QUADRATIC CHABAUTY AND RATIONAL POINTS I: p-ADIC HEIGHTS

JENNIFER S. BALAKRISHNAN AND NETAN DOGRA

Abstract. We describe how p-adic heights can be used to find rational points on higher genus curves by making explicit some aspects of Kim's nonabelian Chabauty program. We give the first examples beyond the Chabauty-Coleman method where nonabelian Chabauty can be used to precisely determine the set of rational points of a curve defined over $\mathbb{Q}$ or a quadratic number field.

Contents

1. Introduction

Let X be a smooth projective curve of genus $g > 1$ defined over a number field K. By Faltings' work on the Mordell conjecture, the set of K-rational points on X, denoted $X(K)$, is known to be finite [17]. However, the method of proof is not constructive and does not produce the set $X(K)$. Nevertheless, in certain cases, it is possible to compute $X(K)$, and perhaps the most widely applicable technique is the p-adic method of Chabauty and Coleman.

The Chabauty-Coleman method imposes linear conditions on the Jacobian of X, and in an essential way, requires that the Mordell-Weil rank of the Jacobian is less than g. Kim has proposed that one can lift this restriction on rank by replacing the Jacobian of X with an object known as the Selmer variety [22]. In this paper, we discuss new techniques for studying Selmer varieties, which we translate into methods for determining the set $X(K)$ in a number of new cases. In particular, we study certain curves whose Jacobians have Mordell-Weil rank equal to g.

Date: January 5, 2016.

To give some context for our results, let us begin by recalling the Chabauty-Coleman method. Let J denote the Jacobian of X, let p be a prime of good reduction, and let $\mathfrak{p}$ be a prime above p. Let

$$\log_J : J(K_{\mathfrak{p}}) \to H^0(X_{\mathfrak{p}}, \Omega^1)^*$$

be the $\mathfrak{p}$-adic logarithm map for the abelian variety J. Suppose that $X(K) \neq \emptyset$, and for convenience, that we know one point b in $X(K)$. If the Mordell-Weil rank of J is less than g, the method of Chabauty [9] produces a finite set of $\mathfrak{p}$-adic points on X, which we shall denote $X(K_{\mathfrak{p}})_1$. The set $X(K_{\mathfrak{p}})_1$ is a subset of $X(K_{\mathfrak{p}})$, and further, $X(K)$ is a subset of $X(K_{\mathfrak{p}})_1$. Following Coleman [11] the set $X(K_{\mathfrak{p}})_1$ may be interpreted as the zeroes of a p-adic path integral

$$X(K_{\mathfrak{p}})_1 = \left\{ z \in X(K_{\mathfrak{p}}) : \int_b^z \omega = 0 \right\}$$

for some differential ω in $H^0(X_{K_{\mathfrak{p}}}, \Omega^1_X)$. By further interpreting this p-adic path integral as a p-adic power series and solving for its zeros, in practice, one can often recover $X(K)$. This is known as the *Chabauty-Coleman method*.

The Chabauty-Coleman method requires that the Mordell-Weil rank of the Jacobian be less than the genus, which is somewhat restrictive. As such one would like to have a refinement of the Jacobian which remembers more information about the set $X(K)$. The insight of Kim [21] is that rather than trying to generalise the Jacobian of X, it is easier its Galois cohomological avatar: the Selmer group. In [22], Kim defined a family of *Selmer varieties* $\mathrm{Sel}(U_n)$ giving a decreasing sequence of subsets [2]

$$X(K_{\mathfrak{p}})_1 \supset X(K_{\mathfrak{p}})_2 \supset \dots$$

of $X(K_{\mathfrak{p}})_n$, which can be computed in terms of *iterated* p-adic path integrals. The sets $X(K_{\mathfrak{p}})_n$ contain $X(K)$, so by proving finiteness of $X(K_{\mathfrak{p}})_n$ and explicitly computing it, one can hope to recover $X(K)$. Note that when $K = \mathbb{Q}$, conjectures of Bloch and Kato imply that $X(\mathbb{Q}_p)_n$ is finite for n sufficiently large [22].

However, at present the only documented example of a curve X where $X(K_{\mathfrak{p}})_n$ has been proved to give more information than $X(K_{\mathfrak{p}})_1$ is when $K = \mathbb{Q}$ and X is a curve whose Jacobian is isogenous to a product of CM abelian varieties. In this case, Coates and Kim prove in [10] that for $n \gg 0$, $X(\mathbb{Q}_p)_n$ is finite. Even in this case it is not clear how to actually compute $X(\mathbb{Q}_p)_n$.

In this paper, we give techniques to handle some cases beyond the scope of classical Chabauty, by computing finite sets containing $X(K_{\mathfrak{p}})_2$. The methods used are a generalisation of those employed to study integral points on hyperelliptic curves using p-adic heights [6], combined with new methods for relating unipotent path torsors to p-adic heights [16].

In [6], one works with a hyperelliptic curve $X/\mathbb{Q}$ of genus g with a model

$$y^2 = f(x) = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_0, \qquad a_i \in \mathbb{Z}. \tag{1}$$

Let T_0 denote the set of primes of bad reduction for this model and let p be a prime of good reduction. Suppose that the polynomial f does not reduce to a square in $(\mathbb{Z}/q)[x]$ for any prime q. Let $Y = \mathrm{Spec}(\mathbb{Z}[x, y]/(y^2 - f(x)))$, so that $Y(\mathbb{Z})$ denotes the set of integral solutions to (1). Using p-adic heights, one can compute $Y(\mathbb{Z})$:

Theorem 1 ("Quadratic Chabauty", [6])**.** *Let $\Omega \subset \mathbb{Q}_p$ be the explicitly computable, finite set of values taken by the sum of the local heights*

$$-\sum_{v \in T_0} h_v(z_v - \infty),$$

for (z_v) in $\prod_{v \in T_0} Y(\mathbb{Z}_v)$. Suppose that the Mordell-Weil rank of J is g. Then there is a symmetric bilinear map

$$B : H^0(X_{\mathbb{Q}_p}, \Omega^1)^* \times H^0(X_{\mathbb{Q}_p}, \Omega^1)^* \to \mathbb{Q}_p$$

such that $Y(\mathbb{Z}) \subset Y(\mathbb{Z}_p)$ is contained inside the finite set of solutions to

$$h_p(z - \infty) + B(\log_J(z - \infty), \log_J(z - \infty)) \in \Omega.$$

In the present work, we give a generalisation of this theorem which also allows us to study *rational* points in some special cases where the Mordell-Weil rank is not less than the genus. To state our results more precisely, we fix some notation. Let K be $\mathbb{Q}$ or an imaginary quadratic field, and let X/K be a smooth projective curve of genus $g > 1$ with a K-rational point b. Let T_0 be the set of primes of bad reduction for X, let p be a prime of $\mathbb{Q}$ such that $\{v|p\} \cap T_0$ is empty, and let $T = T_0 \cup \{v|p\}$. We show that $X(K_{\mathfrak{p}})_2$ is finite whenever the rank of $J(K)$ minus the rank of the Néron-Severi group of J, denoted $\mathrm{NS}(J)$, is less than $g - 1$ (see Lemma 3).

In particular, the main example we consider is the situation when the rank of the Jacobian of X is g and the rank of $\mathrm{NS}(J)$ is greater than 1 (for a result applying when the rank is greater than the genus, see Proposition 2). We further assume that the map

$$J(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p \xrightarrow{\simeq} J(K_{\mathfrak{p}}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

is an isomorphism. Let $\overline{X} := X \times_K \overline{K}$. By our assumptions on the Néron-Severi group, there is a cycle Z in $X \times X$ whose image in $\wedge^2 H^1_{\acute{e}t}(\overline{X})$ under

$$\mathbb{Q}_p(-1) \to H^2_{\acute{e}t}(\overline{X} \times \overline{X}, \mathbb{Q}_p) \to H^1_{\acute{e}t}(\overline{X}, \mathbb{Q}_p) \otimes H^1_{\acute{e}t}(\overline{X}, \mathbb{Q}_p) \to \wedge^2 H^1_{\acute{e}t}(\overline{X}, \mathbb{Q}_p)$$

is nonzero (where the maps are, from left to right, the cycle class, the Kunneth projector, and the antisymmetric projection), and such that the intersection number of Z with $\Delta - X \times P_1 - P_2 \times X$ is zero, where P_1 and P_2 are any points on X. For distinct points b and z in X intersecting $\Delta_X^{-1} Z$ properly, we associate a cycle $D(b, z)$ to the triple (b, z, Z) (see Definition 11).

Theorem 2. *Let X/K be a smooth projective curve of genus $g > 1$. Let $b, z, D(b, z)$ be as above. Let $X' := X - i_\Delta^{-1}|Z|$.*
(i): For each prime $v \nmid p$, $h_v(z, D(b, z))$ takes only finitely many values for z in $X'(\mathbb{Q}_v)$. If v is a prime of potential good reduction, then $h_v(z, D(b, z))$ is identically zero.
(ii): Suppose the rank of $J(K)$ is g and the rank of $\mathrm{NS}(J)$ is greater than 1. Let $\Omega \subset \mathbb{Q}_p$ be the finite set of values taken by the sum of local heights

$$-\sum_{v \nmid p} h_v(z_v, D(b, z_v))$$

for (z_v) in $\prod_{v \nmid p} X'(K_v)$. Then there is a symmetric bilinear map

$$B : H^0(X_{K_{\mathfrak{p}}}, \Omega^1)^* \times H^0(X_{K_{\mathfrak{p}}}, \Omega^1)^* \to \mathbb{Q}_p$$

such that the set of z in $X'(K_{\mathfrak{p}})$ for which

$$h_{\mathfrak{p}}(z, D(b,z)) - B(\log_J(z-b), D(b,z)) \in \Omega$$

is finite and contains $X(K_{\mathfrak{p}})_2 \cap X'(K_{\mathfrak{p}})$.

To produce an algorithm using Theorem 2 to find a finite set containing $X(K_{\mathfrak{p}})_2$, one needs to explicitly compute the cycle Z and the local heights h_v. In this paper we focus on the simplest such example, which we describe below.

Remark 1. There is also an affine version of this result (describing integral points of X under weakened assumptions on the Néron-Severi group of J), and in §7 we show that Theorem 1 can be recovered from this.

Remark 2. It should perhaps be emphasised that the link with p-adic heights is not needed to prove finiteness of $X(K_{\mathfrak{p}})_2$. Indeed, the proof of finiteness of $X(K_{\mathfrak{p}})_2$, given our assumptions on the ranks of the Mordell-Weil and Néron-Severi groups of the Jacobian, is very short (see Lemma 3). Furthermore the method of producing algebraic functions on the Albanese variety which contain the image of the Selmer variety does not depend on the link with p-adic heights, although it is inspired by Nekovář's construction of the p-adic height pairing.

Let X/K be a genus 2 bielliptic curve with affine equation

$$y^2 = x^6 + ax^4 + bx^2 + c,$$

with $a, b, c \in K$. The problem of determining the rational points of X was previously considered by Flynn and Wetherell [18]. Let E_1 and E_2 be the elliptic curves over K defined by the equations

$$E_1 : y^2 = x^3 + ax^2 + bx + c \qquad\qquad E_2 : y^2 = x^3 + bx^2 + acx + c^2$$

and let f_1 and f_2 denote the corresponding maps

$$\begin{array}{cccc} f_1 : & X & \longrightarrow & E_1 \\ & (x,y) & \mapsto & (x^2, y) \end{array} \qquad \begin{array}{cccc} f_2 : & X & \longrightarrow & E_2 \\ & (x,y) & \mapsto & (cx^{-2}, cyx^{-3}). \end{array}$$

Let h_{E_1} and h_{E_2} denote the height pairings on E_1 and E_2 corresponding to an idele class character

$$\chi : G_K^{\mathrm{ab}} \to \mathbb{Q}_p$$

and an isotropic splitting of the Hodge filtration. In the case when $K = \mathbb{Q}$, we take $\mathfrak{p} = (p)$ to be a prime of good reduction. In the case when K is an imaginary quadratic extension, we take p to be a prime of $\mathbb{Q}$ which splits as $\mathfrak{p}\overline{\mathfrak{p}}$ in K, and take χ to be a character which is trivial on $\mathcal{O}_{\overline{\mathfrak{p}}}^{\times}$.

Theorem 3. *Let X/K be a genus 2 bielliptic curve*

$$y^2 = x^6 + ax^4 + bx^2 + c.$$

(i): For all v not above p,

$$h_{E_1,v}(f_1(z)) - h_{E_2,v}(f_2(z)) - 2\chi_v(x(z))$$

takes only finitely many values, and for almost all v it is identically zero.
(ii): Let Ω denote the explicitly computable, finite set of values taken by

$$-\sum_{v \nmid p}(h_{E_1,v}(f_1(z_v)) - h_{E_2,v}(f_2(z_v)) - 2\chi_v(x(z_v)))$$

for (z_v) in $\prod_{v \nmid p} X(K_v)$. Suppose E_1 and E_2 each have Mordell-Weil rank 1, and let $P_i \in E_i(K)$ be points of infinite order. Let $\alpha_i = \frac{h_{E_i}(P_i)}{[K:\mathbb{Q}] \log_{E_i}(P_i)^2}$. Then $X(K)$ is contained in the finite set of z in $X(K_{\mathfrak{p}})$ satisfying

$$h_{E_1,\mathfrak{p}}(f_1(z)) - h_{E_2,\mathfrak{p}}(f_2(z)) - 2\chi_{\mathfrak{p}}(x(z)) - \alpha_1 \log_{E_1}(f_1(z))^2 + \alpha_2 \log_{E_2}(f_2(z))^2 \in \Omega.$$

We show how Theorem 3 can be used in conjunction with other techniques to determine the set $X(K)$. In our first example, X is a hyperelliptic curve with affine equation $y^2 = x^6 - 2x^4 - x^2 + 1$ over $K = \mathbb{Q}$. Applying the theorem with $p = 3$ produces the finite set $X(\mathbb{Q}_3)_U$, including a few "extra" points which do not appear to be in $X(\mathbb{Q})$. In fact, an argument invoking the 3-adic formal group of an underlying elliptic curve can eliminate these points from consideration, thereby finding for us the set $X(\mathbb{Q})$. In our second example, $X = X_0(37)$ and $K = \mathbb{Q}(i)$. Using Theorem 3 for one prime p produces a number of extra p-adic points. Nevertheless, applying the theorem for a suitably chosen collection of primes and then carrying out the Mordell-Weil sieve (as done by J. Steffen Müller and described in Appendix A) allows one to find $X(K)$.

The organisation of the paper is as follows. In Section 2 we review the Chabauty-Kim method. In Section 3 we describe the particular curves and quotients of fundamental groups we consider and explain why they give new instances of non-density of the localisation map. In Section 4 we recall the notion of mixed extensions and Nekovář's construction of p-adic height functions on such objects. In Section 5, we explain how to replace G-equivariant U-torsors with mixed extensions in the category of G-representations and use this to construct local height functions on the Selmer variety, and hence to give equations for the image of the localisation map. Section 6 gives an algebro-geometric characterisation of the mixed extensions constructed out of path torsors, and hence relates height functions on the Selmer variety to Nekovář's height pairing on algebraic cycles. In Section 7, we review some properties of Coleman-Gross height pairings on hyperelliptic curves and use this to relate our results to the results in [6]. We conclude in Section 8 by translating these techniques into a quadratic Chabauty method for finding rational points on certain bielliptic curves and present a few examples. Appendix A, by J. Steffen Müller, discusses how the Mordell-Weil sieve can be used in conjunction with quadratic Chabauty to find rational points and describes the sieving carried out to recover $X_0(37)(\mathbb{Q}(i))$.

2. The Chabauty-Kim method

We begin by recasting the Chabauty-Coleman method in a motivic framework and then use this to describe Kim's generalisation. Nothing in the section is new, although as far as we are aware, the statement of Lemma 1 is not in the literature. In this section, X is a smooth projective curve of genus g over a number field K. By a curve over a field K we shall always mean a separated, geometrically integral scheme over K of dimension 1.

2.1. **The Chabauty-Coleman method.**

Let T_0 denote the set of primes of bad reduction for X, let p be a prime of $\mathbb{Q}$ which splits completely in K and is coprime to T_0. Let $T = T_0 \cup \{v|p\}$, and fix a prime $\mathfrak{p}$ lying above p. Let G_T denote the maximal quotient of the Galois group of K unramified outside T. Unless otherwise indicated when we write G we will mean either G_T or G_v for v a prime of K.

Let $V := H^1_{\acute{e}t}(\overline{X}, \mathbb{Q}_p(1))$ and define $H^1_f(G_T, V)$ to be the subspace of the space of continuous cohomology classes in $H^1(G_T, V)$ which are crystalline at all primes above p. Let

$$\kappa : \mathrm{Div}^0(X) \otimes \mathbb{Q}_p \to H^1(G_T, V)$$

be the map sending a divisor $\sum \mu_i z_i$ to the Kummer class of $[\sum \mu_i z_i] \in J(K) \otimes \mathbb{Q}$ in $H^1(G_T, T_pJ) \otimes \mathbb{Q}_p = H^1(G_T, V)$. Then κ lands in the subspace $H^1_f(G_T, V)$, and there is a commutative diagram

$$\begin{tikzcd}
X(K) \arrow[r, "\kappa"] \arrow[d] & H^1_f(G_T, V) \arrow[d, "\mathrm{loc}_{\mathfrak{p}}"] \arrow[dr] & \\
X(K_{\mathfrak{p}}) \arrow[r, "\kappa_{\mathfrak{p}}"] & H^1_f(G_{\mathfrak{p}}, V) \arrow[r, "\simeq"] & D_{\mathrm{dR}}(V)/F^0
\end{tikzcd}$$

where the top map sends z to $\kappa(z - b)$, and the bottom right isomorphism is via p-adic Hodge theory. The composite map $j : X(K_{\mathfrak{p}}) \to D_{\mathrm{dR}}(V)/F^0$ may be described, via the isomorphism

$$D_{\mathrm{dR}}(V)/F^0 \simeq H^1_{\mathrm{dR}}(X)^*/F^0 \simeq H^0(X, \Omega^1)^*,$$

as the functional sending a global differential η to the Coleman integral $\int_b^z \eta$. Since the Mordell-Weil rank of J is less than g, there is a differential ω in $H^0(X, \Omega^1)^*$ which annihilates the image of $J(K) \otimes \mathbb{Q}_p$. Hence $X(K) \subset X(K_{\mathfrak{p}})$ lies in the set of points for which $\int_b^z \omega = 0$.

2.1.1. *Refinements over number fields.* In [31], Siksek explains a refinement of the classical Chabauty-Coleman method over number fields. As explained in loc. cit., heuristically one might expect that if X is a curve of genus g defined over a number field K of degree d over $\mathbb{Q}$, then the Chabauty-Coleman method works whenever the rank of $J(K)$ is less than or equal to $d(g-1)$ (as the Weil restriction of X is now a g-dimensional subscheme of the Weil restriction of its Jacobian). In [31, Theorem 2] a precise technical condition on linear independence of p-adic integrals is given which is sufficient to ensure that the Chabauty-Coleman method produces a finite set of points in $\prod_{\mathfrak{p}|p} X(K_{\mathfrak{p}})$.

