\ W_v^{\text{bad}} \cup \{0\} & \text{otherwise,} \end{cases}$$

where W_v^{bad} is defined in Table 1.

Proof. By a similar argument to the proof of Proposition 2.2, each non trivial coset of $E(F_v)/E_0(F_v)$ is represented by an element in $\mathcal{X}(\mathcal{O}_v)$ and there exists at least one point in $\mathcal{X}(\mathcal{O}_v)$ which reduces to a nonsingular point in $\bar{E}_{ns}(\mathbb{F}_v)$ if and only if $\#\bar{E}_{ns}(\mathbb{F}_v) > 1$.

Kodaira symbol	$[E(F_v):E_0(F_v)]$	W_v^{bad}
$\mathrm{I}_n(n\geq 2)$	2 (nonsplit)	$\left\{-\frac{n}{4}\log q_v\right\}$
	n (split)	$\left\{-\frac{i(n-i)}{n}\log q_v : 1\leq i\leq \left\lfloor\frac{n}{2}\right\rfloor\right\}$
III	2	$\left\{-\frac{1}{2}\log q_v\right\}$
IV	3	$\left\{-\frac{2}{3}\log q_v\right\}$
I_0^*	2 or 4	$\{-\log q_v\}$
$\mathrm{I}_n^*(n\geq 1)$	2	$\{-\log q_v\}$
	4	$\left\{-\log q_v, -\frac{n+4}{4}\log q_v\right\}$
IV^*	3	$\left\{-\frac{4}{3}\log q_v\right\}$
III^*	2	$\left\{-\frac{3}{2}\log q_v\right\}$

Table 1. The sets W_v^{bad}.

By Lemma 2.1(i), if $P\in\mathcal{X}(\mathcal{O}_v)$ reduces to a nonsingular point, then $\lambda_v(P)=0$; by Lemma 2.3, such P exists unless $q_v=2$ and E is split multiplicative at 2.

Therefore, by Lemma 2.1(ii), it suffices to show that W_v^{bad} coincides exactly with the values of $n_v\lambda_v$ on $E(F_v)/E_0(F_v)\setminus\{0\}$. For this, we use the work of Cremona, Prickett and Siksek [Cremona et al. 2006] for the local heights of the real canonical height. The proof of [loc. cit., Proposition 6] can be used verbatim here with the p-adic logarithm in place of the real one and Table 1 is nothing but the translation of [Cremona et al. 2006, Table 2] to the p-adic setting. □

2A2. The p-adic local Néron function at a prime $v\mid p$ is not unique: it depends on a choice of subspace $N_v\subset H^1_{\text{dR}}(E/F_v)$ complementary to the space of holomorphic differentials (see [Coleman and Gross 1989]). Let ξ_v be the one-form of the second kind with a double pole at O and no others, representative of the class in N_v dual to ω with respect to the cup product (i.e., such that $[\omega]\cup[\xi_v]=1$). Let $\operatorname{tr}_{F_v/\mathbb{Q}_p}$ denote the field trace. Then by [Balakrishnan and Besser 2015, Theorem 4.1], for all $P\in E(F_v)\setminus\{O\}$ one has

$$\lambda_v(P)=\frac{1}{n_v}\operatorname{tr}_{F_v/\mathbb{Q}_p}\left(2\int_b^P \omega\xi_v\right).$$

In particular,

$$\xi_v=\eta+\gamma\omega\quad\text{for some }\gamma\in F_v$$

and hence

$$\lambda_v(P)=\frac{1}{n_v}\operatorname{tr}_{F_v/\mathbb{Q}_p}(2D_2(P)+\gamma\operatorname{Log}(P)^2).$$

In [Balakrishnan and Besser 2015, Corollary 3.2], it is shown that if E has good ordinary reduction at v and N_v is the unit root eigenspace of Frobenius, then λ_v is related to the logarithm of the v-adic sigma function of Mazur and Tate [1991].

In fact, it is easy to see that their proof shows the following stronger result.

Proposition 2.5. *Let $x(t)$ be the Laurent series expansion of x in terms of the parameter for the formal group $t = -x/y$. Let $\sigma_v^{(\gamma)}(t) = t + \cdots \in F_v[[t]]$ be the unique odd*[4] *function satisfying*

$$x(t) + \gamma = -\frac{d}{\omega}\left(\frac{1}{\sigma_v^{(\gamma)}}\frac{d\sigma_v^{(\gamma)}}{\omega}\right)$$

and let V be a neighbourhood of O on which $\sigma_v^{(\gamma)}$ converges. Then, for all $P \in V \setminus \{O\}$, we have

$$\lambda_v(P) = -\frac{2}{n_v}\operatorname{tr}_{F_v/\mathbb{Q}_p}(\log_v(\sigma_v^{(\gamma)}(P))),$$

where $\log_v : F_v^\times \to F_v$ *extends* $\log$.

For our applications, we may assume that there is an isomorphism $F_v \simeq \mathbb{Q}_p$, which is now fixed. Since λ_v is not unique, we will use the following convention. If the reduction is good *ordinary* at each prime v above p, we choose N_v to be the unit root eigenspace of Frobenius, i.e.,

$$\gamma = C,$$

where C is defined in (2). If P belongs to the formal group at v, then Proposition 2.5 says that

$$\lambda_v(P) = -2\log(\sigma_p(P)),$$

where σ_p is the Mazur–Tate p-adic sigma function. Furthermore, in this case the global p-adic height coincides with the p-adic height of Mazur–Tate.

If E is good *supersingular* at some prime $v \mid p$, we let, for each $v \mid p$,

$$\gamma = \frac{a_1^2 + 4a_2}{12},$$

so that $\sigma_p^{(\gamma)}$ is the p-adic sigma function of Bernardi [1981]. This choice of γ gives a power series $\sigma_v^{(\gamma)}(t)$ with coefficients in F (and in fact $\mathbb{Q}$ in our case), which is related to the Taylor expansion $\sigma(z)$ of the complex Weierstrass sigma function by the change of variables $z = L_v(t)$, where L_v is the formal group logarithm. Unlike the p-adic sigma function of Mazur and Tate, the one of Bernardi does not converge on the whole formal group over $\overline{F_v}$, as it may not have p-adically integral coefficients, as a power series in t. However, since we are assuming that $F_v \simeq \mathbb{Q}_p$, the function $\sigma_p^{(\gamma)}$ converges on all the points P of the formal group whose coordinates are defined over F_v, since these satisfy $\operatorname{ord}_v(t(P)) > 1/(p-1)$.

In both the ordinary and supersingular cases, λ_v satisfies (see [Coleman and Gross 1989; Mazur and Tate 1991; Bernardi 1981]):

[4] Odd as a function on a subset of the formal group and not as a function of t.

(i) λ_v is locally analytic on $\mathcal{X}(\mathcal{O}_v)$.

(ii) For all $P \in E(F_v)$ and all $m \geq 1$ with $mP \neq O$,

$$\lambda_v(mP) = m^2\lambda_v(P) - \frac{2}{n_v}\operatorname{tr}_{F_v/\mathbb{Q}_p}(\log_v(f_m(P))).$$

(iii) For all $P, Q \in E(F_v)$ such that $P, Q, P \pm Q \neq O$,

$$\lambda_v(P+Q) + \lambda_v(P-Q) = 2\lambda_v(P) + 2\lambda_v(Q) - \frac{2}{n_v}\operatorname{tr}_{F_v/\mathbb{Q}_p}(\log_v(x(P)-x(Q))).$$

(iv) If ψ is an automorphism of E defined over F_v, then $\lambda_v(\psi(P)) = \lambda_v(P)$ for all $P \in E(F_v)$. In view of the assumption that $F_v \simeq \mathbb{Q}_p$ and by Deuring's criterion, at supersingular primes this is simply saying that λ_v is an even function. At ordinary primes, let ζ be the root of unity such that $\psi^*(\omega) = \zeta\omega$. Then $f_m(\psi(P)) = \zeta^{1-m^2} f_m(P)$ by [Mazur and Tate 1991, Appendix I, Proposition 2], and the Mazur–Tate p-adic sigma function satisfies $\sigma_p(\psi(P)) = \zeta\sigma_p(P)$ if P is in the formal group [Mazur and Tate 1991, §3]. The claim then follows since $\log(\zeta) = 0$. Note that invariance under any automorphism would also hold if we used the Bernardi sigma function to define the local heights at ordinary primes, since for curves of j-invariant 0 or 1728 the weight 2 Eisenstein series vanishes, so the Bernardi and Mazur–Tate p-adic sigma function are equal.

We also remark that if L/F is a finite field extension, w is a prime of L above v, where v is any prime of F, and $P \in E(F_v)$, then

$$\lambda_v(P) = \lambda_w(P).$$

2B. ***Proof of Theorems 1.6 and 1.7.*** It would be pointless to reproduce here the whole proofs, as they are straightforward from Section 2A and the proofs in [Balakrishnan et al. 2018]. Thus we content ourselves with giving a sketch and correcting a few imprecisions in [loc. cit., Theorem 1.12].

We start with some notation and we refer the reader to [Kim 2005; 2009; Balakrishnan et al. 2018] for more details. Let $T = S \cup \{p\}$ and denote by G_T the Galois group of the maximal extension of $\mathbb{Q}$ unramified outside T. For a prime q, write G_q for the absolute Galois group of $\mathbb{Q}_q$. For $q \in T$, G_q may be identified with a subgroup of G_T. For $q \notin T$, this is not possible; however, we may still define maps $G_q \to G_T$ which are trivial on the inertia subgroup $I_q \leq G_q$.

Let U be the unipotent p-adic étale fundamental group of $\mathcal{X}_{\overline{\mathbb{Q}}}$ at b and U_n the quotient of U by the n-th level of its central series.

For each prime q and $n \geq 1$, we have commutative diagrams

$$\begin{tikzcd}
\mathcal{X}(\mathbb{Z}) \arrow[r] \arrow[d] & \mathcal{X}(\mathbb{Z}_q) \arrow[d, "j_q^n"] \\
H^1_f(G_T, U_n) \arrow[r, "\mathrm{loc}_q^n"] & H^1(G_q, U_n)
\end{tikzcd}$$

Here the H^1 are cohomology sets and $H^1_f(G_T, U_n) = (\mathrm{loc}_p^n)^{-1}(H^1_f(G_p, U_n))$, where $H^1_f(G_p, U_n)$ is the subset of $H^1(G_p, U_n)$ of crystalline U_n-torsors. We are interested in determining

$$\mathcal{X}(\mathbb{Z}_p)_n = (j_p^n)^{-1}(\mathrm{loc}_p^n(\mathrm{Sel}^n(\mathcal{X}))),$$

where the Selmer scheme $\mathrm{Sel}^n(\mathcal{X})$ is defined as

$$\mathrm{Sel}^n(\mathcal{X}) = \bigcap_{q \neq p} (\mathrm{loc}_q^n)^{-1}(\mathrm{Im}\, j_q^n).$$

From now on, we will focus on $n = 2$ and will drop the superscript n from the maps j_q and loc_q.

Proof of Theorem 1.6. If $\mathcal{X}(\mathbb{Z}_q)$ is empty for some q, then $\mathcal{X}(\mathbb{Z}_p)_2$ is trivially empty. Lemma 2.3 shows that this occurs precisely when E has good reduction at q, where $q = 2$ or 3, and $\bar{E}(\mathbb{F}_q) = \{O\}$, or when E has split multiplicative reduction of type I_1 at $q = 2$. This shows (1).

We may now suppose that $\mathcal{X}(\mathbb{Z}_q) \neq \varnothing$ for all q (including $q = p$). Since $E(\mathbb{Q})$ has rank 0 and the p-primary part of the Tate–Shafarevich group is finite, by Lemma 5.2 in [Balakrishnan et al. 2018],

$$\mathrm{Sel}^2(\mathcal{X}) \subset H^1_f(G_T, \mathbb{Q}_p(1)),$$

where $H^1_f(G_T, \mathbb{Q}_p(1)) \subset H^1_f(G_T, U_2)$ via $0 \to \mathbb{Q}_p(1) \to U_2 \to V_p(E) \to 0$.

For $q \neq p$, we have

$$j_q : \mathcal{X}(\mathbb{Z}_q) \to H^1(G_q, U_2) \simeq H^1(G_q, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p,$$

the last map being $c \mapsto \log \chi \cup c \in H^2(G_q, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$, where χ is the p-adic cyclotomic character and $\cup$ is the cup product (note $\log \chi \in H^1(G_q, \mathbb{Q}_p)$). The middle bijection is proved in [Balakrishnan et al. 2018, §4.1.5]. Thus, finding the image of j_q is equivalent to finding

$$\{\phi_q(z) := \log \chi \cup j_q(z) : z \in \mathcal{X}(\mathbb{Z}_q)\}.$$

Theorem 4.1.6 in [Balakrishnan et al. 2018] shows that

$$2\phi_q : \mathcal{X}(\mathbb{Z}_q) \to \mathbb{Q}_q, \qquad z \mapsto 2(\log \chi \cup j_q(z))$$

is the restriction to $\mathcal{X}(\mathbb{Z}_q)$ of a p-adic local Néron function in the sense of Section 2A1 and must thus be equal to the function λ_q.

In particular, for each $q \neq p$, the set $2\phi_q(\mathcal{X}(\mathbb{Z}_q))$ is the finite set described by Propositions 2.2 and 2.4.

The cup product $\log \chi \cup c$, for $c \in H^1_f(G_p, \mathbb{Q}_p(1))$, and local reciprocity also yield an isomorphism

$$\psi_p : H^1_f(G_p, \mathbb{Q}_p(1)) \xrightarrow{\sim} H^2(G_p, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$$

and we get a commutative diagram

$$\begin{tikzcd}
H^1_f(G_T, \mathbb{Q}_p(1)) \arrow[r, hook, "\bigoplus_{q \in T} \mathrm{loc}_q"] \arrow[d, "g = \log \chi \cup \cdot"] & H^1_f(G_p, \mathbb{Q}_p(1)) \oplus \bigoplus_{q \in S} H^1(G_q, \mathbb{Q}_p(1)) \arrow[d, "\wr"] \\
H^2(G_T, \mathbb{Q}_p(1)) \arrow[r, hook, "\bigoplus_{q \in T} \mathrm{loc}_q"] & \bigoplus_{q \in T} H^2(G_q, \mathbb{Q}_p(1)) \simeq \bigoplus_{q \in T} \mathbb{Q}_p
\end{tikzcd}$$

On the other hand, by global class field theory and Hilbert's Theorem 90, the image of $H^2(G_T,\mathbb{Q}_p(1))$ in the bottom row is the kernel of the map

$$\bigoplus_{q\in T}\mathbb{Q}_p\to\mathbb{Q}_p,\qquad (a_q)\to\sum_q a_q$$

and by dimension considerations, one concludes that the map g is in fact also an isomorphism.

From above we know that the image of $\bigoplus_{q\in S} j_q(\mathcal{X}(\mathbb{Z}_q))$ in $\bigoplus_{q\in S}\mathbb{Q}_p$ is precisely $\left(\frac{1}{2}\right)\bigoplus_{q\in S} W_q$, where

- if $[E(\mathbb{Q}_q):E_0(\mathbb{Q}_q)]=1$, then $W_q=\{0\}$;
- if $[E(\mathbb{Q}_q):E_0(\mathbb{Q}_q)]\neq 1$, then
$$W_q=\begin{cases}W_q^{\text{bad}} & \text{if } q=2 \text{ and } E \text{ is split multiplicative at } q,\\ W_q^{\text{bad}}\cup\{0\} & \text{otherwise}\end{cases}$$
and W_q^{bad} is defined in Proposition 2.4.

Let $W=\prod_{q\in S} W_q$. It follows from the above that for every $w=(w_q)_{q\in S}\in W$ there exists a unique $c\in H^1_f(G_T,\mathbb{Q}_p(1))$ with $2(\log\chi\cup\operatorname{loc}_q(c))=w_q$ for every $q\in S$. Further, this satisfies $2\psi_p(\operatorname{loc}_p(c))=-\|w\|$. On the other hand, if $q\notin T$ and $c\in H^1_f(G_T,\mathbb{Q}_p(1))$ then $\operatorname{loc}_q(c)=0$ and $\operatorname{Im}(j_q)=\{0\}$ by Proposition 2.2. Therefore,

$$\operatorname{Sel}^2(\mathcal{X})=\bigcap_{q\in S}\operatorname{loc}_q^{-1}(\operatorname{Im} j_q)$$

and

$$\operatorname{loc}_p(\operatorname{Sel}^2(\mathcal{X}))=\bigcup_{w\in W}\{c\in H^1_f(G_p,\mathbb{Q}_p(1)):2\psi_p(c)+\|w\|=0\}.$$

It remains to compute the preimage of this set under j_p. As is shown in [Balakrishnan et al. 2018, §5.7], we find

$$\mathcal{X}(\mathbb{Z}_p)_2=\{z\in\mathcal{X}(\mathbb{Z}_p):\operatorname{Log}(z)=0,\,2D_2(z)+\|w\|=0\};$$

indeed, the condition $\operatorname{Log}(z)=0$ is equivalent to requiring that

$$j_p(z)\in H^1_f(G_p,\mathbb{Q}_p(1))\subset H^1_f(G_p,U_2)$$

and the other condition comes from the explicit formula

$$\psi_p(j_p(z))=D_2(z)\quad\text{for } j_p(z)\in H^1_f(G_p,\mathbb{Q}_p(1)).\qquad\square$$

Remark 2.6. The corrections to the proof in [Balakrishnan et al. 2018] made here are the following. First of all, if $\mathcal{X}(\mathbb{Z}_q)$ is empty for some q, the proof does not hold. Of course this is a trivial case (treated in (1)), but it is not clear that the union given in [loc. cit., Theorem 1.12] should be empty. In fact, in Example 4.2 we find a curve satisfying the hypotheses of Theorem 1.6(1), but for which $\bigcup_{w\in W}\phi(w)\neq\varnothing$.

Secondly, if the reduction type at q is nonsplit multiplicative of type I_m, with $m>2$, not all the values in their sets W_q will be attained by a point in $E(\mathbb{Q}_q)\setminus E_0(\mathbb{Q}_q)$. Therefore, if a prime in S is nonsplit multiplicative, their statement should just be an inclusion of $\mathcal{X}(\mathbb{Z}_p)_2$ into the union of the $\Psi(w)$. One should note, however, that it seems like this was taken care of in the computations when the Tamagawa number at q is 1, but not when it is 2 (and hence m is even).

For the same reasons, if $q = 2$ is a prime of split multiplicative reduction of type I_m, with $m > 0$, the element 0 should not be included in W_q.

We remark that in all the examples they provided the set they computed turned out to be equal to $\mathcal{X}(\mathbb{Z})$ and hence to $\mathcal{X}(\mathbb{Z}_p)_2$.

