ISRAEL JOURNAL OF MATHEMATICS **00** (XXXX), 1–48
DOI: 10.1007/s00000000000000000000000

EXPLICIT QUADRATIC CHABAUTY OVER NUMBER FIELDS

BY

Jennifer S. Balakrishnan

Jennifer S. Balakrishnan, Department of Mathematics and Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA

AND

Amnon Besser

Amnon Besser, Department of Mathematics
Ben-Gurion University of the Negev
P.O.B. 653
Be'er-Sheva 84105
Israel

AND

Francesca Bianchi

Francesca Bianchi, Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence
University of Groningen, Groningen, The Netherlands

AND

J. Steffen Müller

J. Steffen Müller, Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence
University of Groningen, Groningen, The Netherlands

ABSTRACT

We generalize the explicit quadratic Chabauty techniques for integral points on odd degree hyperelliptic curves and for rational points on genus 2 bielliptic curves to arbitrary number fields using restriction of scalars. This is achieved by combining equations coming from Siksek's extension of classical Chabauty with equations defined in terms of p-adic heights attached to independent continuous idele class characters. We give several examples to show the practicality of our methods.

1. Introduction

Let K be a number field and let X/K be a smooth projective curve of genus $g \geq 2$. Then, by Faltings' theorem, the set of rational points $X(K)$ is finite, but at present no general algorithm for the computation of $X(K)$ is known. When the Mordell-Weil rank r of the Jacobian J/K is less than g, the method of Chabauty [16], made effective by Coleman [17, 30], can often be used to compute a finite subset of $X(K_{\mathfrak{p}})$ containing $X(K)$, for any prime $\mathfrak{p}$ of good reduction for X. Combined with other techniques such as the Mordell-Weil sieve [14], this suffices to compute $X(K)$ exactly in many situations. In principle, this method can be used also to compute rational points on elliptic curves, but it only applies to the trivial case $r = 0$.

The method of Chabauty-Coleman relies on the image of the map

$$\log\colon J(K) \otimes K_{\mathfrak{p}} \to H^0(X_{K_{\mathfrak{p}}}, \Omega_1)^{\vee} \tag{1.1}$$

having positive codimension, which is used to write down abelian integrals vanishing at the rational points. Kim [23, 24] proposed to extend this approach to curves with $r \geq g$, by replacing the Jacobian with non-abelian Selmer varieties and the abelian integrals with iterated Coleman integrals. This requires techniques from p-adic Hodge theory and, in general, appears to be quite difficult to use for computations of $X(K)$. However, the simplest non-abelian instance of Kim's program has been made explicit in various circumstances.

For now suppose that $K = \mathbb{Q}$. The basic idea is to use a p-adic height function, which is a quadratic form $h\colon J(\mathbb{Q}) \to \mathbb{Q}_p$. We can decompose h into a sum $h = \sum_v h_v$ of local terms $h_v\colon \mathrm{Div}^0(X_{\mathbb{Q}_v}) \to \mathbb{Q}_p$, where v runs through all prime numbers and $h_v(D) = 0$ for all but finitely many v if $D \in \mathrm{Div}^0(X_{\mathbb{Q}})$

(see [18, 1]). If (1.1) is injective, then we can write down a basis $\mathcal{Q}$ of the quadratic forms on $J(\mathbb{Q}) \otimes \mathbb{Q}_p$ in terms of products of abelian integrals, and we can write h as a linear combination $h = \sum_{q \in \mathcal{Q}} \alpha_q q$ over $\mathbb{Q}_p$. Hence we find

$$\sum_{q \in \mathcal{Q}} \alpha_q q - h_p = \sum_{v \neq p} h_v. \tag{1.2}$$

The left hand side can be pulled back to $X(\mathbb{Q})$ and extended to a locally analytic function on a subset $\mathcal{S}_p \subset X(\mathbb{Q}_p)$. If the pull-back of the right hand side vanishes on $\prod_{v \neq p} \mathcal{S}_v \cap X(\mathbb{Q})$ for some $\mathcal{S}_v \subset X(\mathbb{Q}_v)$ or, more generally, if we can control the image, then we get a locally analytic function on $\mathcal{S}_p$ which takes values on $\prod_v \mathcal{S}_v \cap X(\mathbb{Q})$ in an explicitly computable finite subset of $\mathbb{Q}_p$.

One context in which this idea has been made explicit is the one of integral points on certain hyperelliptic curves. Suppose that X is hyperelliptic, given by a model $y^2 = f(x)$, where $f \in \mathbb{Z}[x]$ is monic of odd degree and has no repeated roots. It is shown in [2] that

(1) the function $\tau(z) := h_p(z - \infty)$ is a Coleman function on $X(\mathbb{Q}_p) \setminus \{\infty\}$, which can be expressed as a double Coleman integral ([2, Theorem 2.2]);
(2) for $v \neq p$, the function $z \mapsto h_v(z - \infty)$ takes values on the v-integral points of $X(\mathbb{Q}_v)$ in an explicitly computable finite set $T_v \subset \mathbb{Q}_p$ ([2, Proposition 3.3]), which is the set $\{0\}$ for almost all v.

These results do not use Kim's approach directly; the first uses p-adic Arakelov theory whereas the second is based on intersection theory on arithmetic surfaces. Let $\mathcal{U} = \operatorname{Spec} \mathbb{Z}[x, y]/(y^2 - f(x))$. Together with the discussion above, it is then easy to deduce

THEOREM 1.1 ([2, Theorem 3.1]): *Suppose that $r = g$ and that the map in* (1.1) *is an isomorphism. Then there exists an explicitly computable finite set $T \subset \mathbb{Q}_p$ and an explicitly computable non-constant Coleman function $\rho\colon \mathcal{U}(\mathbb{Z}_p) \to \mathbb{Q}_p$ such that $\rho(\mathcal{U}(\mathbb{Z})) \subset T$.*

Here and in the following we write that certain p-adic objects are *explicitly computable* if we can provably compute them to any desired p-adic precision; see Remark 6.1.