2.2. **The Chabauty-Kim method.** We now explain how this motivic approach generalises. Given a rational point b in X, let $\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X}, b)$ denote the unipotent $\mathbb{Q}_p$-étale fundamental group of $\overline{X}$ with basepoint b [14]. Recall that this is equal to the $\mathbb{Q}_p$-Malcev completion of the usual étale fundamental group. In particular, as a pro-algebraic group (i.e. forgetting about the Galois action) it is isomorphic to the quotient of a free pro-unipotent group on $2g$ generators by one quadratic relation. Let $U^{(0)} := \pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X}, b)$, and for $i > 0$ define $U^{(n)} := [U^{(0)}, U^{(n-1)}]$. Define

$$U_n = U_n(b) = \pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X}, b)/U^{(n)},$$

and define

$$U[n] := \mathrm{Ker}(U_n \to U_{n-1}).$$

We will mostly be interested in the case when $n = 2$. In this case, using the standard presentation of the topological fundamental group of a surface of genus g there is an exact sequence

$$0 \to H^2_{\acute{e}t}(\overline{X}, \mathbb{Q}_p)^* \xrightarrow{\cup^*} \wedge^2 V \to U[2] \to 0. \tag{2}$$

Define

$$P_n(b,z) := \pi_1^{\acute{e}t}(\overline{X};b,z) \times_{\pi_1^{\acute{e}t}(\overline{X},b)} U_n(b).$$

Then the assignment $z \mapsto [P_n(b,z)]$ defines a map

$$X(K) \to H^1(G_T, U_n(b)).$$

One of the fundamental insights of the theory of Selmer varieties is that the cohomology spaces $H^1(G, U(b))$ carry a much richer structure than merely that of a pointed set, and that this extra structure has Diophantine applications. For the following theorem we take G to be either G_v or G_T:

Theorem 4 (Kim [21])**.** *Let U be a finite-dimensional unipotent group over $\mathbb{Q}_p$, admitting a continuous action of G. Suppose $H^0(G, U^i/U^{i+1})(\mathbb{Q}_p) = 0$ for all i. Then the functor*

$$R \mapsto H^1(G, U(R))$$

is represented by an affine algebraic variety over $\mathbb{Q}_p$, such that the six-term exact sequence in nonabelian cohomology is a diagram of schemes over $\mathbb{Q}_p$.

In this paper we will never distinguish between a cohomology variety and its $\mathbb{Q}_p$-points. We now take $U = U(b)$ to be a finite-dimensional G_T-stable quotient of $U_n(b)$ whose abelianisation equals V. Note that since the abelianisation of $U(\mathbb{Q}_p)$ has weight -1, it satisfies the hypotheses of the theorem, and hence $H^1(G, U)$ has the structure of the $\mathbb{Q}_p$-points of an algebraic variety over $\mathbb{Q}$. For z a point of X, we denote by $P(z) = P(b,z)$ the push-out of $P_n(b,z)$ by $U_n \to U$.

2.3. **Local conditions.** To go from the cohomology varieties $H^1(G_T, U)$ to Selmer varieties, one must add local conditions. For each $v \nmid p$, there is a *local unipotent Kummer map*

$$\begin{aligned} j_v : X(K_v) &\to H^1(G_v, U) \\ z &\mapsto [P(z)] \end{aligned}$$

which is trivial when v is a prime of potential good reduction and has finite image in general [23]. For $v|p$, by the work of Olsson [25], the assignment $x \mapsto [P(x)]$ lands inside the subspace of *crystalline* torsors $H^1_f(G_\mathfrak{p}, U)$. We define

$$j_\mathfrak{p} : X(K_\mathfrak{p}) \to H^1_f(G_\mathfrak{p}, U).$$

There is then a commutative diagram

$$\begin{tikzcd}
X(K) \arrow[r] \arrow[d] & H^1(G_T, U) \arrow[d, "\prod \mathrm{loc}_v"] \\
\prod_{v \in T} X(K_v) \arrow[r] & \prod_{v \in T} H^1(G_v, U).
\end{tikzcd} \tag{3}$$

It is also shown in [21] that the localisation morphisms are morphisms of varieties, and the set of crystalline cohomology classes has the structure of the $\mathbb{Q}_p$-points of a variety. At any prime $v \nmid p$, the image of $X(K_v)$ in $H^1(G_v, U(x))$ is finite [23]. We would like to understand the following subscheme of $H^1(G_T, U(x))$:

Definition 1. The *Selmer variety* of U, denoted $\mathrm{Sel}(U)$, is the reduced scheme associated to the subscheme of $H^1(G_T, U)$ consisting of cohomology classes c satisfying the following conditions:

(1) $\mathrm{loc}_v(c)$ comes from an element of $X(K_v)$ for all v prime to p,

(2) $\mathrm{loc}_v(c)$ is crystalline for all v above p,
(3) the projection of c to $H^1(G_T, V)$ lies in the image of $\mathrm{Jac}(X)(K) \otimes \mathbb{Q}_p$.

Remark 3. We have included the third condition to avoid any assumptions on the finiteness of the Shafarevich-Tate group of the Jacobian of X in the statement of our results. Consequently, our notation differs slightly from other work on Chabauty-Kim theory.

Remark 4. In the present work, we are only interested in $\mathbb{Q}_p$-points; the only relevance of the scheme structure is to ensure that certain maps are algebraic.

We shall denote by $H^1_{\mathcal{O}_K}(G_T, U) \subset \mathrm{Sel}(U)$ the subvariety of cohomology classes which are trivial at all v in T_0. Hence $H^1_{\mathcal{O}_K}(G_T, U)$ consists of cohomology classes which are trivial at all places prime to p, crystalline at primes above p, and whose image in $H^1(G_T, V)$ lies in the image of $J(K) \otimes \mathbb{Q}_p$.

2.4. **Applications to Diophantine geometry.** Let $\mathfrak{p}$ be a prime above p. We have a refinement of the commutative diagram (3):

$$\begin{tikzcd}
X(K) \arrow[r, "j"] \arrow[d] & \mathrm{Sel}(U(b)) \arrow[d, "\mathrm{loc}_{\mathfrak{p}}"] \\
X(K_{\mathfrak{p}}) \arrow[r, "j_{\mathfrak{p}}"] & H^1_f(G_{\mathfrak{p}}, U(b)).
\end{tikzcd}$$

The map $j_{\mathfrak{p}}$ is not algebraic, but is locally analytic, i.e., on each residue disk in $X(K_{\mathfrak{p}})$, we have that $j_{\mathfrak{p}}$ is given by a p-adic power series. Furthermore by [22], $j_{\mathfrak{p}}$ has Zariski dense image. Hence if $\mathrm{loc}_{\mathfrak{p}}$ is not dominant, then the set $j_{\mathfrak{p}}^{-1}(\mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}(U)))$ is finite.

Definition 2. Define the set $X(K_{\mathfrak{p}})_U \subset X(K_{\mathfrak{p}})$ to be $j_{\mathfrak{p}}^{-1}(\mathrm{loc}_{\mathfrak{p}}(\mathrm{Sel}(U)))$. When $U = U_n$, we write $X(K_{\mathfrak{p}})_{U_n}$ as $X(K_{\mathfrak{p}})_n$.

Remark 5. The sets $X(K_{\mathfrak{p}})_n$ are contained in the set of points which are *weakly global of level* n, defined in [2]. If the p-primary part of the Shafarevich-Tate group of the Jacobian of X is finite, then the two sets are equal.

2.5. **Properties of** $\mathrm{Sel}(U)$**.** In this subsection we recall some properties of the varieties $\mathrm{Sel}(U)$. We make repeated use of the twisting construction in nonabelian cohomology, as in [30, I.5.3]. For topological groups U and W, equipped with a continuous homomorphism $U \to \mathrm{Aut}(W)$, and a continuous U-torsor P, we shall denote by $W^{(P)}$ the group obtained by twisting W by the U-torsor P:

$$W^{(P)} := W \times_U P.$$

Given a group U with an action of G and a continuous G-equivariant U-torsor P, we may form a group $U^{(P)}$ which is the twist of U by the U-torsor P, where U acts on itself by conjugation. There is a bijection

$$H^1(G, U) \to H^1(G, U^{(P)})$$

which sends G-equivariant U-torsors to G-equivariant $U^{(P)}$-torsors. We will make use of the following properties of the twisting constructions:

- If $U \to W$ is a homomorphism of G-groups, then the diagram

$$\begin{tikzcd} H^1(G,U) \arrow[r] \arrow[d] & H^1(G,U^{(P)}) \arrow[d] \\ H^1(G,W) \arrow[r] & H^1(G,W^{(Q)}) \end{tikzcd}$$

commutes, where P is a G-equivariant U-torsor and Q is the W-torsor $P \times_U W$.

- If H is a subgroup of G, U is a G-group and P is a G-equivariant U-torsor, then the following diagram commutes:

$$\begin{tikzcd} H^1(G,U) \arrow[r] \arrow[d] & H^1(G,U^{(P)}) \arrow[d] \\ H^1(H,U) \arrow[r] & H^1(H,U^{(P)}). \end{tikzcd}$$

In our cases of interest these morphisms will actually be morphisms of schemes, by functoriality. It follows from the two commutative diagrams above that if P is a crystalline U-torsor then the map

$$H^1(G_{\mathfrak{p}},U) \to H^1(G_{\mathfrak{p}},U^{(P)})$$

sends crystalline U-torsors to crystalline $U^{(P)}$-torsors, and that if P is a G_T-equivariant U-torsor whose image in $H^1(G_T,V)$ lies in $J(K) \otimes \mathbb{Q}_p$, then twisting by P sends the preimage of $J(\mathbb{Q}) \otimes \mathbb{Q}_p$ in $H^1(G,U)$ to the preimage of $J(\mathbb{Q}) \otimes \mathbb{Q}_p$ in $H^1(G,U^{(P)})$. This is summarised in the following lemma.

Lemma 1. *Via the twisting construction,* $\mathrm{Sel}(U)$ *is isomorphic to N disjoint copies of $H^1_{\mathcal{O}_K}(G_T,U)$, where N is the size of the image of* $\mathrm{Sel}(U)$ *in*

$$\prod_{v \in T_0} j_v(X(K_v)) \subset \prod_{v \in T_0} H^1(G_v,U).$$

3. Non-density of the localisation map

For the rest of this paper we take K to be $\mathbb{Q}$ or an imaginary quadratic extension of $\mathbb{Q}$. Unless otherwise stated, we will henceforth take U to be a quotient of U_2 surjecting onto V. From the standard presentation of the topological fundamental group of a smooth surface of genus g in terms of $2g$ generators and 1 quadratic relation, the natural map

$$\wedge^2 V \to U[2]$$

gives an exact sequence

$$0 \to H^2_{ét}(\overline{X})^* \xrightarrow{\cup^*} \wedge^2 V \to U[2] \to 0. \tag{4}$$

Hence the quotients U intermediate between U_2 and V correspond to Galois subrepresentations of $\wedge^2 V / H^2_{ét}(\overline{X})^*$. Note that for any such choice of U, there is an inclusion $X(K_{\mathfrak{p}})_2 \subset X(K_{\mathfrak{p}})_U$. In this paper we restrict attention to the case where $[U,U]$ is isomorphic to $\mathbb{Q}_p(1)^n$.

3.1. **Finiteness results.** The reason for considering quotients of the fundamental group which are extensions of V by $\mathbb{Q}_p(1)^n$ is that

$$H^1_f(G_T,\mathbb{Q}_p(1)) \simeq \mathcal{O}_K^\times \otimes \mathbb{Q}_p = 0,$$

and

$$H^1_f(G_\mathfrak{p},\mathbb{Q}_p(1)) \simeq \mathcal{O}_\mathfrak{p}^\times \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p,$$

hence $\dim H^1_f(G_T,\mathbb{Q}_p(1))=0$ and $\dim H^1_f(G_\mathfrak{p},\mathbb{Q}_p(1))=1$.

Remark 6. This is the only place where our restrictions on K are essential.

In many situations the Galois cohomology computation above is enough to prove non-density of the localisation map for $\mathrm{Sel}(U)$.

Lemma 2. *Let U be a quotient of U_2 which is an extension of V by $\mathbb{Q}_p(1)^n$. Let p be a prime of $\mathbb{Q}$ such that X has good reduction at all primes above p, and let $\mathfrak{p}$ be a prime above p.*
(i): The dimension of $\mathrm{Sel}(U)$ is bounded by $\mathrm{rk}\, J(K)$.
(ii): The dimension of $H^1_f(G_\mathfrak{p},U)$ is equal to $g+n$.

Proof. (i): Consider the commutative diagram with exact rows

$$\begin{tikzcd}
H^1(G_T,[U,U]) \arrow[r] \arrow[d] & H^1(G_T,U) \arrow[r] \arrow[d] & H^1(G_T,V) \arrow[d] \\
\prod_{v\in T} H^1(G_v,[U,U]) \arrow[r] & \prod_{v\in T} H^1(G_v,U) \arrow[r] & \prod_{v\in T} H^1(G_v,V).
\end{tikzcd}$$

As explained in §2.5, to prove non-density of the localisation map, we may assume that the local conditions at primes away from p are trivial. Hence we reduce to proving non-density of the map

$$H^1_{\mathcal{O}_K}(G_T,U) \to H^1_f(G_\mathfrak{p},U).$$

Via the exact sequence of pointed varieties

$$H^1_f(G_T,[U,U]) \to H^1_f(G_T,U) \to H^1_f(G_T,V)$$

the dimension of $H^1_{\mathcal{O}_K}(G_T,U)$ is bounded by $\mathrm{rk}\, J(K)$.
(ii): The computation of the dimension of $H^1_f(G_\mathfrak{p},U)$ follows [22, §2]. By p-adic Hodge theory we have an isomorphism

$$H^1_f(G_\mathfrak{p},U) \simeq D_{\mathrm{dR}}(U)/F^0,$$

and this gives a short exact sequence

$$1 \to D_{\mathrm{dR}}([U,U])/F^0 \to H^1_f(G_\mathfrak{p},U) \to D_{\mathrm{dR}}(V)/F^0 \to 1.$$

Since $[U,U]\simeq \mathbb{Q}_p(1)^n$, the dimension of $H^1_f(G_\mathfrak{p},U)$ is $g+n$. □

Now we consider the problem of finding such a quotient of U_2. Note that

$$\mathrm{Hom}_{G_T}(\mathbb{Q}_p(1),\wedge^2 V) \simeq \mathrm{Hom}_{G_T}(\mathbb{Q}_p, H^2_{ét}(\overline{J},\mathbb{Q}_p(1)))$$

and hence the rank of this vector space is at least the rank of the Néron-Severi group of J. (Furthermore this is an equality, since H^2 of an abelian variety satisfies the Tate conjecture [17].) On the other hand by §2, the representation $U[2]$ is isomorphic to the cokernel of $\mathbb{Q}_p(1) \xrightarrow{\cup^*} \wedge^2 V$. Hence from Lemma 2 one may deduce the following lemma.

Lemma 3. *Suppose X is a curve of genus g, such that* $\operatorname{rk} J(K) < g + \operatorname{rk} \mathrm{NS}(J) - 1$. *Then $X(K_{\mathfrak{p}})_U$ is finite.*

The remainder of this article is concerned with making Lemma 3 more explicit.

4. Mixed extensions and Nekovář's p-adic height function

In this section we introduce some notation for mixed extensions in an abelian category, discuss the relationship between mixed extensions and cohomology with values in unipotent groups, and then review Nekovář's p-adic height function on mixed extensions.

4.1. **Mixed extensions.**

Let $\mathcal{A}$ be an abelian category. Let $W_0, \ldots, W_n$ be objects of $\mathcal{A}$, such that for all $i < j$

$$\mathrm{Hom}_{\mathcal{A}}(W_i, W_j) = 0.$$

Definition 3. We define a *mixed extension with graded pieces* $W_0, \ldots, W_n$ to be a tuple $(M, (M_i, \alpha_i))$, where M is an object of $\mathcal{A}$,

$$M = M_0 \hookleftarrow M_1 \hookleftarrow M_2 \hookleftarrow \ldots \hookleftarrow M_{n+1} = 0$$

is a filtration in $\mathcal{A}$ and $\alpha_0, \ldots, \alpha_n$ are isomorphisms

$$\alpha_i : M_i / M_{i+1} \simeq W_i.$$

A mixed extension $(M, (M_i, \alpha_i))$ as above will sometimes be denoted simply by M.

Definition 4. Let $(M, (M_i, \alpha_i))$ and $(N, (N_i, \beta_i))$ be mixed extensions with graded pieces $W_0, \ldots, W_n$. A *morphism of mixed extensions* is a sequence of commuting isomorphisms

$$r_i : M_i \xrightarrow{\simeq} N_i$$

such that if r_i denotes the induced morphism $M_{i-1}/M_i \to N_{i-1}/N_i$, then for all i, $\beta_i \circ r_i = \alpha_i$.

We denote by $\mathcal{C}(\mathcal{A}; W_0, \ldots, W_n)$ the category of mixed extensions with graded pieces $W_0, \ldots, W_n$, and by $C(\mathcal{A}; W_0, \ldots, W_n)$ the set of isomorphism classes. Note that our assumption on $\mathrm{Hom}_{\mathcal{A}}(W_i, W_j)$ implies that an object of $\mathcal{C}(\mathcal{A}; W_0, \ldots, W_n)$ has no nontrivial automorphisms. For any $0 \leq i < j \leq n$ we have a tautological functor

$$\varphi_{i,j} : \mathcal{C}(\mathcal{A}; W_0, \ldots, W_n) \to \mathcal{C}(\mathcal{A}; W_i, \ldots, W_j)$$

which induces a map

$$\varphi_{i,j} : C(\mathcal{A}; W_0, \ldots, W_n) \to C(\mathcal{A}; W_i, \ldots, W_j).$$

Remark 7. The reason for the term "mixed extension" is as follows: if $n = 2$ and M is an object in $\mathcal{C}(\mathcal{A}; W_0, W_1, W_2)$, then in the notation of [19] M is a *mixed extension* of $\varphi_{0,1}(M)$ and $\varphi_{1,2}(M)$.

In the case $n = 1$, we have an isomorphism

$$C(\mathcal{A}; W_0, W_1) \simeq \mathrm{Ext}^1(W_0, W_1)$$

and in particular we can add mixed extensions with two graded pieces. For general n, if M and N are objects in $\mathcal{C}(\mathcal{A}; W_0, \ldots, W_n)$ such that $\varphi_{1,n-1}(M) \simeq \varphi_{1,n-1}(N)$, then the Baer sum of M and N, denoted $M +_{1,n-1} N$, will again be an object in $\mathcal{C}(\mathcal{A}; W_0, \ldots, W_n)$. Similarly, if $\varphi_{2,n}(M) \simeq \varphi_{2,n}(N)$, then we can form $M +_{2,n} N$.

Definition 5. Let A be an abelian group. A function

$$\alpha : C(\mathcal{A}; W_0, \ldots, W_n) \to A$$

is said to be *bi-additive* if, whenever $\varphi_{1,n-1}(M) = \varphi_{1,n-1}(N)$, we have

$$\alpha(M +_{1,n-1} N) = \alpha(M) + \alpha(N),$$

and whenever $\varphi_{2,n}(M) = \varphi_{2,n}(N)$, we have

$$\alpha(M +_{2,n} N) = \alpha(M) + \alpha(N).$$

4.2. **Relation to nonabelian cohomology.** Now suppose that $\mathcal{A} = \mathrm{Rep}_{\mathbb{Q}_p}(G)$ is the category of continuous p-adic representations of a profinite group G. Let $W_0, \ldots, W_n$ be objects in $\mathrm{Rep}_{\mathbb{Q}_p}(G)$.

Definition 6. Define $U(W_0, \ldots, W_n)$ to be the subset of $\oplus_{0 \leq i,j \leq n} W_i^* \otimes W_j$ consisting of elements whose $W_i^* \otimes W_j$ component is zero if $i > j$ and the identity endomorphism if $i = j$.

Note that $U(W_0, \ldots, W_n)$ is a unipotent group with a compatible action of G.

Definition 7. Let $(M, (M_i, \alpha_i))$ be an object in $\mathcal{C}(\mathrm{Rep}_{\mathbb{Q}_p}(G); W_0, \ldots, W_n)$. Define $\Phi(M)$ to be the set of isomorphisms of vector spaces

$$\rho : M \xrightarrow{\simeq} W_0 \oplus \ldots \oplus W_n$$

such that $\rho(M_i) = W_i \oplus \ldots \oplus W_n$ and the induced quotient homomorphism

$$\rho_i : M_i / M_{i+1} \to W_i$$

is equal to α_i.

$\Phi(M)$ has the structure of a G-equivariant $U(W_0, \ldots, W_n)$ torsor, and this induces a map

$$\Phi : C(\mathrm{Rep}_{\mathbb{Q}_p}(G); W_0, \ldots, W_n) \to H^1(G, U(W_0, \ldots, W_n)).$$

Lemma 4. *Φ is a bijection.*

Proof. To construct an inverse to Φ, define Φ' to be the functor from the category of equivalence classes of G-equivariant U-torsors to $\mathcal{C}(\mathrm{Rep}_{\mathbb{Q}_p}(G); W_0, \ldots, W_n)$ sending a torsor P to the twist of $W_0 \oplus \ldots \oplus W_n$ by P. □

Under this correspondence, when $G = G_{\mathfrak{p}}$, the subcategory of crystalline $G_{\mathfrak{p}}$ representations is sent to $H^1_f(G_{\mathfrak{p}}, U(W_0, \ldots, W_n))$, and similarly for semistable representations. Define

$$H^1_{\mathrm{st}}(G_T, U(W_0, \ldots, W_n)) \subset H^1(G_T, U(W_0, \ldots, W_n))$$

to be the subvariety of U-torsors which are semistable at all primes above p (with no conditions at the primes in T_0). We will henceforth use $C(\mathrm{Rep}_{\mathbb{Q}_p}(G); W_0, \ldots, W_n)$ and $H^1(G, U(W_0, \ldots, W_n))$ interchangeably.