Remark 2.7. The proof of [Balakrishnan et al. 2018, Theorem 1.12] is rather technical. However, for an elliptic curve of any rank, denoting by $\mathcal{X}(\mathbb{Z})_{\text{tors}}$ the set of points of $\mathcal{X}(\mathbb{Z})$ of finite order, the easier statement

$$\mathcal{X}(\mathbb{Z})_{\text{tors}} \subseteq \bigcup_{w \in W} \{z \in \mathcal{X}(\mathbb{Z}_p) : \operatorname{Log}(z) = 0, 2D_2(z) + \|w\| = 0\} \tag{5}$$

is elementary to prove. Indeed, the condition $\operatorname{Log}(z) = 0$ cuts out the torsion points in $\mathcal{X}(\mathbb{Z}_p)$. On the other hand, let

$$\gamma = \begin{cases} C & \text{if } E \text{ is ordinary at } p, \\ \frac{1}{12}(a_1^2 + 4a_2) & \text{otherwise.} \end{cases}$$

Then we have

$$\begin{cases} \operatorname{Log}(z) = 0, \\ 2D_2(z) + \|w\| = 0 \end{cases} \iff \begin{cases} \operatorname{Log}(z) = 0 \\ 2D_2(z) + \gamma \operatorname{Log}(z)^2 + \|w\| = 0 \end{cases} \iff \begin{cases} \operatorname{Log}(z) = 0 \\ \lambda_p(z) + \|w\| = 0 \end{cases}$$

and, for $z \in \mathcal{X}(\mathbb{Z})$, $h_p(z) = \lambda_p(z) + \|w\|$ for some $w \in W$, where h_p and λ_p are the global and local p-adic heights of Section 2A. In particular, if $z \in \mathcal{X}(\mathbb{Z})_{\text{tors}}$, we have $h_p(z) = 0$. In fact, we could have also obtained a height function by setting the local height at p to be the dilogarithm $2D_2(z)$.

Proof of Theorem 1.7. The proof of part (1) is identical to the proof of Theorem 1.6(1). The proof of part (2) is straightforward from Section 2B and the proof of [Balakrishnan et al. 2018, Proposition 5.12]: the idea is that any two quadratic functions on the rank-one $E(\mathbb{Q})$ must be linearly dependent. Note that in the semistable case our statement is slightly different, as our set W is smaller if there are primes of nonsplit multiplicative reduction of type I_m, with $m > 2$ and also if $q = 2$ is a prime of split multiplicative reduction (cf. Remark 2.6). □

Remark 2.8. Theorem 1.7 is a consequence of the quadraticity of the p-adic height and of the square of the elliptic curve logarithm. Of course, that the latter function is quadratic follows from the linearity of the logarithm. We remark that Log^2 is in fact the p-adic height attached to the basis element ω of the Dieudonné module of E, in the language of generalised p-adic heights (see for instance [Stein and Wuthrich 2013, §4]), whereas the p-adic height h_p of Mazur–Tate is the one attached to an eigenvector with unit eigenvalue under the action of Frobenius. We could remove the assumption that p is ordinary in the statement of Theorem 1.7 if we replaced C with $\frac{1}{12}(a_1^2 + 4a_2)$ and let h_p be the global p-adic height that we defined in Section 2A when p is supersingular.

3. Obstructions to $\mathcal{X}(\mathbb{Z}) = \mathcal{X}(\mathbb{Z}_p)_2$ in rank 0.

We now derive some criteria for $\mathcal{X}(\mathbb{Z}_p)_2 \supsetneq \mathcal{X}(\mathbb{Z})$. In Section 4, we will compute $\mathcal{X}(\mathbb{Z}_p)_2$ for several curves and provide explicit examples for the results of this section. Since a necessary condition for $z \in \mathcal{X}(\mathbb{Z}_p)_2$ is that $\operatorname{Log}(z) = 0$, which can only occur if $z \in \mathcal{X}(\mathbb{Z}_p)_{\mathrm{tors}}$, after having fixed all appropriate embeddings, we must have

$$\mathcal{X}(\mathbb{Z}_p)_2 \subset \mathcal{E}(\overline{\mathbb{Z}})_{\mathrm{tors}} = E(\overline{\mathbb{Q}})_{\mathrm{tors}}.$$

In Section 3D we derive a stronger necessary condition, which roughly says that if a point lies in $\mathcal{X}(\mathbb{Z}_p)_2$, then its local heights cannot distinguish it from a point defined over $\mathbb{Q}$. To motivate the intuition behind this, it is more natural to first investigate sufficient conditions. In particular, we consider two reasons why extra points could arise in $\mathcal{X}(\mathbb{Z}_p)_2$: invariance of local heights under automorphism (Section 3A) and existence of noncyclotomic local heights over certain number fields (Section 3B). Sometimes, a combination of the two is needed, as is the case in Proposition 3.14, which provides us with infinitely many curves over $\mathbb{Q}$ with points over a quartic field appearing in $\mathcal{X}(\mathbb{Z}_p)_2$ for suitable choices of p. In Section 3C, we use this to deduce Theorem 1.4.

We start by proving an elementary fact: any obstruction to $\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z})$ must come from points defined over number fields larger than $\mathbb{Q}$.

Proposition 3.1. *Suppose that E satisfies the assumptions of Theorem 1.6(2) and that p is an odd prime of good reduction. Then*

$$\mathcal{X}(\mathbb{Z}_p)_2 \cap \mathcal{E}(\mathbb{Z}) = \mathcal{X}(\mathbb{Z}).$$

Proof. Suppose $P \in \mathcal{X}(\mathbb{Z}_p)_2 \cap \mathcal{E}(\mathbb{Z})$. In particular, $\operatorname{Log}(P) = 0$, so P is torsion and hence $h_p(P) = 0$. On the other hand, since $P \in \mathcal{X}(\mathbb{Z}_p)_2$,

$$\lambda_p(P) + \|w\| = 0$$

for some $w \in W$. Therefore,

$$\sum_{q \neq p} \lambda_q(P) = \|w\|.$$

By definition, we have

$$\sum_{q \neq p} \lambda_q(z) = \sum_{q \neq p} \alpha_q \log q, \qquad \|w\| = \sum_{q \neq p} \beta_q \log q$$

for some $\alpha_q, \beta_q \in \mathbb{Q}$, $\alpha_q = 0$ for all but finitely many q, $\beta_q = 0$ for all $q \notin S$ and $\beta_q \leq 0$ for all q. Thus

$$\log\Bigl(\prod_{q \neq p} q^{d(\alpha_q - \beta_q)}\Bigr) = 0,$$

for some nonzero integer d such that $d(\alpha_q - \beta_q) \in \mathbb{Z}$ for all q. This implies that $\alpha_q = \beta_q$ for all q, since the kernel of the p-adic logarithm is the subgroup of $\mathbb{Q}_p^\times$ generated by p and by the roots of unity. Suppose that z is not integral at q. Then by Lemma 2.1(i), $\alpha_q > 0$, but $\beta_q \leq 0$, a contradiction. □

Remark 3.2. According to [Silverman 2009, VII Application 3.5], if $P \in \mathcal{E}(\mathbb{Z})_{\mathrm{tors}}$ then P is integral at all primes except possibly at 2 if P is 2-torsion. Thus the only q for which the proof of Proposition 3.1 is nonempty is $q = 2$. However, note that, with minor changes, the same proof shows the perhaps less trivial fact that $\mathcal{X}(\mathbb{Z}_p)'_2 \cap \mathcal{E}(\mathbb{Z}) = \mathcal{X}(\mathbb{Z})$ in rank 1.

Remark 3.3. Unlike in Section 2A, given a prime v of a number field, henceforth the notation λ_v will be used for the local height at v computed with respect to the model $\mathcal{E}$, which may not be minimal at v. The translation with the values computed with respect to a minimal model (Lemma 2.1 and Proposition 2.4) is given by (4).

3A. ***Automorphisms.*** Recall that local heights are even functions. Therefore, if K is a quadratic field with $\mathrm{Gal}(K/\mathbb{Q}) = \langle\tau\rangle$ and $z \in \mathcal{X}(\mathcal{O}_K)$ satisfies $\tau(z) = -z$, then

$$h_p(z) = \sum_q \lambda_{\mathfrak{q}}(z) = \lambda_{\mathfrak{p}}(z) + \sum_{q \in S} \lambda_{\mathfrak{q}}(z),$$

where $\mathfrak{q}$ (resp. $\mathfrak{p}$) is any prime of K above q (resp. p). Intuitively, in terms of local p-adic heights, the point z behaves as if it were defined over $\mathbb{Q}$; if furthermore z is a torsion point and p is split in K, then z will give rise to a point in $\mathcal{X}(\mathbb{Z}_p)_2$, provided that $\lambda_{\mathfrak{q}}(z) \in W_q$ at every $q \in S$. If the j-invariant of E is different from 0 and 1728, the automorphism group of $E/\overline{\mathbb{Q}}$ is generated by $z \mapsto -z$. On the other hand, if $j(E) \in \{0, 1728\}$, we can use the invariance of our local heights under any automorphism (cf. property (v) in Section 2A1 and property (iv) in Section 2A2) to generalise the above example as follows.

Proposition 3.4. *Suppose that E satisfies the assumptions of Theorem 1.6 and that p is an odd prime of good reduction. Let K be a Galois extension of $\mathbb{Q}$, such that there is an embedding $\rho : K \hookrightarrow \mathbb{Q}_p$. Extend ρ to a map $\mathcal{E}(\mathcal{O}_K) \hookrightarrow \mathcal{E}(\mathbb{Z}_p)$. Let $z \in \mathcal{X}(\mathcal{O}_K)_{\mathrm{tors}}$ and suppose that for every $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ there exists $\psi_\tau \in \mathrm{Aut}(E/\overline{\mathbb{Q}})$ such that $\tau(z) = \psi_\tau(z)$.*

(1) *For each rational prime q, let $\mathfrak{q}$ be one (any) prime of K above q and let $\lambda_{\mathfrak{q}}$ be the local height at $\mathfrak{q}$ with respect to the model $\mathcal{E}$. If*

$$\sum_{q \in S} \lambda_{\mathfrak{q}}(z) = \|w\|$$

for some $w \in W$, then $\rho(z) \in \mathcal{X}(\mathbb{Z}_p)_2$.

(2) *In particular, if $z = \psi'(P)$ for some $\psi' \in \mathrm{Aut}(E/\overline{\mathbb{Q}})$ and some $P \in \mathcal{X}(\mathbb{Z})$, then $\rho(z) \in \mathcal{X}(\mathbb{Z}_p)_2$.*

Proof. The assumption that z is a torsion point implies that $h_p(z) = 0$ and $\mathrm{Log}(z) = 0$. Since for $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ there is an automorphism ψ_τ of E which acts on z in the same way as τ and local heights are invariant under automorphisms, for each prime $\mathfrak{q}$ of K we have

$$\lambda_{\mathfrak{q}}(z) = \lambda_{\mathfrak{q}}(\psi_\tau(z)) = \lambda_{\mathfrak{q}}(\tau(z)) = \lambda_{\tau^{-1}(\mathfrak{q})}(z).$$

Therefore,

$$0 = [K : \mathbb{Q}]h_p(z) = [K : \mathbb{Q}]\Bigl(\lambda_p(\rho(z)) + \sum_{q \in S} \lambda_{\mathfrak{q}}(z)\Bigr)$$

and (1) follows. For (2), since $z=\psi'(P)$, we have, similarly to above,

$$\lambda_{\mathfrak{q}}(z)=\lambda_{\mathfrak{q}}(\psi'(P))=\lambda_q(P).$$

In particular, the hypothesis of (1) is satisfied. □

We now list a few consequences of Proposition 3.4. See Section 4 for explicit examples.

Corollary 3.5. *Suppose that E satisfies the assumptions of Theorem 1.6 and that p is an odd prime of good ordinary reduction. Suppose that*

$$\mathcal{E}: y^2+a_3y=x^3+a_6 \quad \textit{for some } a_6\in\mathbb{Z} \textit{ and } a_3\in\{0,1\},$$

and that there exists $y_0\in\mathbb{Z}$ such that $a_6-y_0^2-a_3y_0$ is a cube in $\mathbb{Z}$ and the points over $\overline{\mathbb{Q}}$ with y-coordinate equal to y_0 have finite order. Then $s(x)=x^3+a_6-y_0^2-a_3y_0$ splits completely in $\mathbb{Q}_p$ and for each root $\alpha\in\mathbb{Z}_p$ of $s(x)$, $\pm(\alpha,y_0)\in\mathcal{X}(\mathbb{Z}_p)_2$.

Remark 3.6. If in the corollary we have $a_3=1$, then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to a subgroup of $\mathbb{Z}/3\mathbb{Z}$, since $E(\mathbb{Q})[2]=\{O\}$ and E has good reduction at 2 with $\#\bar{E}(\mathbb{F}_2)=3$. By looking at the third division polynomial for E, it is then straightforward to check that Corollary 3.5 applies nontrivially only if $4a_6=-(27n^6+1)$ for some $n\in\mathbb{Z}$, $n\equiv 1 \bmod 2$. All such curves are isomorphic over $\mathbb{Q}$ to the elliptic curve 27.a3 [LMFDB 2019]. When $a_3=0$, there are infinitely many curves nonisomorphic over $\mathbb{Q}$ for which the corollary applies with $y_0=0$: see for example Section 3C. There is also at least one curve for which the Corollary applies to points of order 6, namely 36.a4 (see Table 2).

Proof. Since E has vanishing j-invariant, its automorphism group $\operatorname{Aut}(E/\overline{\mathbb{Q}})$ is a cyclic group of order 6 generated by $\psi: E\to E$, $\psi(x,y)=(\zeta x,-y-a_3)$, for a primitive third root of unity ζ.

Let $x_0\in\mathbb{Z}$ such that $x_0^3=y_0^2+a_3y_0-a_6$. We may assume that $y_0^2+a_3y_0-a_6$ is nonzero, as otherwise the statement of the corollary is trivial. Thus $s(x)$ has three distinct roots x_0, ζx_0 and ζ^2x_0 in $\overline{\mathbb{Z}}$.

Note also that, by Deuring's criterion [Lang 1973, Chapter 13, Theorem 12], the primes of good ordinary reduction for E split completely in $\mathbb{Q}(\zeta)$, so $s(x)$ splits completely over $\mathbb{Q}_p$. Successively applying ψ to $(x_0,y_0)\in\mathcal{X}(\mathbb{Z})$ and localising at p we obtain all points of the form $\pm(\alpha,y_0)$. The corollary then follows from Proposition 3.4(2). □

The following corollary to Proposition 3.4 is a special case of the motivating example of the beginning of this subsection.

Corollary 3.7. *Suppose that E satisfies the assumptions of Theorem 1.6 and that p is an odd prime of good reduction. Let K be a quadratic field, in which p splits. Fix an embedding $\rho: K\hookrightarrow\mathbb{Q}_p$ and let τ be the nontrivial element in* $\operatorname{Gal}(K/\mathbb{Q})$. *Assume that no prime in S ramifies in K and that, if $q\in S$ is inert, then either E has Kodaira symbol* I_0^* *at q with Tamagawa number at least* 2 *or E has maximal Tamagawa number for its Kodaira symbol. Then*

$$\mathcal{X}(\mathbb{Z}_p)_2\supset\mathcal{X}(\mathbb{Z})\cup\{\rho(z)\in\mathcal{X}(\mathbb{Z}_p): z\in\mathcal{X}(\mathcal{O}_K)_{\text{tors}},\ \tau(z)=-z\}.$$

Proof. Since no prime in S ramifies in $K/\mathbb{Q}$, Tate's algorithm [Silverman 1994, IV, §9] shows that the equation for $\mathcal{E}$ defines a global minimal model for the base change E/K and that the Kodaira symbol at $\mathfrak{q} \mid q$ is the same as the Kodaira symbol at q. The Tamagawa number does not change if q is split in K; if q is inert, by assumption the Tamagawa number is unvaried, except possibly if the Kodaira symbol is I_0^*.

If q splits in K, fix a prime $\mathfrak{q}$ above it and an isomorphism $\rho_q : K_{\mathfrak{q}} \simeq \mathbb{Q}_q$. Let $z \in \mathcal{X}(\mathcal{O}_K)_{\mathrm{tors}}$ such that $\tau(z) = -z$. With the notation as in Proposition 3.4 and by Proposition 2.4, we have

$$\sum_{q\in S} \lambda_{\mathfrak{q}}(z) = \sum_{\substack{q\in S\\ q \text{ split}}} \lambda_q(\rho_q(z)) + \sum_{\substack{q\in S\\ q \text{ inert}}} \lambda_{\mathfrak{q}}(z) = \|w\|$$

for some $w \in W$. For the last step note that Proposition 2.4 gives the values of $2\lambda_{\mathfrak{q}}(z)$ for $\mathfrak{q}$ inert. However, the norm of $\mathfrak{q}$ is q^2. The corollary then follows from Proposition 3.4(1) with $\psi = -\mathrm{id} \in \mathrm{Aut}(E/\overline{\mathbb{Q}})$. □

Remark 3.8. Another source of quadratic points in $\mathcal{X}(\mathbb{Z}_p)_2$ comes from elliptic curves with j-invariant equal to 1728. Suppose that E satisfies the assumptions of Theorem 1.6, that p is an odd prime of good reduction and that

$$\mathcal{E} : y^2 = x^3 + a_4 x \quad \text{for some } a_4 \in \mathbb{Z},\ -a_4 \notin \mathbb{Z}^2.$$

Let $z \in \{(\pm\sqrt{-a_4}, 0)\}$ and $K = \mathbb{Q}(\sqrt{-a_4})$ be its field of definition. Let $\psi \in \mathrm{Aut}(E/\overline{\mathbb{Q}})$ be defined by $\psi(x, y) = (-x, iy)$. Then $\psi(z) = \tau(z)$, where $\mathrm{Gal}(K/\mathbb{Q}) = \langle\tau\rangle$. Therefore, under suitable conditions on how the reduction types change in $K/\mathbb{Q}$ and on the splitting of p in K, the localisations of the points z appear in $\mathcal{X}(\mathbb{Z}_p)_2$.

The following corollary explains how points over biquadratic extensions can show up in $\mathcal{X}(\mathbb{Z}_p)_2$ when the j-invariant is zero. For ease of notation, we assume that the a_3-coefficient in the equation defining $\mathcal{E}$ is zero, but this assumption could be removed.

Corollary 3.9. *Suppose that E satisfies the assumptions of Theorem 1.6 and that p is an odd prime of good ordinary reduction. Suppose that*

$$\mathcal{E} : y^2 = x^3 + a_6 \quad \textit{for some } a_6 \in \mathbb{Z}$$

and that there exists $x_0 \in \mathbb{Z}$ such that the points over $\overline{\mathbb{Q}}$ with x-coordinate equal to x_0 have finite order. Assume that p splits in $\mathbb{Q}(\sqrt{x_0^3 + a_6})$. Let $K = \mathbb{Q}(\sqrt{-3}, \sqrt{x_0^3 + a_6})$. For each rational prime q, let $\mathfrak{q}$ be one (any) prime of K above q and $\lambda_{\mathfrak{q}}$ the local height at $\mathfrak{q}$ with respect to the model $\mathcal{E}$. Let $\beta \in \mathbb{Z}_p$ be a root of $t(y) = y^2 - x_0^3 - a_6$. If

$$\sum_{q\in S} \lambda_{\mathfrak{q}}(x_0, \beta) = \|w\|$$

for some $w \in W$, then for each root $\alpha \in \mathbb{Z}_p$ of $s(x) = x^3 - x_0^3$ and for each root $\beta \in \mathbb{Z}_p$ of $t(y) = y^2 - x_0^3 - a_6$, we have $(\alpha, \beta) \in \mathcal{X}(\mathbb{Z}_p)_2$.