The first goal of the present article is to extend Theorem 1.1 to general number fields. Fix a prime number p such that X has good reduction at all $\mathfrak{p} \mid p$ and fix a nontrivial continuous idele class character $\chi\colon \mathbb{A}_K^*/K^* \to \mathbb{Q}_p$. This choice induces $\mathbb{Q}_p$-linear maps $t_{\mathfrak{p}}^{\chi}\colon K_{\mathfrak{p}} \to \mathbb{Q}_p$ for all $\mathfrak{p} \mid p$ and a p-adic height pairing h^{χ}

with values in $\mathbb{Q}_p$. This can be decomposed into a sum of local height pairings and the local heights $h_{\mathfrak{p}}^{\chi}$ are of the form $t_{\mathfrak{p}}^{\chi} \circ \tau_{\mathfrak{p}}$ for some Coleman functions $\tau_{\mathfrak{p}}$. Following a similar extension of classical Chabauty due to Siksek [34], we work in $X(K \otimes \mathbb{Q}_p)$ rather than in $X(K_{\mathfrak{p}})$ for a single place $\mathfrak{p} \mid p$, and we consider the composition

$$\log\colon J(K) \otimes \mathbb{Q}_p \to \mathrm{Res}_{K/\mathbb{Q}}(J)(\mathbb{Q}) \otimes \mathbb{Q}_p \to \mathrm{Lie}(\mathrm{Res}_{K/\mathbb{Q}}(J))_{\mathbb{Q}_p}\,. \tag{1.3}$$

Let $\sigma\colon X(K) \hookrightarrow X(K \otimes \mathbb{Q}_p)$ denote the embedding induced by the product of the completion maps $K \hookrightarrow K \otimes \mathbb{Q}_p = \prod_{\mathfrak{p}|p} K_{\mathfrak{p}}$.

THEOREM 1.2: *Suppose that* (1.3) *is injective. Then there exists an explicitly computable finite set $T^{\chi} \subset \mathbb{Q}_p$ and an explicitly computable non-constant locally analytic function $\rho^{\chi}\colon \mathcal{U}(\mathcal{O}_K \otimes \mathbb{Z}_p) \to \mathbb{Q}_p$, both dependent on χ, such that $\rho^{\chi}(\sigma(\mathcal{U}(\mathcal{O}_K))) \subset T^{\chi}$.*

Remark 1.3: One can obtain a slight practical improvement of the theorem by noting that the sets T^{χ} arise, just as in [2], from possible values of the local components h_v^{χ}, and these values are highly dependent for varying χ because they are just the products of a certain intersection pairing with a constant depending on χ_v (see (2.6)). Thus, picking a basis $\{\chi_i\}$ for the space of idele class characters one may prove that the vector valued function $\underline{\rho} = (\rho^{\chi_1}, \ldots)$ takes on $\sigma(\mathcal{U}(\mathcal{O}_K))$ a finite computable set of possible values, which is smaller than the obvious product of the T^{χ_i}. For simplicity we ignore this point here.

See Theorem 4.2 below and its proof. Note that both Theorem 1.1 and Theorem 1.2 hold true when $g = 1$.

The method of [2] was generalized by the first author and Dogra in [6] to rational points on smooth projective curves, satisfying some additional conditions. In contrast to the proof of Theorem 1.1 in [2], this generalization uses Kim's approach directly, relating certain Selmer varieties to p-adic heights as constructed by Nekovář [31], via p-adic Hodge theory.

In a special case, this was turned into an explicit algorithm to compute a finite set of p-adic points containing the rational points of X. In particular, let X be a bielliptic curve of genus 2 over a number field K. Then X admits degree 2 maps φ_1, φ_2 to two elliptic curves E_1 and E_2, respectively.

THEOREM 1.4 ([6, Theorem 1.4]): *Suppose that K is $\mathbb{Q}$ or an imaginary quadratic field in which p splits, and that E_1 and E_2 each have rank 1 over K; let*

$\mathfrak{p} \mid p$. Then there exist a nontrivial continuous idele class character χ, an explicitly computable finite set $T^\chi \subset \mathbb{Q}_p$ and an explicitly computable non-constant Coleman function $\rho^\chi \colon X(K_\mathfrak{p}) \to \mathbb{Q}_p$, such that $\rho^\chi(X(K)) \subset T^\chi$.

This explicit result from [6] can alternatively be proved only from properties of the local heights on the elliptic curves E_i and Theorem 1.1 for each E_i. Therefore, our approach to Theorem 1.2 can be used to extend this elementary proof of Theorem 1.4 to general number fields K.

THEOREM 1.5: *Suppose that* (1.3) *is an injection for each E_i; let $\mathcal{Q}_i$ denote a set of $\mathbb{Q}_p$-valued functions on $E_i(K \otimes \mathbb{Q}_p)$ which restricts to a basis of quadratic forms on $E_i(K)$. For every nontrivial continuous idele class character χ, there exist explicitly computable constants $\alpha^\chi_{q_1}, \beta^\chi_{q_2} \in \mathbb{Q}_p$ and an explicitly computable finite set $T^\chi \subset \mathbb{Q}_p$ such that the function*

$$\rho^\chi \colon \tilde{X}(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$$

defined by

$$\begin{aligned}\rho^\chi(\underline{z}) := &\sum_{\mathfrak{p}\mid p} (h^\chi_\mathfrak{p}(\varphi_1(z_\mathfrak{p})) - h^\chi_\mathfrak{p}(\varphi_2(z_\mathfrak{p})) - 2\chi_\mathfrak{p}(x(z_\mathfrak{p})))\\ &- \sum_{q_1 \in \mathcal{Q}_1} \alpha^\chi_{q_1} q_1(\varphi_1(\underline{z})) + \sum_{q_2 \in \mathcal{Q}_2} \beta^\chi_{q_2} q_2(\varphi_2(\underline{z}))\end{aligned}$$

satisfies

$$\rho^\chi(\sigma(\tilde{X}(K))) \subset T^\chi;$$

here $\tilde{X}(K \otimes \mathbb{Q}_p)$ is the subset of $X(K \otimes \mathbb{Q}_p)$ where ρ^χ is well-defined and $\sigma(\tilde{X}(K))$ is its intersection with $\sigma(X(K))$.

See Theorem 5.2 for a more precise formulation. If we want to use Theorem 1.2 (respectively Theorem 1.5) to actually compute integral (respectively rational) points, then we need enough functions ρ^χ so that their common zero set is finite. In order to achieve this, we require at least $[K : \mathbb{Q}] = \dim \mathrm{Res}_{K/\mathbb{Q}} X$ such functions.