4.3. **Nekovář's p-adic height pairing on mixed extensions.** In this section we recall the construction of Nekovář's p-adic height pairing [24]. We will only work in the context of a smooth projective curve over K and p a prime of good reduction. Our categories will be G representations (for $G = G_T$ or G_v) and our objects will be $W_0 = \mathbb{Q}_p$,$W_1 = V$,$W_2 = \mathbb{Q}_p(1)$. The variety $C(\mathrm{Rep}_{\mathbb{Q}_p}(G); \mathbb{Q}_p, V, \mathbb{Q}_p(1))$ has a natural involution defined by

$$M \mapsto M^*(1).$$

We say a function

$$\alpha : C(\mathrm{Rep}_{\mathbb{Q}_p}(G); \mathbb{Q}_p, V, \mathbb{Q}_p(1)) \to \mathbb{Q}_p$$

is *symmetric* if $\alpha(M) = \alpha(M^*(1))$. Nekovář's p-adic height pairing is defined via a family of local height functions

$$h_v : H^1(G_v, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) \to \mathbb{Q}_p,$$

for v prime to p, and

$$h_v : H^1_{\mathrm{st}}(G_v, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) \to \mathbb{Q}_p$$

for v above p, which are continuous, bi-additive and symmetric. The input for Nekovář's construction is a class χ in $H^1(G_T, \mathbb{Q}_p)$ and a splitting

$$s : H^1_{\mathrm{dR}}(X_{K_v}, \mathbb{Q}_p) \to F^1 H^1_{\mathrm{dR}}(X_{K_v}, \mathbb{Q}_p) \tag{5}$$

of the Hodge filtration of $H^1_{\mathrm{dR}}(X_{K_v})$ at every prime v above p.

4.3.1. *v prime to p.* For v not above p, the construction of local height pairings is immediate given the weight monodromy conjecture for curves [27], which implies that

$$H^0(G_v, V) = H^1(G_v, V) = 0,$$

and hence by the six-term exact sequence in nonabelian cohomology,

$$H^1(G_v, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) \simeq H^1(G_v, \mathbb{Q}_p(1)).$$

This gives a function

$$. \cup \chi_v : H^1(G_v, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) \to \mathbb{Q}_p$$

via the isomorphism $H^2(G_v, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$ coming from local class field theory.

4.3.2. *v above p.* For v above p, the construction of local height pairings uses p-adic Hodge theory. As we will only be interested in the crystalline case, we restrict attention to describing Nekovář's functional on crystalline mixed extensions

$$h_v : H^1_f(G_v, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) \to \mathbb{Q}_p.$$

The construction is analogous to the case when v was prime to p: given a mixed extension M in the category of filtered ϕ-modules, with graded pieces $\mathbb{Q}_p, D_{\mathrm{cr}}(V)$ and $D_{\mathrm{cr}}(1)$, one constructs an extension c of $\mathbb{Q}_p$ by $D_{\mathrm{cr}}(1)$, identifies this as an element c' of $H^1_f(G_p, \mathbb{Q}_p(1))$, and then defines

$$h(M) := c' \cup \chi_v.$$

We now sketch the construction of c. Note that (in the category of admissible filtered ϕ-modules) $\mathrm{Ext}^1(\mathbb{Q}_p, D_{\mathrm{cr}}(1)) \simeq D_{\mathrm{dR}}(1)$, so one may equivalently think of c as an element of $D_{\mathrm{dR}}(\mathbb{Q}_p(1))$. Let $(M, (M_i, \alpha_i))$ be a mixed extension with graded pieces $\mathbb{Q}_p, D_{\mathrm{cr}}(V)$ and $D_{\mathrm{cr}}(\mathbb{Q}_p(1))$. The extension class of M in $\mathrm{Ext}^1(\mathbb{Q}_p, M_1)$ defines an element of M_1/F^0. Using the splitting s specified in (5), one lifts this to an element of M_1. For weight reasons there is a canonical ϕ-equivariant splitting of the inclusion $M_2 \hookrightarrow M_1$, and hence via α_2 one obtains an element c of $D_{\mathrm{dR}}(\mathbb{Q}_p(1))$, as required.

In the language of [22] we may define the local height of a crystalline mixed extension as follows. There is an isomorphism [22, §2]:

$$H^1_f(G_v, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) \simeq D_{\mathrm{dR}}(U(\mathbb{Q}_p, V, \mathbb{Q}_p(1)))/F^0.$$

As for G-representations, we define a unipotent group $U(\mathbb{Q}_p, D_{\mathrm{cr}}(V), D_{\mathrm{cr}}(\mathbb{Q}_p(1)))$ with filtration and ϕ-action and a filtered unipotent group $U(\mathbb{Q}_p, D_{\mathrm{dR}}(V), D_{\mathrm{dR}}(\mathbb{Q}_p(1)))$. These are then isomorphic to $D_{\mathrm{cr}}(U(\mathbb{Q}_p, V, \mathbb{Q}_p(1)))$ and $D_{\mathrm{dR}}(U(\mathbb{Q}_p, V, \mathbb{Q}_p(1)))$ respectively. The quotient $U(\mathbb{Q}_p, D_{\mathrm{dR}}(V), D_{\mathrm{dR}}(\mathbb{Q}_p(1)))/F^0$ parametrises mixed extensions with graded pieces $\mathbb{Q}_p, D_{\mathrm{cr}}(V)$ and $D_{\mathrm{cr}}(\mathbb{Q}_p(1))$ in the category of filtered ϕ-modules. Arguing as above, a splitting of the Hodge filtration determines an algebraic function

$$U(\mathbb{Q}_p, D_{\mathrm{dR}}(V), D_{\mathrm{dR}}(\mathbb{Q}_p(1)))/F^0 \to D_{\mathrm{dR}}(\mathbb{Q}_p(1)).$$

In particular we obtain the following lemma.

Lemma 5. *The local height function*

$$h_v : H^1_f(G_v, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) \to \mathbb{Q}_p$$

is algebraic.

4.3.3. *Global heights.* We define

$$h : H^1_{\mathrm{st}}(G_T, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) \to \mathbb{Q}_p$$

to be the composite of

$$H^1_{\mathrm{st}}(G_T, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) \xrightarrow{\prod_{v\in T}\mathrm{loc}_v} \prod_{v\in T_0} H^1(G_v, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) \times \prod_{v|p} H^1_{\mathrm{st}}(G_v, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1)))$$

with

$$\prod_{v\in T_0} H^1(G_v, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) \times \prod_{v|p} H^1_{\mathrm{st}}(G_v, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) \xrightarrow{\prod h_v} \mathbb{Q}_p.$$

By Poitou-Tate duality, h factors through

$$\varphi_{0,1} \times \varphi_{1,2} : H^1_{\mathrm{st}}(G_T, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) \to H^1_f(G_T, V) \times H^1_f(G_T, V),$$

using the fact that $H^1_{\mathrm{st}}(G_T, V) \simeq H^1_f(G_T, V)$. By additivity, symmetry and continuity, it hence factors through

$$\begin{aligned} H^1_{\mathrm{st}}(G_T, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))) &\to \mathrm{Sym}^2 H^1_f(G_T, V) \\ M &\mapsto \varphi_{0,1}(M)(\varphi_{1,2}(M)^*(1)). \end{aligned}$$

5. Selmer varieties and mixed extensions

We now return to Selmer varieties. Here U will be an extension of V by $\mathbb{Q}_p(1)$. To obtain equations for $X(K_{\mathfrak{p}})_2$, we use Nekovář's construction to define a map

$$\mathrm{Sel}(U) \to \mathbb{Q}_p.$$

A natural analogue of Nekovář's construction is to start with the input of a cohomology class χ in $H^1(G_T, \mathbb{Q}_p)$, and to define, at all primes v in T_0, an algebraic function

$$H^1_*(G_v, U) \to \mathbb{Q}_p$$

which, restricted to $H^1(G_v, \mathbb{Q}_p(1))$, is simply the cup product with χ.

Given a splitting of the Hodge filtration, one may certainly do this, but from the point of view of finding equations for Selmer varieties, it is better to have a construction with some kind of linearity properties analogous to those of the global height pairing. For this reason, in this section we define a way to embed $\mathrm{Sel}(U)$ into $H^1_{\mathrm{st}}(G_T, U(\mathbb{Q}_p, V, \mathbb{Q}_p(1))$ via twisting. We then apply Nekovář's construction, giving (via composition) local functions $\mathrm{Sel}(U) \to \mathbb{Q}_p$. Note that if $\mathbb{Q}_p(1)$ is replaced by a different Galois representation W of motivic weight -2 arising in $U[2]$, one may mimic Nekovář's construction with the cohomology class χ replaced by a cohomology class in $H^1(G_T, W^*(1))$ which is nontrivial and noncrystalline at $\mathfrak{p}$ (assuming one can prove such a class exists). This will be pursued in future work.

5.1. **Twisting the enveloping algebra.** To construct a mixed extension associated to an element of $H^1(G,U)$, we define a G-representation with an equivariant U-module structure, which will be denoted $A(b)$, and then send a U-torsor P to the twist of $A(b)$ by P.

$A(b)$ will be defined to be a certain finite-dimensional quotient of the universal enveloping algebra of $\pi_1^{\acute{e}t,\mathbb{Q}_p}(\overline{X}, b)$. By the theory of Malcev completion, this has a very concrete description, which we now recall. Let I denote the kernel of

$$\mathbb{Q}_p[\pi_1^{\acute{e}t}(\overline{X}, x)] \to \mathbb{Q}_p$$
$$\sum \lambda_\gamma \gamma \mapsto \sum \lambda_\gamma.$$

Since $\pi_1^{\acute{e}t}(\overline{X}, x)$ is isomorphic to the profinite completion of a free group F_{2g} on $2g$ generators modulo one relation lying in $[F_{2g}, F_{2g}]$, we have that $A_\infty(x)$ is isomorphic to the completion of an algebra obtained by quotienting a free associative $\mathbb{Q}_p$-algebra R_{2g} on $2g$ generators by a 2-sided ideal generated by an element $e \in I^2$.

Definition 8. Let $A_n(b) = \mathbb{Q}_p[\pi_1^{\acute{e}t}(\overline{X}, x)]/I^{n+1}$.

$A_n(b)$ is equipped with the structure of a Galois-equivariant $\pi_1^{\acute{e}t}(\overline{X}, x)$-module, since it is a quotient of the group algebra by a Galois stable ideal. Hence for any Galois-equivariant $\pi_1^{\acute{e}t}(\overline{X}, x)$ torsor P we can twist $A_n(b)$ by P to get a Galois representation $A_n(b)^{(P)}$. When $P = \pi_1^{\acute{e}t}(\overline{X}; x, y)$, $A_n(b)^{(P)}$ may be identified with the Galois-equivariant $A_n(b)$-module $A_n(b,z)$ obtained by tensoring $\mathbb{Q}_p[\pi_1^{\acute{e}t}(\overline{X}; x, y)]$, thought of as a $\mathbb{Q}_p[\pi_1^{\acute{e}t}(\overline{X}, x)]$-module, with $A_n(b)$. For this reason we refer to it $A_n(b,z)$ as a *path module.* It follows from the theory of Malcev completion that the action of $\pi_1^{\acute{e}t}(\overline{X}, b)$ on $A_n(b)$ factors through the homomorphism

$$\pi_1^{\acute{e}t}(\overline{X}, b) \to U_n(b).$$

Furthermore, $A_n(b)$ is a quotient of the enveloping algebra of $U_n(b)$, and a faithful representation of $U_n(b)$. More generally we can view the $\mathbb{Q}_p$-vector space generated by the torsor of paths from b to z, denoted $\mathbb{Q}_p[\pi_1^{\acute{e}t}(\overline{X}; b, z)]$, as a G-equivariant free rank 1 module over $\mathbb{Q}_p[\pi_1^{\acute{e}t}(\overline{X}, b)]$. Hence we may make the following definition.

Definition 9. Let $A_n(b,z)$ be the G-equivariant free rank 1 $A_n(b)$ module

$$\mathbb{Q}_p[\pi_1^{\acute{e}t}(\overline{X}; b, z)] \times_{\mathbb{Q}_p[\pi_1^{\acute{e}t}(\overline{X}; b, z)]} A_n(b).$$

Note that $A_n(b,z)$ is naturally equipped with a G-stable filtration

$$A_n(b,z) \supset I A_n(b,z) \supset \ldots \supset I^{n+1} A_n(b,z) = 0.$$

coming from the I-adic filtration on $\mathbb{Q}_p[\pi_1^{\acute{e}t}(\overline{X}; b, z)]$, and that the action of $A_n(b)$ respects this action. We define

$$A[k] := I^k A_n(b)/I^{k+1}A_n(b).$$

A second viewpoint is that $A_n(b,z)$ is the twist of $A_n(b)$ by $[\pi_1^{\acute{e}t}(\overline{X}; b, z)]$ via the left action of $\pi_1^{\acute{e}t}(\overline{X}, b)$ on $A_n(b)$. There is also a more general construction: for all k, $I^k A_n(b)$ admits compatible actions of $U_n(b)$ and G. Hence for any G-equivariant $U_n(b)$ torsor P we may construct the twist $A_n(b)^{(P)}$ of $A_n(b)$ by P. In the case when P is $\pi_1^{\acute{e}t}(\overline{X}; b, z) \times_{\pi_1^{\acute{e}t}(\overline{X}, b)} U_n(b)$, we have that $A_n^{(P)}$ is just $A_n(b,z)$. The action of U_n on I^k/I^{k+1} is trivial, hence for any such P we have an isomorphism

$$I^k A_n(b)^{(P)}/I^{k+1}A_n(b)^{(P)} \simeq I^k A_n(b)/I^{k+1}A_n(b).$$

Hence we obtain a well-defined map

$$\begin{aligned}[\,.\,] : H^1(G, U_n) &\to H^1(G, U(A[0], A[1], \ldots, A[n])) \\ P &\mapsto [A_n(b)^{(P)}].\end{aligned}$$

An equivalent definition of this map would be to define $\mathrm{Aut}(A_n(b))$ to denote the group of unipotent automorphisms of $A_n(b)$ as a filtered vector space (i.e. automorphisms of $A_n(b)$ which respect the filtration and are the identity on the associated graded). Then there is a group homomorphism

$$U_n(b) \to \mathrm{Aut}(A_n(b))$$

and an induced map on cohomology

$$H^1(G, U_n) \to H^1(G, \mathrm{Aut}(A_n(b))).$$

There is also an isomorphism

$$H^1(G, \mathrm{Aut}(A_n(b))) \to H^1(G, U(\mathbb{Q}_p, A[1], \ldots, A[n]))$$

coming from the G-equivariant $(\mathrm{Aut}(A_n(b)), U(\mathbb{Q}_p, A[1], \ldots, A[n]))$-bitorsor of isomorphisms of filtered vector spaces

$$A_n(b) \xrightarrow{\simeq} \oplus_{k=0}^n A[k],$$

(see [30], Proposition 35). The map $[\,.\,]$ defined above is simply the composite.

We now focus on the depth 2 case. There is a short exact sequence

$$0 \to A[2] \to A_2(b) \to A_1(b) \to 0$$

compatible with the action of G and U. $A[2]$ is canonically isomorphic to $[U_2, U_2] \oplus \mathrm{Sym}^2 V$.

Definition 10. Suppose the rank of $\mathrm{NS}(J)$ is bigger than 1. Let

$$\xi : A[2] \to \mathbb{Q}_p(1)$$

be a surjection whose restriction to $[U_2, U_2]$ is nonzero and factors through $[U_2, U_2] \to [U, U]$. Define $A(b)$ to be the mixed extension with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$ obtained by pushing out $A[2] \hookrightarrow A_2(b)$ by $\xi : A[2] \to \mathbb{Q}_p(1)$. We define $IA(b)$ to be the kernel of the projection

$$A(b) \to \mathbb{Q}_p.$$

The representation $A(b)$ has a compatible U-action, and hence for any U-torsor P we obtain a mixed extension $A(b)^{(P)}$ with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$. Since the projection map $A(b) \to \mathbb{Q}_p$ and the inclusion map $\mathbb{Q}_p(1) \to A(b)$ are U-equivariant, for any P we have exact sequences

$$0 \to IA(b)^{(P)} \to A(b)^{(P)} \to \mathbb{Q}_p \to 0$$

and

$$0 \to \mathbb{Q}_p(1) \to A(b)^{(P)} \to A_1(b)^{(P)} \to 0.$$

When $P = P(b,z)$ we denote $A(b)^{(P)}$ by $A(b,z)$ and $IA(b)^{(P)}$ by $IA(b,z)$. When we want to emphasise the dependence on X, we write $A(X)(b)$ and $A(X)(b,z)$. By our assumptions on the homomorphism $A[2] \to \mathbb{Q}_p(1)$, $A(b)$ is a faithful U-representation. Note that since the U-action on $A[2]$ is trivial, we could define $A(b)^{(P)}$ to be the pushout of $A[2] \hookrightarrow A_2(b)^{(P)}$ by $A[2] \to \mathbb{Q}_p(1)$. As in the above discussion of the map $[\ .\ ]$, the map from $H^1(G,U)$ to $H^1(G,U(\mathbb{Q}_p,V,\mathbb{Q}_p(1)))$ is algebraic.

5.2. **Description of $h(A(b,z))$.** Let U be a quotient of U_2 which is an extension of V by $\mathbb{Q}_p(1)$. Let $A(b)$ be the corresponding quotient of the enveloping algebra of U. We now consider the maps

$$\begin{aligned} H^1(G_v,U) &\to \mathbb{Q}_p \\ P \quad &\mapsto h_v(A(b)^{(P)}) \\ H^1(G_T,U) &\to \mathbb{Q}_p \\ P \quad &\mapsto h(A(b)^{(P)}). \end{aligned}$$

The following lemma follows from the work of Kim and Tamagawa [23].

Lemma 6. *Let v be a prime of K that is coprime to p. Then the map*

$$\begin{aligned} X(K_v) &\to \mathbb{Q}_p \\ z &\mapsto h_v(A(b,z)) \end{aligned}$$

is identically zero when v is a prime of potential good reduction and has finite image in general.

Proof. If v is a prime of potential good reduction then there is a finite Galois extension $L|K_v$ such that for every L-point z, the U-torsor $P(z)$ admits a G_L-equivariant trivialisation. From [30, §$I.5.8$], there is a short exact sequence

$$1 \to H^1(\mathrm{Gal}(L|K_v),U^{G_L}) \to H^1(G_{K_v},U) \to H^1(G_L,U),$$

and hence every G_{K_v}-equivariant U-torsor is trivial, since $U^{G_L} = 1$.

For the general case, we use [23, Corollary 0.2], which says that the map

$$j_v : X(K_v) \to H^1(G_{K_v},U)$$

has finite image. This implies the lemma, as the map $z \mapsto h_v(A(b,z))$ factors through j_v. □

We now consider global properties of $A(b,z)$. The mixed extension $A(b,z)$ is a mixed extension of $A_1(b,z)$ and $IA(b,z)^*(1)$. To understand the height of $A(b,z)$, we first need to understand the map

$$H^1(G,U) \to \mathrm{Ext}^1(V,\mathbb{Q}_p(1))$$

defined by sending a torsor P to the twist of $IA(b)$ by P (when $P = P(b,z)$, the twist of $IA(b)$ by P is $IA(b,z)$). Let $\langle , \rangle : V \times V \to \mathbb{Q}_p(1)$ be the homomorphism induced from the Weil pairing and let ${}_0 : V \to \mathrm{Hom}(V, \mathbb{Q}_p(1))$ denote the homomorphism sending v to $w \mapsto \langle w, v\rangle$. Let $\tau = \tau_Z : V \to \mathrm{Hom}(V, \mathbb{Q}_p(1))$ denote the homomorphism sending v to $w \mapsto [\widetilde{w}, \widetilde{v}]$, where $\widetilde{w}$ and $\widetilde{v}$ are lifts of w and v to U. Let τ_* denote the induced homomorphism

$$H^1(G,U) \to H^1(G,V) \to \mathrm{Ext}^1(V, \mathbb{Q}_p(1)).$$

We will also denote by τ_* the map $H^1(G,V) \to \mathrm{Ext}^1(V, \mathbb{Q}_p(1))$ through which the above map factors. Then by definition of the twisting construction there is an equality of extensions of $\mathbb{Q}_p(1)$ by V:

$$[IA(b,z)] = [IA(b)] + \tau_*([P(b,z)]).$$

Let $a(Z)$ denote the linear map

$$H^1_f(G_T, V) \to H^1_f(G_T, V)$$

defined by $a(Z) := \tau_0^{-1} \circ \tau_*$. Then by §4.3.3 we have the following lemma.