Proof. If $x_0^3 + a_6$ is a square in $\mathbb{Z}$, the statement is precisely Corollary 3.5. Thus, we may assume that either

(i) K has degree 4 over $\mathbb{Q}$, or

(ii) $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\sqrt{x_0^3 + a_6})$.

Let $\zeta \in K$ be a primitive third root of unity. The automorphism group $\operatorname{Aut}(E/K)$ is generated by $\psi : E \to E$, $\psi(x, y) = (\zeta x, -y)$. In case (i), the Galois group of K over $\mathbb{Q}$ is generated by two elements: σ, whose fixed field is $\mathbb{Q}(\sqrt{x_0^3 + a_6})$ and τ, whose fixed field is $\mathbb{Q}(\sqrt{-3})$. In case (ii), the Galois group is generated by $\sigma : \sqrt{-3} \mapsto -\sqrt{-3}$. Let $P = (a, b)$ where $a \in K$ is a root of $s(x)$ and $b \in K$ is a root of $t(y)$. Then in (i)

$$\sigma(P) \in \{P, -\psi(P), \psi^2(P)\}, \qquad \tau(P) = -P.$$

Similarly, in case (ii), we have

$$\sigma(P) \in \{-P, \psi(P), -\psi^2(P)\}.$$

Therefore, we may apply Proposition 3.4(1). □

3B. *Noncyclotomic p-adic heights.* The set $\mathcal{X}(\mathbb{Z}_p)_2$ is a finite set of p-adic points containing $\mathcal{X}(\mathbb{Z})$. After having fixed a choice of a subspace of $H^1_{\mathrm{dR}}(E/\mathbb{Q}_p)$ complementary to the space of holomorphic forms, there is only one Coleman–Gross global height pairing on $E(\mathbb{Q})$, up to multiplication by a constant. The definition of $\mathcal{X}(\mathbb{Z}_p)_2$ depends on this height function. Nevertheless, when analysing what points could arise in the set $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$, we should bear in mind that other global height functions may exist on $E(F)$, where F is a number field, and that these also vanish on $E(F)_{\mathrm{tors}}$. In particular, suppose that there exists at least one embedding $\rho : F \hookrightarrow \mathbb{Q}_p$. It may happen that, for some $w \in W$ and some $Q \in \mathcal{X}(\mathcal{O}_F)$,

$$2D_2(\rho(Q)) + \gamma \operatorname{Log}(\rho(Q))^2 + \|w\| = h_p^\star(Q)$$

for some noncyclotomic global height $h_p^\star$. Then, if Q is in addition a torsion point, we have $\rho(Q) \in \mathcal{X}(\mathbb{Z}_p)_2$.

In order to introduce these more general types of heights, we need to recall the definition and properties of an idele class character.

Definition 3.10. Let $\mathbb{A}_F^\times$ be the group of ideles of F. An idele class character is a continuous homomorphism

$$\chi = \sum_{\mathfrak{q}} \chi_{\mathfrak{q}} : \mathbb{A}_F^\times / F^\times \to \mathbb{Q}_p;$$

here the sum is over all places of F.

We list some properties of an idele class character χ (see [Balakrishnan et al. 2019b] for more details).

(PI) The local character $\chi_{\mathfrak{q}}$ is trivial at an archimedean place $\mathfrak{q}$. Thus, henceforth $\mathfrak{q}$ will always denote a finite prime.

(PII) At a prime $\mathfrak{q}$ not above p, the local character $\chi_{\mathfrak{q}}$ vanishes on the units $\mathcal{O}_{\mathfrak{q}}^\times$. Thus, the value of $\chi_{\mathfrak{q}}$ at a uniformiser determines $\chi_{\mathfrak{q}}$ completely.

(PIII) At a prime $\mathfrak{p}$ above p, the restriction of the character $\chi_{\mathfrak{p}}$ to $\mathcal{O}_{\mathfrak{p}}^{\times}$ equals the composition

$$\mathcal{O}_{\mathfrak{p}}^{\times} \xrightarrow{\log_{\mathfrak{p}}} F_{\mathfrak{p}} \xrightarrow{t_{\mathfrak{p}}} \mathbb{Q}_p$$

for some $\mathbb{Q}_p$-linear map $t_{\mathfrak{p}}$. Here $\log_{\mathfrak{p}}$ is the restriction to $\mathcal{O}_{\mathfrak{p}}^{\times}$ of the extension of log to $F_{\mathfrak{p}}^{\times}$.

(PIV) The character χ is completely determined by the trace maps $(t_{\mathfrak{p}})_{\mathfrak{p}|p}$ and, conversely, a tuple of $\mathbb{Q}_p$-linear maps $(t_{\mathfrak{p}} : F_{\mathfrak{p}} \to \mathbb{Q}_p)_{\mathfrak{p}|p}$ gives an idele class character χ if and only if

$$\sum_{\mathfrak{p}|p} t_{\mathfrak{p}}(\log_{\mathfrak{p}}(\rho_{\mathfrak{p}}(\epsilon))) = 0 \quad \text{for all } \epsilon \in \mathcal{O}_F^{\times}, \tag{6}$$

where $\rho_{\mathfrak{p}} : F \hookrightarrow F_{\mathfrak{p}}$ is the completion (see [Balakrishnan et al. 2019b] for a proof).

In particular, it suffices to check that (6) is satisfied for a set of fundamental units and (PIV) gives a concrete method for classifying all idele class characters for a given number field F. The maximal number of independent characters is at least $r_2 + 1$, where r_2 is the number of conjugate pairs of nonreal embeddings of F into $\mathbb{C}$ (with equality if Leopoldt's conjecture holds for F).

For instance, for any number field F, the *cyclotomic* idele class character is the idele class character corresponding to the tuple of trace maps $(\mathrm{tr}_{F_{\mathfrak{p}}/\mathbb{Q}_p})_{\mathfrak{p}|p}$. When $F = \mathbb{Q}$ (or F is a totally real abelian number field), this is the only nontrivial idele class character, up to multiplication by a scalar. The p-adic height we have considered so far is implicitly associated to this character.

More generally though, we can define a p-adic height as a composition of two maps: firstly, we associate to a point $P \in E(F)$ an idele $i(P)$ and, secondly, we apply to $i(P)$ an idele class character χ. We denote the corresponding local and global heights by $\lambda_{\mathfrak{q}}^{\chi}$ and h_p^{χ}, respectively. The theory of local heights that we outlined in the cyclotomic case in Section 2A goes through unvaried at the primes $\mathfrak{q} \nmid p$, after replacing the p-adic logarithm with $-\chi_{\mathfrak{q}}/n_{\mathfrak{q}}$. At the primes $\mathfrak{p} \mid p$, we may assume here that we always work with points not in the residue disk of the point at infinity.[5] So let $z \in \mathcal{X}(\mathcal{O}_{\mathfrak{p}})$ and $m \in \mathbb{N}$ such that mz is in the domain of convergence of $\sigma_{\mathfrak{p}}^{(\gamma)}$. Then

$$\lambda_{\mathfrak{p}}^{\chi}(z) = -\frac{2}{m^2}\frac{\chi_{\mathfrak{p}}}{n_{\mathfrak{p}}}\left(\frac{\sigma_{\mathfrak{p}}^{(\gamma)}(mz)}{f_m(z)}\right) = -\frac{2}{m^2 n_{\mathfrak{p}}} t_{\mathfrak{p}}\left(\log_{\mathfrak{p}}\left(\frac{\sigma_{\mathfrak{p}}^{(\gamma)}(mz)}{f_m(z)}\right)\right), \tag{7}$$

since

$$\mathrm{ord}_{\mathfrak{p}}(\sigma_{\mathfrak{p}}^{(\gamma)}(mz)) = \mathrm{ord}_{\mathfrak{p}}(x(mz)y(mz)^{-1}) = \mathrm{ord}_{\mathfrak{p}}(f_m(z))$$

(see Section 4A and the proof of Theorem 3.18 for how to interpret (7) when $mz = O$). We will omit χ from our notation when using the cyclotomic character.

Example 3.11. Let F be an imaginary quadratic field in which p splits. Then by (PIV), any pair of $\mathbb{Q}_p$-linear maps $\mathbb{Q}_p \to \mathbb{Q}_p$ gives rise to an idele class character. In particular, choosing (id, −id) gives the so-called *anticyclotomic* character.

[5] There is a subtlety in the disk at infinity which has to do with the choice of branch of the $\mathfrak{p}$-adic logarithm. See also [Balakrishnan et al. 2019b, Remark 2.1].

We now give an instance of how the existence of noncyclotomic heights for imaginary quadratic fields can give rise to points in $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$.

Proposition 3.12. *Suppose that E satisfies the assumptions of Theorem 1.6 and that p is an odd prime of good reduction. Let K be an imaginary quadratic field in which p splits. Fix an embedding $\rho : K \hookrightarrow \mathbb{Q}_p$. Suppose that $z \in \mathcal{X}(\mathcal{O}_K)_{\mathrm{tors}}$ has good reduction at all primes that split in K. Then*

$$2D_2(\rho(z)) + \sum_{q\in S} \lambda_{\mathfrak{q}}(z) = 0,$$

where $\mathfrak{q}$ is a prime of K above q. In particular, if $\sum_{q\in S} \lambda_{\mathfrak{q}}(z) = \|w\|$ for some $w \in W$, then $\rho(z) \in \mathcal{X}(\mathbb{Z}_p)_2$.

Proof. It suffices to show that $2D_2(\rho(z)) + \sum_{q\in S} \lambda_{\mathfrak{q}}(z)$ is the value at z of a height function on $E(K)$, since then the assumption that z is a torsion point will imply the vanishing. The height function that we are after is the one corresponding to an idele class character $\mathbb{A}_K^\times / K^\times \to \mathbb{Q}_p$ which vanishes on $\mathcal{O}_{\bar{\mathfrak{p}}}^\times$, if $\mathfrak{p}$ is the prime corresponding to the embedding ρ. Indeed, with the notation of (PIV), consider the idele class character corresponding to $(\mathrm{id} : K_{\mathfrak{p}} \simeq \mathbb{Q}_p \to \mathbb{Q}_p, 0 : K_{\bar{\mathfrak{p}}} \simeq \mathbb{Q}_p \to \mathbb{Q}_p)$. Then

$$\lambda_{\mathfrak{p}}(z) = \lambda_{\mathfrak{p}}^{\chi}(z) \quad \text{and} \quad \lambda_{\bar{\mathfrak{p}}}^{\chi}(z) = 0.$$

Further, since χ factors through $\mathbb{A}_K^\times / K^\times$ and in view of (PII), if there is a unique prime $\mathfrak{q}$ above q, we have

$$\chi_{\mathfrak{q}}(q) = -\chi_{\mathfrak{p}}(q) - \chi_{\bar{\mathfrak{p}}}(q) = -\log(q),$$

so that $2\lambda_{\mathfrak{q}}^{\chi} = \lambda_{\mathfrak{q}}$ for all primes which are either inert or ramified. Thus $2h_p^{\chi}(z) = 2D_2(\rho(z)) + \sum_{q\in S} \lambda_{\mathfrak{q}}(z)$. □

In some cases, extra points in $\mathcal{X}(\mathbb{Z}_p)_2$ are explained by a combination of automorphisms and noncyclotomic idele class characters, as in Proposition 3.14. Before we state it and prove it, we first need an auxiliary lemma.

Lemma 3.13. *Let F be a number field and let L be a finite extension of F. Suppose that $\chi : \mathbb{A}_F^\times / F^\times \to \mathbb{Q}_p$ is an idele class character determined by the tuple of $\mathbb{Q}_p$-linear maps $(t_{\mathfrak{p}} : F_{\mathfrak{p}} \to \mathbb{Q}_p)_{\mathfrak{p}\mid p}$. Then the tuple $(t_{\mathfrak{q}}^L : L_{\mathfrak{q}} \to \mathbb{Q}_p)_{\mathfrak{q}\mid p}$, defined by $t_{\mathfrak{q}}^L = t_{\mathfrak{p}} \circ \mathrm{tr}_{L_{\mathfrak{q}}/F_{\mathfrak{p}}}$ for $\mathfrak{q} \mid \mathfrak{p}$, determines an idele class character $\chi^L : \mathbb{A}_L^\times / L^\times \to \mathbb{Q}_p$ such that $\chi^L|_{\mathbb{A}_F^\times / F^\times} = [L : F]\chi$.*

Proof. Each $t_{\mathfrak{q}}^L$ is $\mathbb{Q}_p$-linear as a composition of $\mathbb{Q}_p$-linear maps. We need to check that (PIV) is satisfied. If $\epsilon \in \mathcal{O}_L^\times$, then

$$\begin{aligned}\sum_{\mathfrak{q}\mid p} t_{\mathfrak{q}}^L(\log_{\mathfrak{q}}(\rho_{\mathfrak{q}}(\epsilon))) = \sum_{\mathfrak{p}\mid p} t_{\mathfrak{p}} \circ \Bigl(\sum_{\mathfrak{q}\mid \mathfrak{p}} \mathrm{tr}_{L_{\mathfrak{q}}/F_{\mathfrak{p}}} \circ \log_{\mathfrak{q}}(\rho_{\mathfrak{q}}(\epsilon))\Bigr) &= \sum_{\mathfrak{p}\mid p} t_{\mathfrak{p}} \circ \log_{\mathfrak{p}} \Bigl(\prod_{\mathfrak{q}\mid \mathfrak{p}} N_{L_{\mathfrak{q}}/F_{\mathfrak{p}}}(\rho_{\mathfrak{q}}(\epsilon))\Bigr) \\ &= \sum_{\mathfrak{p}\mid p} t_{\mathfrak{p}} \circ \log_{\mathfrak{p}} \bigl(\rho_{\mathfrak{p}}(N_{L/F}(\epsilon))\bigr) = 0,\end{aligned}$$

since $N_{L/F}(\epsilon) \in \mathcal{O}_F^\times$. By construction, the resulting idele class character χ^L restricts to $[L : F]\chi$ on $\mathbb{A}_F^\times / F^\times$. □

Proposition 3.14. *Let d be a nonzero square-free integer and let E^d be the quadratic twist of $X_0(49)$ by d; assume that E^d satisfies the assumptions of Theorem 1.6 and let $\mathcal{X}^d$ be the complement of the origin in the minimal regular model of E^d. Let $p \nmid 7d$ be an odd prime with at least 3 primes lying above it in $L = \mathbb{Q}[x]/(x^4+7d^2)$. Then*

$$\mathcal{X}^d(\mathbb{Z}_p)_2 \supseteq \mathcal{X}^d(\mathbb{Z}) \cup \{\pm\rho(Q)\}$$

for some $Q \in \mathcal{X}^d(\mathcal{O}_L)$ of order 4 and for every embedding $\rho : L \hookrightarrow \mathbb{Q}_p$.

Remark 3.15. The proposition also holds in rank 1 if we replace $\mathcal{X}^d(\mathbb{Z}_p)_2$ with $\mathcal{X}^d(\mathbb{Z}_p)_2'$.

Proof. The elliptic curve $E = X_0(49)$ has reduced minimal model

$$\mathcal{E} : y^2 + xy = x^3 - x^2 - 2x - 1; \tag{8}$$

however, since we are considering quadratic twists of E, it is more convenient to work (at least until we introduce heights) with the model

$$\mathcal{E}_{\text{short}} : y^2 = x^3 - 2835x - 71442,$$

as then the twist E^d of E by the nonzero square-free integer d admits the Weierstrass equation

$$\mathcal{E}^d_{\text{short}} : y^2 = x^3 - 2835d^2x - 71442d^3.$$

Recall that E^d has complex multiplication by $K = \mathbb{Q}(a)$, where a is a root of x^2+7. Over $K[x, y]$, the fourth division polynomial f_4^d of $\mathcal{E}^d_{\text{short}}$ has the factorisation

$$f_4^d(x, y) = 4y(x - 9ad)(x + 9ad)(x + (-18a + 63)d)(x + (18a + 63)d)(x^2 - 126xd - 5103d^2).$$

In particular, since

$$x^3 - 2835d^2x - 71442d^3 = (x - 63d)(x + (-9/2a + 63/2)d)(x + (9/2a + 63/2)d),$$

all the points of order 2 are defined over K. As for the points of order 4, we see that, as a polynomial in x, $f_4^d(x, y)/y$ has two roots in $\mathbb{Q}(\sqrt{7})$ and four roots in K. Substituting the latter roots into the equation for $\mathcal{E}^d_{\text{short}}$, we find that the y-coordinates of the points with $x = 9ad$ and $x = -(18a + 63)d$ are defined over $\mathbb{Q}(\sqrt{-ad})$, whereas those with $x = -9ad$ and $x = -(-18a + 63)d$ are over $\mathbb{Q}(\sqrt{ad})$.

Therefore, over the quartic field $L = K[x]/(x^2 - ad) = K(b) \cong \mathbb{Q}[x]/(x^4+7d^2)$, $E^d(L)[4] \cong \mathbb{Z}/2 \times \mathbb{Z}/4$. Let $\mathrm{Gal}(L/K) = \langle \bar{\tau} \rangle$ and let

$$Q_{\text{short}} = (18b^2 - 63d, \pm(54b^3 - 378bd)) \in \mathcal{E}^d_{\text{short}}(L)[4], \qquad P_{\text{short}} = (63d, 0).$$

Then Q_{short} satisfies

$$\bar{\tau}(Q_{\text{short}}) = -Q_{\text{short}}. \tag{9}$$

Let Q be the image of Q_{short} in a minimal model $\mathcal{E}^d$ for E^d over $\mathbb{Z}$ and let P be the image of P_{short}. Note that

- if $d \equiv 1 \mod 4$, we may apply to $\mathcal{E}^d_{\text{short}}$ the change of variables
$$x \mapsto 36x - 9d, \qquad y \mapsto 216y + 108x$$
to obtain the integral model
$$\mathcal{E}^d_1 : y^2 + xy = x^3 - \frac{3d+1}{4}x^2 - 2d^2x - d^3.$$
The discriminant of $\mathcal{E}^d_1$ is $\Delta = -7^3d^6$, so by [Silverman 2009, VII, Remark 1.1] $\mathcal{E}^d_1$ is a minimal model for $E^d/\mathbb{Q}$ and we may set $\mathcal{E}^d = \mathcal{E}^d_1$. Then $x(P) = 2d \in \mathbb{Z}$ and $x(Q) \in \mathcal{O}_K$.
- if $d \equiv 2, 3 \mod 4$, then we may take
$$\mathcal{E}^d : y^2 = x^3 - 3dx^2 - 32d^2x - 64d^3,$$
which has discriminant $\Delta = -2^{12} \cdot 7^3 \cdot d^6$. Minimality of $\mathcal{E}^d$ at the primes different from 2 follows as in the case $d \equiv 1 \mod 4$. At the prime 2, it can be deduced following Tate's algorithm. We have $x(P) = 8d \in \mathbb{Z}$ and $x(Q) \in \mathcal{O}_K$.