Over the rational numbers, the space of continuous $\mathbb{Q}_p$-valued idele class characters has dimension 1, so up to a scalar factor, Theorem 1.2 (respectively Theorem 1.5) only leads to one locally analytic function which vanishes at the integral (respectively rational) points. In general, the dimension of this space is at least $r_2 + 1$, where r_2 is the number of conjugate pairs of non-real embeddings of K into $\mathbb{C}$ (with equality if Leopoldt's conjecture holds). Hence we can expect

$r_2 + 1$ independent functions. Combining our functions with Siksek's work, we expect that generically, we get a method to compute integral or rational points when

$$r + \mathrm{rk}(\mathcal{O}_K^\times) \leq [K : \mathbb{Q}] \cdot g\,. \tag{1.4}$$

As in Siksek's work, our approach will usually fail if X can be defined over a subfield F of K and if

$$\mathrm{rk}(\mathrm{Jac}(X)/F) + \mathrm{rk}(\mathcal{O}_F^\times) > [F : \mathbb{Q}] \cdot g.$$

It would be interesting to investigate conditions which guarantee that our functions cut out a finite set. See recent work of Dogra [20] and of Hast [22] for discussions of finiteness issues related to ours, but working directly with Kim's approach.

However, the focus of this article is on developing methods for *computing* integral or rational points, not on theoretical conditions guaranteeing finiteness. To illustrate the practicality of our method, we give several examples [1] , combining our techniques with the Mordell-Weil sieve following [3] and [6, Appendix B]. In particular, we compute

- the $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$-integral points on the genus 2 curve defined by $y^2 = x^5 - x^4 + x^3 + x^2 - 2x + 1$, see Example 6.5. Its Jacobian is an optimal quotient of $J_0(188)$ and has rank 2 over $\mathbb{Q}$ and rank 4 over $\mathbb{Q}(\sqrt{-3})$.
- the $\mathbb{Q}(i)$-rational points on the bielliptic modular curve $X_0(91)^+$, see Example 7.1. Note that Theorem 1.4 does not apply here, since the Mordell-Weil rank of the Jacobian of $X_0(91)^+$ over $\mathbb{Q}(i)$ is 4. Its rank over $\mathbb{Q}$ is 2.
- the $\mathbb{Q}(\sqrt{34})$-rational points on the bielliptic curve $X\colon y^2 = x^6 + x^2 + 1$, see Example 7.2. Inspired by a problem in Diophantus' *Arithmetica*, Wetherell determined the rational points on X in his thesis [38]. The rank of the Jacobian of X over $\mathbb{Q}$ is 2 and the rank over $\mathbb{Q}(\sqrt{34})$ is 3.

It is immediate that Siksek's method does not apply to these examples because the respective ranks are too large. They might be amenable to an approach via elliptic curve Chabauty as in [13] (the relevant Galois group in the first example is of order 10), but to our knowledge the only existing implementations of this

[1] We focus on examples over quadratic fields because some of the restrictions of our method are much easier to satisfy for such fields than for a higher degree number field, see Remark 6.6.

method require the base field to be $\mathbb{Q}$. We are also not aware of any method for computing integral points on hyperelliptic curves over number fields that could have succeeded in the first example.

The outline of the paper is as follows: After setting some notation, we give an explicit description of continuous idele class characters and the p-adic heights associated to them in Section 2. We then recall Siksek's extension of Chabauty-Coleman in Section 3. In Section 4 we extend the quadratic Chabauty techniques for integral points on odd degree hyperelliptic curves introduced in [2] and prove Theorem 1.2. Similarly, Section 5 is devoted to an extension of the explicit methods for bielliptic curves of genus 2 from [6] and contains a proof of Theorem 1.5. We then turn to algorithmic details of these methods and give several examples for curves of small genus defined over quadratic fields in Sections 6 and 7. Finally, we discuss how we can provably find the solutions of the power series equations resulting from our methods in Appendix A.

It would be interesting to extend the explicit results in [5] and [7] to general number fields. We have not attempted this, but rather focused on extending those quadratic Chabauty results which do not require p-adic Hodge theory.

Acknowledgements

We thank Keith Conrad for useful correspondence about his notes [19] and for consequently including a power series version of the multivariate Hensel's Lemma, which was needed for this work. We also thank the referee for several helpful remarks. Part of the work described in this article was carried out during a visit of the first and the fourth author to Ben-Gurion University. We would like to thank the Center for Advanced Studies in Mathematics at Ben-Gurion University for their hospitality and support. The first author is supported in part by NSF grant DMS-1702196, the Clare Boothe Luce Professorship (Henry Luce Foundation), and Simons Foundation grant #550023. The third author was supported by EPSRC and by Balliol College through a Balliol Dervorguilla scholarship. The third and fourth author acknowledge support from NWO through a VIDI grant.

1.1. NOTATION. We fix, once and for all, the following notation.

K	a number field,
$\mathcal{O}_K$	the ring of integers of K,
d	the extension degree $[K:\mathbb{Q}]$,
(r_1, r_2)	the signature of K,
r_K	the rank $r_1 + r_2 - 1$ of the unit group $\mathcal{O}_K^*$,
h_K	the class number of K,
K_v	the completion of K at a place v,
p	an odd prime number, unramified in K,
$\mathfrak{p}_1, \dots, \mathfrak{p}_m \subset \mathcal{O}_K$	the primes of $\mathcal{O}_K$ lying above p,
$\sigma_j \colon K \hookrightarrow K_j := K_{\mathfrak{p}_j}$	the completion of K at $\mathfrak{p}_j$,
$\mathcal{O}_j$	the ring of integers of K_j,
$\xi_{\mathfrak{q}}$	a generator of $\mathfrak{q}^{h_K}$ if $\mathfrak{q} \subset K$ is a prime ideal.
$(K \otimes \mathbb{Q}_p)^\vee$	$\prod_{j=1}^m \mathrm{Hom}_{\mathbb{Q}_p}(K_j, \mathbb{Q}_p)$.

2. p-adic heights

2.1. CONTINUOUS IDELE CLASS CHARACTERS. In this section, we recall continuous idele class characters

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

and discuss how to construct them explicitly. These characters are of great importance in Iwasawa theory, as they correspond to $\mathbb{Z}_p$-extensions of K. We shall not use this interpretation; for us, the main application is the explicit construction of p-adic heights in §2.2.