Lemma 7. *Suppose $D_1, \ldots, D_n$, $E_1, \ldots, E_n$ are divisors in $\mathrm{Div}^0(X)$ satisfying*

$$\sum \kappa(D_i)\kappa(E_i) = \kappa(z-b)(\tau_0^{-1}(IA(b)) + a(Z)(\kappa(z-b)))$$

in $\mathrm{Sym}^2 H^1_f(G_T, V)$. Then $\sum h(D_i, E_i) = h(A(b,z))$.

Using the above lemmas, one obtains equations for the finite set $X(K_{\mathfrak{p}})_U$. First we should be a bit more specific about our choice of p-adic height. If $K = \mathbb{Q}$ then up to scalars, there is a unique choice of character χ. Recall that in the imaginary quadratic case, we have a decomposition $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. We henceforth take χ to be an idele class character which vanishes on $\mathcal{O}^\times_{\overline{\mathfrak{p}}}$. By class field theory the space of such characters is one-dimensional, and hence χ is uniquely determined up to scalars. Since the mixed extensions $A(b,z)$ are crystalline at all primes above p, this means that

$$h(A(b,z)) = h_{\mathfrak{p}}(A(b,z)) + \sum_{v \in T_0} h_v(A(b,z)).$$

Let $\omega_0, \ldots, \omega_{g-1}$ be a basis of $H^0(X_{\mathfrak{p}}, \Omega^1)$.

Proposition 1. *Suppose $\mathrm{rk}\, J(K) = g$, that $\mathrm{rk}\, \mathrm{NS}(J) > 1$, and that the map*

$$J(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p \to H^1_f(G_{\mathfrak{p}}, V) \tag{6}$$

is an isomorphism. Let b be a K-rational point of X. Then the set

$$\Omega = \{-\sum_{v \in T_0} h_v(A(b, z_v)) : (z_v) \in \prod_{v \in T_0} X(K_v)\}.$$

is finite, and there are constants c_{ij}, d_i (for $0 \le i \le g-1$) such that $X(K_{\mathfrak{p}})_U$ is finite, and equal to the set of z in $X(K_{\mathfrak{p}})$ satisfying

$$h_{\mathfrak{p}}(A(b,z)) + \sum_{i,j} c_{ij} \left(\int_{z-b} \omega_i \right) \left(d_j + \sum a(Z)_{jk} \int_b^z \omega_k \right) \in \Omega.$$

Proof. By injectivity of (6) for all $0 \leq i \leq g-1$ there is a κ_i in $H^1_f(G_T, V)$ such that $\mathrm{loc}_{\mathfrak{p}}(\kappa_i) = \omega_i^*$ via the isomorphism $H^1_f(G_{\mathfrak{p}}) \simeq H^0(X_{\mathfrak{p}}, \Omega^1)^*$. Let $H_{i,j}$ be a mixed extension with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$ such that $\varphi_{0,1}(H_{ij}) = \kappa_i$ and $\varphi_{1,2}(H_{ij}) = \kappa_j^*(1)$. Define $c_{ij} = -h(H_{ij})$. Define d_i by

$$\mathrm{loc}_{\mathfrak{p}}(IA(b)^*(1)) = \sum d_i \omega_i^*.$$

Then since (6) is an isomorphism, we have

$$\varphi_{0,1}(A(b,z)) = \sum \left(\int_b^z \omega_i \right) \kappa_i$$

and

$$\varphi_{1,2}(A(b,z)) = \sum_i \left(d_i + \sum a(Z)_{jk} \int_b^z \omega_k \right) \kappa_i^*(1).$$

Hence in $\mathrm{Sym}^2 H^1_f(G_T, V)$,

$$\varphi_{0,1}(A(b,z))\varphi_{1,2}(A(b,z)) = \sum \left(\int_{z-b} \omega_i \right) \left(d_j + \sum a(Z)_{jk} \int_b^z \omega_k \right) \kappa_i \kappa_j,$$

giving an equality of global heights

$$h(A(b,z)) = \sum_{i,j} \left(\int_{z-b} \omega_i \right) \left(d_j + \sum a(Z)_{jk} \int_b^z \omega_k \right) h(H_{ij}).$$

This establishes that K-rational points satisfy the above equation. By §4.3.2 and §5.1, for any β in $\mathbb{Q}_p$, and any functional

$$B : H^1_f(G_{\mathfrak{p}}, V) \otimes H^1_f(G_{\mathfrak{p}}, V) \to \mathbb{Q}_p,$$

the equation

$$h_{\mathfrak{p}}(A(b)^{(P)}) + B(A_1(b)^{(P)}, (IA(b)^{(P)})^*(1)) = \beta$$

defines a codimension one subvariety W_α of $H^1_f(G_{\mathfrak{p}}, U)$. For $P = A(b,z)$, the left hand side of this equation is equal to

$$h_{\mathfrak{p}}(A(b,z)) + \sum_{i,j} \left(\int_{z-b} \omega_i \right) \left(d_j + \sum a(Z)_{jk} \int_b^z \omega_k \right) B(\omega_i^* \otimes \omega_j^*) = \beta.$$

Then, as in [22], $j_{\mathfrak{p}}^{-1}(W_\alpha)$ is finite, completing the proof of the proposition. □

To complete the proof of Theorem 2, we need to relate $h(A(b,z))$ to a height pairing between algebraic cycles. This identification is explained in §6.

5.3. **Equations for $X(K_{\mathfrak{p}})_U$ when the Mordell-Weil rank is bigger than the genus.** We briefly consider the case where the rank is bigger than the genus. Then the formula becomes more complicated, as to get constraints on the height of $A(b,z)$, one needs to know the class of $A_1(b,z)$ in $H^1_f(G_T, V)$, and this can no longer be recovered directly from its image in $H^1_f(G_p, V)$. Instead one shows that the the class of a point in $H^1(G_T, V)$ is "overdetermined" by the linear and quadratic relations it satisfies and produces an equation just involving functions on $X(K_{\mathfrak{p}})$ by taking an appropriate resultant.

For convenience we fix a connected component of $\mathrm{Sel}(U_2)$ corresponding to

$$\alpha = (\alpha_v) \in \prod_{v \in T_0} j_2(X(K_v)),$$

and describe

$$X(K_{\mathfrak{p}})_\alpha := j_{\mathfrak{p}}^{-1} \operatorname{loc}_{\mathfrak{p}}((\prod_{v \in T_0} j_v)^{-1}(\alpha)) \subset X(K_{\mathfrak{p}})_U.$$

Suppose that $\operatorname{rk} J(K) = n = g + k$, and that $\operatorname{rk} \mathrm{NS}(J) > k$. Let

$$(Z_0, \ldots, Z_k) : \mathbb{Q}_p(-1)^{k+1} \hookrightarrow \operatorname{Ker}(\wedge^2 H^1_{\acute{e}t}(\overline{X}) \xrightarrow{\cup} H^2_{\acute{e}t}(\overline{X})).$$

be an injective Galois-equivariant homomorphism, let U_{Z_m} be the quotient of U_2 corresponding to Z_m, and let $A_{Z_m}(b)$ denote the corresponding quotient of $A_2(b)$. For $0 \leq m \leq k$, define α_m to be minus the sum of the local heights of $A_{Z_m}(b)^{(P)}$ away from p:

$$\alpha_m := -\sum_{v \in T_0} h_v(A_{Z_m}(b)^{(\alpha_v)}).$$

Let $D_0, \ldots, D_{n-1}$ be elements of $\operatorname{Pic}^0(X)$ generating $\operatorname{Pic}^0(X) \otimes \mathbb{Q}$. For $0 \leq m \leq k$, let $(a(Z_m)_{ij})_{0 \leq i,j < n}$ denote the matrix of the endomorphism of $J(K) \otimes \mathbb{Q}$ induced by Z_m, and let the image of $IA_{Z_m}(b)$ in $H^1(G_T, V)$ equal $\sum c(Z_m)_i \kappa(D_i)$. Define polynomials $F_0, \ldots, F_n$ in $\mathbb{Q}_p[S_0, \ldots, S_{n-1}, T_0, \ldots, T_{n-1}]$ by

$$F_m = T_m - \sum_{j=0}^{n-1} S_j \int_{D_j} \omega_m$$

for $0 \leq m \leq g-1$, and

$$F_m = T_m - \alpha_{m-g} - \sum_{0 \leq i,j < n} h(D_i, D_j) S_i (c(Z_{m-g})_j S_j + \sum_{0 \leq l < n} a(Z_{m-g})_{lj} S_l)$$

for $g \leq m \leq n$.

Proposition 2. *Let $F = \operatorname{Res}(F_0, \ldots, F_n) \in \mathbb{Q}_p[T_0, \ldots, T_n]$ be the resultant of the polynomials $F_0, \ldots, F_n$. Then the set of z in $X(K_{\mathfrak{p}})$ such that*

$$F\left(\int_b^z \omega_0, \ldots, \int_b^z \omega_{g-1}, h_{\mathfrak{p}}(A_{Z_0}(b,z)), \ldots, h_{\mathfrak{p}}(A_{Z_k}(b,z))\right) = 0$$

is finite, and contains $X(K_{\mathfrak{p}})_\alpha$.

6. Chabauty-Kim theory and p-adic heights

This section is concerned with relating the mixed extensions $A(b,z)$ defined above to the mixed extensions arising from the theory of motivic height pairings as developed by Nekovář [24] and Scholl [29]. Such relations have been established in the case of fundamental groups of affine elliptic curves in work of Balakrishnan and Besser [3] and Balakrishnan, Dan-Cohen, Kim and Wewers [2] and in the case of affine hyperelliptic curves in work of Balakrishnan, Besser and Müller [6].

6.1. **Notation.** In this section we will repeatedly consider various Ext groups of constructible $\mathbb{Q}_p$-sheaves on $\overline{X} \times \overline{X}$. As all cohomology will be étale, we will omit subscripts. For codimension 1 cycles $Z_1, Z_2 \subset X \times X$, we will write $H^i(\overline{X} \times \overline{X} - |Z_1|; |Z_2|)$ to mean

$$\operatorname{Ext}^i(j_{1!}j_1^*\mathbb{Q}_p, j_{2!}j_2^*\mathbb{Q}_p) := \mathbb{Q}_p \otimes \varprojlim \operatorname{Ext}^i(j_{1!}j_1^*\mathbb{Z}/p^n\mathbb{Z}, j_{2!}j_2^*\mathbb{Z}/p^n\mathbb{Z}),$$

where j_1 and j_2 are the open immersions of the complements of Z_1 and Z_2 into $X \times X$, and the Ext groups are in the category of constructible sheaves on $\overline{X} \times \overline{X}$.

We write $D.E$ to mean the intersection number of the cycles. For a smooth variety S and a cycle E in $Z^i(S)$ we write $\widetilde{\mathrm{cl}}_E$ to mean the induced homomorphism

$$\mathbb{Q}_p(-k) \to H^{2k}_E(\overline{S})$$

and write cl_E to mean the composite map

$$\mathbb{Q}_p(-k) \to H^{2k}_E(\overline{S}) \to H^{2k}(\overline{S}).$$

6.2. **The height pairing on algebraic cycles.** To relate fundamental groups to p-adic heights, we first explain what the local height functions defined above have to do with height pairings. We restrict attention to the case of the p-adic height pairing on the curve X. Given a pair (Z,W) of cycles in $\mathrm{Div}^0(X)$ with disjoint support $|Z|$ and $|W|$, we construct a mixed extension $H(Z,W)$ with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$ as a subquotient of $H^1(\overline{X}-|Z|;|W|)(1)$ as follows [24, §5.6]. The representation $H^1(\overline{X}-|Z|;|W|)(1)$ is a mixed extension with graded pieces $\mathrm{Ker}(H^2_{|Z|}(\overline{X}) \to H^2(\overline{X}))(1)$, V and $\mathrm{Ker}(H^2_{|W|}(\overline{X}) \to H^2(\overline{X}))^*$. Pulling back by

$$\mathbb{Q}_p \xrightarrow{\widetilde{\mathrm{cl}}_Z} \mathrm{Ker}(H^2_{|Z|}(\overline{X}) \to H^2(\overline{X}))(1)$$

and then pushing out by the dual of

$$\mathbb{Q}_p(-1) \xrightarrow{\widetilde{\mathrm{cl}}_W} \mathrm{Ker}(H^2_{|W|}(\overline{X}) \to H^2(\overline{X}))$$

gives a mixed extension with graded pieces $\mathbb{Q}_p, V$ and $\mathbb{Q}_p(1)$, denoted $H_X(Z,W)$. Composing with h_v gives, at each prime, a functional

$$(Z,W) \mapsto h_v(H(Z,W)).$$

By [24, §2], this is bi-additive, symmetric, and if $Z=\mathrm{div}(f)$ then

$$h_v(Z,W) = \chi_v(f(W)).$$

We denote $h_v(H_X(Z,W))$ simply by $h_v(Z,W)$. Given cycles Z and W in $\mathrm{Div}^0(X_K)$ with disjoint support one defines the global p-adic height $h(Z,W)$ associated to χ, s to be the sum over all v of $h_v(Z,W)$. The function h is bilinear and factors through $\mathrm{Pic}^0(X) \times \mathrm{Pic}^0(X)$ (unlike the local heights).

6.3. **Beilinson's formula.** The proof of the relation to p-adic heights is to use a motivic interpretation of $A_n(b,z)$, due to Beilinson [15, Proposition 3.4], and then do a little diagram chasing. To state Beilinson's theorem, let Y be a smooth geometrically connected variety over a field K of characteristic zero. Let b and z be K-points of Y. As before let

$$A_n(Y)(b) := \mathbb{Q}_p[\pi_1^{\acute{e}t}(\overline{Y},b)]/I^{n+1}$$

and

$$A_n(Y)(b,z) := \mathbb{Q}_p[\pi_1^{\acute{e}t}(\overline{Y},b,z)] \otimes_{\mathbb{Q}_p[\pi_1^{\acute{e}t}(\overline{Y},b)]} A_n(Y)(b).$$

Theorem 5 (Beilinson, [15], Proposition 3.4)**.** *Let Y^n denote the n-fold product of Y over K. Let D_0 denote $b \times Y^{n-1}$, D_n denote $Y^{n-1} \times z$, and for $0<i<n$, define D_i to be the codimension one subscheme of Y^n on which the ith and $(i+1)$th co-ordinates are equal.*
(i): When $b \neq z$, there is an isomorphism of G_K-representations

$$A_n(Y)(b,z) \simeq H^n(\overline{Y}^n; \bigcup_{i=0}^n D_i)^*.$$

(ii): When $b = z$ there is an isomorphism of G_K-representations

$$A_n(Y)(b) \simeq H^n(\overline{Y}^n; \bigcup_{i=0}^{n} D_i)^* \oplus \mathbb{Q}_p.$$

We will be interested in applying Theorem 5 in the case when $n = 2$, for the smooth projective curve X and for the affine curve $Y := X - x$ obtained by removing a K-point of X. Define $S := Y \times Y$.

Let b and z be distinct, and both not equal to x. Define $X_1 := \{b\} \times \overline{X}$,$X_2 := \overline{X} \times \{z\}$, and define

$$i_1, i_2, i_\Delta : \overline{X} \hookrightarrow \overline{X} \times \overline{X}$$

to be the closed immersions of X_1, X_2 and Δ respectively into $\overline{X} \times \overline{X}$. For future use we also let

$$\pi_1, \pi_2 : \overline{X} \times \overline{X} \to \overline{X}$$

denote the projection maps. We use the same notation for the corresponding maps with X and $X \times X$ replaced by Y and $Y \times Y$.

We first describe the difference between $H^2(\overline{Y} \times \overline{Y}; X_1 \cup X_2 \cup \Delta)$ and $H^2(\overline{X} \times \overline{X}; X_1 \cup X_2 \cup \Delta)$. There is a short exact sequence

$$0 \to H^1(\overline{Y}; b \cup z) \to H^2(\overline{Y} \times \overline{Y}; X_1 \cup X_2 \cup \Delta) \to H^2(\overline{Y} \times \overline{Y}; X_1 \cup X_2) \to 0.$$

There is also an isomorphism

$$H^2(\overline{S}; X_1 \cup X_2) \simeq H^1(\overline{X}) \otimes H^1(\overline{X})$$

coming from the composite of the Kunneth decomposition

$$H^2(\overline{S}; X_1 \cup X_2) \simeq H^1(\overline{Y}; b) \otimes H^1(\overline{Y}; z)$$

together with the isomorphisms

$$H^1(\overline{Y}; b) \simeq H^1(\overline{Y}; z) \simeq H^1(\overline{Y}) \simeq H^1(\overline{X}).$$

Hence we get a short exact sequence

$$0 \to H^1(\overline{Y}; b \cup z) \to H^2(\overline{Y} \times \overline{Y}; X_1 \cup X_2 \cup \Delta) \to H^1(\overline{X}) \otimes H^1(\overline{X}) \to 0.$$

The dual of $A_2(X)(b, z)$ is isomorphic to $H^2(\overline{X} \times \overline{X}; X_1 \cup X_2 \cup \Delta)$, which sits in an exact sequence

$$0 \to H^1(\overline{X}; b \cup z) \to H^2(\overline{X} \times \overline{X}; X_1 \cup X_2 \cup \Delta) \to H^2(\overline{X} \times \overline{X}) \xrightarrow{(i_1^*, i_2^*, i_\Delta^*)} H^2(\overline{X})^{\oplus 3} \to 0.$$

The natural map

$$H^2(\overline{X} \times \overline{X}; X_1 \cup X_2 \cup \Delta) \to H^2(\overline{Y} \times \overline{Y}; X_1 \cup X_2 \cup \Delta)$$

is injective and gives a short exact sequence

$$0 \to H^2(\overline{X} \times \overline{X}; X_1 \cup X_2 \cup \Delta) \to H^2(\overline{Y} \times \overline{Y}; X_1 \cup X_2 \cup \Delta) \to H^2(\overline{X}) \to 0.$$

Via the above, if Z is a cycle in $X \times X$ whose image in $H^2(\overline{Y} \times \overline{Y})$ is nonzero then Z defines a subobject of $H^2(\overline{Y} \times \overline{Y}; X_1 \cup X_2 \cup \Delta)$. If the intersection number of Z with $\Delta - X_1 - X_2$ is zero then this subobject is in the image of $H^2(\overline{X} \times \overline{X}; X_1 \cup X_2 \cup \Delta)$ (specifically, its image in $H^2(\overline{X} \times \overline{X})$ is the Kunneth projector of Z).

6.4. $h(A(b,z))$ **as a height pairing between algebraic cycles.** Via Beilinson's cohomological characterisation of the mixed extension $A_2(Y)(b,z)$, characterising the local heights of $A(b,z)$ in terms of the height pairings on algebraic cycles is reduced to relating subquotients of $H^1(\overline{Y}-|Z_1|;|Z_2|)$ to subquotients of $H^2(\overline{Y}\times\overline{Y};|W|)$, where the divisors W arise from Beilinson's theorem.

Let Z be a divisor of $\overline{S}$ intersecting X_1, X_2 and Δ properly. We somewhat abusively denote the composite map

$$\mathbb{Q}_p(-1)\xrightarrow{\mathrm{cl}_Z}H^2(\overline{S})\to H^1(\overline{X})^{\otimes 2}\xrightarrow{\simeq}H^2(\overline{S};X_1\cup X_2)$$

by cl_Z, where the last map is the isomorphism induced by

$$H^2(\overline{S};X_1\cup X_2)\to H^2(\overline{S}).$$

Definition 11. Define $D(b,z)\in\mathrm{Div}^0(X)$ to be the cycle $i_\Delta^*Z-i_1^*Z-i_2^*Z+(Z.X_1+Z.X_2-Z.\Delta)x$.