Now, let p be an odd prime of good reduction for E^d which splits in K. By Deuring's criterion, this is equivalent to requiring that p is a prime of good ordinary reduction. Let $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. The prime p is unramified also in L, since we are assuming that it is of good reduction. We suppose furthermore that $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1\overline{\mathfrak{q}_1}$, $\bar{\mathfrak{p}}\mathcal{O}_L = \mathfrak{q}_2$ or $\bar{\mathfrak{p}}\mathcal{O}_L = \mathfrak{q}_2\overline{\mathfrak{q}_2}$, for some primes $\mathfrak{q}_1$ and $\mathfrak{q}_2$ of L. These conditions, together, are equivalent to those of the statement of the proposition.

By Lemma 3.13, the idele class character on $\mathbb{A}_K^\times/K^\times$ which is trivial on $\mathcal{O}_{\bar{\mathfrak{p}}}^\times$ (and which we used also in the proof of Proposition 3.12) extends to an idele class character on $\mathbb{A}_L^\times/L^\times$. In particular, the tuple of linear maps
$$\biggl(\mathrm{id}_{L_{\mathfrak{q}_1} \simeq \mathbb{Q}_p}, \mathrm{id}_{L_{\overline{\mathfrak{q}_1}} \simeq \mathbb{Q}_p}, 0 : \prod_{\mathfrak{q}\mid\bar{\mathfrak{p}}} L_{\mathfrak{q}} \to \mathbb{Q}_p\biggr)$$
determines an idele class character χ. Consider the associated global height h_p^χ on $E^d(L)$ with local heights λ_v^χ with respect to the model $\mathcal{E}^d$. Since Q is a torsion point, we must have
$$h_p^\chi(Q) = 0.$$
It follows from (9) and the definition of χ that
$$\lambda^\chi_{\mathfrak{q}_1}(Q) = \lambda^\chi_{\overline{\mathfrak{q}_1}}(Q) = \lambda_{\mathfrak{q}_1}(Q) \quad \text{and} \quad \lambda^\chi_{\mathfrak{q}}(Q) = 0 \quad \text{for } \mathfrak{q} \mid \bar{\mathfrak{p}}.$$
Furthermore, using (PII) and the fact that χ is trivial on $L^\times$, we find that, for a fixed rational prime ℓ,
$$\sum_{v\mid\ell} \chi_v(\ell) = -2\log\ell. \tag{10}$$

Since $P \in \mathcal{X}^d(\mathbb{Z})$, where $\mathcal{X}^d$ is the complement of the origin in $\mathcal{E}^d$, in order to prove the proposition it then suffices to show that

$$\frac{1}{2}\sum_{v \nmid p} n_v \lambda_v^{\chi}(Q) = \sum_{\ell \nmid p} \lambda_\ell(P),$$

where the left sum runs over primes of L and the right sum over rational primes.

In view of Lemma 3.13 and (4), we are allowed to perform isomorphisms over extensions of L to calculate local heights. In particular, the change of variables $(x, y) \mapsto (36dx - 9d, 216d\sqrt{d}y + 108d\sqrt{d}x)$, defined over $\mathbb{Q}(\sqrt{d})$, maps $\mathcal{E}^d_{\text{short}}$ to (8), which has discriminant -7^3. Under this isomorphism,

$$x(P_{\text{short}}) \mapsto 2 \in \mathbb{Z} \quad \text{and} \quad x(Q_{\text{short}}) \mapsto \frac{a-3}{2} \in \mathcal{O}_K.$$

Therefore, the local heights of P and Q away from $7p$ are trivial when computed with respect to (8). Using (10) and letting $d' = 7^{-\operatorname{ord}_7(d)}d$, we then have

$$\frac{1}{2}\sum_{v \nmid 7p} n_v \lambda_v^{\chi}(Q) = -\frac{1}{12[F:L]}\sum_{w \nmid 7p} \chi_w^F(\Delta^{-1}) = \begin{cases} -\log d' & \text{if } d \equiv 1 \bmod 4, \\ -\log 4d' & \text{otherwise,} \end{cases}$$

where $F = L(\sqrt{d})$, the second sum runs over the primes w of F and the character χ^F is the idele class character of F obtained from χ as in Lemma 3.13. Similarly, to calculate heights of P away from $7p$ we may base change to $\mathbb{Q}(\sqrt{d})$ and get

$$\sum_{\ell \nmid 7p} \lambda_\ell(P) = \frac{1}{2}\sum_{u \nmid 7p} n_u \lambda_u(P) = \frac{1}{2}\sum_{u \nmid 7p} \frac{n_u}{6}\log(|\Delta|_u) = \begin{cases} -\log d' & \text{if } d \equiv 1 \bmod 4, \\ -\log 4d' & \text{otherwise,} \end{cases}$$

where u runs over primes of $\mathbb{Q}(\sqrt{d})$.

It remains to calculate the local contributions at primes above 7. For this, it is convenient to work with $\mathcal{E}^d_{\text{short}}$ which is minimal over $\mathbb{Z}_7$. Let v be the unique prime above 7 in L. Then $\operatorname{ord}_v(\Delta) = 12 + 24\operatorname{ord}_7(d)$. On the other hand, by [Silverman 2009, VII, Exercise 7.2], a minimal equation at v has discriminant of valuation at most 11. Therefore, E^d has good reduction at v and, since we are not in characteristic 2 or 3, a minimal equation at v is obtained from $\mathcal{E}^d_{\text{short}}$ via $(x, y) \mapsto (\pi_7^{\operatorname{ord}_v(\Delta)/6}x, \pi_7^{\operatorname{ord}_v(\Delta)/4}y)$, where π_7 is a uniformiser at v. Under such a change of variables, P_{short} and Q_{short} are mapped to v-adically integral points. Comparing discriminants as above, we then conclude that

$$\frac{1}{2}\sum_{v \nmid p} n_v \lambda_v^{\chi}(Q) = \sum_{\ell \nmid p} \lambda_\ell(P) = \begin{cases} -\frac{1}{2}\log 7 - \log d & \text{if } d \equiv 1 \bmod 4, \\ -\frac{1}{2}\log 7 - \log 4d & \text{otherwise.} \end{cases} \qquad \square$$

3C. ***Proof of Theorem 1.4.*** In this subsection we explain how Theorem 1.4 can be deduced either from Corollary 3.5 or from Proposition 3.14. For an elliptic curve E over $\mathbb{Q}$, denote by $L(E, s)$ its complex L-function.

Theorem 3.16 [Waldspurger 1981; Vignéras 1981; Murty and Murty 1997, Chapter 6, Theorem 1.1]. *Let E be an elliptic curve over $\mathbb{Q}$. There exist infinitely many nonzero square-free integers d such that the quadratic twist E^d of E by d satisfies $L(E^d, 1) \neq 0$.*

Theorem 3.17 [Kolyvagin 1988]. *Let E be an elliptic curve over $\mathbb{Q}$ such that $L(E, 1) \neq 0$. Then the rank of $E(\mathbb{Q})$ is zero and the Tate–Shafarevich group of $E/\mathbb{Q}$ is finite.*

It follows from Theorems 3.16 and 3.17 that there are infinitely many twists of $X_0(49)$ satisfying the hypotheses of Proposition 3.14. For each such curve, by Chebotarev's density theorem, there are infinitely many primes for which the proposition holds.

We now see how Corollary 3.5 also provides us with an alternative proof of Theorem 1.4. Consider the elliptic curve E with label 36.a3 [LMFDB 2019] which has reduced minimal equation

$$\mathcal{E} : y^2 = x^3 - 27.$$

We have $\mathcal{E}(\mathbb{Z}) = \mathcal{E}(\mathbb{Z})[2] = \{O, (3, 0)\}$. It follows that every quadratic twist E^d of E by a nonzero square-free integer d satisfies $E^d(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. The equation

$$\mathcal{E}^d : y^2 = x^3 - 27d^3$$

has discriminant equal to $-2^4 \cdot 3^9 \cdot d^6$ and is hence globally minimal, except if $3 \mid d$, in which case we apply $(x, y) \mapsto (9x, 27y)$ to obtain a minimal model. Thus, the point of exact order 2 of E^d defined over $\mathbb{Q}$ is integral. Therefore, by Theorems 3.16 and 3.17, there exist infinitely many d for which Corollary 3.5 holds with $y_0 = 0$.

3D. ***A necessary condition: quadratic saturation.*** In Sections 3A and 3B we proved sufficient conditions for a point in $\mathcal{X}(\mathbb{Z}_p)$ to belong to $\mathcal{X}(\mathbb{Z}_p)_2$. We now prove the necessary condition given by Theorem 1.8, which we restate here for the reader's convenience.

Theorem 3.18. *Let $E/\mathbb{Q}$ and p be as in Theorem 1.6. Suppose that $z \in \mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$. Then z is the localisation of a torsion point P over a number field K and, for each rational prime q, the value $\lambda_{\mathfrak{q}}(P)$ of the local height $\lambda_{\mathfrak{q}}$ is independent of the prime $\mathfrak{q} \mid q$ of K.*

Proof. As we observed at the beginning of this section, a point $z \in \mathcal{X}(\mathbb{Z}_p)_2$ is necessarily the p-adic localisation of a point $P \in \mathcal{E}(\overline{\mathbb{Z}})_{\text{tors}}$. Let K be the minimal number field over which the coordinates of P are defined. Let $m \in \mathbb{Z}$, $m \neq 0$, such that $mP = O$. Since $z \in \mathcal{X}(\mathbb{Z}_p)$, there exists an embedding ψ of K into $\mathbb{Q}_p$ under which P is mapped to z, i.e., a prime $\mathfrak{p}_0$ of K such that $\mathfrak{p}_0 \mid p$ and

$$\lambda_{\mathfrak{p}_0}(P) = \lambda_p(z) = -\|w\| =: -\sum_{q \in S} \alpha_q \log q \quad \text{for some } w \in W, \alpha_q \in \mathbb{Q}.$$

For any prime $\mathfrak{p} \mid p$ of K, the value $\lambda_{\mathfrak{p}}(P)$ can be computed as follows. Let $x(t), y(t) \in K[[t]]$ be coordinates around P, i.e., $P = (x(0), y(0))$, the power series $x(t), y(t)$ converge in the intersection over $\mathfrak{p} \mid p$ of small enough $\mathfrak{p}$-adic neighbourhoods of P and t vanishes to order 1 at P. Let $Q(t) = m(x(t), y(t)) \in E(K((t)))$. Since $K[[t]]$ is a complete DVR with residue field K, by [Wuthrich 2004, Proposition 1] the t-adic valuation of $-x(Q(t))/y(Q(t))$ equals the one of $f_m(x(t), y(t))$. More precisely, since f_m vanishes to order 1 at every point of order dividing m, we have

$$\begin{aligned} -x(Q(t))/y(Q(t)) &= at + O(t^2) \quad \text{for some } a \in K^\times, \\ f_m(x(t), y(t)) &= ct + O(t^2) \quad \text{for some } c \in K^\times. \end{aligned}$$

Since $\sigma_p^{(\gamma)}(T) = T + O(T^2)$, by Section 2A2(ii) we then have

$$\begin{aligned} \lambda_{\mathfrak{p}}(P) &= \lim_{t\to 0} -\frac{2}{n_{\mathfrak{p}} m^2} \operatorname{tr}_{K_{\mathfrak{p}}/\mathbb{Q}_p} \left(\log_{\mathfrak{p}} \left(\frac{\sigma_p^{(\gamma)}(-x(Q(t))/y(Q(t)))}{f_m(x(t), y(t))} \right)\right) \\ &= -\frac{2}{n_{\mathfrak{p}} m^2} \operatorname{tr}_{K_{\mathfrak{p}}/\mathbb{Q}_p} \log_{\mathfrak{p}} \left(\frac{a}{c}\right), \end{aligned}$$

where $\log_{\mathfrak{p}}$ is an extension of log to $K_{\mathfrak{p}}^\times$.

In particular, if d is the least common multiple of the denominators of the α_q, then

$$\log\left(\psi\left(\frac{a}{c}\right)^{2d}\right) = \log\left(\prod_{q\in S} q^{d\alpha_q m^2}\right).$$

Since $\mathfrak{p}$ is a prime of good reduction, we also have $\operatorname{ord}_{\mathfrak{p}}(a/c) = 0$ (strictly speaking we could also avoid using this fact, since the branch of the logarithm corresponding to the cyclotomic character vanishes at p), so

$$\left(\frac{a}{c}\right)^{2d} = \zeta \prod_{q\in S} q^{d\alpha_q m^2}$$

for some root of unity $\zeta \in K$. Thus

$$\lambda_{\mathfrak{p}}(P) = -\frac{1}{d n_{\mathfrak{p}} m^2} \operatorname{tr}_{K_{\mathfrak{p}}/\mathbb{Q}_p} \log_{\mathfrak{p}} \left(\zeta \prod_{q\in S} q^{d\alpha_q m^2}\right) = -\sum_{q\in S} \alpha_q \log q$$

is independent of $\mathfrak{p}$.

Let now $\mathfrak{q}$ be a prime not above p. By Section 2A1(ii), (iv), we have

$$\lim_{R\to P} \frac{1}{m^2}(\lambda_{\mathfrak{q}}(mR) + 2\log|f_m(R)|_{\mathfrak{q}}) = \lim_{R\to P} \lambda_{\mathfrak{q}}(R) = \lambda_{\mathfrak{q}}(P).$$

Since mR is in the formal group at $\mathfrak{q}$, then

$$\begin{aligned} \lambda_{\mathfrak{q}}(P) &= \lim_{R\to P} \frac{1}{m^2}\big(\log|x(mR)|_{\mathfrak{q}} |f_m(R)|_{\mathfrak{q}}^2\big) \\ &= \lim_{R\to P} \frac{1}{m^2} \log\left(\left|\frac{x(mR)}{y(mR)}\right|_{\mathfrak{q}}^{-2} |f_m(R)|_{\mathfrak{q}}^2 \right) \\ &= \frac{1}{m^2} \log\left(\left|\frac{c}{a}\right|_{\mathfrak{q}}^2\right) = \frac{1}{d} \log\left(\left|\prod_{q\in S} q^{-d\alpha_q}\right|_{\mathfrak{q}}\right), \end{aligned}$$

which completes the proof. □

Corollary 3.19. *If $z \in \mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$ is the localisation of a point P defined over K, we have $P \in \mathcal{X}(\mathcal{O}_K)$.*

Proof. The proof is similar to that of Proposition 3.1. Note that a torsion point defined over an arbitrary number field can fail to be integral at $\mathfrak{q}$ only if its order is q^n for some n (where q is the norm of $\mathfrak{q}$) and $\operatorname{ord}_{\mathfrak{q}}(q) \geq q^n - q^{n-1}$ (cf. [Silverman 2009, VIII, Theorem 7.1]). □

Theorem 3.18 is in some sense a natural analogue of a conjecture of Stoll for the classical abelian Chabauty method [Stoll 2006, Conjecture 9.5], which appears in an unpublished draft of [Stoll 2007]. Let us restrict to the case when C is a hyperelliptic curve over $\mathbb{Q}$ of genus g, whose Jacobian J has rank $g-2$ over $\mathbb{Q}$ (for the conjecture in its full generality see [Stoll 2006]). Suppose that $\iota : C \hookrightarrow J$ is an embedding such that $\iota(C)$ generates J and that J is simple. Stoll's conjecture predicts the existence of a finite subscheme $Z \subset J$ and a set R of primes which has density 1 in the set of all primes such that, for each $\ell \in R$, we have

$$\overline{J(\mathbb{Q})} \cap \iota(C(\mathbb{Q}_\ell)) \subset Z(\mathbb{Q}_\ell),$$

where $\overline{J(\mathbb{Q})}$ is the ℓ-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_\ell)$.

In [Balakrishnan et al. 2019c] some evidence for Stoll's conjecture was collected when $g = 3$, with the scheme Z being the intersection of $\iota(C)$ with the saturation of $J(\mathbb{Q})$, that is

$$Z = \{\iota(P) \in J : n\iota(P) \in J(\mathbb{Q}) \text{ for some } n \in \mathbb{Z}_{\geq 1}\}.$$

In our setting of an elliptic curve of rank 0, it is clear that $\mathcal{X}(\mathbb{Z}_p)_2$ should be contained in the saturation of the Mordell–Weil group $E(\mathbb{Q})$, since $E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}}$ and the equation $\operatorname{Log} z = 0$ cuts out the torsion points in $E(\mathbb{Q}_p)$. However, this is not a very strong requirement in the elliptic curve case, because the curve and the Jacobian are identified.

Theorem 3.18 asserts that the extra constraint $\lambda_p(z) = -\|w\|$, for some $w \in W$, leads to another type of "saturation", in the sense that we have to consider those points for which the local heights behave as if the point were defined over $\mathbb{Q}$.

Note that Stoll's conjecture assumes that $g - r + l \geq 3$, where $l = 1$ is the level, in the sense that the Chabauty–Coleman method computes the cohomologically global points of level 1. In the situation discussed here we have $g = 1$, $r = 0$, $l = 2$, i.e., $g - r + l = 3$, so one could naively hope that for rank 1 similar conjectures could be formulated at level 3.

4. Algorithm and computations in rank 0

4A. ***The algorithm.*** We wish to explicitly compute the sets $\phi(w)$ and $\psi(w)$ from Theorems 1.6 and 1.7. Each of $D_2(z)$ and $\operatorname{Log}(z)$ are locally analytic functions on $\mathcal{X}(\mathbb{Z}_p)$. In other words, given a point $\bar{P} \in \bar{E}(\mathbb{F}_p) \setminus \{O\}$ and a fixed point $P \in \mathcal{X}(\mathbb{Z}_p)$ reducing to $\bar{P}$ modulo p, one can pick a uniformiser $t \in \mathbb{Q}_p(E)$ at P, which reduces to a uniformiser at $\bar{P}$. Then, for each $Q \in \mathcal{X}(\mathbb{Z}_p)$ in the residue disk of P, we have

$$\operatorname{Log}(Q) = f_P(t(Q)) \quad \text{and} \quad D_2(Q) = g_P(t(Q))$$

for some $f_P(x), g_P(x) \in \mathbb{Q}_p[[x]]$ convergent at all $x \in \mathbb{Z}_p$ with $|x|_p < 1$.