First we note the following:

- For any prime $\mathfrak{q} \nmid p$ we have $\chi_{\mathfrak{q}}(\mathcal{O}_{K_{\mathfrak{q}}}^*) = 0$ because of continuity. So if $\pi_{\mathfrak{q}}$ is a uniformizer in $K_{\mathfrak{q}}$, then $\chi_{\mathfrak{q}}$ is completely determined by $\chi_{\mathfrak{q}}(\pi_{\mathfrak{q}})$. Equivalently, we can use $\chi_{\mathfrak{q}}(q)$, where q is the underlying prime number, or $\chi_{\mathfrak{q}}(\xi_{\mathfrak{q}})$.

- For any $j \in \{1, \dots, m\}$, there is a $\mathbb{Q}_p$-linear map t_j^χ such that we can decompose

$$\begin{array}{ccc} \mathcal{O}_j^* & \xrightarrow{\chi_{\mathfrak{p}_j}} & \mathbb{Q}_p, \\ & {\scriptstyle \log_j} \searrow \quad \nearrow {\scriptstyle t_j^\chi} & \\ & K_j & \end{array} \tag{2.1}$$

because $\chi_{\mathfrak{p}_j}$ takes values in the torsion-free group $(\mathbb{Q}_p, +)$. We call the t_j^χ *trace maps*.

Remark 2.1: If a continuous idele class character χ is ramified at $\mathfrak{p}_j$, that is, if the local character $\chi_{\mathfrak{p}_j}$ does not vanish on $\mathcal{O}_j^*$, then we can extend $\log_j$ to

$$\log_j \colon K_j^* \to K_j \tag{2.2}$$

in such a way that the diagram (2.1) remains commutative.

By the above, a continuous idele class character of K determines an element t^χ of $(K \otimes \mathbb{Q}_p)^\vee$. We now show that the converse also holds.

LEMMA 2.2: *A continuous idele class character $\chi \colon \mathbb{A}_K^*/K^* \to \mathbb{Q}_p$ is uniquely determined by*

$$t^\chi = (t_1^\chi, \dots, t_m^\chi) \in (K \otimes \mathbb{Q}_p)^\vee$$

where the t_j^χ are as in (2.1).

Proof. We first show that t^χ determines $\chi_{\mathfrak{p}_j}$ for $1 \le j \le m$. Indeed, since $\sigma_i(\xi_{\mathfrak{p}_j})$ is a unit in $\mathcal{O}_i$ for $i \neq j$, we have

$$\chi_{\mathfrak{p}_j}(\sigma_j(\xi_{\mathfrak{p}_j})) = -\sum_{i \neq j} \chi_{\mathfrak{p}_i}(\sigma_i(\xi_{\mathfrak{p}_j})) = -\sum_{i \neq j} t_i^\chi(\log_i(\sigma_i(\xi_{\mathfrak{p}_j}))),$$

so $\chi_{\mathfrak{p}_j}$ is completely determined by t^χ.

Now let $\mathfrak{q}$ be a prime not dividing p. Then $\chi_\mathfrak{q}$ is determined by its value on $\xi_\mathfrak{q}$ (embedded into $K_\mathfrak{q}$ via $\sigma_\mathfrak{q}$) and vanishes on $\mathcal{O}_\mathfrak{q}^*$. Hence $\chi_\mathfrak{q}$ is completely determined by t^χ, since

$$\chi_\mathfrak{q}(\sigma_\mathfrak{q}(\xi_\mathfrak{q})) = -\sum_{i=1}^m \chi_{\mathfrak{p}_i}(\sigma_i(\xi_\mathfrak{q})) = -\sum_{i=1}^m t_i^\chi(\log_i(\sigma_i(\xi_\mathfrak{q}))). \qquad \blacksquare$$

More generally, the proof of Lemma 2.2 shows that every $t \in (K \otimes \mathbb{Q}_p)^\vee$ determines a character $\chi\colon \mathbb{A}_K^* \to \mathbb{Q}_p$ via (2.1). We now investigate which $t \in (K \otimes \mathbb{Q}_p)^\vee$ give rise to a continuous idele class character.

LEMMA 2.3: *A homomorphism*

$$t = (t_1, \ldots, t_m) \in (K \otimes \mathbb{Q}_p)^\vee$$

gives rise to a continuous idele class character χ if and only if

$$t_1(\log_1(\sigma_1(\varepsilon))) + \ldots + t_m(\log_m(\sigma_m(\varepsilon))) = 0 \tag{2.3}$$

for all $\varepsilon \in \mathcal{O}_K^*$.

Proof. Suppose that χ is a continuous idele class character, determined by $t = t^\chi \in (K \otimes \mathbb{Q}_p)^\vee$ as in Lemma 2.2. Note that for a unit $\varepsilon \in \mathcal{O}_K^*$ the value $\chi_{\mathfrak{q}}(\varepsilon)$ depends only on $t_{\mathfrak{q}}$ for $\mathfrak{q} \mid p$ and is 0 for all other primes $\mathfrak{q}$. Hence (2.3) must be satisfied.

Conversely, suppose that $t \in (K \otimes \mathbb{Q}_p)^\vee$ and let χ denote the character $\chi\colon \mathbb{A}_K^\times \to \mathbb{Q}_p$ associated to t as in Lemma 2.2. Given $\beta \in K^*$, we need to show that $\chi(\beta) = 0$. Suppose that $(\beta) = \prod \mathfrak{q}_i^{e_i}$ is the decomposition of the fractional ideal (β), for primes $\mathfrak{q}_i$ of K. Then

$$(\beta^{h_K}) = \prod \mathfrak{q}_i^{h_K e_i} = \prod (\xi_{\mathfrak{q}_i})^{e_i} = \left(\prod \xi_{\mathfrak{q}_i}^{e_i}\right),$$

so that $\beta^{h_K} = \prod \xi_{\mathfrak{q}_i}^{e_i} u$ for some unit $u \in \mathcal{O}_K^*$. But since the construction of χ was done so that $\chi(\xi_{\mathfrak{q}}) = 0$ for every $\mathfrak{q}$ and $\chi(u) = 0$ for every unit, we see that $\chi(\beta^{h_K}) = 0$ and hence $\chi(\beta) = 0$. ∎