Let $E_Z=E_Z(b,z)$ be the mixed extension with graded pieces obtained by pulling back $H^2(\overline{S};X_1\cup X_2\cup\Delta)(1)$ by the image of Z:

$$\begin{tikzcd}
E_Z \arrow[r] \arrow[d] & \mathbb{Q}_p \arrow[d, "\mathrm{cl}_Z"] \\
H^2(\overline{S};X_1\cup X_2\cup\Delta)(1) \arrow[r] & H^1(\overline{Y})\otimes H^1(\overline{Y})(1).
\end{tikzcd}$$

As in §5.1, if cl_Z is nonzero it defines a surjection $A[2](Y)\to\mathbb{Q}_p(1)$ and hence a quotient $A(b,z)$ of $A_2(Y)(b,z)$. The representation $A(b,z)$ is the dual of E_Z. If the intersection number of Z with $\Delta-X_1-X_2$ is zero then $A(b,z)$ in fact comes from a quotient of $A_2(X)(b,z)$. The following theorem says that the mixed extension $A(b,z)$ is exactly the one built out of the zero divisors $z-b$ and $D(b,z)$. In [13, Theorem 2.2], Darmon, Rotger and Sols proved that the Abel-Jacobi class of $D(b,z)$ is equal to the extension of $\mathbb{Z}$-mixed Hodge structure corresponding to the motive whose étale realisation is $IA(b,z)$. This generalised previous work of Kaenders [20]. The theorem below refines this to determine $A(b,z)$ as a mixed extension of $\kappa(z-b)$ and $IA(b,z)^*(1)$.

Theorem 6. *Let Z be any codimension 1 cycle in $X\times X$ whose image in $H^2(\overline{Y}\times\overline{Y})$ is nonzero. The mixed extension E_Z is isomorphic to $H_X(z-b,i_\Delta^*Z-i_1^*Z-i_2^*Z+mx)(-1)$, where m is the intersection number of Z with $X_1+X_2-\Delta$.*

Proof. For any cycle W we have a commutative diagram with exact columns and rows

$$\begin{tikzcd}
H^1_{|i_\Delta^*W|}(\overline{Y};\{b\}\cup\{z\}) \arrow[r] \arrow[d] & H^2_{|W|}(\overline{S};X_1\cup X_2\cup\Delta) \arrow[r] \arrow[d] & H^2_{|W|}(\overline{S};X_1\cup X_2) \arrow[d] \\
H^1(\overline{Y};\{b\}\cup\{z\}) \arrow[r] \arrow[d] & H^2(\overline{S};X_1\cup X_2\cup\Delta) \arrow[r] \arrow[d] & H^2(\overline{S};X_1\cup X_2) \arrow[d] \\
H^1(\overline{Y}-|i_\Delta^*W|;\{b\}\cup\{z\}) \arrow[r] & H^2(\overline{S}-|W|;X_1\cup X_2\cup\Delta) \arrow[r] & H^2(\overline{S}-|W|;X_1\cup X_2).
\end{tikzcd}$$

To prove the theorem, we first find a cycle W such that the image of $\mathrm{cl}_Z(\mathbb{Q}_p(-1))$ in $H^2(\overline{S}-|W|;X_1\cup X_2)$ is zero. This identifies E_Z with a subspace of $H^1(\overline{Y}-|i_\Delta^*W|;\{b\}\cup\{z\})$. One then determines the subspace exactly by giving a cohomological interpretation of the inclusion of the weight 2 part of E_Z inside the weight 2 part of $H^1(\overline{Y} - |i_\Delta^* W|; \{b\} \cup \{z\})$.

Let $\pi_2^* i_1^* Z$ denote the divisor obtained by fibering the divisor $i_1^* Z$ of X with X (so that if $i_1^* Z = \sum n_i x_i$, then $\pi_2^* i_1^* Z = \sum n_i x_i \times \overline{X}$). Similarly define $\pi_1^* i_2^* Z$. Define

$$W := Z - \pi_2^* i_1^* Z - \pi_1^* i_2^* Z.$$

Lemma 8. *The image of* $\mathrm{cl}_Z(\mathbb{Q}_p(-1))$ *in* $H^2(\overline{S} - |W|; X_1 \cup X_2)$ *is zero.*

Proof. Let $D := \overline{X} \times \overline{X} - \overline{S}$. It is enough to show that $\mathrm{cl}_Z(\mathbb{Q}_p(-1))$ is in the image of

$$H^2_{|W| \cup D}(\overline{X} \times \overline{X}; X_1 \cup X_2) \to H^2(\overline{S}; X_1 \cup X_2).$$

Let $W_1 := |i_1^* W| \cup i_1^{-1} D$ and $W_2 := |i_2^* W| \cup i_2^{-1} D$. There is a commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & H^2_{|W| \cup D}(\overline{X} \times \overline{X}; X_1 \cup X_2) \arrow[r] \arrow[d] & H^2_{|W| \cup D}(\overline{X} \times \overline{X}) \arrow[r] \arrow[d] & H^2_{W_1}(X) \oplus H^2_{W_1}(X) \arrow[d] \\
 & H^2(\overline{X} \times \overline{X}; X_1 \cup X_2) \arrow[r] & H^2(\overline{X} \times \overline{X}) \arrow[r] & H^2(X_1) \oplus H^2(X_2).
\end{tikzcd}$$

The class of Z in $H^2(\overline{X} \times \overline{X})$ lifts to an element of $H^2_{W \cup D}(\overline{X} \times \overline{X})$ by construction. Hence to show $\mathrm{cl}_Z(\mathbb{Q}_p(-1))$ lifts to an element of $H^2_{W \cup D}(\overline{X} \times \overline{X}; X_1 \cup X_2)$ it is enough to show it lies in the kernel of

$$H^2_{W \cup D}(\overline{X} \times \overline{X}) \xrightarrow{i_1^* \oplus i_2^*} H^2_{W_1}(X) \oplus H^2_{W_1}(X).$$

This is the case since, in $H^2_{W_1}(X)$, $i_1^* \pi_2^* i_1^* Z = i_1^* Z$ and $i_1^* \pi_1^* i_2^* Z = 0$, and similarly for $H^2_{W_2}(X)$. □

Hence we deduce that E_Z is a subobject of $H^1(\overline{Y} - |i_\Delta^* W|; b \cup z)$, and all that remains is to determine the homomorphism

$$\mathbb{Q}_p(-1) \to H^2_{|W| \cup x}(\overline{X})$$

induced by this identification. Let $\delta : \mathrm{Ker}(\gamma) \to \mathrm{Coker}(\alpha)$ denote the connecting homomorphism associated to

$$\begin{tikzcd}
 & H^1(\overline{Y}; b \cup z) \arrow[r] \arrow[d, "\alpha"] & H^2(\overline{S}; X_1 \cup X_2 \cup \Delta) \arrow[r] \arrow[d, "\beta"] & H^2(\overline{S}; X_1 \cup X_2) \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & H^1(\overline{Y} - |i_\Delta^* W|; b \cup z) \arrow[r] & H^2(\overline{S} - |W|; X_1 \cup X_2 \cup \Delta) \arrow[r] & H^2(\overline{S} - |W|; X_1 \cup X_2). &
\end{tikzcd}$$

Then by construction E_Z is isomorphic to the pullback of $H^1(\overline{Y} - |i_\Delta^* W|; b \cup z)$ by the homomorphism

$$\mathbb{Q}_p(-1) \to \mathrm{Ker}(\gamma) \xrightarrow{\delta} \mathrm{Coker}(\alpha) \to H^2_{|i_\Delta^* W|}(\overline{Y}; b \cup z).$$

We claim that the diagram

$$\begin{tikzcd}
\mathrm{Ker}(\gamma) \arrow[r, "\delta"] & \mathrm{Coker}(\alpha) \arrow[d] \\
H^2_{|W|}(\overline{S}; X_1 \cup X_2) \arrow[u] \arrow[r, "i_\Delta^*"] & H^2_{|i_\Delta^* W|}(\overline{Y}; b \cup z)
\end{tikzcd}$$

commutes. This follows from the definition of the long exact sequence in cohomology associated to a short exact sequence of sheaves: for example it is implied by the following lemma, whose proof we sketch.

Lemma 9. *For $1 \leq i, j \leq 3$, let $I^\bullet_{i,j}$ be complexes of abelian groups, and let*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & I^\bullet_{1,1} \arrow[r] \arrow[d] & I^\bullet_{1,2} \arrow[r] \arrow[d] & I^\bullet_{1,3} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & I^\bullet_{2,1} \arrow[r] \arrow[d] & I^\bullet_{2,2} \arrow[r] \arrow[d] & I^\bullet_{2,3} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & I^\bullet_{3,1} \arrow[r] \arrow[d] & I^\bullet_{3,2} \arrow[r] \arrow[d] & I^\bullet_{3,3} \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

be a commutative diagram of abelian groups with exact columns and rows. Define

$$\begin{aligned}
J_1 &:= \mathrm{Ker}(H^i(I^\bullet_{2,3}) \to H^{i+1}(I^\bullet_{2,1})) \\
J_2 &:= \mathrm{Coker}(H^{i-1}(I^\bullet_{3,3}) \to H^i(I^\bullet_{3,1})) \\
K_1 &:= \mathrm{Ker}(H^i(I^\bullet_{1,3}) \to H^{i+1}(I^\bullet_{2,1})) \\
K_2 &:= \mathrm{Coker}(H^{i-1}(I^\bullet_{3,3}) \to H^{i+1}(I^\bullet_{1,1})).
\end{aligned}$$

Let

$$\delta : \mathrm{Ker}(J_1 \to H^i(I^\bullet_{3,3})) \to \mathrm{Coker}(H^i(I^\bullet_{2,1}) \to J_2)$$

be the connecting homomorphism associated to

$$\begin{tikzcd}
 & H^i(I_{2,1}) \arrow[r] \arrow[d] & H^i(I_{2,2}) \arrow[r] \arrow[d] & J_1 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & J_2 \arrow[r] & H^i(I_{3,2}) \arrow[r] & H^i(I_{3,3}). &
\end{tikzcd}$$

Then the diagram

$$\begin{tikzcd}
 & \mathrm{Ker}(J_1 \to H^i(I_{3,3})) \arrow[r, "\delta"] & \mathrm{Coker}(H^i(I_{2,1}) \to J_2) \arrow[dr] & \\
K_1 \arrow[ur] \arrow[dr] & & & K_2 \\
 & H^i(I_{1,3}) \arrow[r] & H^{i+1}(I_{1,1}) \arrow[ur] &
\end{tikzcd}$$

commutes.

Proof. Let $d^k_{i,j}$ be the differential $I^k_{i,j} \to I^{k+1}_{i,j}$ and let $Z^k_{i,j} = \mathrm{Ker}(d^k_{i,j})$. Consider the following function from K_1 and K_2: start with v_1 in K_1, lift to v_2 in $Z^i_{1,3}$, lift that to get v_3 in $I^i_{2,2}$, take differentials to get v_4 in $Z^{i+1}_{2,2}$, check that this can be lifted to v_5 in $Z^{i+1}_{1,1}$, take its image in K_2. We claim the top and bottom maps from K_1

to K_2 are both instances of this construction. In the top map, one starts with an element in $Z^i_{1,3}$, maps it to an element of $Z^i_{2,3}$, lifts it to an element of $Z^i_{2,2}$, maps it down to $Z^i_{3,2}$, lifts it to an element of $Z^i_{3,1}$, lifts that to an element of $I^i_{2,1}$, maps it to an element of $Z^{i+1}_{2,1}$ and finally lifts that to an element of $Z^{i+1}_{1,1}$. In the bottom map, one starts with an element in $Z^i_{1,3}$, lifts it to an element of $I^i_{1,2}$, maps that down to an element of $Z^{i+1}_{1,2}$, and then lifts that to an element of $Z^{i+1}_{1,1}$. This proves the claim, since $I^\bullet_{1,2}$ and $I^\bullet_{2,1}$ are both subcomplexes of $I^\bullet_{2,2}$, and the differentials on $I^\bullet_{1,2}$ and $I^\bullet_{2,1}$ are just the restriction of the differential on $I^\bullet_{2,2}$. □

By commutativity of the diagram

$$\begin{tikzcd}
H^2_{|W|}(\overline{S}; X_1 \cup X_2) \arrow[r] \arrow[d, "i^*_\Delta"] & H^2_{|W|}(\overline{S}) \arrow[d, "i^*_\Delta"] \\
H^2_{|i^*_\Delta W|}(\overline{Y}; b \cup z) \arrow[r, "\simeq"] & H^2_{|i^*_\Delta W|}(\overline{Y})
\end{tikzcd}$$

we deduce that E_Z is isomorphic to the pullback of $H^1(\overline{Y} - |i^*_\Delta W|; b \cup z)$ by

$$\widetilde{\mathrm{cl}}_{i^*_\Delta W} : \mathbb{Q}_p(-1) \to H^2_{|i^*_\Delta W|}(\overline{Y}).$$

Finally, we show that this implies that the map

$$\mathbb{Q}_p(-1) \to \mathrm{Ker}(H^2_{|i^*_\Delta W| \cup x}(\overline{X}) \to H^2(\overline{X}))$$

is equal to

$$\widetilde{\mathrm{cl}}_{i^*_\Delta W - (W.\Delta)x} \to H^2_{|i^*_\Delta W| \cup x}(\overline{X}).$$

Via the isomorphism

$$H^1(\overline{X}; b \cup z) \simeq H^1(\overline{Y}; b \cup z),$$

one obtains an isomorphism

$$H^2_{|i^*_\Delta W|}(\overline{Y}) \simeq \mathrm{Ker}(H^2_{|i^*_\Delta W| \cup x}(\overline{X}) \to H^2(\overline{X}))$$

which sends the class of a cycle $\sum d_i(z_i)$ with support in $W \cap Y$ to $\sum d_i(z_i) - (\sum d_i)x$. This completes the proof of the theorem. □

7. p-adic heights on hyperelliptic curves

In this section we recall facts about height pairings and use them to relate the height pairing of the cycles $z - b$ and $D(b, z)$ to the height pairings arising in Theorems 1 and 3. We fix a choice of idele class character χ and an isotropic splitting of the Hodge filtration on $H^1_{\mathrm{dR}}(X_{K_\mathfrak{p}})$.

By the work of Besser [7], Nekovář's p-adic height pairing is equal to the p-adic height pairing of Coleman and Gross defined in [12]. In [3, §2], it is shown that one may extend the Coleman-Gross local height pairing to divisors with non-disjoint support, although as in the case of the real-valued height pairing such an extension will in general depend on a choice of a global tangent vector at each point. As explained in [6] there is a canonical choice of such a tangent vector when X is a hyperelliptic curve with a fixed odd degree model.

We write $h_v(D)$ to mean $h_v(D, D)$, and $h(D)$ to mean $\sum_v h_v(D)$. When $X = E$ is an elliptic curve with origin ∞, for z in $E(K_v)$ we define

$$h_v(z) := h_v((z) - (\infty)).$$

7.1. **Height identities.**

Let X be a hyperelliptic curve, and let w denote the hyperelliptic involution on X. In this subsection we briefly review the theory of height pairings on hyperelliptic curves [3, 4].

Definition 12. For a divisor D on X, define $D^+ := D + w^*D$ and $D^- := D - w^*D$.

Lemma 10. *For any divisors $D_1, D_2 \in \mathrm{Div}^0(X)$,*

$$h_v(D_1, D_2) = \frac{1}{4} h_v(D_1^+, D_2^+) + \frac{1}{4} h_v(D_1^-, D_2^-).$$

Part (i) of the next lemma is proved in [6] (see (4.3) and the subsequent discussion). Part (ii) also follows straightforwardly from the proof.

Lemma 11. *Let X be a hyperelliptic curve of genus g, defined by an equation of the form*

$$y^2 = x^{2g+1} + \sum_{i=0}^{2g} a_i x^i.$$

Let ∞ denote the point at infinity.
(i) Let z be a point of X not equal to ∞, with $y(z) \neq 0$. Then

$$h_v(z^+ - 2\infty) = 2\chi_v(y(z)) + 2\chi_v(2).$$

(ii) Let z_1, z_2 be points of X not equal to ∞. Suppose $x(z_1) \neq x(z_2)$. Then

$$h_v(z_1^+ - 2\infty, z_2^+ - 2\infty) = 2\chi_v(x(z_1) - x(z_2)).$$

Proof. As explained in [6, §4], one finds normalised parameters at z and $w(z)$ are given by $x - x(z)/2y(z)$, and that $-y/x^{g+1}$ is a normalised parameter at infinity. The lemma now follows from the definition of the Coleman-Gross pairing on divisors of non-disjoint support. □

As a corollary we deduce

Lemma 12. *Let E be an elliptic curve*

$$y^2 = x^3 + ax^2 + bx + c.$$

Then for any z_1, z_2 in E both not equal to ∞, and with $x(z_1) \neq x(z_2)$,

$$2h_v(z_1 - \infty) + 2h_v(z_2 - \infty) - h_v(z_1 - z_2) - h_v(z_1 - w(z_2)) = 2\chi_v(x(z_1) - x(z_2)).$$

Proof. We first break the left hand side into symmetric and antisymmetric parts. The antisymmetric part equals

$$\frac{1}{2} h_v(z_1^-) + \frac{1}{2} h_v(z_2^-) - \frac{1}{4} h_v(z_1^- - z_2^-) - \frac{1}{4} h_v(z_1^- + z_2^-).$$

By expanding out this can be seen to be zero. The symmetric part equals

$$\frac{1}{2} h_v(z_1^+ - 2\infty) + \frac{1}{2} h_v(z_2^+ - 2\infty) - \frac{1}{2} h_v(z_1^+ - z_2^+).$$

Expanding, this equals

$$\frac{1}{2} h_v(z_1^+ - 2\infty, z_2^+ - 2\infty) + \frac{1}{2} h_v(z_2^+ - 2\infty, z_1^+ - 2\infty),$$

hence the result now follows from Lemma 11. □

Lemma 13. *For any z not equal to ∞,*

$$h_v(z - \infty, w(z) - \infty) + h_v(z - \infty, z - \infty) = \chi_v(2y(z)).$$

Proof. The antisymmetric parts of $h_v(z-\infty, w(z)-\infty)$ and $h_v(z-\infty, z-\infty)$ cancel out, hence the left hand side is equal to $\frac{1}{2}h_v(z^+ - 2\infty)$, which equals $\chi_v(2y(z))$ by Lemma 11. □

7.2. **Integral points on hyperelliptic curves.** Let X be a hyperelliptic curve given by an equation of the form

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

where $f(x)$ is a monic polynomial in $\mathcal{O}_K[x]$ of degree $2g+1$. Let $Y = X - \infty$. Take Z to be the cycle $\Gamma_w = \{(z, w(z))\} \subset X \times X$. Let $\{z_1, \dots, z_n\}$ denote the set of $\overline{K}$ points of X with y-coordinate zero, and let W denote the divisor $\sum_i z_i$. Let b and z be points of Y with nonzero y-coordinate. Then

$$\begin{aligned} i_1^*\Gamma_w &= w(b) \\ i_2^*\Gamma_w &= w(z) \\ i_\Delta^*\Gamma_w &= W + \infty \end{aligned}$$

hence $D(b, z) = W - w(b) - w(z) - (2g-1)\infty$. So the class of $A(Y)(b, z)$ is dual to $H_X(z - b, W - w(b) - w(z) - (2g-1)\infty)$, by Theorem 6. The following lemma illustrates how Theorem 1 may be deduced from Theorem 6 together with the affine version of Theorem 2.