On the other hand, let $\gamma = C$ if p is of good ordinary reduction and $\gamma = \frac{1}{12}(a_1^2 + 4a_2)$ if p is of good supersingular reduction. By Proposition 2.5 and Section 2A2(ii), provided that $mQ \neq O$, where $m = \#\bar{E}(\mathbb{F}_p)$, then

$$2D_2(Q) + \gamma \operatorname{Log}(Q)^2 = -\frac{2}{m^2} \log\left(\frac{\sigma_p^{(\gamma)}(mQ)}{f_m(Q)}\right). \tag{11}$$

Since there are finitely many[6] points in each residue disk satisfying $mQ = O$, the local expansion of the right-hand side of (11) in terms of the local parameter t holds in the whole residue disk. In fact, the local expansion of $\sigma_p^{(\gamma)}(mQ)$ and $f_m(Q)$ have precisely the same zeros with the same multiplicity 1 and two p-adic power series which agree at infinitely many points in $\mathbb{Z}_p$ of absolute value less than 1 are equal by the p-adic Weierstrass preparation theorem [Koblitz 1984, Chapter IV, §4, Theorem 14]. Note that we already used this in the proof of Theorem 3.18.

By the same observation as in Remark 2.7, we obtain a way of computing the intersections of $\phi(w)$ and $\psi(w)$ with each residue disk using local expansions of the p-adic sigma function (of Mazur–Tate or Bernardi) and the m-th division polynomial,[7] in place of the double Coleman integral $D_2(z)$.

The function $\operatorname{Log} : \mathcal{X}(\mathbb{Z}_p) \to \mathbb{Q}_p$ is odd; the function $\lambda_p : \mathcal{X}(\mathbb{Z}_p) \to \mathbb{Q}_p$ is even (cf. property (iv) in Section 2A2). Therefore,

$$z \in \phi(w) \iff -z \in \phi(w)$$

and it will thus suffice to consider residue disks up to $\bar{P} \mapsto -\bar{P}$. The same holds for $\psi(w)$.

We also notice that different models can be used for computing the p-adic heights and the single Coleman integrals. In fact, we defined local p-adic heights using an integral minimal model and, for instance, there is an implementation for the Mazur–Tate p-adic sigma function in SageMath due to Harvey [2008] (see also [Mazur et al. 2006]). On the other hand, for Coleman computations on SageMath (see [Balakrishnan et al. 2010]), one requires the elliptic curve to be described by a Weierstrass model whose a_1 and a_3 coefficients are zero and there is no requirement on minimality; the only requirement on integrality is $\mathbb{Z}_p$-integrality. To avoid explicit Coleman integration computations, we could also work directly with the formal logarithm.

4B. ***Examples for Section 3.*** In the examples that follow, as well as in the ones of the next sections, we avoid making distinctions between the curve $E/\mathbb{Q}$ and the model $\mathcal{E}/\mathbb{Z}$. The Weierstrass equations that we work with are always minimal and reduced, unless stated otherwise.

Example 4.1 (Corollary 3.7, Proposition 3.12). Consider the rank 0 elliptic curve 17.a1 [LMFDB 2019]

$$E : y^2 + xy + y = x^3 - x^2 - 91x - 310 \tag{12}$$

and the prime $p = 5$ of good ordinary reduction.

[6] In fact, at most one.

[7] Computationally, it is more convenient to take m to be the order of $\bar{P}$ in $\bar{E}(\mathbb{F}_p)$, i.e., to choose potentially different values of m for different residue disks.

Since none of the conditions of Theorem 1.6(1) are satisfied, we need to explicitly compute $\mathcal{X}(\mathbb{Z}_p)_2$ as a union of $\phi(w)$. The curve has split multiplicative reduction at 17 with Kodaira symbol I_1 and good reduction everywhere else: thus, $W = \{0\}$. We find

$$\mathcal{X}(\mathbb{Z}_p)_2 = \{(-5, 2 \pm \rho(i))\},$$

where $\rho : \mathbb{Z}[i] \hookrightarrow \mathbb{Z}_p$ is a fixed embedding. If a priori our computations only return approximations of p-adic points, by Corollary 3.7 the p-adic points found are the localisations of the points over $\mathbb{Z}[i]$ listed above. Let us nevertheless explain it in detail for this example.

The Weierstrass equation (12) defines a global minimal model also for the base-change $E/\mathbb{Q}(i)$ and the prime p splits in $K = \mathbb{Q}(i)$. We extend ρ to a map $E(K) \hookrightarrow E(\mathbb{Q}_p)$. The point

$$Q = (-5, 2+i) \in E(K)$$

is integral with respect to the global minimal model above and satisfies

$$4Q = O.$$

Thus, since the reduction types at the bad primes of $E/\mathbb{Q}(i)$ are the same as over $\mathbb{Q}$, we have

$$0 = h_p(Q) = \tfrac{1}{2}(\lambda_{\mathfrak{p}_1}(Q) + \lambda_{\mathfrak{p}_2}(Q)),$$

where $p\mathbb{Z}[i] = \mathfrak{p}_1\mathfrak{p}_2$ and explicitly (without loss of generality)

$$\lambda_{\mathfrak{p}_1}(Q) = \lambda_p(\rho(Q)), \qquad \lambda_{\mathfrak{p}_2}(Q) = \lambda_p(\rho(\tau(Q))),$$

where $\mathrm{Gal}(K/\mathbb{Q}) = \langle\tau\rangle$, so $\tau(Q) = (-5, 2-i)$. On the other hand, $\tau(Q) = -Q$ and λ_p is an even function. Therefore

$$0 = \lambda_p(\rho(Q)) = \lambda_p(\rho(\tau(Q))).$$

Note that Proposition 3.12 also explains why the p-adic localisation of the point Q belongs to $\mathcal{X}(\mathbb{Z}_p)_2$.

Example 4.2 (Proposition 3.12, 3.4(1)). Consider the elliptic curve 121.d3 [LMFDB 2019]

$$E : y^2 + y = x^3 - x^2 - 40x - 221 \tag{13}$$

and the prime $p = 5$, at which E has good ordinary reduction. We have

$$\#\bar{E}(\mathbb{F}_2) = 1$$

and thus

$$\mathcal{X}(\mathbb{Z}_p)_2 = \varnothing$$

by Theorem 1.6(1). On the other hand, we can still compute $\bigcup_{w\in W} \phi(w)$ of Theorem 1.7(2). The curve has additive reduction of type I_1^* at 11 with Tamagawa number 2 and has good reduction everywhere else. Therefore,

$$W = \{0, -\log 11\}.$$

We find that $\phi(0)=\varnothing$, but

$$\phi(-\log 11)=\bigl\{\bigl(-7,\rho\bigl(\tfrac{1}{2}(-1\pm 11\sqrt{-11})\bigr)\bigr),\bigl(4,\rho\bigl(\tfrac{1}{2}(-1\pm 11\sqrt{-11})\bigr)\bigr)\bigr\},$$

where $\rho:\mathbb{Z}[(1+\sqrt{-11})/2]\hookrightarrow\mathbb{Z}_p$ is a fixed embedding.

Let $K=\mathbb{Q}(\sqrt{-11})$. The prime 11 ramifies in $K/\mathbb{Q}$ and E/K has split multiplicative reduction of type I_2 at $\mathfrak{q}$, where $\mathfrak{q}^2=11$. Let

$$Q\in\bigl\{\bigl(-7,\tfrac{1}{2}(-1\pm 11\sqrt{-11})\bigr),\bigl(4,\tfrac{1}{2}(-1\pm 11\sqrt{-11})\bigr)\bigr\}\subset E(K).$$

The point Q has order 5. Unlike in Example 4.1, the Weierstrass equation (13) is minimal at all primes except at $\mathfrak{q}$ and hence we cannot use straightforwardly the explicit formulae for the local height at $\mathfrak{q}$ given in Section 2A1. The curve E/K admits the global minimal model

$$E^{\min}:y^2+y=x^3-x^2$$

and the image of Q in $E^{\min}(K)$ has good reduction at $\mathfrak{q}$, so that $\lambda_{\mathfrak{q}}^{\min}(Q)=0$. Equation (4) then yields $\lambda_{\mathfrak{q}}(Q)=-\log 11$. Therefore, by Proposition 3.12, we have

$$0=\lambda_p(\rho(Q))+\lambda_{\mathfrak{q}}(Q)=\lambda_p(\rho(Q))-\log 11.$$

Similarly to Example 4.1, the appearance of $\rho(Q)$ in $\phi(-\log 11)$ is also justified by Proposition 3.4(1).

Example 4.3 (Remark 3.8). Consider the elliptic curve 14112.q1 [LMFDB 2019]

$$E:y^2=x^3-9261x \tag{14}$$

and the prime $p=5$, which is of good ordinary reduction. Note that p splits in $K=\mathbb{Q}(\sqrt{21})$ and by Remark 3.8, the localisations of the point $Q^{\pm}=(\pm 21\sqrt{21},0)$ belong to $\mathcal{X}(\mathbb{Z}_p)_2$ provided that (1/2) times the sum of its local heights at bad primes is in $\|W\|$. Both at 3 and 7, the curve has bad reduction of additive type III* with Tamagawa number 2; at 2 the curve has reduction of type III with Tamagawa number 2. Thus, $W=W_2\times W_3\times W_7$, with $W_q=\bigl\{0,-\tfrac{3}{2}\log q\bigr\}$ for each $q\in\{3,7\}$ and $W_2=\bigl\{0,-\tfrac{1}{2}\log 2\bigr\}$.

A global minimal model for the base-change of E to K is given by $y^2=x^3-21x$. Furthermore, 2 is inert in K and its reduction type does not change. The primes 3 and 7 become of type I_0^* with Tamagawa number 4. By Propositions 2.4 and 3.4(1) (see also Remark 3.8), we then find that $Q^{\pm}$ is indeed in $\mathcal{X}(\mathbb{Z}_p)_2$.

Our computation of $\mathcal{X}(\mathbb{Z}_p)_2$ recovers precisely the integral points and the ones coming from $Q^{\pm}$.

Example 4.4 (Proposition 3.4(1)). Consider the elliptic curve 11025.y2 [LMFDB 2019] whose reduced minimal model is

$$E:y^2+y=x^3+15006$$

and let $p=13$, which is the smallest prime of good ordinary reduction for E. Note that E has vanishing j-invariant. We find that

$$\mathcal{X}(\mathbb{Z}_p)_2=\{\pm(0,122)\}\cup\{\pm(\zeta_3^i\sqrt[3]{120050},367):0\le i\le 2\}, \tag{15}$$

where ζ_3 is a primitive third root of unity and we assume that we have fixed an embedding of $\mathbb{Q}(\zeta_3, \sqrt[3]{120050})$ into $\mathbb{Q}_p$. As usual, the equality (15) is deduced from computations combined with theoretical results. In this particular example, the theory needed is that the Galois group of $\mathbb{Q}(\zeta_3, \sqrt[3]{120050})/\mathbb{Q}$ acts on the order-6 points $\pm(\zeta_3^i\sqrt[3]{120050}, 367)$ by automorphisms. We leave the reader to check that these points also have the right local heights at bad primes.

Example 4.5 (Corollary 3.5, 3.9). Consider the elliptic curve 900.g3 [LMFDB 2019] with reduced minimal model

$$E : y^2 = x^3 - 3375$$

and the prime 19, which is of good ordinary reduction for E. We have

$$\mathcal{X}(\mathbb{Z}_{19})_2 = \{(\zeta_3^i 15, 0), (-\zeta_3^i 30, \pm\sqrt{-30375}) : 0 \le i \le 2\}$$

where ζ_3 is a primitive third root of unity and we assume that we have fixed an embedding of $\mathbb{Q}(\zeta_3, \sqrt{-30375})$ into $\mathbb{Q}_{19}$.

4C. ***Large-scale data.*** Using the database [LMFDB 2019], we could run the code on all the 86213 elliptic curves over $\mathbb{Q}$ of rank 0 and conductor less than or equal to 30000; for each curve we let p be the smallest prime ≥ 5 of good ordinary reduction.[8]

Out of these, we found exactly 470 pairs (E, p) for which $\mathcal{X}(\mathbb{Z}_p)_2 \supsetneq \mathcal{X}(\mathbb{Z})$. The 10 such pairs with E of conductor ≤ 100 are listed in Table 2.

We summarise the results of the computations in Propositions 4.6, 4.7, 4.9.

Proposition 4.6. *Let E be an elliptic curve of rank* 0 *and conductor less than or equal to* 30000 *and let $p \ge 5$ be the smallest prime of good ordinary reduction. Assume that $j(E) \notin \{0, 1728, -3375\}$. Then $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$ is either empty or consists of localisations of points defined over the ring of integers of a quadratic field K on which the Galois group of $K/\mathbb{Q}$ acts as multiplication by ± 1.*

Proposition 4.7. *Let E be an elliptic curve of rank* 0 *and conductor less than or equal to* 30000 *and let $p \ge 5$ be the smallest prime of good ordinary reduction. If $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$ contains localisations of points defined over a quadratic field K, these points satisfy the hypotheses of Proposition 3.4, i.e., the nontrivial element of* $\mathrm{Gal}(K/\mathbb{Q})$ *acts on them in the same way as an automorphism of E.*

Remark 4.8. In view of the large data collected, it might have been tempting to expect that Propositions 4.6 and 4.7 would be true for arbitrary prime and conductor. It turns out that this is not the case: varying the prime for the curve 8712.u5 [LMFDB 2019] (which does not have CM), we found some quadratic points on which Galois does not act by automorphisms (cf. Example 4.11). We note nevertheless that in the latter case the extra points were explained by Proposition 3.12.

[8] We could have allowed p to equal 3 and used the method of [Balakrishnan 2016] to compute the quantities involved in the 3-adic heights. Some computations with supersingular primes were carried out for Section 4D.

LMFDB	p	SS/CM	$\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$	Order	Explanation
17.a1	5	SS	$(-5, 2 \pm i)$	4	Cor. 3.7/Prop. 3.12
27.a3	7	$j = 0$	$\pm\big(\frac{1}{2}(-3 \pm 3\sqrt{-3}), 4\big)$	3	Cor. 3.5/Prop. 3.12
32.a4	5	$j = 1728$	$(-2, \pm 4i)$	4	Prop. 3.4(1)/Prop. 3.12
36.a3	7	$j = 0$	$\big(\frac{1}{2}(-3 \pm 3\sqrt{-3}), 0\big)$	2	Cor. 3.5/Prop. 3.12
36.a4	7	$j = 0$	$\big(\frac{1}{2}(1 \pm \sqrt{-3}), 0\big)$	2	Cor. 3.5/Prop. 3.12
			$\pm(-1 \pm \sqrt{-3}, 3)$	6	Cor. 3.5/Prop. 3.12
49.a2	11	$j = -3375$	$\pm\big(\frac{1}{2}(-7b^2 + 25), \frac{1}{4}(-49b^3 + 7b^2 - 49b - 25)\big)$	4	Prop. 3.14
49.a4	11	$j = -3375$	$\pm\big(\frac{1}{2}(b^2 - 3), \frac{1}{4}(b^3 - b^2 - 7b + 3)\big)$	4	Prop. 3.14
75.b4	11	–	$(27, -14 \pm 5\sqrt{5})$	4	Prop. 3.4(1)
75.b6	11	–	$\big(12, \frac{1}{2}(-13 \pm 25\sqrt{5})\big)$	4	Prop. 3.4(1)
			$\big(2, -\frac{3}{2}(1 \pm 5\sqrt{5})\big)$	4	Prop. 3.4(1)
75.b7	11	–	$\big(2, \frac{1}{2}(-3 \pm 5\sqrt{5})\big)$	4	Prop. 3.4(1)

Table 2. All curves of rank 0 and conductor ≤ 100 for which $\mathcal{X}(\mathbb{Z}_p)_2 \supsetneq \mathcal{X}(\mathbb{Z})$ ($p \geq 5$ smallest good ordinary prime); b satisfies $x^4 + 7 = 0$. The curve is given in the first column as an LMFDB label [LMFDB 2019]. In the third column, SS means "semistable" and "–" neither semistable nor CM.

We now turn to the extra points in our data defined over number fields of degree[9] at least equal to 3. By Proposition 4.6, these can only show up if E has complex multiplication and, in fact, its j-invariant is one of 0, 1728, -3375. There was only one curve beside the one of Example 4.4 where cubic points were recovered, namely the curve 19881.g2 [LMFDB 2019]. As in Example 4.4, the curve has j-invariant equal to zero and the appearance of these points in $\mathcal{X}(\mathbb{Z}_p)_2$ is explained by Proposition 3.4.

Finally, we recovered points defined over number fields of degree 4 on the curve 14112.q2 ($j = 1728$) [LMFDB 2019], which is explained by Proposition 3.4, and on all the twists of the modular curve $X_0(49)$, as predicted by Proposition 3.14. In fact the inclusion in the statement of Proposition 3.14 is an equality in all the following cases.

Proposition 4.9. *Let E be an elliptic curve of rank* 0, *conductor less than or equal to* 30000 *and* $j(E) = -3375$. *Then* $\mathcal{X}(\mathbb{Z}_{11})_2 = \mathcal{X}(\mathbb{Z}) \cup \{\pm Q\}$, *where Q has order* 4 *and comes from a point over the ring of integers of the smallest number field L over which* $E(L)[4] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

[9] Note that by degree we mean the degree of the smallest number field over which a point in $\mathcal{X}(\mathbb{Z}_p)_2$ is defined and not the degree of the number field containing all the coordinates of the points in $\mathcal{X}(\mathbb{Z}_p)_2$, which could be larger.

4D. ***Variation of the prime.*** In what follows, we assume that the rank of the elliptic curve is equal to zero. However, the discussion could easily go through word for word with $\mathcal{X}(\mathbb{Z}_p)'_{2,\mathrm{tors}}$ in place of $\mathcal{X}(\mathbb{Z}_p)_2$.

We have established that there exist curves of rank 0 and primes p for which $\mathcal{X}(\mathbb{Z}_p)_2 \supsetneq \mathcal{X}(\mathbb{Z})$. The next question we ask is whether there always exists a (not necessarily ordinary) prime for which the cohomologically global points of level 2 are precisely the global integral points. It turns out that the answer is negative, as we will see in Example 4.11 below.

Let us first gather some intuition on what is happening. Recall that, after having fixed all appropriate embeddings,

$$\phi(w) \subset \mathcal{E}(\overline{\mathbb{Z}})_{\mathrm{tors}} = E(\overline{\mathbb{Q}})_{\mathrm{tors}}.$$

Therefore, if $P \in E(F)_{\mathrm{tors}}$ for some minimal number field F, by picking p such that $[F_v : \mathbb{Q}_p] > 1$ for all $v \mid p$, we can guarantee that $P \notin \mathcal{X}(\mathbb{Z}_p)_2$. For instance in Example 4.1, if we pick $p' = 7$, which is of good ordinary reduction and which is inert in $\mathbb{Q}(i)$, we find $\mathcal{X}(\mathbb{Z}_{p'})_2 = \mathcal{X}(\mathbb{Z}) = \varnothing$.

Note that, in view of Corollary 3.5 and Section 3C, there exist (infinitely many) curves for which $\mathcal{X}(\mathbb{Z}_p)_2$ is strictly larger than $\mathcal{X}(\mathbb{Z})$ for all odd primes p of good *ordinary* reduction. More generally, if E has complex multiplication by the quadratic field K and there exist points defined over K and satisfying the assumptions of Proposition 3.4(1), then these points will show up in $\mathcal{X}(\mathbb{Z}_p)_2$ for any good ordinary odd prime p by Deuring's criterion. On the other hand, Deuring's criterion also implies that the good supersingular primes cannot split in K.