We deduce the following result:

COROLLARY 2.4: *The continuous idele class characters of K form a $\mathbb{Q}_p$-vector space V_K of dimension $\geq r_2 + 1$. If Leopoldt's conjecture* [26] *holds for K, then we have $\dim_{\mathbb{Q}_p} V_K = r_2 + 1$. In particular, this holds if $K/\mathbb{Q}$ is an abelian extension.*

Proof. The space V_K has dimension precisely $d - r_K = r_2 + 1$ if the equations (2.3) are independent; otherwise its dimension is larger. Leopoldt's conjecture [26] predicts that the p-adic regulator of K is nonzero, which is equivalent to independence of the equations (2.3). Brumer [15] proved Leopoldt's conjecture for abelian $K/\mathbb{Q}$. ∎

Remark 2.5: For our applications it suffices that $\dim_{\mathbb{Q}_p} V_K \geq r_2 + 1$.

Remark 2.6: Corollary 2.4 is classical, see for instance [28], but our proof yields a method for actually determining a basis of V_K, provided we know the class number h_K, fundamental units and a method for computing, for each prime $\mathfrak{q}$ of K, a generator $\xi_{\mathfrak{q}} \in K^*$ of the principal ideal $\mathfrak{q}^{h_K}$.

Example 2.7: If $t = (t_1, \ldots, t_m) \in (K \otimes \mathbb{Q}_p)^\vee$, where $t_j = \mathrm{tr}_{K_j/\mathbb{Q}_p}$, then the equation (2.3) translates into the trivially satisfied equation $\log(N_{K/\mathbb{Q}}(\varepsilon)) = 0$,. This choice of t gives rise to a continuous idele class character χ^{cyc}, which one obtains by composing the usual idele class character over $\mathbb{Q}$ (corresponding to $t_1 = \mathrm{id}_{\mathbb{Q}_p}$) with the norm on the idele class group. We call χ^{cyc} the *cyclotomic* character; it cuts out the cyclotomic $\mathbb{Z}_p$-extension of K. Note that in the case of a totally real number field, if Leopoldt's conjecture holds, then every continuous idele class character is a scalar multiple of χ^{cyc} by Corollary 2.4.

Example 2.8: If p is totally split in K, then the trace maps correspond to scalar multiplication on $K_j \cong \mathbb{Q}_p$, so by Lemma 2.3, the space V_K of continuous idele class characters is isomorphic to the subspace of all $(c_1, \ldots, c_d) \in \mathbb{Q}_p^d$ such that

$$c_1 \log(\sigma_1(\varepsilon)) + \ldots + c_d \log(\sigma_d(\varepsilon)) = 0 \tag{2.4}$$

for all $\varepsilon \in \mathcal{O}_K^*$.

Example 2.9: Let K be imaginary quadratic. Denote by $c\colon \mathbb{A}_K^*/K^* \to \mathbb{A}_K^*/K^*$ the involution induced by complex conjugation. We say that a continuous idele class character $\chi \in V_K$ is *anticyclotomic* if $\chi \circ c = -\chi$. Such characters cut out the anticyclotomic $\mathbb{Z}_p$-extension of K and play an important role in Iwasawa theory. The space V_K of continuous idele class characters is spanned by the cyclotomic character and any nontrivial anticyclotomic character.

If we assume, in addition, that p splits completely in K, then it turns out that $\chi \in V_K$ is anticyclotomic if and only if

$$c_1 + c_2 = 0$$

in the notation of Example 2.8. In this case, we call the character χ^{anti} corresponding to the choice $c_1 = 1$ and $c_2 = -1$ *the anticyclotomic* character. See [9, §1] for an explicit construction of χ^{anti}.

2.2. Coleman-Gross p-adic height pairings. We keep the notation of §2.1. Let X/K be a smooth projective geometrically irreducible curve of genus $g > 0$

with good reduction at $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ and let J denote its Jacobian. The rank $\mathrm{rk}(J/K)$ will be denoted by r. We fix, for every $j \in \{1, \dots, m\}$, a splitting

$$H^1_{\mathrm{dR}}(X/K_j) = H^0(X/K_j, \Omega^1) \oplus W_j \,,$$

such that W_j is isotropic with respect to the cup product pairing. For instance, when $\mathfrak{p}_j$ is ordinary, we can take the unit root subspace with respect to Frobenius.

There are several ways of attaching a p-adic height pairing

$$h^\chi \colon J(K) \times J(K) \to \mathbb{Q}_p \tag{2.5}$$

to a continuous idele class character $\chi \in V_K$, see for instance the work of Schneider [33], Mazur-Tate [29], Coleman-Gross [18] and Nekovář [31]. The pairing h^χ depends on our fixed choices of W_j. If the reduction is ordinary, W_j is the unit root subspace of Frobenius at all j, and χ is ramified above p, the constructions of Schneider, Mazur-Tate, Coleman-Gross and Nekovář are all known to be equivalent. The p-adic height pairing is bilinear and functorial, see [29, §3.4]. It is furthermore symmetric, since we assume all W_j to be isotropic. Denote by $\mathcal{B}$ the space of $\mathbb{Q}_p$-valued bilinear forms on $J(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p$. The function $V_K \to \mathcal{B}$ mapping χ to h^χ is $\mathbb{Q}_p$-linear. The dimension of its image is bounded from above by

$$\min\left\{\dim_{\mathbb{Q}_p} V_K, \frac{r(r+1)}{2}\right\} \geq \min\left\{r_2 + 1, \frac{r(r+1)}{2}\right\} \,,$$

where the inequality is an equality if Leopoldt's conjecture holds for K (see Corollary 2.4). Lower bounds on the dimension are much more difficult. For instance, when the reduction is ordinary, the cyclotomic height attached to the unit root splitting has been conjectured to be non-degenerate by Schneider, but this remains open to date.

As in [2], we follow the approach of Coleman-Gross. Let $\chi = \sum_v \chi_v \in V_K$ be a nontrivial continuous idele class character, with corresponding trace maps $t^\chi = (t_1^\chi, \dots, t_m^\chi) \in (K \otimes \mathbb{Q}_p)^\vee$. Coleman and Gross construct local bi-additive symmetric p-adic height pairings h_v^χ for every non-archimedean place v of K on divisors of degree 0 with disjoint support. Then they define the global p-adic height pairing to be their sum $h^\chi = \sum_v h_v^\chi$; this turns out to respect linear equivalence and hence gives a well-defined symmetric bilinear pairing (2.5).