Lemma 14. *For any prime v,*

$$h_v(z - b, D(b, z)) = h_v(z - \infty) - h_v(b - \infty).$$

Proof. First, note that additivity yields

$$h_v(z - b, D(b, z)) = h_v(z - b, W - (2g+1)\infty) - h_v(z - b, 2\infty - w(z) - w(b)).$$

Since $2(g+1)\infty - W = \mathrm{div}(y)$, the first term is equal to $\chi(y(z)) - \chi(y(b))$. For the second term, since $z - b$ and $2\infty - w(z) - w(b)$ are disjoint,

$$h_v(z-b, 2\infty-w(z)-w(b)) = \frac{1}{2}h_v(z-b, 2\infty-w(z)-w(b)) + \frac{1}{2}h_v(2\infty-w(z)-w(b), z-b).$$

By additivity

$$\begin{aligned} h_v(z - b, 2\infty - w(z) - w(b)) = {} & h_v(z - \infty, \infty - w(z)) + h_v(z - \infty, \infty - w(b)) \\ & + h_v(\infty - b, \infty - w(z)) + h_v(\infty - b, \infty - w(b)) \end{aligned}$$

and similarly for $h_v(2\infty - w(z) - w(b), z - b)$. Using the fact that $h_v(D_1, D_2) = h_v(w(D_1), w(D_2))$, this gives

$$h_v(z - b, 2\infty - w(z) - w(b)) = h_v(z - \infty, \infty - w(z)) + h_v(\infty - b, \infty - w(b)).$$

The result now follows from Lemma 13. □

7.3. **Rational points on bielliptic curves.** In this subsection we return to the case where X is a genus 2 curve of the form

$$y^2 = x^6 + ax^4 + bx^2 + c,$$

and explain how to deduce Theorem 3 from Theorem 2. Let h_v and h denote (local and global, resp.) heights on X, $h_{E_1,v}$ and h_{E_1} heights on E_1, and $h_{E_2,v}$ and h_{E_2} heights on E_2. Recall from the introduction the associated elliptic curves E_i and morphisms $f_i : X \to E_i$. Define $Z_1 \subset X \times X$ to be the graph of the automorphism

$$g_1 : (x, y) \mapsto (-x, y)$$

and Z_2 to be the graph of

$$g_2 : (x, y) \mapsto (-x, -y).$$

As explained in §6.4, the fact that the intersection number of $Z_1 - Z_2$ with $\Delta - X_1 - X_2$ is zero implies that Z defines a quotient of the fundamental group of $\overline{X}$, and a quotient $A(b, z)$ of $A(X)(b, z)$. Note that

$$\begin{aligned} i_1^*(Z_1 - Z_2) &= g_1(z) - g_2(z) \\ i_2^*(Z_1 - Z_2) &= g_1(b) - g_2(b) \\ i_\Delta^*(Z_1 - Z_2) &= (0, \sqrt{c}) + (0, -\sqrt{c}) - \infty - w(\infty) \end{aligned}$$

so $D(b, z) = (0, \sqrt{c}) + (0, -\sqrt{c}) - \infty - w(\infty) - g_1(z) + g_2(z) - g_1(b) + g_2(b)$. The following lemma completes the proof of Theorem 3.

Lemma 15. *For any b and z with $x(b) \neq x(z)$ and both not equal to zero or infinity,*

$$\begin{aligned} h_v(z - b, D(b, z)) = h_{E_1,v}(f_1(z) - \infty) - h_{E_1,v}(f_1(b) - \infty) - h_{E_2,v}(f_2(z) - \infty) \\ + h_{E_2,v}(f_2(b) - \infty) + 2\chi(x(b)) - 2\chi(x(z)). \end{aligned}$$

Proof. Define divisors D_1 and D_2 on E_1 and E_2 respectively by

$$\begin{aligned} D_1 &= w(f_1(z)) + w(f_1(b)) - 2\infty \\ D_2 &= w(f_2(z)) + w(f_2(b)) - 2\infty. \end{aligned}$$

Then

$$\infty + w(\infty) - (0, \sqrt{c}) - (0, -\sqrt{c}) - g_1(z) + g_2(z) - g_1(b) + g_2(b) = f_1^*(D_1) - f_2^*(D_2),$$

hence

$$\begin{aligned} h_v(z - b, D(b, z)) = h_{E_1,v}(f_1(z) - f_1(b), w(f_1(z)) + w(f_1(b)) - 2\infty) \\ - h_{E_2,v}(f_2(z) - f_2(b), w(f_2(z)) + w(f_2(b)) - 2\infty). \end{aligned}$$

As in the proof of Lemma 14,

$$\begin{aligned} h_{E_1,v}(f_1(z) - f_1(b), w(f_1(z)) + w(f_1(b)) - 2\infty) = h_{E_1,v}(f_1(z) - \infty) - h_{E_1,v}(f_1(b) - \infty) \\ + \chi(y(f_1(z))) - \chi(y(f_1(b))) \end{aligned}$$

and similarly for f_2. Hence

$$\begin{aligned} h_v(z - b, D(b, z)) = h_{E_1,v}(f_1(z) - \infty) - h_{E_1,v}(f_1(b) - \infty) - h_{E_2,v}(f_2(z) - \infty) \\ + h_{E_2,v}(f_2(b) - \infty) + \chi(y(f_1(z))y(f_2(b))/y(f_1(b))y(f_2(z))). \end{aligned}$$

The lemma now follows from recalling that $y(f_1(z))/y(f_2(z)) = cx(z)^2$. □

The proof of Theorem 2 now follows from Theorem 6 together with Lemma 15.

8. Computing $X(K_{\mathfrak{p}})_U$

In this section, we explain how to use Theorem 3 in practice and describe the computation of $X(K_{\mathfrak{p}})_U$. We give two numerical examples of $X(K_{\mathfrak{p}})_U$ and further discuss how one might effectively extract $X(K)$ from $X(K_{\mathfrak{p}})_U$.

8.1. **Another formula for $X(K_\mathfrak{p})_U$.** We record the following slight variant of Theorem 3, which turns the computation into one which can be carried out over two affine patches covering $X(K)$.

Corollary 1. *Let X/K be a genus 2 bielliptic curve*

$$y^2 = x^6 + ax^4 + bx^2 + c$$

over $K = \mathbb{Q}$ or an imaginary quadratic field.
(i): For all $v \nmid p$,

$$h_{E_1,v}(f_1(z) + (0, \sqrt{c})) + h_{E_1,v}(f_1(z) + (0, -\sqrt{c})) - 2h_{E_2,v}(f_2(z))$$

and

$$h_{E_2,v}(f_2(z) + (0, c)) + h_{E_2,v}(f_2(z) + (0, -c)) - 2h_{E_1,v}(f_1(z))$$

each take only finitely many values, and for almost all v are identically zero.
(ii): Suppose $\operatorname{rk} E_1(K) = \operatorname{rk} E_2(K) = 1$, and let $P_i \in E_i(K)$ be points of infinite order. Let $\alpha_i = \frac{h_{E_i}(P_i)}{[K:\mathbb{Q}]\log_{E_i}(P_i)^2}$. Let Ω_1 denote the finite set of values taken by

$$\sum_{v \nmid p} \left(h_{E_1,v}(f_1(z) + (0, \sqrt{c})) + h_{E_1,v}(f_1(z) + (0, -\sqrt{c})) - 2h_{E_2,v}(f_2(z))\right),$$

for (z_v) in $\prod_{v \nmid p} X(K_v)$. Then $X(K)$ is contained in the finite set of z in $X(K_\mathfrak{p})$ satisfying

$$\begin{aligned}(7)\quad \rho_1(z) := 2h_{E_2,\mathfrak{p}}(f_2(z)) - h_{E_1,\mathfrak{p}}(f_1(z) + (0, \sqrt{c})) - h_{E_1,\mathfrak{p}}(f_1(z) + (0, -\sqrt{c}))\\ - 2\alpha_2 \log_{E_2}(f_2(z))^2 + 2\alpha_1(\log_{E_1}(f_1(z))^2 + \log_{E_1}((0, \sqrt{c}))^2) \in \Omega_1.\end{aligned}$$

Let Ω_2 denote the finite set of values taken by

$$\sum_{v \nmid p} \left(h_{E_2,v}(f_2(z) + (0, c)) + h_{E_2,v}(f_2(z) + (0, -c)) - 2h_{E_1,v}(f_1(z))\right).$$

Then $X(K)$ is contained in the finite set of z in $X(K_\mathfrak{p})$ satisfying

$$\begin{aligned}(8)\quad \rho_2(z) := 2h_{E_1,\mathfrak{p}}(f_1(z)) - h_{E_2,\mathfrak{p}}(f_2(z) + (0, c)) - h_{E_2,\mathfrak{p}}(f_2(z) + (0, -c))\\ - 2\alpha_1 \log_{E_1}(f_1(z))^2 + 2\alpha_2(\log_{E_2}(f_2(z))^2 + \log_{E_2}((0, c))^2) \in \Omega_2.\end{aligned}$$

Proof. This follows from Theorem 3 together with Lemma 12. □

8.2. **Finding all points in $X(K_\mathfrak{p})_U$.** Now using Corollary 1, we calculate $X(K_\mathfrak{p})_U$ as the union of points found in the following two computations:

$$X(K_\mathfrak{p})_U = \{z \in X(K_\mathfrak{p})_U : x(z) \notin \mathfrak{p}, \rho_1(z) \in \Omega_1\} \cup \{z \in X(K_\mathfrak{p})_U : x(z) \in \mathfrak{p}, \rho_2(z) \in \Omega_2\}.$$

We explain in Algorithm 1 below how to compute each of the following terms:

$$\begin{aligned}\rho_1(t) = \underbrace{2h_{E_2,\mathfrak{p}}(f_2(t))}_{\text{Steps 7d,e,f}} - \underbrace{h_{E_1,\mathfrak{p}}(f_1(t) + (0, \sqrt{c}))}_{\text{Steps 7b,e,f}} - \underbrace{h_{E_1,\mathfrak{p}}(f_1(t) + (0, -\sqrt{c}))}_{\text{Steps 7c,e,f}})\\ - \underbrace{2\alpha_2}_{\text{Step 3}} \underbrace{\log_{E_2}(f_2(t))^2}_{\text{Step 7g}} + \underbrace{2\alpha_1}_{\text{Step 3}} (\underbrace{\log_{E_1}(f_1(t))^2}_{\text{Step 7g}} + \underbrace{\log_{E_1}((0, \sqrt{c}))^2}_{\text{Step 3}})\end{aligned}$$

as power series over $K_\mathfrak{p}$, which allows us to search for the points $z \in X(K_\mathfrak{p})_U$ that are solutions to the equation $\rho_1(z) = \beta$ for $\beta \in \Omega_1$.

We recall an interpretation of the local height $h_\mathfrak{p}$ as a double Coleman integral, which is used in Algorithm 1:

Lemma 16. *We have that $h_{E_i,\mathfrak{p}}(z) = \int_\infty^z \omega_0 \bar{\omega_0}$, where $\bar{\omega_0}$ is the dual to $\omega_0 = \frac{dx}{2y}$ under the cup product pairing on $H^1_{dR}(E_i)$.*

Proof. See [6, §4], where the the local height h_p of $z - \infty$ is denoted as $\tau(z)$. □

Algorithm 1 (Computing the set $\{z \in X(K_\mathfrak{p})_U : x(z) \notin \mathfrak{p}, \rho_1(z) \in \Omega_1\}$)**.**
Input: *Genus 2 curve X/K defined by an equation $y^2 = x^6 + ax^4 + bx^2 + c$ such that the corresponding $E_1(K), E_2(K)$ each have Mordell-Weil rank 1, a good ordinary prime p, finite set of values Ω_1.*
Output: *The following subset of $X(K_\mathfrak{p})_U : \{z \in X(K_\mathfrak{p})_U : x(z) \notin \mathfrak{p}, \rho_1(z) \in \Omega_1\}$.*

1. *Compute points $P_1 \in E_1(K)$ and $P_2 \in E_2(K)$ of infinite order.*
2. *Compute global p-adic heights $h_{E_1}(P_1)$ and $h_{E_2}(P_2)$, using minimal models for E_1, E_2.*
3. *Compute*
$$\log_{E_1}((0,\sqrt{c}))^2 = \left(\int_\infty^{(0,\sqrt{c})} \omega_0\right)^2, \quad \alpha_i = \frac{h_{E_i}(P_i)}{[K:\mathbb{Q}](\int_\infty^{P_i} \omega_0)^2}, \quad i = 1,2.$$
4. *Compute the cup product pairing between elements in $H^1_{dR}(E_1)$ and also between elements in $H^1_{dR}(E_2)$; use this to compute $\bar{\omega_0}$ for E_1 and $\bar{\omega_0}$ for E_2, to write $h_{E_i,\mathfrak{p}} = \int \omega_0\bar{\omega_0}$.*
5. *Enumerate the list of points $\mathcal{D} = X(\mathbb{F}_\mathfrak{p}) \setminus \{(0, \pm\sqrt{c})\}$.*
6. *Initialise an empty set R.*
7. *For each $D \in \mathcal{D}$:*
    - (a) *Compute Q, a lift of D, and a local coordinate $(x(t), y(t))$ at Q.*
    - (b) *Compute $S_1 := f_1(Q) + (0,\sqrt{c})$. Likewise compute $f_1((x(t), y(t))) + (0,\sqrt{c})$ using the addition law on the elliptic curve, which sends the local coordinate to this residue disk.*
    - (c) *Compute $f_1(Q) - (0,\sqrt{c})$. Likewise compute $f_1((x(t), y(t))) - (0,\sqrt{c})$ using the addition law on the elliptic curve, which gives a local coordinate in the residue disk.*
    - (d) *Compute $f_2(Q)$. We have $f_2(x(t)) = (x(t))^{-2}$ gives the x-coordinate of a local coordinate in the residue disk of $f_2(Q)$.*
    - (e) *Compute the following local heights at $\mathfrak{p}$ of the points in Steps 7b - 7d: $h_{E_1,\mathfrak{p}}(f_1(Q) + (0,\sqrt{c})), h_{E_1,\mathfrak{p}}(f_1(Q) - (0,\sqrt{c})), h_{E_2,\mathfrak{p}}(f_2(Q))$.*
    - (f) *Using Step 4, for each of the points in Steps 7b - 7d, use the local coordinates computed to calculate a power series expansion of $h_{E_i,\mathfrak{p}}$ in the disk of the respective point, using Step 7e to set the global constant of integration. For example, for S_1, first compute a local coordinate $S_1(t) = (x_1(t), y_1(t))$ at S_1 (if S_1 is non-Weierstrass, $x_1(t) = t + x(S_1)$) and use it to compute*
    $$h_{E_1,\mathfrak{p}}(S_1(t)) = h_{E_1,\mathfrak{p}}(S_1) - 2\left(\int_{S_1}^{S_1(t)} \omega_0\bar{\omega}_0 + \int_{S_1}^{S_1(t)} \omega_0 \int_\infty^{S_1} \bar{\omega}_0\right).$$
    Then use the parametrisation computed in Step 7b so that this power series within the disk of S_1 uses the correct parameter, that induced by the local parameter at Q.

(g) *Compute* $\log_{E_i}(f_i(Q)(t)) = \log_{E_i}(f_i(Q)) + \int_{f_i(Q)(t)} \omega_0$ *; e.g., compute the constant of integration* $\log_{E_i}(f_i(Q))$*, then compute a local parameter* $f_i(Q)(t) = (x_i(t), y_i(t))$ *at* $f_i(Q)$ *to compute* $\int_{f_i(Q)(t)} \omega_0$*, then correct the parametrisation so that this power series with the disk of* $f_i(Q)$ *uses the correct parameter, that induced by the local parameter at* Q*, as in Step 7f.*

(h) *Finally, let* $\rho_1(t)$ *be the appropriately weighted sum of contributions from Steps 3, 7f, and 7g, as in Equation 7.*

(i) *For each* $\beta \in \Omega_1$*, compute the set of roots of* $\rho_1(t) = \beta$*. For each root* r*, append* $X(x(r), y(r)) \in X(K_\mathfrak{p})$ *with multiplicity to the set* R*.*

(8) *Output* R*, the subset* $\{z \in X(K_\mathfrak{p})_U : x(z) \notin \mathfrak{p}, \rho_1(z) \in \Omega_1\} \subset X(K_\mathfrak{p})_U$*.*

The computation of $\rho_2(z) \in \Omega_2$ is carried out in an analogous manner and only involves the two residue disks of $X(K_\mathfrak{p})$ not considered in Step 5 of Algorithm 1. Putting this together yields the following algorithm to compute $X(K_\mathfrak{p})_U$:

Algorithm 2 (Computing $X(K_\mathfrak{p})_U$)**.**
Input: *Genus 2 curve* X/K *given by an equation* $y^2 = x^6 + ax^4 + bx^2 + c$ *such that the corresponding* $E_1(K), E_2(K)$ *each have Mordell-Weil rank 1, a good ordinary prime* p*, finite set of values* Ω_1, Ω_2*.*
Output: *The set* $X(K_\mathfrak{p})_U$*, which is a finite set containing* $X(K)$*.*

(1) *Carry out Algorithm 1 as written to compute the set* $\{z \in X(K_\mathfrak{p})_U : x(z) \notin \mathfrak{p}, \rho_1(z) \in \Omega_1\}$*.*

(2) *Carry out Algorithm 1 with the appropriate modifications: input* Ω_2*, compute the power series expansions of terms present in* ρ_2*, and take* $\mathcal{D}$ *to be the remaining points in* $X(\mathbb{F}_\mathfrak{p})$*, i.e., the points* z *with* $x(z) \in \mathfrak{p}$*. The output is the set* $\{z \in X(K_\mathfrak{p})_U : x(z) \in \mathfrak{p}, \rho_2(z) \in \Omega_2\}$*.*

(3) *Return the union of points found in Steps 1 and 2. This is* $X(K_\mathfrak{p})_U$*.*

We now give two examples illustrating Algorithm 2, carried out using Sage [33].

8.3. **Example 1: Rational points on a genus 2 bielliptic curve with rank 2 Jacobian.** We compute $X(\mathbb{Q})$, where X is the genus 2 curve

$$X : y^2 = x^6 - 2x^4 - x^2 + 1.$$

Let E_1 and E_2 be the corresponding elliptic curves, which each have Mordell-Weil rank 1 over $\mathbb{Q}$ and integral j-invariant. On E_1, the point $P_1 = (0, 1)$ is of infinite order, and on E_2, the point $P_2 = (0, 1)$ is of infinite order. We take χ to be the cyclotomic character, normalised so that $\chi_p(z) = \log_p(z)$ and for $v \neq p$, $\chi_v(z) = -v(z)\log_p(v)$. Moreover, E_1 and E_2 each have good ordinary reduction at $p = 3$. We determine a finite set containing $X(\mathbb{Q}_3)_2$ and use this to determine $X(\mathbb{Q})$ exactly. We are not able to determine whether $X(\mathbb{Q}_3)_2 = X(\mathbb{Q})$.

8.3.1. *Local contributions away from* p. The curve X has bad reduction at 2, potential good reduction at 7 and good reduction at all other primes. Hence to determine the set Ω we need to determine the possible values of

$$h_{E_1,2}(f_1(z)) - h_{E_2,2}(f_2(z)) - 2\chi_2(x(z)).$$

First note that $X(\mathbb{Q}_2)$ has no $\mathbb{Q}_2$ points whose x-co-ordinate has valuation zero (e.g. by checking mod 8). It will turn out that the above functions can (each) only take two possible values, corresponding to $v(x) > 0$ and $v(x) < 0$, where v denotes the 2-adic valuation. We compute local heights on E_1. The equation given above for E_1 is not minimal at 2. A minimal equation is given by

$$y^2 = v^3 + v^2 - 2v - 1$$

(so $x = v + 1$). E_1 has type II reduction, which means that the singular point mod 2 doesn't lift to a $\mathbb{Q}_2$ point. Hence

$$h_{E_1,2}(f_1(z)) = 2\max\{0, -v_2(x(z))\}\log_p(2).$$

We compute local heights on E_2. The equation given for E_2 is minimal, and it has type IV reduction. The unique singular point of the special fibre is $(0, 1)$. By Silverman, the formula for the local height at points (x_0, y_0) of bad reduction is given by

$$h_{E_2,2}((x_0, y_0)) = -\frac{2}{3}(1 + v(y_0))\log_p(2).$$

Hence the possible values of $h_{E_2,2}(f_2(z))$ are $2\max\{0, v(x(z))\}\log_p(2)$ when the valuation of $x(z)$ is positive, and $-\frac{2}{3}\log_p(2)$ when the valuation of $x(z)$ is negative. Hence

$$h_{E_1,2}(f_1(z)) - h_{E_2,2}(f_2(z)) - 2\chi_2(x(z)) = \begin{cases} 0 & v(x(z)) < 0 \\ -\frac{2}{3}\log_p(2) & v(x(z)) > 0. \end{cases}$$

Finally $h_{E_2,2}((0, 1)) = -\frac{2}{3}\log_p(2)$ and $h_{E_1,2}((0, 1)) = 0$.