We ran the code on all the 470 curves of Section 4C for which we had found some extra points: this time, we varied the good ordinary prime until we found a prime for which no extra points showed up or we proved that such prime does not exist. If a good ordinary prime p for which $\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z}_p)$ does not exist, we repeated the calculations with supersingular primes. We summarise the results in the following theorem (which includes also the statement of Theorem 1.5).

Theorem 4.10. *Let E be an elliptic curve over $\mathbb{Q}$ of rank* 0 *and conductor less than or equal to* 30000. *Then there exists a good ordinary odd prime p for which $\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z})$, unless*:

(1) *E is 32.a4* ($j = 1728$) [LMFDB 2019];

(2) *E is one of the* 20 *elliptic curves of rank* 0 *with $j = 0$ and $\mathbb{Z}/2\mathbb{Z} \subset E(\mathbb{Q})$ or E is 27.a3* ($j = 0$) [LMFDB 2019];

(3) *E is 8712.u5* [LMFDB 2019].

Moreover, in cases (1) and (2), $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z}) \neq \varnothing$ for all good ordinary odd primes p, but there exists a supersingular prime p for which $\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z}_p)$; in case (3) $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z}) \neq \varnothing$ for all good (*ordinary and supersingular*) *primes p.*

Proof. That there exists a good ordinary prime for which Conjecture 1.1 holds at level 2 for all curves not in (1), (2) and (3) is shown computationally. The assertion of cases (1) and (2) follows from the discussion before the statement of the theorem together with explicit computations of $\mathcal{X}(\mathbb{Z}_p)_2$ at some supersingular primes p. Finally, we treat the curve 8712.u5 in detail in Example 4.11. □

Example 4.11. Consider the elliptic curve 8712.u5, given by

$$E : y^2 = x^3 + 726x + 9317. \tag{16}$$

We have $S = \{2, 3, 11\}$: in particular, the reduction is of type III with Tamagawa number 2 at 2, of type I_1^* with Tamagawa number 4 at 3 and of type I_0^* with Tamagawa number 2 at 11. Thus $W = W_2 \times W_3 \times W_{11}$, where

$$W_2 = \bigl\{0, -\tfrac{1}{2}\log 2\bigr\}, \quad W_3 = \bigl\{0, -\log 3, -\tfrac{5}{4}\log 3\bigr\}, \quad W_{11} = \{0, -\log 11\}.$$

Consider

$$A := \bigl\{(-44, \pm 99\sqrt{-11}), (22, \pm 33\sqrt{33}), \bigl(\tfrac{11}{2}(1 \pm 3\sqrt{-3}), 0\bigr)\bigr\} \subset \mathcal{X}(\bar{\mathbb{Z}})_{\mathrm{tors}}.$$

If $p \notin S$, then p splits in at least one of $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{33})$ and $\mathbb{Q}(\sqrt{-3})$ and therefore $A \cap \mathcal{X}(\mathbb{Z}_p) \neq \varnothing$ (after having fixed embeddings). The fact that

$$A \cap \mathcal{X}(\mathbb{Z}_p)_2 \neq \varnothing,$$

then follows from Proposition 3.4(1) (for the points over $\mathbb{Q}(\sqrt{-11})$ and $\mathbb{Q}(\sqrt{33})$), Proposition 3.12 (for the points over $\mathbb{Q}(\sqrt{-3})$) and the following table, which shows how the reduction changes at the primes in S. The symbol "–" means that the reduction type has not changed. In the last column, there are the possible values of $\lambda_{\mathfrak{q}}(\mathcal{X}(\mathcal{O}_{\mathfrak{q}}))$ where $\mathcal{O}_{\mathfrak{q}}$ is the ring of integers of the completion $K_{\mathfrak{q}}$ at a prime $\mathfrak{q}$ above q in the field K. We briefly explain how the table is computed. When the prime q splits in K, there is nothing to show: $\lambda_{\mathfrak{q}}(\mathcal{X}(\mathcal{O}_{\mathfrak{q}})) = W_q$ if $\mathfrak{q} \mid q$. If q is inert, by Tate's algorithm, (16) is minimal at $\mathfrak{q} \mid q$ and the Kodaira symbol is unchanged. Once we know the Tamagawa number at $\mathfrak{q}$, we can find $\lambda_{\mathfrak{q}}(\mathcal{X}(\mathcal{O}_{\mathfrak{q}}))$ directly from Proposition 2.4. Finally, if q ramifies in K, then $\lambda_{\mathfrak{q}}(\mathcal{X}(\mathcal{O}_{\mathfrak{q}}))$ may be deduced from Proposition 2.4, Lemma 2.1(i) and (4). Note that some points in $\mathcal{X}(\mathcal{O}_{\mathfrak{q}})$ may map to nonintegral points in a minimal model at $\mathfrak{q}$ (see also Lemma 6.4).

K	q	splitting	reduction (Tamagawa)	$\lvert\Delta/\Delta_{\min}\rvert_{\mathfrak{q}}$	$\lambda_{\mathfrak{q}}(\mathcal{X}(\mathcal{O}_{\mathfrak{q}}))$
$\mathbb{Q}(\sqrt{-11})$	2	inert	–	1	W_2
	3	split	–	1	W_3
	11	ramified	good	11^{-6}	W_{11}
$\mathbb{Q}(\sqrt{33})$	2	split	–	1	W_2
	3	ramified	nonsplit I_2 (2)	3^{-6}	W_3
	11	ramified	good	11^{-6}	W_{11}
$\mathbb{Q}(\sqrt{-3})$	2	inert	–	1	W_2
	3	ramified	nonsplit I_2 (2)	3^{-6}	W_3
	11	inert	I_0^* (4)	1	W_{11}

5. The rank 1 case

5A. ***Algebraic nonrational points in $\mathcal{X}(\mathbb{Z}_p)_2'$ in rank 1.*** We retain the notation of Theorems 1.6 and 1.7. The set consisting of the torsion points in $\psi(w)$ is equal to $\phi(w)$. Therefore, the results of Section 3 translate into results for $\mathcal{X}(\mathbb{Z}_p)'_{2,\mathrm{tors}}$.

Since each $\psi(w)$ is defined by a single p-adic equation, in most cases it is expected that $\mathcal{X}(\mathbb{Z}_p)_2'$ should be strictly larger than $\mathcal{X}(\mathbb{Z})$. The question we investigate in this subsection is which algebraic nontorsion points could arise in $\mathcal{X}(\mathbb{Z}_p)_2'$. The following elementary lemma shows that if a nontorsion point in $\mathcal{X}(\mathbb{Z}_p)_2'$ comes from a quadratic point in the saturation of $E(\mathbb{Q})$, then its belonging to $\mathcal{X}(\mathbb{Z}_p)_2'$ cannot be explained by automorphisms (cf. Section 3A).

Lemma 5.1. *Let E be an elliptic curve over $\mathbb{Q}$ and K a quadratic field with* $\mathrm{Gal}(K/\mathbb{Q}) = \langle\tau\rangle$. *Let $P \in E(K) \setminus E(\mathbb{Q})$ such that $mP \in E(\mathbb{Q})$ for some nonzero integer m. Then, if $\psi(P) = \tau(P)$ for some $\psi \in \mathrm{Aut}(E/\overline{\mathbb{Q}})$, P has finite order.*

Proof. The hypotheses on P imply that $\psi \neq \mathrm{id}$. Since $mP \in E(\mathbb{Q})$, we have $O = mP - \tau(mP) = m(P - \tau(P))$. If $\psi = -\mathrm{id}$, then

$$\begin{cases} \tau(P) = -P \\ m(P - \tau(P)) = O \end{cases} \iff \begin{cases} \tau(P) = -P \\ 2mP = O; \end{cases}$$

thus, P has order dividing $2m$.

For more general ψ, let

$$[\,\cdot\,] : R \simeq \mathrm{End}(E)$$

where $R \subset \mathbb{C}$. Then there exists a root of unity ζ such that $\psi(P) = [\zeta]P$. Therefore,

$$\begin{cases} \tau(P) = [\zeta]P \\ m(P - \tau(P)) = O \end{cases} \iff \begin{cases} \tau(P) = [\zeta]P \\ [m(1-\zeta)]P = O \end{cases}$$

and so $P \in E(K)[mN_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta)]$. □

We could try and use noncyclotomic idele class characters to motivate the existence of some algebraic points of infinite order in $\mathcal{X}(\mathbb{Z}_p)_2'$, following the ideas of Section 3B. For example, what we could hope to prove is that at a certain $z \in \mathcal{X}(\overline{\mathbb{Z}})$ satisfying $mz \in E(\mathbb{Q})$ for some nonzero integer m, the quantity $2D_2(z) + C(\mathrm{Log}(z))^2 + \|w\|$, for some $w \in W$, equals the value of *some* p-adic height function at z. If such a p-adic height comes from a character which restricts to the cyclotomic character on $\mathbb{A}_{\mathbb{Q}}^{\times}$ with the right normalisations, then looking at the equation defining $\psi(w)$ we see that this is enough to show $z \in \mathcal{X}(\mathbb{Z}_p)_2'$.

However, our computations (more on this in Section 5B) also recovered some algebraic nontorsion points defined over real quadratic fields and we know that the space of idele class characters of a real quadratic field is one-dimensional. Therefore, in the following proposition we present a sufficient condition for a point defined over a quadratic field to belong to $\mathcal{X}(\mathbb{Z}_p)_2'$, which looks less geometric or algebraic in nature compared to the results of Section 3. However, we then discuss in Remark 5.3 when we expect the hypotheses of the proposition to be satisfied.

Proposition 5.2. *Suppose that E satisfies the assumptions of Theorem 1.7 and that p is an odd prime of good ordinary reduction. Let K be a quadratic field in which p splits. Fix an embedding $\rho : K \hookrightarrow \mathbb{Q}_p$ and let τ be the nontrivial element in* $\mathrm{Gal}(K/\mathbb{Q})$. *Suppose that $z \in \mathcal{X}(\mathcal{O}_K)$ is such that $mz \in E(\mathbb{Q}) \setminus \{O\}$ for some nonzero integer m and that*

$$f_m(z) = \zeta f_m(\tau(z)), \tag{17}$$

for some root of unity ζ. For each rational prime q, let $\mathfrak{q}$ be one (any) prime of K above q and $\lambda_{\mathfrak{q}}$ the local height at $\mathfrak{q}$ with respect to the model $\mathcal{E}$. If

$$\sum_{q \in S} \lambda_{\mathfrak{q}}(z) = \|w\|$$

for some $w \in W$, then $\rho(z) \in \mathcal{X}(\mathbb{Z}_p)'_2$.

Proof. Let $\mathfrak{q} \nmid p$. By quasiquadraticity (Section 2A1(iv)) applied twice and the assumptions on z and m, we have

$$\begin{aligned}\lambda_{\mathfrak{q}}(z) &= \frac{1}{m^2}\big(\lambda_{\mathfrak{q}}(mz) + 2\log|f_m(z)|_{\mathfrak{q}}\big)\\ &= \frac{1}{m^2}\big(\lambda_{\mathfrak{q}}(\tau(mz)) + 2\log|\zeta f_m(\tau(z))|_{\mathfrak{q}}\big)\\ &= \frac{1}{m^2}\big(\lambda_{\mathfrak{q}}(m\tau(z)) + 2\log|f_m(\tau(z))|_{\mathfrak{q}}\big)\\ &= \lambda_{\mathfrak{q}}(\tau(z)) = \lambda_{\tau(\mathfrak{q})}(z).\end{aligned}$$

Similarly, if $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, then (without loss of generality)

$$m^2\lambda_{\mathfrak{p}_1}(z) = \lambda_p(mz) + 2\log(\rho(f_m(z))) = \lambda_p(mz) + 2\log(\rho(f_m(\tau(z)))) = m^2\lambda_{\mathfrak{p}_2}(z).$$

Therefore,

$$h_p(z) = \lambda_p(\rho(z)) + \|w\|.$$

Since z is in the saturation of $E(\mathbb{Q})$ (i.e., $mz \in E(\mathbb{Q})$), then $z \in \psi(w)$. □

Remark 5.3. Let E, K and p be as in Proposition 5.2. Suppose that $z \in \mathcal{X}(\mathcal{O}_K)$ is such that $mz \in E(\mathbb{Q}) \setminus \{O\}$ and write $x(mz) = n(mz)/(d(mz)^2)$ for some coprime integers $n(mz)$ and $d(mz) > 0$. When can we expect (17) to hold? By [Wuthrich 2004, §2] and our assumptions, we know that

$$\frac{g_m(z)}{f_m(z)^2} = x(mz) = x(m\tau(z)) = \frac{g_m(\tau(z))}{f_m(\tau(z))^2},$$

where $g_m(z)$ can be written as a univariate polynomial in $x(z)$ over $\mathbb{Z}$. For $w \in \{z, \tau(z)\}$, define

$$\delta_m(w) = \frac{f_m(w)}{d(mw)}.$$

By Proposition 1 of [loc. cit.], $\delta_m(w)$ is a unit at all primes at which w has nonsingular reduction. Furthermore, we have

$$\frac{\delta_m(z)}{\tau(\delta_m(\tau(z)))} = \frac{f_m(z)}{\tau(f_m(\tau(z)))} = 1.$$

Thus, if for example z has good reduction at all primes which are split in K, then $\tau(\delta_m(\tau(z))) = \delta_m(\tau(z))$ up to multiplication by elements of $\mathcal{O}_K^\times$: thus, in this case, $f_m(z) = u f_m(\tau(z))$ for some $u \in \mathcal{O}_K^\times$. If K is imaginary then u is a root of unity; otherwise u may or may not be. Note that if K is imaginary, we could have also avoided talking about division polynomials and followed a strategy similar to Proposition 3.12. Conversely, Proposition 5.2 is often not applicable for torsion points as it requires the existence of a *nonzero* multiple of z in $E(\mathbb{Q})$.

5B. ***Computations in rank* 1.** The technique explained in Section 4A to compute $\mathcal{X}(\mathbb{Z}_p)_2$ in the rank 0 case can easily be adapted to compute $\mathcal{X}(\mathbb{Z}_p)_2'$ when the Mordell–Weil group has rank 1. As remarked in Section 5A, the expectation is that $\mathcal{X}(\mathbb{Z}_p)_2'$ should generally be larger than $\mathcal{X}(\mathbb{Z})$.

We ran the code on all the 14783 rank 1 elliptic curves of conductor at most 5000 and let p be the smallest prime greater than or equal to 5 at which the curve has good ordinary reduction. The first observation is that it can happen that there are no points in $\mathcal{X}(\mathbb{Z}_p)_2'$ beside those in $\mathcal{X}(\mathbb{Z})$. For example, the curves of conductor at most 500

- satisfying the assumptions of Theorem 1.7(1) are 254.b1, 430.c1 [LMFDB 2019];
- not satisfying Theorem 1.7(1), but for which $\mathcal{X}(\mathbb{Z}_p)_2' = \mathcal{X}(\mathbb{Z})$ are 297.b1, 325.b1, 325.b2, 467.a1 [LMFDB 2019].

Studying the torsion points of $\mathcal{X}(\mathbb{Z}_p)_2'$ morally provides more data on the extra points that can arise in $\mathcal{X}(\mathbb{Z}_p)_2$ when E has rank 0. No new phenomenon was observed, except that torsion points defined over some degree 4 number fields were also recovered on the two CM elliptic curves 576.e1 and 576.e2 [LMFDB 2019] of j-invariant 54000. The appearance of the latter points can be proved in a similar way to Proposition 3.14.

As far as algebraic nontorsion points are concerned, on 26 curves we identified nontorsion points defined over quadratic extension of $\mathbb{Q}$. All of these were explained by Proposition 5.2 and only on two curves the points were defined over real quadratic fields. We now present an example in which some algebraic torsion and nontorsion points were recovered in $\mathcal{X}(\mathbb{Z}_p)_2' \setminus \mathcal{X}(\mathbb{Z})$. Afterwards, we also include for completeness an example in which the extra algebraic nontorsion points are real.

Example 5.4. Consider the elliptic curve 576.e4 [LMFDB 2019]

$$E : y^2 = x^3 + 8,$$

whose Mordell–Weil group over $\mathbb{Q}$ has rank 1 and is generated, modulo torsion, by the point $z_0 = (1, 3)$. Let $p = 7$, at which E has good ordinary reduction. We have $S = \{2, 3\}$ and $W = W_2 \times W_3$ where

$$W_2 = \{0, -\log 2\} \quad \text{and} \quad W_3 = \left\{0, -\tfrac{1}{2}\log 3\right\}.$$

Write

$$\mathcal{X}(\mathbb{Z}_p)'_2 = \mathcal{X}(\mathbb{Z}_p)'_{2,\text{tors}} \cup \mathcal{X}(\mathbb{Z}_p)'_{2,\text{nontors}},$$

where the subscripts tors and nontors have the obvious meaning. Let $K = \mathbb{Q}(\sqrt{-3})$ and let τ generate the Galois group of $K/\mathbb{Q}$. Assuming that we have fixed an embedding of $\mathbb{Q}(\sqrt{-3})$ into $\mathbb{Q}_p$, we find that

$$\begin{aligned}\mathcal{X}(\mathbb{Z}_p)'_{2,\text{tors}} &= \{(-2,0),\,(1\pm\sqrt{-3},0)\},\\ \mathcal{X}(\mathbb{Z}_p)'_{2,\text{nontors}} &= \pm\{(1,3),\,(2,-4),\,(46,-312),\,(-5\pm\sqrt{-3},6\pm 6\sqrt{-3})\}\cup A^{\text{nonalg?}},\end{aligned}$$

where $A^{\text{nonalg?}}$ denotes the set of points of $\mathcal{X}(\mathbb{Z}_p)'_2$ which have not been recognised as algebraic. Note that $A^{\text{nonalg?}}$ modulo ± consists of 15 points. Corollary 3.5, together with the observation at the beginning of this section, proves why the two-torsion quadratic points $(1\pm\sqrt{-3},0)$ belong to $\mathcal{X}(\mathbb{Z}_p)'_2$.