Following Gross [21, §5], the first- and second-named author removed in [1] the condition that the divisors have to be relatively prime for the local p-adic

height pairings to make sense. For this, p-adic Arakelov theory as developed by the second-named author [10] was used. This extension to arbitrary divisors of degree 0 requires the choice of a tangent vector for every $Q \in X$. If one chooses such vectors consistently for all primes, then one obtains that the sum of the local height pairings is independent of this choice.

We now recall the construction of the local height pairings. First let $\mathfrak{q}$ be a prime of K not dividing p. Then the local height pairing $h_{\mathfrak{q}}^{\chi}$ determined by $\mathfrak{q}$ is defined in terms of intersection theory, as follows: Let D, D' be divisors on $X/K_{\mathfrak{q}}$ of degree 0 and with disjoint support. Fix a proper regular model $\mathcal{X}$ of $X/K_{\mathfrak{q}}$ over $\operatorname{Spec} \mathcal{O}_{K_{\mathfrak{q}}}$ and extend D and D' to $\mathbb{Q}$-divisors $\mathcal{D}, \mathcal{D}'$ on $\mathcal{X}$ which have intersection multiplicity 0 with every vertical divisor. Then we define, as in [18],

$$h_{\mathfrak{q}}^{\chi}(D, D') := \chi_{\mathfrak{q}}(\pi_{\mathfrak{q}})(\mathcal{D} \cdot \mathcal{D}'), \tag{2.6}$$

where $\pi_{\mathfrak{q}}$ is a uniformizer in $K_{\mathfrak{q}}$ and $(\mathcal{D} \cdot \mathcal{D}') \in \mathbb{Q}$ is the intersection multiplicity. A choice of tangent vector makes it possible to define the intersection between two divisors with common component, which can be used to extend the definition (2.6) in a straightforward way, see [21, §6] and [1, Proposition 2.4]. One can define the height pairing at all $\mathfrak{p}_j$ such that χ_j is unramified in an analogous way.

Let $j \in \{1, \dots, m\}$ such that χ_j is ramified and consider the trace map $t_j^{\chi} \colon K_j \to \mathbb{Q}_p$. Suppose that D and D' are divisors of degree 0 on X/K_j. If they have disjoint support, then their local height pairing at $\mathfrak{p}_j$ determined by χ is defined as

$$h_{\mathfrak{p}_j}^{\chi}(D, D') := t_j^{\chi}\left(\int_D \omega_{D'}\right),$$

where $\omega_{D'}$ is a differential of the third kind with residue divisor D', normalized with respect to W_j as in [18, §3]. The integral is a Coleman integral; it depends on the branch $\log_j \colon K_j^* \to K_j$ of the logarithm determined by χ, see Remark 2.1. To extend this to divisors with common support, one uses that

$$h_{\mathfrak{p}_j}^{\chi}(D, D') = t_j^{\chi}(G_D(D'))$$

where G_D is the p-adic Green function on $X_{K_j}(\overline{K_j}) \setminus \operatorname{supp}(D)$ defined in [10]. The choice of a tangent vector at every point of X makes it possible to define $G_D[D'] \in K_j$ for any D' of degree 0, so that $G_D[D'] = G_D(D')$ when D and D' have disjoint support. The general formula for the local height pairing of D

and D' given in [1, Proposition 3.4] is then

$$h^{\chi}_{\mathfrak{p}_j}(D, D') = t^{\chi}_j(G_D[D']).$$

Example 2.10: The local cyclotomic height pairings for D, $D' \in \mathrm{Div}^0(X)$ with disjoint support are given by

$$h^{\mathrm{cyc}}_{\mathfrak{p}_j}(D, D') = \mathrm{tr}_{K_j/\mathbb{Q}_p}\left(\int_{\sigma_j(D')} \omega_{\sigma_j(D)}\right)$$

for $j \in \{1, \dots, m\}$ and

$$h^{\mathrm{cyc}}_{\mathfrak{q}}(D, D') = -\frac{1}{h_K}\log(N(\xi_{\mathfrak{q}})) \cdot (D, D')_{\mathfrak{q}}\,,$$

for primes $\mathfrak{q} \nmid p$.

Example 2.11: We now describe the anticyclotomic height $h^{\mathrm{anti}} := h^{\chi^{\mathrm{anti}}}$ when K is imaginary quadratic, see Example 2.9. In our notation, the local heights $h^{\mathrm{anti}}_{\mathfrak{p}_i}$ are

$$h^{\mathrm{anti}}_{\mathfrak{p}_1}(D, D') = \int_{\sigma_1(D')} \omega_{\sigma_1(D)} \quad \text{and} \quad h^{\mathrm{anti}}_{\mathfrak{p}_2}(D, D') = -\int_{\sigma_2(D')} \omega_{\sigma_2(D)}\,.$$

and the local heights away from p are given by

$$h^{\mathrm{anti}}_{\mathfrak{q}}(D, D') = \frac{1}{h_K}\log\left(\frac{\sigma_2(\xi_{\mathfrak{q}})}{\sigma_1(\xi_{\mathfrak{q}})}\right) \cdot (D, D')_{\mathfrak{q}}\,.$$

Using these formulas, we get a practical method for computing h^{anti}. See [9] for an alternative algorithm.

3. Chabauty over number fields

In this section, we recall a refinement of the method of Chabauty and Coleman over number fields. The idea is that by viewing the K-rational points on X/K as the $\mathbb{Q}$-rational points on the Weil restriction of scalars $\mathrm{Res}_{K/\mathbb{Q}}(X)$ and using $\mathbb{Q}_p$-valued (rather than $K_{\mathfrak{p}}$-valued, for a single $\mathfrak{p} \mid p$) integrals, one can often compute $X(K)$ when the rank of the Jacobian over K is greater than g. This was first suggested by Wetherell at a talk at MSRI in 2000, but he never published the details. Siksek [34] later gave a Chabauty-Coleman method over number fields inspired by Wetherell's work. This allows one to compute $X(K)$ in many cases using a combination of his idea with the Mordell-Weil sieve. See also

Triantafillou's work [36] for a recent application to hyperbolic curves of genus 0 and S-unit equations.