Hence by Lemma 12

$$h_{E_1,2}(f_1(z)+(0,1))+h_{E_1,2}(f_1(z)-(0,1))-2h_{E_2,2}(f_2(z)) = \begin{cases} 0 & v(x(z)) < 0 \\ \frac{4}{3}\log_p(2) & v(x(z)) > 0 \end{cases}$$

and

$$h_{E_2,2}(f_2(z)+(0,1))+h_{E_2,2}(f_2(z)-(0,1))-2h_{E_1,2}(f_1(z))- = \begin{cases} -\frac{4}{3}\log_p(2) & v(x(z)) < 0 \\ -\frac{8}{3}\log_p(2) & v(x(z)) > 0. \end{cases}$$

We deduce $\Omega_1 = \{0, \frac{4}{3}\log_p(2)\}$ and $\Omega_2 = \{-\frac{4}{3}\log_p(3), -\frac{8}{3}\log_p(3)\}$.

8.3.2. *Local contributions at* $p = 3$. Now we consider the contributions at $p = 3$. In the residue disks of $\infty^{\pm}$, we have

$$\begin{aligned}\rho_1(z) = {} & 2h_{E_2,p}(f_2(z)) - h_{E_1,p}(f_1(z) + (0, 1)) - h_{E_1,p}(f_1(z) - (0, 1)) \\ & - 2\alpha_2\log_{E_2}(f_2(z))^2 + 2\alpha_1(\log_{E_1}(f_1(z))^2 + \log_{E_1}((0, 1))^2) \in \Omega_1.\end{aligned}$$

In the disks with $x(z) = 0$, we have

$$\begin{aligned}\rho_2(z) = {} & 2h_{E_1,p}(f_1(z)) - h_{E_2,p}(f_2(z) + (0, 1)) - h_{E_2,p}(f_2(z) - (0, 1)) \\ & - 2\alpha_1\log_{E_1}(f_1(z))^2 + 2\alpha_2(\log_{E_2}(f_2(z))^2 + \log_{E_2}((0, 1))^2) \in \Omega_2.\end{aligned}$$

We carry out Algorithm 1 twice: for the residue disks corresponding to $\overline{\infty^{\pm}}$, we find z with $\rho_1(z) \in \Omega_1$. Then to work with the residue disks corresponding to $\overline{(0, \pm 1)}$ we find z with $\rho_2(z) \in \Omega_2$. This gives $X(\mathbb{Q}_3)_U$:

$X(\mathbb{F}_3)$	recovered $x(z)$ in residue disk	$z \in X(\mathbb{Q})$	$\rho_i(z) = \beta$
$\overline{\infty^{\pm}}$	$3^{-1} + 1 + 3^3 + 2 \cdot 3^4 + O(3^6)$		$\rho_1(z) = 0$
	$2 \cdot 3^{-1} + 1 + 2 \cdot 3 + 2 \cdot 3^2 + 3^3 + 2 \cdot 3^5 + O(3^6)$		$\rho_1(z) = 0$
	$\infty^{\pm}$	$\infty^{\pm}$	$\rho_1(z) = \frac{4}{3}\log_3(2)$
$\overline{(0, \pm 1)}$	$2 \cdot 3 + 3^2 + 3^3 + 3^4 + 3^5 + O(3^6)$	$(\frac{3}{2}, \pm\frac{1}{8})$	$\rho_2(z) = -\frac{8}{3}\log_3(2)$
	$3 + 3^2 + 3^3 + 3^4 + 3^5 + O(3^6)$	$(-\frac{3}{2}, \pm\frac{1}{8})$	$\rho_2(z) = -\frac{8}{3}\log_3(2)$
	$O(3^6)$	$(0, \pm 1)$	$\rho_2(z) = -\frac{4}{3}\log_3(2)$

Theorem 7. *We have* $X(\mathbb{Q}) = \left\{(0, \pm 1), \left(\frac{3}{2}, \pm\frac{1}{8}\right), \left(-\frac{3}{2}, \pm\frac{1}{8}\right), \infty^{\pm}\right\}$.

Proof. We wish to compute $X(\mathbb{Q})$ from $X(\mathbb{Q}_3)_U$. To do this, we must do two things: prove that the points in $X(\mathbb{Q}_3)_U$ which do not appear to be rational actually are not rational and check the multiplicities of all recovered points, to rule out the possibility that the table collapses multiple points that are just 3-adically close to the points in the table to the indicated precision. We start with the second task. Our computation shows that the solution $x(z) = O(3^6)$ occurs as a root of $\rho(z) = -\frac{4}{3}\log_3(2)$ with multiplicity two, which gives the known global points $(0, \pm 1)$ and two points 3-adically close to $(0, \pm 1)$. Likewise, solving $\rho(z) = \frac{4}{3}\log_3(2)$ yields $\infty^{\pm}$ on X and two points 3-adically close to $\infty^{\pm}$. The other points in the table, however, occur as roots with multiplicity 1. Note that $\rho(z)$ is an even function, so by considering the local expansion of ρ at each of the global points $(0, 1), (0, -1), \infty^{+}, \infty^{-}$, we see that its power series expansion must have a global double root at each of these points.

Now we show that the "extra" $\mathbb{Q}_3$ points recovered in the disks of $\infty^{\pm}$ cannot be rational, for the following formal group consideration. Consider $z \in X(\mathbb{Q}_3)$ with $v_3(x(z)) = -1$. Then the corresponding point $f_1(z)$ on E_1 has $v_3(x(f_1(z))) = -2$. However, note that $E_1(\mathbb{F}_3)$ has order 3 and $E_1(\mathbb{Q})$ is generated by P, where $P = (0, 1)$. Thus the smallest multiple of P in the formal group is $3P = (-\frac{8}{81}, -\frac{757}{729})$, which implies that the $v_3(x(Q)) \leq -4$ for any $Q \in \langle 3P \rangle$. So $f_1(z)$ cannot be rational and thus $z \notin X(\mathbb{Q})$. Thus we conclude $X(\mathbb{Q}) = \left\{(0, \pm 1), \left(\frac{3}{2}, \pm\frac{1}{8}\right), \left(-\frac{3}{2}, \pm\frac{1}{8}\right), \infty^{\pm}\right\}$. □

8.4. **Example 2:** $X_0(37)(\mathbb{Q}(i))$**.** Over $\mathbb{Q}$, $X_0(37)$ has the model

$$y^2 = -x^6 - 9x^4 - 11x^2 + 37.$$

Recall that $X_0(37)$ has good reduction away from 37. For convenience we make the change of variables $(x, y) \mapsto (ix, y)$ so that we take as our working model

$$X : y^2 = x^6 - 9x^4 + 11x^2 + 37.$$

Let J denote the Jacobian of X. Note that $X_0(37)$ and X are isomorphic over $K = \mathbb{Q}(i)$ and that $\operatorname{rk} J(\mathbb{Q}) = \operatorname{rk} J_0(37)(\mathbb{Q}(i)) = 2$. We thank Daniels and Lozano-Robledo [1] for bringing this example to our attention.

In this subsection we construct finite sets of $\mathfrak{p}$-adic points containing $X(K_{\mathfrak{p}})_2$ for various primes $\mathfrak{p}$ of good ordinary reduction. Using the Mordell-Weil sieve, as carried out by J. Steffen Müller and described in Appendix A, this is then used to determine $X(\mathbb{Q}(i))$. For convenience, we work with the following models of E_1 and E_2:

$$E_1 : y^2 = x^3 - 16x + 16 \qquad\qquad E_2 : y^2 = x^3 - x^2 - 373x + 2813$$

with maps from X to E_1 and E_2:

$$\begin{array}{llll} f_1 : & X & \longrightarrow & E_1 \\ & (x, y) & \mapsto & (x^2 - 3, y) \end{array} \qquad \begin{array}{llll} f_2 : & X & \longrightarrow & E_2 \\ & (x, y) & \mapsto & (37x^{-2} + 4, 37yx^{-3}). \end{array}$$

We take $P_1 = (0, 4) \in E_1(K)$ and $P_2 = (4, 37) \in E_2(K)$. We use primes p which are good, ordinary, and, so that we work over $\mathbb{Q}_p$ and not a quadratic extension, split in K and $\mathbb{Q}(\sqrt{37})$: we take $p = 41, 73$, and 101. For each of these primes p, we choose a prime $\mathfrak{p}$ lying above it in $\mathcal{O}_K$, and take χ to be a non-trivial idele class character of K which is trivial on $\mathcal{O}_{\overline{\mathfrak{p}}}^{\times}$. Hence $h_{\overline{\mathfrak{p}}}(A(b,z))$ will be identically zero. We normalise χ so that $\chi_{37}(37) = -\log_p(37)$.

8.4.1. *Local calculations at* 37. In this subsection we prove that for all $b, z \in X(\mathbb{Q}_{37})$ with $x(z)$ and $x(b)$ not equal to infinity,

$$\begin{aligned} &h_{E_1,37}(f_1(z)) - h_{E_1,37}(f_1(b)) - h_{E_2,37}(f_2(z)) + \\ &h_{E_2,37}(f_2(b)) + 2\chi_{37}(x(z)) - 2\chi_{37}(x(b)) = 0. \end{aligned}$$

Recall that by Lemma 15 this is equivalent to the statement that the inertia subgroup of $G_{\mathbb{Q}_{37}}$ acts trivially on $A(b,z)$. In [16] this is proved directly. As that proof involves other tools we do not want to introduce, we shall prove this by determining the local heights explicitly.

Lemma 17. *For all z in $X(\mathbb{Q}_{37})$, we have*
(i): $h_{E_1,37}(f_1(z)) = 2\chi_{37}(x(z))$.
(ii): $h_{E_2,37}(f_2(z)) = \frac{2}{3}\chi_{37}(37)$.

Proof. Note that there are no $\mathbb{Q}_{37}$ points of X for which $x(z)$ has positive 37-adic valuation. The Weierstrass equations given for E_1 and E_2 are both minimal at 37. The Weierstrass equation for E_1 is also regular hence all $\mathbb{Q}_{37}$ points are points of good reduction. This establishes part (i). The elliptic curve E_2 has split multiplicative reduction of type I3. The singular point of $E_2(\mathbb{F}_{37})$ is $(4,0)$, and all points of $E_{2,\mathbb{Q}_{37}}$ in the image of $X(\mathbb{Q}_{37})$ reduce to this point. By Silverman's algorithm [32, Theorem 5.2], we deduce that for all z in $X(\mathbb{Q}_{37})$, $h_{E_2,37}(f_2(z)) = \frac{2}{3}\chi_{37}(37)$. This completes the proof of part (ii). □

By Lemmas 12 and 15, this gives

$$\begin{aligned} &2h_{E_2,37}(f_2(z)) - h_{E_1,37}(f_1(z) + (-3,\sqrt{37})) - h_{E_1,37}(f_1(z) - (-1,\sqrt{37})) \\ &\quad = 2h_{E_2,37}(f_2(z)) - 2h_{E_1,37}(f_1(z)) - 2h_{E_1,37}((-3,\sqrt{37})) + 2\chi_{37}(x(f_1(z)) - 3) \\ &\quad = \frac{4}{3}\chi_{37}(37) - 4\chi_{37}(x(z)) + 4\chi_{37}(x(z)) = \frac{4}{3}\chi_{37}(37). \end{aligned}$$

Similarly

$$\begin{aligned} &2h_{E_1,37}(f_1(z)) - h_{E_2,37}(f_2(z) + (4,37)) - h_{E_2,37}(f_2(z) + (4,-37)) \\ &\quad = 2h_{E_1,37}(f_1(z)) - 2h_{E_2,37}(f_2(z)) - 2h_{E_2,37}((4,37)) + 2\chi_{37}(x(f_2(z)) - 4) \\ &\quad = 4\chi_{37}(x(z)) - \frac{8}{3}\chi_{37}(37) + 2\chi_{37}(37x(z)^{-2}) = -\frac{2}{3}\chi_{37}(37). \end{aligned}$$

This gives $\Omega_1 = \{\frac{4}{3}\log_p(37)\}$ and $\Omega_2 = \{-\frac{2}{3}\log_p(37)\}$.

Hence $X(K_{\mathfrak{p}})_U$ may be computed by determining the solutions to

$$\begin{aligned} \rho_1(z) &= 2h_{E_2,\mathfrak{p}}(f_2(z)) - h_{E_1,\mathfrak{p}}(f_1(z) + (-3,\sqrt{37})) - h_{E_1,\mathfrak{p}}(f_1(z) + (-3,-\sqrt{37})) \\ &\qquad - 2\alpha_2 h_{E_2}(f_2(z)) + 2\alpha_1(h_{E_1}(f_1(z)) + \log_{E_1}((-3,\sqrt{37}))^2) \in \Omega_1, \\ \rho_2(z) &= 2h_{E_1,\mathfrak{p}}(f_1(z)) - h_{E_2,\mathfrak{p}}(f_2(z) + (4,37)) - h_{E_2,\mathfrak{p}}(f_2(z) + (4,-37)) \\ &\qquad - 2\alpha_1 h_{E_1}(f_1(z)) + 2\alpha_2(h_{E_2}(f_2(z)) + \log_{E_2}((4,37))^2) \in \Omega_2. \end{aligned}$$

Using the two automorphisms of the bielliptic curve, we reduce the number of residue disks considered. In the tables below, for each disk corresponding to the four choices $\overline{(\pm x, \pm y)}$ we give details for the disk corresponding to $\overline{(x,y)}$ with $x, y < \frac{p}{2}$. We fix an identification $X(K_{\mathfrak{p}}) \simeq X(\mathbb{Q}_p)$. Here is data for $X(\mathbb{Q}_{41})_U$:

$X(\mathbb{F}_{41})$	recovered $x(z)$ in residue disk	$z \in X(K)$
$(1,9)$	$1 + 16 \cdot 41 + 23 \cdot 41^2 + 5 \cdot 41^3 + 23 \cdot 41^4 + O(41^5)$	
	$1 + 6 \cdot 41 + 23 \cdot 41^2 + 30 \cdot 41^3 + 14 \cdot 41^4 + O(41^5)$	
$(2,1)$	$2 + O(41^5)$	$(2,1)$
	$2 + 19 \cdot 41 + 36 \cdot 41^2 + 15 \cdot 41^3 + 26 \cdot 41^4 + O(41^5)$	
$(4,18)$		
$(5,12)$	$5 + 25 \cdot 41 + 26 \cdot 41^2 + 26 \cdot 41^3 + 31 \cdot 41^4 + O(41^5)$	
	$5 + 14 \cdot 41 + 12 \cdot 41^3 + 33 \cdot 41^4 + O(41^5)$	
$(6,1)$	$6 + 18 \cdot 41^2 + 31 \cdot 41^3 + 6 \cdot 41^4 + O(41^5)$	
	$6 + 30 \cdot 41 + 35 \cdot 41^2 + 11 \cdot 41^3 + O(41^5)$	
$(7,15)$		
$(9,4)$	$9 + 9 \cdot 41 + 34 \cdot 41^2 + 22 \cdot 41^3 + 24 \cdot 41^4 + O(41^5)$	$(i,4)$
	$9 + 39 \cdot 41 + 14 \cdot 41^2 + 6 \cdot 41^3 + 17 \cdot 41^4 + O(41^5)$	
$(12,5)$		
$(13,19)$	$13 + 10 \cdot 41 + 2 \cdot 41^2 + 15 \cdot 41^3 + 29 \cdot 41^4 + O(41^5)$	
	$13 + 7 \cdot 41 + 8 \cdot 41^2 + 32 \cdot 41^3 + 14 \cdot 41^4 + O(41^5)$	
$(16,1)$	$16 + 13 \cdot 41 + 6 \cdot 41^3 + 18 \cdot 41^4 + O(41^5)$	
	$16 + 12 \cdot 41 + 8 \cdot 41^2 + 9 \cdot 41^3 + 32 \cdot 41^4 + O(41^5)$	
$(17,20)$	$17 + 24 \cdot 41 + 37 \cdot 41^2 + 16 \cdot 41^3 + 28 \cdot 41^4 + O(41^5)$	
	$17 + 19 \cdot 41 + 20 \cdot 41^2 + 7 \cdot 41^3 + 7 \cdot 41^4 + O(41^5)$	
$(18,20)$	$18 + 3 \cdot 41 + 7 \cdot 41^2 + 9 \cdot 41^3 + 38 \cdot 41^4 + O(41^5)$	
	$18 + 41 + 34 \cdot 41^2 + 3 \cdot 41^3 + 32 \cdot 41^4 + O(41^5)$	
$(19,3)$		
$(20,6)$	$20 + 7 \cdot 41 + 40 \cdot 41^2 + 22 \cdot 41^3 + 7 \cdot 41^4 + O(41^5)$	
	$20 + 23 \cdot 41 + 26 \cdot 41^2 + 17 \cdot 41^3 + 22 \cdot 41^4 + O(41^5)$	
∞^+	∞^+	∞^+
$(0,18)$	$32 \cdot 41 + 13 \cdot 41^2 + 16 \cdot 41^3 + 8 \cdot 41^4 + O(41^5)$	
	$9 \cdot 41 + 27 \cdot 41^2 + 24 \cdot 41^3 + 32 \cdot 41^4 + O(41^5)$	

Here we compute $X(\mathbb{Q}_{73})_U$:

$X(\mathbb{F}_{73})$	recovered $x(z)$ in residue disk	$z \in X(K)$ (or $X(\mathbb{Q}(\sqrt{3}))$)
$(2,1)$	$2 + 61 \cdot 73 + 50 \cdot 73^2 + 71 \cdot 73^3 + 56 \cdot 73^4 + O(73^5)$	
	$2 + O(73^5)$	$(2,1)$
$(5,26)$	$5 + 63 \cdot 73 + 4 \cdot 73^2 + 42 \cdot 73^3 + 25 \cdot 73^4 + O(73^5)$	
	$5 + 39 \cdot 73 + 65 \cdot 73^2 + 33 \cdot 73^3 + 60 \cdot 73^4 + O(73^5)$	
$(7,16)$	$7 + 62 \cdot 73 + 31 \cdot 73^2 + 33 \cdot 73^3 + 44 \cdot 73^4 + O(73^5)$	
	$7 + 29 \cdot 73 + 67 \cdot 73^2 + 69 \cdot 73^3 + 17 \cdot 73^4 + O(73^5)$	
$(9,34)$		
$(10,30)$	$10 + 53 \cdot 73 + 35 \cdot 73^2 + 21 \cdot 73^3 + 67 \cdot 73^4 + O(73^5)$	
	$10 + 39 \cdot 73 + 40 \cdot 73^2 + 17 \cdot 73^3 + 59 \cdot 73^4 + O(73^5)$	
$(18,17)$		
$(19,2)$		
$(20,15)$		
$(21,4)$	$21 + 17 \cdot 73 + 70 \cdot 73^2 + 42 \cdot 73^3 + 18 \cdot 73^4 + O(73^5)$	
	$21 + 52 \cdot 73 + 67 \cdot 73^2 + 20 \cdot 73^3 + 27 \cdot 73^4 + O(73^5)$	$(\sqrt{3},4)$
$(23,31)$	$23 + 18 \cdot 73 + 59 \cdot 73^2 + 23 \cdot 73^3 + 2 \cdot 73^4 + O(73^5)$	
	$23 + 70 \cdot 73 + 53 \cdot 73^2 + 21 \cdot 73^3 + 50 \cdot 73^4 + O(73^5)$	
$(25,25)$		
$(27,4)$	$27 + 62 \cdot 73 + 28 \cdot 73^2 + 56 \cdot 73^3 + 58 \cdot 73^4 + O(73^5)$	$(i,4)$
	$27 + 24 \cdot 73 + 30 \cdot 73^2 + 20 \cdot 73^3 + 65 \cdot 73^4 + O(73^5)$	