Consider now

$$Q \in \{\pm(-5\pm\sqrt{-3},6\pm 6\sqrt{-3})\}.$$

We show why $Q \in \mathcal{X}(\mathbb{Z}_p)'_{2,\text{nontors}}$. Without loss of generality we assume that $Q=(-5+\sqrt{-3},6+6\sqrt{-3})$. As

$$Q = -z_0 + (1-\sqrt{-3},0),$$

$2Q \in E(\mathbb{Q})$. We have

$$f_2(Q) = 2y(Q) = \left(\tfrac{1}{2}(-1+\sqrt{-3})\right) f_2(\tau(Q)).$$

Therefore, in order to apply Proposition 5.2, it suffices to verify the condition on the local heights at the bad primes. For each prime $\mathfrak{q}\nmid p$, we could use the formula involving $f_2(Q)$ in order to compute $\lambda_{\mathfrak{q}}(Q)$, as in the proof of the proposition. We choose to compute it instead by the quasiparallelogram law

$$\lambda_{\mathfrak{q}}(Q) = \lambda_{\mathfrak{q}}(z_0) + \lambda_{\mathfrak{q}}(1-\sqrt{-3},0) - \log|\sqrt{-3}|_{\mathfrak{q}} = \lambda_{\mathfrak{q}}(z_0) + \lambda_{\mathfrak{q}}(-2,0) - \log|\sqrt{-3}|_{\mathfrak{q}},$$

which gives

$$\lambda_{\mathfrak{q}}(Q) = \begin{cases} -\frac{1}{2}\log 3 & \text{if } \mathfrak{q}\mid 3,\\ -\log 2 & \text{if } \mathfrak{q}\mid 2,\\ 0 & \text{if } \mathfrak{q}\nmid 2,3,p.\end{cases}$$

The fact that Q is in $\mathcal{X}(\mathbb{Z}_p)'_2$ then follows from Proposition 5.2.

Example 5.5. Consider the elliptic curve 525.c1 [LMFDB 2019]

$$E : y^2 + xy = x^3 + x^2 - 450x + 3375.$$

Let p be an odd prime of good ordinary reduction split in $\mathbb{Q}(\sqrt{5})$ and fix an embedding $\mathbb{Q}(\sqrt{5}) \hookrightarrow \mathbb{Q}_p$. Then by Proposition 5.2 with $m=2$, the infinite order points

$$\pm\left(10\pm 5\sqrt{5},\,\tfrac{5}{2}(23\mp\sqrt{5})\right)$$

belong to $\mathcal{X}(\mathbb{Z}_p)'_2$.

6. Rational points on bielliptic curves

Let C be a smooth projective curve over $\mathbb{Q}$ of genus g and whose Jacobian J has Mordell–Weil rank equal to g. Assume in addition that the Néron–Severi group of J has rank at least equal to 2, that p is an odd prime of good reduction for C and that the p-adic closure of $J(\mathbb{Q})$ has finite index in $J(\mathbb{Q}_p)$. Balakrishnan and Dogra [2018, Theorem 1.2] used the Chabauty–Kim method to explicitly describe a finite set

$$C(\mathbb{Q}_p)_Z \subset C(\mathbb{Q}_p),$$

which depends upon the choice of a correspondence $Z \subset C \times C$ and which contains all the $\mathbb{Q}$-rational points of C. Note that one has $C(\mathbb{Q}_p)_2 \subset C(\mathbb{Q}_p)_Z$. The authors then made Theorem 1.2 algorithmic when C is a bielliptic curve of genus 2, under the extra assumption that J is ordinary at p (we remove this hypothesis here). Let

$$C : y^2 = x^6 + a_4x^4 + a_2x^2 + a_0, \qquad a_i \in \mathbb{Q},$$

be a genus 2 bielliptic curve with a rank-2 Jacobian and consider the associated maps $\varphi_i : C \to (E_i, O_{E_i})$, described affinely by

$$\begin{aligned} E_1 &: y^2 = x^3 + a_4x^2 + a_2x + a_0, & \varphi_1(x, y) &= (x^2, y) \\ E_2 &: y^2 = x^3 + a_2x^2 + a_4a_0x + a_0^2, & \varphi_2(x, y) &= (a_0x^{-2}, a_0yx^{-3}). \end{aligned}$$

Assume that each of E_1 and E_2 has rank 1. Then one may pick Z in such a way that $C(\mathbb{Q}_p)_Z$ can be described in terms of local and global p-adic heights of the images of the points of C in the two elliptic curves (we assume that the given equations for E_1 and E_2 are minimal at p). The superscript ^{E_i} indicates on which curve we are computing these quantities. Let P_i be a point of infinite order in $E_i(\mathbb{Q})$ and write

$$c_i = \frac{h_p^{E_i}(P_i)}{\operatorname{Log}^{E_i}(P_i)^2},$$

where, as usual, $h_p^{E_i}$ is the global p-adic height of Mazur–Tate or Bernardi depending on whether the reduction is ordinary or not. Let $Q_1 = (0, \sqrt{a_0}) \in E_1(\mathbb{Q}(\sqrt{a_0}))$ and $Q_2 = (0, a_0) \in E_2(\mathbb{Q})$. We assume that a_0 is a square in $\mathbb{Q}_p$. Furthermore, let

$$\begin{aligned} C^{(1)}(\mathbb{Q}_p) &= C(\mathbb{Q}_p) \setminus (](0, \sqrt{a_0})[\cup](0, -\sqrt{a_0})[), \\ C^{(2)}(\mathbb{Q}_p) &= C(\mathbb{Q}_p) \setminus (]\infty^+[\cup]\infty^-[), \\ C^{(i)}(\mathbb{Q}) &= C(\mathbb{Q}) \cap C^{(i)}(\mathbb{Q}_p) \quad \text{for } i = 1, 2, \end{aligned}$$

where the inverted square brackets denote the residue disk modulo p around the given point and $\infty^\pm = (1 : \pm 1 : 0) \in C(\mathbb{Q})$.

Theorem 6.1 (Balakrishnan–Dogra[10]). *For each $i \in \{1, 2\}$, the following set is finite*:

$$W^i = \left\{ \sum_{q \neq p} \bigl(\lambda_q^{E_i}(\varphi_i(z_q) + Q_i) + \lambda_q^{E_i}(\varphi_i(z_q) - Q_i) - 2\lambda_q^{E_{3-i}}(\varphi_{3-i}(z_q))\bigr) : (z_q) \in \prod_{q \neq p} C(\mathbb{Q}_q) \setminus \{\varphi_i^{-1}(\pm Q_i)\} \right\}.$$

[10] With a small correction; see Remark 6.2.

Furthermore,

$$C^{(i)}(\mathbb{Q}) \subset \Big\{ z \in C^{(i)}(\mathbb{Q}_p) : 2\lambda_p^{E_{3-i}}(\varphi_{3-i}(z)) - \lambda_p^{E_i}(\varphi_i(z)+Q_i) - \lambda_p^{E_i}(\varphi_i(z)-Q_i) \\ - 2c_{3-i}\operatorname{Log}^{E_{3-i}}(\varphi_{3-i}(z))^2 + 2c_i \operatorname{Log}^{E_i}(\varphi_i(z))^2 + 2h_p^{E_i}(Q_i) \in W^i \Big\}.$$

The second assertion in Theorem 6.1 can be derived from the parallelogram law satisfied by the global p-adic height (as a consequence of Section 2A1(iii) and Section 2A2(iii)) and the fact that there is at most one quadratic function (up to multiplication by a scalar) on each of $E_1(\mathbb{Q})$ and $E_2(\mathbb{Q})$, due to the assumption on their ranks, in analogy to the proof of Theorem 1.7. The set of p-adic points described in the theorem is $C(\mathbb{Q}_p)_Z \cap C^{(i)}(\mathbb{Q}_p)$. We will explicitly determine the sets W^i for Example 6.3. For a general bielliptic curve we will give in Proposition 6.5 a description of a finite set containing W^i, hence giving a proof of finiteness of W^i.

Remark 6.2. If Q_1 is not defined over $\mathbb{Q}$, with the notation $\lambda_q^{E_1}(\varphi_1(z) \pm Q_1)$ in Theorem 6.1 we mean $\lambda_{\mathfrak{q}}^{E_1}(\varphi_1(z) \pm Q_1)$, where $\mathfrak{q}$ is any prime of $\mathbb{Q}(\sqrt{a_0})$ lying above the rational prime q. Indeed, since $\tau(Q_1) = -Q_1$, where $\langle\tau\rangle = \mathrm{Gal}(\mathbb{Q}(\sqrt{a_0})/\mathbb{Q})$, there is no dependence on $\mathfrak{q} \mid q$ and

$$h_p^{E_1}(Q_1) = \sum_q \lambda_q^{E_1}(Q_1).$$

The equations defining the sets $C(\mathbb{Q}_p)_Z \cap C^{(1)}(\mathbb{Q}_p)$ in [Balakrishnan and Dogra 2018, Corollary 8.1] contain a typo in the case when Q_1 is not in the saturation of $E_1(\mathbb{Q})$, which we have corrected in Theorem 6.1. Their formula has the term $2c_1 \operatorname{Log}^{E_1}(Q_1)^2$ in place of $2h_p^{E_1}(Q_1)$ and does not hold unless the two quantities are equal.

One of the advantages of computing rational points using Theorem 6.1 for a bielliptic curve, rather than the more general techniques developed in [Balakrishnan et al. 2019a], is that we do not need to have prior knowledge of any affine point in $C(\mathbb{Q})$.

Balakrishnan, Dogra and Müller [Balakrishnan and Dogra 2018] used Theorem 6.1, combined with the Mordell–Weil sieve, to determine precisely the rational points of two bielliptic curves. As in Section 4A, we suggest here that one can replace the computations of double Coleman integrals with computations involving the p-adic sigma function and division polynomials. We use the resulting algorithm to compute $C(\mathbb{Q}_p)_Z$ for a bielliptic curve whose rational points were already found using different Chabauty-type techniques by Wetherell [1997, Proposition 5.1] and Flynn and Wetherell [1999, Example 3.1]. Our methods lead to an alternative provable determination of $C(\mathbb{Q})$.

Example 6.3. Consider the bielliptic curve

$$C : y^2 = x^6 + x^2 + 1;$$

the associated elliptic curves are 496.a1 and 248.a1 [LMFDB 2019], given by the minimal models

$$E_1 : y^2 = x^3 + x + 1, \qquad E_2 : y^2 = x^3 + x^2 + 1.$$

We have

$$Q_1 = (0, 1) \in E_1(\mathbb{Q}), \qquad Q_2 = (0, 1) \in E_2(\mathbb{Q}).$$

Both elliptic curves have rank 1. Let $p = 3$, which is a prime of good reduction for C. Since E_1 is supersingular at p, we use Bernardi's p-adic height for our calculations.

Claim 1. *If $q \neq p, 2$ and $z \in C(\mathbb{Q}_q) \setminus \{\varphi_i^{-1}(\pm Q_i)\}$, then*

$$w_{q,i}(z) := \lambda_q^{E_i}(\varphi_i(z) + Q_i) + \lambda_q^{E_i}(\varphi_i(z) - Q_i) - 2\lambda_q^{E_{3-i}}(\varphi_{3-i}(z)) = 0.$$

Proof. The curves E_1 and E_2 have everywhere good reduction except at 2 and 31. At 31, the Tamagawa number of each E_i is trivial. Assume first that $\varphi_i(z) \neq O_{E_i}$. Then, for each $q \neq p$, the quasiparallelogram law (3) gives

$$w_{q,i}(z) = 2\bigl(\lambda_q^{E_i}(\varphi_i(z)) + \lambda_q^{E_i}(Q_i) - \log|x(\varphi_i(z))|_q - \lambda_q^{E_{3-i}}(\varphi_{3-i}(z))\bigr);$$

thus, if $q \neq 2$, by Lemma 2.1(i),

$$\begin{aligned} w_{q,i}(z) &= 2(\log(\max\{1, |x(\varphi_i(z))|_q\}) - \log(\max\{1, |x(\varphi_{3-i}(z))|_q\}) - \log|x(\varphi_i(z))|_q) \\ &= 2(\log(\max\{1, |x(\varphi_i(z))|_q\}) - \log(\max\{1, |x(\varphi_i(z))|_q^{-1}\}) - \log|x(\varphi_i(z))|_q) = 0. \end{aligned}$$

It remains to consider the case $\varphi_i(z) = O_{E_i}$. Then $\varphi_{3-i}(z) \in \{\pm Q_{3-i}\}$ and

$$w_{q,i}(z) = 2\lambda_q^{E_i}(Q_i) - 2\lambda_q^{E_{3-i}}(Q_{3-i}) = 0$$

by Proposition 2.2, since Q_i and Q_{3-i} are integral and the Tamagawa numbers at q are equal to 1. □

Claim 2. *We have*

$$W^1 = \{0, \log 2\}, \qquad W^2 = \{-\log 2, -2\log 2\}.$$

Proof. By Claim 1,

$$W^i = \bigl\{w_{2,i}(z) := \lambda_2^{E_i}(\varphi_i(z) + Q_i) + \lambda_2^{E_i}(\varphi_i(z) - Q_i) - 2\lambda_2^{E_{3-i}}(\varphi_{3-i}(z)) : z \in C(\mathbb{Q}_2) \setminus \{\varphi_i^{-1}(\pm Q_i)\}\bigr\}.$$

First note that the curve E_1 has Tamagawa number equal to 1 at 2, whereas E_2 has Tamagawa number equal to 2 and reduction type III. If $|x(z)|_2 \leq 1$, then $\varphi_2(z)$ has good reduction at 2 and $\lambda_2^{E_2}(\varphi_2(z)) = \log|x(z)^{-2}|_2$; otherwise $\varphi_2(z)$ reduces to a singular point modulo 2 and, by Proposition 2.4, $\lambda_2^{E_2}(\varphi_2(z)) = -\frac{1}{2}\log 2$. Furthermore $\lambda_2^{E_2}(Q_2) = -\frac{1}{2}\log 2$. Therefore, similarly to the proof of Claim 1, if $\varphi_1(z) \neq O_{E_1}$, then by the quasiparallelogram law we have

$$w_{2,1}(z) = 2\bigl(\lambda_2^{E_1}(\varphi_1(z)) - \lambda_2^{E_2}(\varphi_2(z)) - \log|x(\varphi_1(z))|_2\bigr) = \begin{cases} 0 & \text{if } |x(z)|_2 \leq 1, \\ \log 2 & \text{if } |x(z)|_2 > 1; \end{cases}$$

for the remaining points $z = \infty^{\pm}$ we get

$$w_{2,1}(z) = -2\lambda_2^{E_2}(Q_2) = \log 2,$$

thus proving the claim for W^1. The set W^2 is determined in a very similar fashion and we leave the details to the reader. □

We can now compute $C(\mathbb{Q}_p)_Z$ as a union of the two $C(\mathbb{Q}_p)_Z \cap C(\mathbb{Q}_p)^{(i)}$. We find

$$C(\mathbb{Q}_p)_Z = \left\{\infty^{\pm}, (0, \pm 1), \left(\pm\tfrac{1}{2}, \pm\tfrac{9}{8}\right)\right\} \sqcup A \tag{18}$$

where A is a set of size 4. Note, however, that up to the automorphisms $(x, y) \mapsto (-x, y)$, $(x, y) \mapsto (x, -y)$ and their composites, A actually consists of one point:

$$P = (2\cdot 3 + 2\cdot 3^3 + 2\cdot 3^5 + 3^8 + O(3^9), 2 + 2\cdot 3 + 2\cdot 3^3 + 2\cdot 3^5 + 3^6 + 2\cdot 3^8 + O(3^9)).$$

We follow the same strategy to the one of the proof of [Balakrishnan and Dogra 2018, Theorem 8.6] to rule out the possibility that P could be rational. The image of the point P under φ_2 is a point in $E_2(\mathbb{Q}_p)$ whose x-coordinate has valuation $\operatorname{ord}_p(x(\varphi_2(P))) = -2$. On the other hand, the Mordell–Weil group $E_2(\mathbb{Q}) \cong \mathbb{Z}$ is generated by Q_2 and, thus, if $\varphi_2(P) \in E_2(\mathbb{Q})$, there must exist a multiple of Q_2 whose x-coordinate has p-adic valuation equal to -2. As the smallest multiple of Q_2 in the formal group at p is $6Q_2 = \left(\frac{55}{81}, -\frac{971}{729}\right)$, we have reached a contradiction, since the set of points in the formal group whose x-coordinate has valuation at most -4 is a group.

6A. ***Explicit formulae for the sets W^i.*** Theorem 6.1 asserts that the sets W^i, for $i = 1, 2$, are finite, but does not describe them explicitly. In order to obtain an implementation for the computations of the sets $C(\mathbb{Q}_p)_Z \cap C^{(i)}(\mathbb{Q}_p)$ for an arbitrary genus 2 bielliptic curve C, it would be convenient to have a characterisation of W^i that can be made algorithmic, in analogy with that of the sets W_q of Theorems 1.6 and 1.7.

We assume in this section that the coefficients a_0, a_2, a_4 defining C are in $\mathbb{Z}$.

For $i = 1, 2$, let $W_q^{E_{i,\min}}$ be the set W_q from Section 1 for a global minimal model $E_{i,\min}$ of E_i if q is a prime of bad reduction and with nontrivial Tamagawa number. If $E_{i,\min}$ has good reduction at $q \in \{2, 3\} \setminus \{p\}$ and $\bar{E}_{i,\min}(\mathbb{F}_q) = \{O\}$ or $q = 2$ and $E_{i,\min}$ has split multiplicative reduction I_1 at q, let $W_q^{E_{i,\min}} = \varnothing$. For all other $q \neq p$, let $W_q^{E_{i,\min}} = \{0\}$.

Let $W_q^{E_i}$ be the set of values attained by $\lambda_q^{E_i}$ on the points of $E_i(\mathbb{Q}_q)$ of the form (x, y) with $x, y \in \mathbb{Z}_q$. Let

$$V_q^{E_i} = W_q^{E_i} \cup \{0\}.$$

Write

$$\delta^{E_i} = \frac{\Delta^{E_i}}{\Delta^{E_{i,\min}}},$$

where Δ^{E_i} and $\Delta^{E_{i,\min}}$ are the discriminants of E_i and $E_{i,\min}$.

For sets A, B of elements in a field F, we write $A + B$ for their Minkowski addition and $-A$ for the set consisting of the additive inverses of the elements in A. If $A = \{a\}$, we write $a + B$ for $A + B$.

Lemma 6.4.

$$W_q^{E_i} = \tfrac{1}{6}\log|\delta^{E_i}|_q + \left(W_q^{E_{i,\min}} \cup \left\{2k \log q : 1 \le k \le \tfrac{1}{12}\operatorname{ord}_q(\delta^{E_i})\right\}\right).$$

In particular, $W_q^{E_i}$ is finite; it equals $\{0\}$ for all but finitely many q.

Proof. Let x, y and $x_{\min}$, $y_{\min}$ be the Weierstrass coordinates for E_i and $E_{i,\min}$, respectively. Then there exist $u, r, s, t \in \mathbb{Q}$, $u \neq 0$, such that

$$x = u^2 x_{\min} + r, \qquad y = u^3 y_{\min} + s u^2 x_{\min} + t.$$

Since $\operatorname{ord}_q(\Delta^{E_{i,\min}}) \le \operatorname{ord}_q(\Delta^{E_i})$ for each prime q, the scalars u, r, s, t are furthermore all integral (see [Connell 1999, Lemma 5.3.1]).