We keep the notation of the previous section. We also assume that there is a rational point $P_0 \in X(K)$, and we let $\iota\colon X \hookrightarrow J := \mathrm{Jac}(X)$ denote the Abel-Jacobi map corresponding to it. We write $X(K \otimes \mathbb{Q}_p)$ for the subset $X(K_1)\times\cdots\times X(K_m)$ of $X(\bar{\mathbb{Q}}_p)^m$. Let $\sigma\colon X(K) \hookrightarrow X(K\otimes\mathbb{Q}_p)$ be the embedding induced by $\sigma_j\colon X(K) \hookrightarrow X(K_j)$.

Siksek's goal is to explicitly construct $d = [K : \mathbb{Q}]$ locally analytic functions

$$\rho_1, \ldots, \rho_d\colon X(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$$

such that

(i) we have $\rho_l(\sigma(X(K))) = 0$ for all $1 \le l \le d$;
(ii) the set

$$B := \{\underline{z} \in X(K \otimes \mathbb{Q}_p) :\ \rho_l(\underline{z}) = 0 \ \text{ for all } \ 1 \le l \le d\}$$

is finite.

We need (at least) d such functions to cut out a finite subset of $X(K \otimes \mathbb{Q}_p)$ for reasons of dimension.

With a view toward explicit computations and generalizations, we now discuss how the functions ρ_l can be constructed in terms of Coleman integrals. Let $j \in \{1, \ldots, m\}$ and let $z_j \in X(K_j)$. If ω is a holomorphic 1-form on X/K_j, then the integral $\int_{P_0}^{z_j} \omega$ is an element of K_j. We can compose it with a trace map $t_j \in \mathrm{Hom}_{\mathbb{Q}_p}(K_j, \mathbb{Q}_p)$ to obtain a locally analytic function

$$X(K_j) \to \mathbb{Q}_p\,; \ \ z_j \mapsto t_j\left(\int_{P_0}^{z_j} \omega\right).$$

For every $j \in \{1, \ldots, m\}$, we fix a basis $(t_{j,1}, \ldots, t_{j,d_j})$ of $\mathrm{Hom}_{\mathbb{Q}_p}(K_j, \mathbb{Q}_p)$, where $d_j = [K_j : \mathbb{Q}_p]$; we also fix a basis $(\omega_0, \ldots, \omega_{g-1})$ of $H^0(X/K, \Omega^1)$.

Definition 3.1: Let $i \in \{0, \ldots, g-1\}$, let $j \in \{1, \ldots, m\}$ and let $k \in \{1, \ldots, d_j\}$. We define

$$f_i^{(j,k)}(\underline{z}) := t_{j,k}\left(\int_{P_0}^{z_j} \sigma_j(\omega_i)\right) \in \mathbb{Q}_p$$

for $\underline{z} = (z_1, \ldots, z_m) \in X(K \otimes \mathbb{Q}_p)$. For $Q \in X(K)$, we set

$$f_i^{(j,k)}(Q) := f_i^{(j,k)}(\sigma(Q))\,.$$

We fix an ordering of the $f_i^{(j,k)}$ and label their restrictions to $X(K)$ as follows:

$$f_0, \dots, f_{dg-1} \colon X(K) \to \mathbb{Q}_p \,.$$

Extending these functions to Galois-equivariant functions $f_i \colon X(K \otimes \bar{\mathbb{Q}}_p) \to \bar{\mathbb{Q}}_p$ in the obvious way and then to $J(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p$ by additivity, we obtain $\mathbb{Q}_p$-valued linear functionals

$$f_0, \dots, f_{dg-1} \colon J(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p \to \mathbb{Q}_p \,. \tag{3.1}$$

We fix some more notation: Let $(J(K) \otimes \mathbb{Q}_p)^\vee = \mathrm{Hom}_{\mathbb{Q}_p}(J(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p, \mathbb{Q}_p)$, let

$$U = \mathrm{Span}_{\mathbb{Q}_p}(f_0, \dots, f_{dg-1}) \subset (J(K) \otimes \mathbb{Q}_p)^\vee \,,$$

and let

$$n = dg - \dim_{\mathbb{Q}_p}(U)$$

denote the maximal number of independent relations between the f_i.

Suppose that

$$n \geq d \tag{3.2}$$

and fix a set of d independent relations in U. These relations, pulled back via the Abel-Jacobi map ι, extend to explicitly computable locally analytic functions

$$\rho_1, \dots, \rho_d \colon X(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$$

such that

$$\rho_l(\sigma(X(K))) = 0$$

for all $l = 1, \dots, d$. Then, provided the common zero set B of $\rho_1, \dots, \rho_d$ is finite, we can explicitly determine $X(K)$, by first computing B (to suitable p-adic precision) and then identifying $\sigma(X(K)) \subset B$ using the Mordell-Weil sieve, if $g \geq 2$. See [34] for details.

As mentioned previously, over $\mathbb{Q}$ the condition $r < g$ is a sufficient criterion for the method of Chabauty-Coleman to work. But when $K \neq \mathbb{Q}$, it is much more delicate to predict whether the zero set B is finite, as we have to deal with systems of multivariate power series (see also Appendix A). Since $\dim_{\mathbb{Q}_p}(J(K) \otimes \mathbb{Q}_p)^\vee = r$, we have $n \geq dg - r$. Therefore one might guess that for finiteness of B it should be sufficient that

$$r \leq d(g-1). \tag{3.3}$$

This is not the case, as one can find examples where B is infinite because X can be defined over some subfield F of K over which $\mathrm{rk}(J/F) > [F\colon \mathbb{Q}](g-1)$; see [34] for a discussion. Siksek asks whether B is finite whenever

$$\mathrm{rk}(\mathrm{Jac}(Y)/F) \leq [F : \mathbb{Q}](g-1) \tag{3.4}$$

for all subfields F and for every smooth projective curve Y/F such that $Y \times_F K \cong_K X$. This was shown to be false by Dogra [20]; he constructs a hyperelliptic genus 3 curve X with minimal field of definition $K := \mathbb{Q}(\sqrt{33})$ covering a genus 2 curve $X_0/\mathbb{Q}$ whose Jacobian J_0 satisfies $\mathrm{rk}(J_0/\mathbb{Q}) = 2$. This X satisfies the condition (3.4), but the functions ρ_l vanish in the preimage of $X_0(\mathbb{Q}_p)$ in $X(K \otimes \mathbb{Q}_p)$, so B is infinite. Dogra also shows that B is finite whenever $r \leq d(g-1)$ and $\mathrm{Hom}(J(K)_{\bar{\mathbb{Q}},\sigma_1}, J(K)_{\bar{\mathbb{Q}},\sigma_2})$ is trivial for any two distinct embeddings $\sigma_1, \sigma_2\colon K \hookrightarrow \bar{\mathbb{Q}}$, i.e. whenever J and its conjugates do not share an isogeny component over $\bar{\mathbb{Q}}$.