$X(\mathbb{F}_{73})$	recovered $x(z)$ in residue disk	$z \in X(K)$
$(29, 8)$	$29 + 70 \cdot 73 + 21 \cdot 73^2 + 56 \cdot 73^3 + 5 \cdot 73^4 + O(73^5)$	
	$29 + 34 \cdot 73 + 42 \cdot 73^2 + 19 \cdot 73^3 + 54 \cdot 73^4 + O(73^5)$	
$(30, 20)$		
$(36, 17)$	$36 + 70 \cdot 73 + 19 \cdot 73^2 + 11 \cdot 73^3 + 54 \cdot 73^4 + O(73^5)$	
	$36 + 32 \cdot 73 + 23 \cdot 73^2 + 23 \cdot 73^3 + 28 \cdot 73^4 + O(73^5)$	
∞^+	∞^+	∞^+
$(0, 16)$	$61 \cdot 73 + 63 \cdot 73^2 + 51 \cdot 73^3 + 16 \cdot 73^4 + O(73^5)$	
	$12 \cdot 73 + 9 \cdot 73^2 + 21 \cdot 73^3 + 56 \cdot 73^4 + O(73^5)$	

Here we compute $X(\mathbb{Q}_{101})_U$:

$X(\mathbb{F}_{101})$	recovered $x(z)$ in residue disk	$z \in X(K)$
$(2, 1)$	$2 + O(101^7)$	$(2, 1)$
	$2 + 38 \cdot 101 + 11 \cdot 101^2 + 99 \cdot 101^3 + 26 \cdot 101^4 + O(101^5)$	
$(8, 36)$	$8 + 90 \cdot 101 + 39 \cdot 101^2 + 80 \cdot 101^3 + 70 \cdot 101^4 + O(101^5)$	
	$8 + 40 \cdot 101 + 84 \cdot 101^2 + 74 \cdot 101^3 + 15 \cdot 101^4 + O(101^5)$	
$(10, 4)$	$10 + 5 \cdot 101 + 29 \cdot 101^2 + 66 \cdot 101^3 + 10 \cdot 101^4 + O(101^5)$	$(i, 4)$
	$10 + 49 \cdot 101 + 80 \cdot 101^2 + 74 \cdot 101^3 + 8 \cdot 101^4 + O(101^5)$	
$(12, 7)$	$12 + 12 \cdot 101 + 95 \cdot 101^2 + 55 \cdot 101^3 + 48 \cdot 101^4 + O(101^5)$	
	$12 + 36 \cdot 101 + 62 \cdot 101^2 + 97 \cdot 101^3 + 27 \cdot 101^4 + O(101^5)$	
$(14, 21)$	$14 + 62 \cdot 101 + 62 \cdot 101^2 + 41 \cdot 101^3 + 51 \cdot 101^4 + O(101^5)$	
	$14 + 80 \cdot 101 + 72 \cdot 101^2 + 32 \cdot 101^3 + 75 \cdot 101^4 + O(101^5)$	
$(15, 11)$		
$(17, 18)$	$17 + 65 \cdot 101 + 37 \cdot 101^2 + 80 \cdot 101^3 + 45 \cdot 101^4 + O(101^5)$	
	$17 + 50 \cdot 101 + 61 \cdot 101^2 + 89 \cdot 101^3 + 61 \cdot 101^4 + O(101^5)$	
$(18, 45)$		
$(20, 47)$		
$(22, 3)$	$22 + 59 \cdot 101 + 78 \cdot 101^2 + 43 \cdot 101^3 + 53 \cdot 101^4 + O(101^5)$	
	$22 + 96 \cdot 101 + 29 \cdot 101^2 + 43 \cdot 101^3 + 86 \cdot 101^4 + O(101^5)$	
$(24, 19)$		
$(27, 39)$		
$(28, 37)$	$28 + 30 \cdot 101 + 83 \cdot 101^2 + 5 \cdot 101^3 + 23 \cdot 101^4 + O(101^5)$	
	$28 + 37 \cdot 101 + 24 \cdot 101^2 + 78 \cdot 101^3 + 35 \cdot 101^4 + O(101^5)$	
$(30, 46)$		
$(31, 23)$	$31 + 23 \cdot 101 + 11 \cdot 101^2 + 67 \cdot 101^3 + 39 \cdot 101^4 + O(101^5)$	
	$31 + 29 \cdot 101 + 68 \cdot 101^2 + 29 \cdot 101^3 + 24 \cdot 101^4 + O(101^5)$	
$(34, 45)$	$34 + 91 \cdot 101 + 46 \cdot 101^2 + 28 \cdot 101^3 + 34 \cdot 101^4 + O(101^5)$	
	$34 + 51 \cdot 101 + 73 \cdot 101^2 + 34 \cdot 101^3 + 14 \cdot 101^4 + O(101^5)$	
$(37, 22)$		
$(38, 28)$		
$(39, 46)$	$39 + 76 \cdot 101 + 86 \cdot 101^2 + 18 \cdot 101^3 + 64 \cdot 101^4 + O(101^5)$	
	$39 + 31 \cdot 101 + 43 \cdot 101^2 + 10 \cdot 101^3 + 48 \cdot 101^4 + O(101^5)$	
$(46, 6)$		
$(47, 32)$		
$(48, 27)$	$48 + 43 \cdot 101 + 100 \cdot 101^2 + 47 \cdot 101^3 + 19 \cdot 101^4 + O(101^5)$	
	$48 + 21 \cdot 101 + 38 \cdot 101^2 + 80 \cdot 101^3 + 95 \cdot 101^4 + O(101^5)$	
$(50, 5)$	$50 + 59 \cdot 101 + 19 \cdot 101^2 + 64 \cdot 101^3 + 36 \cdot 101^4 + O(101^5)$	
	$50 + 74 \cdot 101 + 69 \cdot 101^2 + 80 \cdot 101^3 + 21 \cdot 101^4 + O(101^5)$	
∞^+	∞^+	∞^+
$(0, 21)$		

Now using a slightly modified Mordell-Weil sieve on the sets $X(\mathbb{Q}_{41})_U, X(\mathbb{Q}_{73})_U$, and $X(\mathbb{Q}_{101})_U$ as described in Appendix A, we find that

$$X(\mathbb{Q}(i)) = \{(\pm 2 : \pm 1 : 1), (\pm i : \pm 4 : 1), (1 : \pm 1 : 0)\},$$

or in other words,

Theorem 8. *We have* $X_0(37)(\mathbb{Q}(i)) = \{(\pm 2i : \pm 1 : 1), (\pm 1 : \pm 4 : 1), (i : \pm 1 : 0)\}$.

Remark 8. It is perhaps interesting to note that the computation of $X(\mathbb{Q}_{73})_U$ recovered the points $(\pm\sqrt{-3}, \pm 4) \in X_0(37)(\mathbb{Q}(\sqrt{-3}))$ as well.

Acknowledgements

It is a pleasure to thank Minhyong Kim for countless enlightening conversations, Ben Moonen and Michael Stoll for helpful suggestions, Harris Daniels and Álvaro Lozano-Robledo for suggesting that we try the example in §8.4, and Steffen Müller for carrying out the Mordell-Weil sieve computation, as described in the appendix. Part of this paper builds on material in the thesis of the second author; he is very grateful to his examiners Guido Kings and Victor Flynn for several suggestions which have improved the present work and to the EPSRC for supporting this research.

Appendix A. Applying the Mordell-Weil sieve, by J. Steffen Müller

The Mordell-Weil sieve. Let K be a number field with ring of integers $\mathcal{O}_K$ and let X/K be a smooth projective geometrically irreducible curve of genus $g \geq 2$ with Jacobian J/K of rank $r = \mathrm{rk}(J/K)$. Fix an embedding $\iota : X \hookrightarrow J$ defined over K. The Mordell-Weil sieve is a technique for obtaining information about rational points on X by combining information about the image of $X(k_v)$ inside $J(k_v)$ under ι for several primes v of $\mathcal{O}_K$, where k_v is the residue field at v. It was introduced by Scharaschkin [28]; further information on the case $K = \mathbb{Q}$ can be found, for instance, in [8] and [26]. Siksek [31] describes a variant of the Mordell-Weil sieve over number fields which is adapted to work well with his explicit Chabauty method over number fields introduced in loc. cit.

The general idea of the Mordell-Weil sieve is as follows: Suppose for simplicity that there are no nontrivial K-torsion points on J (see [5, Remark 6.1] on how to remove this assumption). Also suppose that we know generators $P_1, \ldots, P_r$ of $J(K)$. Let $M > 1$ be an integer and let $C_M \subset J(K)/MJ(K)$ be a set of residue classes c for which we want to show that the image of $X(K)$ under ι does not map to c under the canonical epimorphism $\pi : J(K) \to J(K)/MJ(K)$. Let S be a finite set of primes of $\mathcal{O}_K$ such that X has good reduction at these primes and consider the commutative diagram

$$\begin{tikzcd}
X(K) \arrow[r, "\pi\circ\iota"] \arrow[d] & J(K)/MJ(K) \arrow[d, "\alpha_S"] \\
\prod_{v\in S} X(k_v) \arrow[r, "\beta_S"'] & \prod_{v\in S} J(k_v)/MJ(k_v)\,.
\end{tikzcd}$$

Here $\alpha_S = (\alpha_v)_{v\in S}$ and $\beta_S = (\beta_v)_{v\in S}$, where α_v is induced by reduction $J(K) \to J(k_v)$ and $\beta_v = \pi_v \circ \iota_v$ is the composition of the canonical epimorphism π_v :

$J(k_v) \to J(k_v)/MJ(k_v)$ and the embedding $\iota_v \colon X(k_v) \hookrightarrow J(k_v)$. To prove that $\pi(\iota(X(K))) \cap C_M = \emptyset$ it suffices to show that

$$\alpha_S(C_M) \cap \operatorname{im}(\beta_S) = \emptyset\,.$$

One can also include information at bad primes and "deep" information, see [8].

Now suppose that $P_1, \ldots, P_r \in J(K)$ generate a subgroup of $J(K)$ of finite index. It is often difficult to deduce generators of $J(K)$ from this. In fact, this is impossible at present if $r > 0$ and $g > 3$. Instead one typically proceeds by first saturating G at small primes and then pretending that $G = J(K)$. The final step is to show that the orders $\#J(k_v)$ are coprime to the index $(J(K) : G)$ for all $v \in S$, which implies that G and $J(K)$ have the same image in $J(k_v)$ for all $v \in S$.

Sometimes, however, it is advantageous to work directly with a subgroup G, which is known to be *not* saturated. In this case, one can use the following strategy, suggested by Besser. Suppose that $v \in S$ is a prime such that $\gcd(\#J(k_v),\ (J(K) : G)) > 1$. Let $q_1, \ldots, q_s$ be the primes dividing this gcd. For $i \in \{1, \ldots, s\}$ we let $\ell_i = v_{q_i}(\#J(k_v))$ and set $n = \prod_{i=1}^s q_i^{\ell_i}$. Then the reduction of $nJ(K) := \{nP : P \in J(K)\}$ is contained in the reduction of G modulo v, so the multiple $n\iota_v(P)$ is contained in the reduction of G modulo v for every $P \in X(k_v)$. Therefore, instead of checking whether $\beta_v(P) \in \alpha_v(C_M)$, we check whether $n\beta_v(P) \in \alpha_v(nC_M)$, where $nC_M = \{nc : c \in C_M\}$.

Quadratic Chabauty and the Mordell-Weil sieve. The p-adic techniques described in the main part of the present text yield congruence conditions for rational points on X. More precisely, they can be used to compute, for good ordinary primes $\mathfrak{p}$ of $\mathcal{O}_K$, a finite subset $X(K_{\mathfrak{p}})_U \subset X(K_{\mathfrak{p}})$ (to finite precision) which contains $X(K)$. After identifying the rational points among $X(K_{\mathfrak{p}})_U$, one is left with the task of showing that the remaining elements do not correspond to a rational point.

It is discussed in [5] how to use the Mordell-Weil sieve for this purpose: Suppose for now that $J(K)_{\mathrm{tors}}$ is trivial and that $P_1, \ldots, P_r$ generate $J(K)$. Using linearity of single Coleman integrals, we can compute, for every point $z \in X(K_{\mathfrak{p}})_U$, a tuple $(\tilde{a}_1, \ldots, \tilde{a}_r) \in \left(\mathbb{Z}/p^N\mathbb{Z}\right)^r$ so that if $\iota(z) = a_1P_1 + \ldots + a_rP_r$ for integers $a_1, \ldots, a_r$, then $a_i \equiv \tilde{a}_i \pmod{p^N}$ for all $i \in \{1, \ldots, r\}$. We can apply the p-adic approximation techniques for several primes $p_1, \ldots, p_s$ to $N_1, \ldots, N_s$ respective digits of precision, and set $M = m \cdot p_1^{N_1} \cdots p_s^{N_s}$, where m is an auxiliary integer. Discarding rational points and using the Chinese Remainder Theorem, we find tuples $(\tilde{a}_1, \ldots, \tilde{a}_r) \in (\mathbb{Z}/M\mathbb{Z})^r$ with the following property: If the set C_M of residue classes in $J(K)/MJ(K)$ corresponding to these tuples does not contain the image of a K-rational point on X, then the known K-rational points are the only ones on X. The Mordell-Weil sieve can be used to prove this.

Suppose now that $G \subset J(K)$ is a subgroup of finite index that is generated by the classes of the differences of all known K-rational points on X. The p-adic methods described in the main part of this paper require the computation of p-adic integrals and the current implementation requires this to take place over $\mathbb{Q}_p$, as opposed to an extension field. Since, for the combination with the Mordell-Weil sieve, we need to do this for several primes of good ordinary reduction, we would like to work directly with the group G, and not with its saturation at small primes. This is possible using the approach introduced at the end of the previous subsection.

See [5, §§6 − 8] for more details about fine-tuning the Mordell-Weil sieve when used in combination with quadratic Chabauty; after some slight modifications the statements given there remain valid in the situation considered here.

Computing $X_0(37)(\mathbb{Q}(i))$. We use the Mordell-Weil sieve, combined with the p-adic methods described in the main text, to compute the set of K-rational points on $X_0(37)$, where $K = \mathbb{Q}(i)$. Recall from Section 8.4 that $X : y^2 = x^6 - 9x^4 + 11x^2 + 37$ is a model for $X_0(37)$ over K and that we have $r = \mathrm{rk}(J/K) = 2$. Note that

$$\mathcal{A} := \{(\pm 2, \pm 1), (\pm i : \pm 4), \infty^{\pm}\} \subset X(K)\,,$$

where the sign of Y/X is ± for $\infty^{\pm}$; we want to show that we actually have equality. We use the point $(2, 1)$ as our base point for the Abel-Jacobi map $\iota : X \hookrightarrow J$.

The subgroup G of $J(K)$ generated by the differences of points in $\mathcal{A}$ can be generated by P, Q and R, where $P = [(-2, -1) - (2, -1)]$ and $Q = [(2, 1) - (i, -4)]$ are non-torsion points, and $R = [(-i, 4) - (i, 4)]$ is a generator of $J(K)_{\mathrm{tors}} \cong \mathbb{Z}/3\mathbb{Z}$. The group G is not saturated at 2; for instance, we have

$$16[\infty^+ - (2, 1)] = P - 10Q - R\,.$$

As discussed in the previous subsection, we nevertheless prefer to work with G directly, without first saturating at 2.

A detailed account of the computation of the sets $X(K_{\mathfrak{p}_i})_U$ for $i = 1, 2, 3$, where $\mathfrak{p}_i$ is a prime of $\mathcal{O}_K$ lying above p_i and $p_1 = 41$, $p_2 = 73$ and $p_3 = 101$, is given in §8.4. After taking out the elements corresponding to the known rational points, we get a set of tuples $(\tilde{a}_1, \tilde{a}_2) \in (\mathbb{Z}/M\mathbb{Z})^2$, where $M = 9 \cdot 41^3 \cdot 73^2 \cdot 101^3$, and a corresponding set $C_M \subset G/MG$ containing 2099520 residue classes.

To this end, we run the Mordell-Weil sieve (modified as above) with S containing primes above $7, 13, 17, 29, 101, 109, 199, 239, 313, 373, 677, 757$. We finally show that no odd prime divides both $\mathrm{lcm}\left(\{\#J(k_v) : v \in S\}\right)$ and $(J(K) : G)$; this proves that we indeed have $X(K) = \{(\pm 2 : \pm 1 : 1), (\pm i : \pm 4 : 1), \infty^{\pm}\}$.

References

[1] *Personal communication with H. Daniels and Á. Lozano-Robledo, 2015.*

[2] J. S. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers, *A non-abelian conjecture of Birch and Swinnerton-Dyer type for hyperbolic curves*, arXiv preprint arXiv:1209.0640 (2012).

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

[4] J.S. Balakrishnan and A. Besser, *Computing local p-adic height pairings on hyperelliptic curves*, IMRN **2012** (2012), no. 11, 2405–2444.

[5] J.S. Balakrishnan, A. Besser, and J.S. Müller, *Computing integral points on hyperelliptic curves using quadratic Chabauty*, Math. Comp., to appear.

[6] ———, *Quadratic Chabauty: p-adic height pairings and integral points on hyperelliptic curves*, J. Reine Angew. Math., to appear.

[7] A. Besser, *The p-adic height pairings of Coleman-Gross and of Nekovář*, Number Theory, CRM Proceedings & Lecture Notes, vol. 36, American Mathematical Society, 2004, pp. 13–25.

[8] N. Bruin and M. Stoll, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306.

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

[10] J. Coates and M. Kim, *Selmer varieties for curves with CM Jacobians*, Kyoto J. Math. **50** (2010), no. 4, 827–852.

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

[12] R.F. Coleman and B.H. Gross, *p-adic heights on curves*, Algebraic Number Theory – in honor of K. Iwasawa, Advanced Studies in Pure Mathematics, vol. 17, 1989, pp. 73–81.

[13] H. Darmon, V. Rotger, and I. Sols, *Iterated integrals, diagonal cycles and rational points on elliptic curves*, Publications mathématiques de Besançon. Algèbre et théorie des nombres, 2012/2, Publ. Math. Besançon Algèbre Théorie Nr., vol. 2012/, Presses Univ. Franche-Comté, Besançon, 2012, pp. 19–46.

[14] P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, Galois groups over $\mathbb{Q}$, Publ. MRSI, no. 16, 1989, pp. 79–297.

[15] P. Deligne and A. B. Goncharov, *Groupes fondamentaux motiviques de Tate mixte*, Ann. Sci. École Norm. Sup. (4) **38** (2005), no. 1, 1–56.

[16] N. Dogra, *Topics in the theory of Selmer varieties*, Oxford Ph.D. thesis (2015).

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

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

[19] A. Grothendieck, P. Deligne, N. Katz, et al., *Groupes de monodromie en géométrie algébrique, séminaire de géométrie algébrique du Bois Marie 1967-1969 (SGA 7 I, II)*, Lecture Notes in Mathematics **288**, 340.

[20] R. H. Kaenders, *The mixed Hodge structure on the fundamental group of a punctured Riemann surface*, Proc. Amer. Math. Soc. **129** (2001), no. 5, 1271–1281.

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

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

[23] M. Kim and A. Tamagawa, *The l-component of the unipotent Albanese map*, Math. Ann. **340** (2008), no. 1, 223–235.

[24] J. Nekovář, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Birkhäuser Boston, Boston, MA, 1993, pp. 127–202.

[25] M. C. Olsson, *Towards non-abelian p-adic Hodge theory in the good reduction case*, Mem. Amer. Math. Soc. **210** (2011), no. 990, vi+157.

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

[27] M. Raynaud, *1-motifs et monodromie géométrique*, Astérisque (1994), no. 223, 295–319, Périodes p-adiques (Bures-sur-Yvette, 1988).

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

[29] A. J. Scholl, *Height pairings and special values of L-functions*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 571–598.

[30] J.-P. Serre, *Galois cohomology*, Springer-Verlag, Berlin, 1997, Translated from the French by Patrick Ion and revised by the author.

[31] S. Siksek, *Explicit Chabauty over number fields*, Algebra Number Theory **7** (2013), no. 4, 765–793.

[32] J. H. Silverman, *Computing heights on elliptic curves*, Math. Comp. **51** (1988), no. 183, 339–358.

[33] W. A. Stein et al., *Sage Mathematics Software (Version 6.7)*, The Sage Development Team, 2015, `http://www.sagemath.org`.

Jennifer S. Balakrishnan, Mathematical Institute, University of Oxford, Woodstock Road, Oxford OX2 6GG, UK

Netan Dogra, Radboud University, P.O. Box 9010, 6500 GL Nijmegen, The Netherlands