Now let $P \in E_i(\mathbb{Q}_q)$ such that $x(P), y(P) \in \mathbb{Z}_q$. By (4), we have

$$\lambda_q^{E_i}(P) = \lambda_q^{E_{i,\min}}(P) + \tfrac{1}{6}\log|\delta^{E_i}|_q.$$

If $x_{\min}(P) \in \mathbb{Z}_q$, then $\lambda_q^{E_{i,\min}}(P) \in W_q^{E_{i,\min}}$ by Propositions 2.4, 2.2 and Lemma 2.3. Otherwise, by Lemma 2.1(i), we have $\lambda_q^{E_{i,\min}}(P) = \log|(x(P)-r)/u^2|_q$, where by assumption $|x(P)-r|_q \le 1$ and the valuation of $(x(P)-r)/u^2$ is an even negative integer. Since $\delta^{E_i} = u^{12}$, this completes the proof of $\subseteq$. To see why the inclusion is actually an equality, notice that the preimage of an integral point in $E_{i,\min}(\mathbb{Q}_q)$ is certainly an integral point on $E_i(\mathbb{Q}_q)$. Furthermore, the points on $E_{i,\min}(\mathbb{Q}_q)$ in the formal group are parametrised by $t \in q\mathbb{Z}_q$ as follows: $t \mapsto (x_{\min}(t), y_{\min}(t))$, where

$$x_{\min}(t) = \frac{1}{t^2} - \frac{a_{1,\min}}{t} - a_{2,\min} - a_{3,\min}t + \cdots \in \mathbb{Z}[a_{1,\min}, \dots, a_{6,\min}]((t)),$$

where $a_{1,\min}, \dots, a_{6,\min}$ are the Weierstrass coefficients of $E_{i,\min}$; in particular, we have $\operatorname{ord}_q(x_{\min}(t)) = -2\operatorname{ord}_q(t)$. Thus for each $1 \le k \le \frac{1}{12}\operatorname{ord}_q(\delta^{E_i})$, setting $t = q^k$ gives a point on $E_{i,\min}(\mathbb{Q}_q)$ whose preimage in $E_i(\mathbb{Q}_q)$ has integral x-coordinate. The second assertion of the lemma follows from the explicit description of the sets $W_q^{E_{i,\min}}$. □

Proposition 6.5. *With the notation of Theorem 6.1, suppose that* $\operatorname{ord}_\ell(a_0) \in \{0, 1\}$ *for each prime* ℓ. *For each prime* $q \neq p$, *let*

$$W_q^{1\prime} = \{2v + 2\lambda_q^{E_1}(Q_1) : v \in V_q^{E_1} + (-W_q^{E_2})\} \cup \{2v + 2\lambda_q^{E_1}(Q_1) - 2\log|a_0|_q : v \in W_q^{E_1}\}$$
$$W_q^{2\prime} = \{2v + 2\lambda_q^{E_2}(Q_2) - 2\log|a_0|_q : v \in W_q^{E_2} + (-V_q^{E_1})\} \cup \{2v + 2\lambda_q^{E_2}(Q_2) : v \in -W_q^{E_1}\}.$$

Then W^i *is a subset of the finite set*

$$W^{i\prime} = \Big\{\sum_{q\neq p} w'_{q,i} : w'_{q,i} \in W_q^{i\prime}\Big\} = \Big\{2h_p^{E_i}(Q_i) - 2\lambda_p^{E_i}(Q_i) + \sum_{q\neq p}(w'_{q,i} - 2\lambda_q^{E_i}(Q_i)) : w'_{q,i} \in W_q^{i\prime}\Big\}.$$

Proof. By definition,

$$W^i = \Big\{\sum_{q\neq p} w_{q,i} : w_{q,i} \in W_q^i\Big\},$$

where

$$W_q^i = \{w_{q,i}(z) := \lambda_q^{E_i}(\varphi_i(z) + Q_i) + \lambda_q^{E_i}(\varphi_i(z) - Q_i) - 2\lambda_q^{E_{3-i}}(\varphi_{3-i}(z)) : z \in C(\mathbb{Q}_q) \setminus \{\varphi_i^{-1}(\pm Q_i)\}\}.$$

Let $z \in C(\mathbb{Q}_q) \setminus \{\varphi_i^{-1}(\pm Q_i)\}$. If $\varphi_i(z) = O_{E_i}$, then

$$w_{q,i}(z) = 2\lambda_q^{E_i}(Q_i) - 2\lambda_q^{E_{3-i}}(Q_{3-i}),$$

which belongs to $2\lambda_q^{E_i}(Q_i) - 2W_q^{E_{3-i}}$. When $i = 2$, note that, while it is not always the case that Q_1 is defined over $\mathbb{Q}_q$ (and hence that $\lambda_q^{E_1}(Q_1) \in W_q^{E_1}$), here this follows from the assumption that its preimage under φ_1 is in $C(\mathbb{Q}_q)$.

Otherwise, by the quasiparallelogram law (3), we have

$$\begin{aligned} w_{q,i}(z) &= 2\big(\lambda_q^{E_i}(\varphi_i(z)) + \lambda_q^{E_i}(Q_i) - \log|x(\varphi_i(z))|_q - \lambda_q^{E_{3-i}}(\varphi_{3-i}(z))\big) \\ &= 2\big(\lambda_q^{E_i}(\varphi_i(z)) + \lambda_q^{E_i}(Q_i) + \log|x(\varphi_{3-i}(z))|_q - \log|a_0|_q - \lambda_q^{E_{3-i}}(\varphi_{3-i}(z))\big). \end{aligned}$$

Note that the assumption that $0 \le \operatorname{ord}_q(a_0) \le 1$ implies that, for each $i = 1, 2$,

$$|x(\varphi_i(z))|_q > 1 \Rightarrow |x(\varphi_{3-i}(z))|_q < 1 \tag{19}$$

$$|x(\varphi_{3-i}(z))|_q < 1 \Rightarrow |x(\varphi_i(z))|_q \ge 1. \tag{20}$$

If $|x(\varphi_i(z))|_q > 1$, then $\varphi_i(z)$ reduces to a nonsingular point modulo q, with respect to the Weierstrass equation for E_i. Thus $\lambda_q^{E_i}(\varphi_i(z)) = \log|x(\varphi_i(z))|_q$. Furthermore, by (19), $\varphi_{3-i}(z)$ is integral with respect to the Weierstrass equation defining E_{3-i} and we have $\lambda_q^{E_{3-i}}(\varphi_{3-i}(z)) \in W_q^{E_{3-i}}$. Therefore

$$\frac{w_{q,i}(z)}{2} \in \lambda_q^{E_i}(Q_i) + (-W_q^{E_{3-i}}).$$

Similarly, if $|x(\varphi_{3-i}(z))|_q > 1$, then

$$\frac{w_{q,i}(z)}{2} \in (\lambda_q^{E_i}(Q_i) - \log|a_0|_q) + W_q^{E_i}.$$

It remains to consider the case when $|x(z)|_q = 1$. Then

$$\frac{w_{q,i}(z)}{2} \in W_q^{E_i} + (-W_q^{E_{3-i}}) + \begin{cases} \lambda_q^{E_i}(Q_i) & \text{if } i = 1, \\ \lambda_q^{E_i}(Q_i) - \log|a_0|_q & \text{if } i = 2. \end{cases} \qquad \square$$

Proposition 6.5 and Lemma 6.4 turn Theorem 6.1 into an algorithm for computing a finite set of p-adic points containing $C(\mathbb{Q})$, for an arbitrary genus 2 bielliptic curve C whose associated elliptic curves E_1 and E_2 have Mordell–Weil rank equal to 1. Furthermore, to improve the estimates of the sets W^i provided by Proposition 6.5 we may use the fact that the contributions at primes of potential good reduction for C are trivial (cf. [Balakrishnan and Dogra 2018, Theorem 1.2(i)]). It seems unlikely to the author that the elementary approach of Proposition 6.5 could show the latter for an arbitrary curve, since it is hard to imagine how the proof could be made sensitive to the difference between C being of potential good reduction and its Jacobian only being of potential good reduction. Furthermore, even at primes not of potential good reduction, the sets $W_q^{i'}$ might be larger than W_q^i. Nevertheless, having fixed an explicit curve C, the steps of the proof of the proposition should guide the reader through computing W^i precisely.

Here we are instead interested in an algorithm which does not require prior computations of W^i. So let $W^{i''}$ be obtained from $W^{i'}$ of Proposition 6.5 by replacing $W_q^{i'}$ with $\{0\}$ whenever q is a prime of potential good reduction. We implemented in `SageMath` the results of this section and could test them for several bielliptic curves, including the ones of [Balakrishnan and Dogra 2018] and the bielliptic curve

$$C : y^2 = (x^2+1)(x^2+3)(x^2+7), \tag{21}$$

which appears in [Flynn and Wetherell 1999, p. 532] as the only curve amongst 50 bielliptic curves for which the methods of Flynn and Wetherell to find rational points failed.

For instance, in Example 6.3 and for the curve of [Balakrishnan and Dogra 2018, §8.3] we have $W^i = W^{i'} = W^{i''}$ for each $i = 1$ and $i = 2$, but for the curve of [Balakrishnan and Dogra 2018, §8.4], the sets $W^{i''}$ have size 3, whereas W^i has size 1.

We also remark that in Example 6.3, as well as the two examples of [Balakrishnan and Dogra 2018], the elliptic curve E_1 has trivial Tamagawa number at all primes and E_2 has trivial Tamagawa numbers everywhere except for at one prime where it has Tamagawa number equal to two or three. In other words, finding precise expressions for the sets W^i by hand is straightforward. In Example 6.3 as well as [Balakrishnan and Dogra 2018, §8.3] the task is further simplified by the fact that the Weierstrass equations for E_1 and E_2 have minimal discriminant. On the other hand, we cannot expect this for a generic curve. For example, the elliptic curves corresponding to (21) have Tamagawa numbers (2, 1) respectively (4, 2) at the primes not of potential good reduction and analysing what happens at each prime by hand might be rather tedious. In this case, we find $\#W^{1''} = \#W^{2''} = 18$ and in fact this results in many points in $C(\mathbb{Q}_p)$ that are probably not rational (142 when $p = 5$).

Acknowledgements

I am very grateful to Jennifer Balakrishnan for many useful discussions and for providing me with helpful feedback on several drafts. This paper started from questions raised at group meetings organised by Minhyong Kim in which I took part together with Jamie Beacom, Noam Kantor and Alex Saad. I am indebted to all of them and thank Minhyong for encouraging me to write up. I also thank the anonymous referee, as well as Steffen Müller, and my DPhil examiners Victor Flynn and Chris Wuthrich, for several useful suggestions, which led to many improvements to the article. I was supported by EPSRC and by Balliol College through a Balliol Dervorguilla scholarship, and by an NWO Vidi grant.

References

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

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

[Balakrishnan and Dogra 2018] J. S. Balakrishnan and N. Dogra, "Quadratic Chabauty and rational points, I: p-adic heights", *Duke Math. J.* **167**:11 (2018), 1981–2038. With an appendix by J. S. Müller. MR Zbl

[Balakrishnan et al. 2010] J. S. Balakrishnan, R. W. Bradshaw, and K. S. Kedlaya, "Explicit Coleman integration for hyperelliptic curves", pp. 16–31 in *Algorithmic number theory* (Nancy, France, 2010), edited by G. Hanrot et al., Lecture Notes in Comput. Sci. **6197**, Springer, 2010. MR Zbl

[Balakrishnan et al. 2016] 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. MR Zbl

[Balakrishnan et al. 2018] 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**:1-2 (2018), 369–428. MR Zbl

[Balakrishnan et al. 2019a] J. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, "Explicit Chabauty–Kim for the split Cartan modular curve of level 13", *Ann. of Math.* (2) **189**:3 (2019), 885–944. MR Zbl

[Balakrishnan et al. 2019b] J. S. Balakrishnan, A. Besser, F. Bianchi, and J. S. Müller, "Explicit quadratic Chabauty over number fields", 2019. To appear in *Israel J. Math.* arXiv

[Balakrishnan et al. 2019c] J. S. Balakrishnan, F. Bianchi, V. Cantoral-Farfán, M. Çiperiani, and A. Etropolski, "Chabauty–Coleman experiments for genus 3 hyperelliptic curves", pp. 67–90 in *Research directions in number theory*, edited by J. Balakrishnan et al., Assoc. Women Math. Ser. **19**, Springer, 2019.

[Bernardi 1981] D. Bernardi, "Hauteur p-adique sur les courbes elliptiques", pp. 1–14 in *Séminaire de Théorie des Nombres* (Paris, 1979-1980), edited by M.-J. Bertin, Progr. Math. **12**, Birkhäuser, Boston, 1981. MR Zbl

[Bianchi 2019] F. Bianchi, Code for "Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture", 2019, available at https://github.com/bianchifrancesca/quadratic_chabauty. Sage math code.

[Coates and Kim 2010] J. Coates and M. Kim, "Selmer varieties for curves with CM Jacobians", *Kyoto J. Math.* **50**:4 (2010), 827–852. MR Zbl

[Coleman and Gross 1989] R. F. Coleman and B. H. Gross, "p-adic heights on curves", pp. 73–81 in *Algebraic number theory*, edited by J. Coates et al., Adv. Stud. Pure Math. **17**, Academic Press, Boston, 1989. MR Zbl

[Connell 1999] I. Connell, "Elliptic curve handbook", preprint, 1999, available at http://webs.ucm.es/BUCM/mat/doc8354.pdf.

[Cremona et al. 2006] J. E. Cremona, M. Prickett, and S. Siksek, "Height difference bounds for elliptic curves over number fields", *J. Number Theory* **116**:1 (2006), 42–68. MR Zbl

[Ellenberg and Hast 2017] J. S. Ellenberg and D. R. Hast, "Rational points on solvable curves over $\mathbb{Q}$ via non-abelian Chabauty", preprint, 2017. arXiv

[Flynn and Wetherell 1999] E. V. Flynn and J. L. Wetherell, "Finding rational points on bielliptic genus 2 curves", *Manuscripta Math.* **100**:4 (1999), 519–533. MR Zbl

[Harvey 2008] D. Harvey, "Efficient computation of p-adic heights", *LMS J. Comput. Math.* **11** (2008), 40–59. MR Zbl

[Katz 1976] N. M. Katz, "p-adic interpolation of real analytic Eisenstein series", *Ann. of Math.* (2) **104**:3 (1976), 459–571. MR Zbl

[Kim 2005] M. Kim, "The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel", *Invent. Math.* **161**:3 (2005), 629–656. MR Zbl

[Kim 2009] M. Kim, "The unipotent Albanese map and Selmer varieties for curves", *Publ. Res. Inst. Math. Sci.* **45**:1 (2009), 89–133. MR Zbl

[Kim 2010a] M. Kim, "Massey products for elliptic curves of rank 1", *J. Amer. Math. Soc.* **23**:3 (2010), 725–747. Appendix and correction by J. S. Balakrishnan, K. S. Kedlaya, and M. Kim in **24**:1 (2011), 281–291. MR Zbl

[Kim 2010b] M. Kim, "p-adic L-functions and Selmer varieties associated to elliptic curves with complex multiplication", *Ann. of Math.* (2) **172**:1 (2010), 751–759. MR Zbl

[Koblitz 1984] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2nd ed., Grad. Texts in Math. **58**, Springer, 1984. MR Zbl

[Kolyvagin 1988] V. A. Kolyvagin, "Finiteness of $E(\mathbb{Q})$ and Ш$(E, \mathbb{Q})$ for a subclass of Weil curves", *Izv. Akad. Nauk SSSR Ser. Mat.* **52**:3 (1988), 522–540. In Russian; translated in *Math. USSR-Izv.* **32**:3 (1989), 523–541. MR Zbl

[Lang 1973] S. Lang, *Elliptic functions*, Addison-Wesley, Reading, MA, 1973. MR Zbl

[LMFDB 2019] The LMFDB Collaboration, "The L-functions and modular forms database", electronic reference, 2019, available at http://www.lmfdb.org. Online; accessed 19 March 2019.

[Mazur and Tate 1991] B. Mazur and J. Tate, "The p-adic sigma function", *Duke Math. J.* **62**:3 (1991), 663–688. MR Zbl

[Mazur et al. 2006] B. Mazur, W. Stein, and J. Tate, "Computation of p-adic heights and log convergence", *Doc. Math.* Coates Birthday volume (2006), 577–614. MR Zbl

[Murty and Murty 1997] M. R. Murty and V. K. Murty, *Non-vanishing of L-functions and applications*, Progr. Math. **157**, Birkhäuser, Basel, 1997. MR Zbl

[Pethő et al. 1999] A. Pethő, H. G. Zimmer, J. Gebel, and E. Herrmann, "Computing all S-integral points on elliptic curves", *Math. Proc. Cambridge Philos. Soc.* **127**:3 (1999), 383–402. MR Zbl

[SageMath 2017–2019] W. A. Stein et al., "Sage mathematics software", 2017–2019, available at http://www.sagemath.org. Versions 7.5.1–8.6.

[Silverman 1988] J. H. Silverman, "Computing heights on elliptic curves", *Math. Comp.* **51**:183 (1988), 339–358. MR Zbl

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. **151**, Springer, 1994. MR Zbl

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Grad. Texts in Math. **106**, Springer, 2009. MR Zbl

[Smart 1994] N. P. Smart, "S-integral points on elliptic curves", *Math. Proc. Cambridge Philos. Soc.* **116**:3 (1994), 391–399. MR Zbl

[Stein and Wuthrich 2013] W. Stein and C. Wuthrich, "Algorithms for the arithmetic of elliptic curves using Iwasawa theory", *Math. Comp.* **82**:283 (2013), 1757–1792. MR Zbl

[Stoll 2006] M. Stoll, "Finite descent obstructions and rational points on curves", preprint, 2006, available at https://tinyurl.com/stollpreprint. Draft version no. 8.

[Stoll 2007] M. Stoll, "Finite descent obstructions and rational points on curves", *Algebra Number Theory* **1**:4 (2007), 349–391. MR Zbl

[Stroeker and Tzanakis 1994] R. J. Stroeker and N. Tzanakis, "Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms", *Acta Arith.* **67**:2 (1994), 177–196. MR Zbl

[Vignéras 1981] M.-F. Vignéras, "Valeur au centre de symétrie des fonctions L associées aux formes modulaires", pp. 331–356 in *Séminaire de Théorie des Nombres* (Paris, 1979-1980), edited by M.-J. Bertin, Progr. Math. **12**, Birkhäuser, Boston, 1981. Zbl

[Waldspurger 1981] J.-L. Waldspurger, "Sur les coefficients de Fourier des formes modulaires de poids demi-entier", *J. Math. Pures Appl.* (9) **60**:4 (1981), 375–484. MR Zbl

[Wetherell 1997] J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, Ph.D. thesis, University of California, Berkeley, 1997, available at https://search.proquest.com/docview/304343505.

[Wuthrich 2004] C. Wuthrich, "On p-adic heights in families of elliptic curves", *J. Lond. Math. Soc.* (2) **70**:1 (2004), 23–40. MR Zbl

Communicated by Kiran S. Kedlaya
Received 2019-04-12 Revised 2020-02-01 Accepted 2020-04-23

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

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2020 is US $415/year for the electronic version, and $620/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 14 No. 9 2020