When $r > d(g-1)$, then the method of Siksek is in general not applicable. In the following two sections, we discuss how to extend it using p-adic heights.

4. Quadratic Chabauty for integral points on odd degree hyperelliptic curves over number fields

Suppose that X/K is hyperelliptic, given by an equation $X\colon y^2 = f(x)$, where $f \in \mathcal{O}_K[x]$ is a separable polynomial of degree $2g+1 \geq 3$ which does not reduce to a square modulo any prime. Let ι be the Abel-Jacobi map with respect to $\infty = (1:0:0) \in X(K)$. We denote by $\mathcal{U}$ the affine scheme $\mathrm{Spec}\, \mathcal{O}_K[x,y]/(y^2 - f(x))$.

For the case $K = \mathbb{Q}$, the first, second and fourth author showed in [2, 3] how to compute $\mathcal{U}(\mathbb{Z}) \subset X(\mathbb{Q})$ when $r = g$ using a locally analytic function constructed in terms of the cyclotomic p-adic height. We now show how to generalize this idea to arbitrary number fields. Generically, we expect our method to work when

$$r + r_K \leq dg\,. \tag{4.1}$$

More precisely, we try to construct explicitly computable functions

$$\rho_1, \ldots, \rho_d\colon \mathcal{U}(\mathcal{O}_K \otimes \mathbb{Z}_p) \to \mathbb{Q}_p$$

which are locally analytic on p-integral points and explicitly computable finite subsets $T^{(1)}, \ldots, T^{(d)} \subset \mathbb{Q}_p$ such that

(i) we have $\rho_l(\sigma(\mathcal{U}(\mathcal{O}_K))) \subset T^{(l)}$ for all $1 \le l \le d$;
(ii) the set

$$B := \left\{ \underline{z} \in \mathcal{U}(\mathcal{O}_K \otimes \mathbb{Z}_p) : \ \rho_l(\underline{z}) \in T^{(l)} \ \text{ for all } \ 1 \le l \le d \right\}$$

is finite.

As in Section 3, let U be the $\mathbb{Q}_p$-span of the linear functionals $f_1, \dots, f_{dg-1}$: $J(K) \otimes \mathbb{Q}_p \to \mathbb{Q}_p$. We show how to construct such functions $\rho_1, \dots, \rho_d$ when (4.1) and the following condition are satisfied:

Condition 4.1: $U = (J(K) \otimes \mathbb{Q}_p)^\vee$.

The finiteness of B turns out to be much more difficult to prove. If Condition 4.1 is satisfied, then we have $\dim_{\mathbb{Q}_p} U = r$ and hence

$$n + r = dg\,; \tag{4.2}$$

in particular, we need to have $r \le dg$ for Condition 4.1 to hold, and if $r = dg$, then Condition 4.1 is equivalent to surjectivity of the map in (1.3). We order the f_i so that $(f_0, \dots, f_{r-1})$ is a basis of $(J(K) \otimes \mathbb{Q}_p)^\vee$.

In §2.2 we discussed how a continuous idele class character χ gives rise to a p-adic height pairing h^χ. So let $\chi \in V_K$ be nontrivial with associated trace maps $t^\chi = (t_1^\chi, \dots, t_m^\chi) \in (K \otimes \mathbb{Q}_p)^\vee$. We choose the basis $(\omega_0, \dots, \omega_{g-1})$ of $H^0(X/K, \Omega^1)$ given by $\omega_k := x^k dx/2y$ and we denote the differentials on X/K_j obtained via σ_j by ω_k as well. In order to define the local height pairings for arbitrary divisors of degree 0, we fix a choice of tangent vector for every point $Q \in X$ as in [2]. Namely, we take the tangent vector induced by ω_0 by duality for all affine points. For the point ∞, we pick the dual of the value of ω_{g-1} at ∞. We denote by $(\bar\omega_0, \dots, \bar\omega_{g-1})$ the unique basis of W_j which is dual to $(\omega_0, \dots, \omega_{g-1})$ with respect to the cup product pairing. For $z \in X(K_j) \setminus \{\infty\}$ we define the double Coleman integral

$$\tau_j(z) = -2 \int_{b_0}^{z} \sum_{i=0}^{g-1} \omega_i \bar\omega_i \in K_j\,,$$

where b_0 is the tangential basepoint determined by our choice of tangent vector at ∞. Note that τ_j depends on the branch $\log_j : K_j^* \to K_j$ determined by χ. This is not reflected in our notation, since we are mostly interested in the restriction of τ_j to $\mathcal{U}(\mathcal{O}_j)$.

THEOREM 4.2: *Suppose that Condition 4.1 is satisfied. Then there are explicitly computable constants $\alpha_{ij}^{\chi} \in \mathbb{Q}_p$ and an explicitly computable finite set $T^{\chi} \subset \mathbb{Q}_p$ such that the function*

$$\rho^{\chi} \colon \mathcal{U}(\mathcal{O}_K \otimes \mathbb{Z}_p) \to \mathbb{Q}_p$$

defined by

$$\rho^{\chi}(\underline{z}) := \sum_{j=1}^{m} t_j^{\chi}(\tau_j(z_j)) - \sum_{0 \le i \le j \le r-1} \alpha_{ij}^{\chi} f_i(\underline{z}) f_j(\underline{z}) \,,$$

satisfies

$$\rho^{\chi}(\sigma(\mathcal{U}(\mathcal{O}_K))) \subset T^{\chi} \,.$$

Proof. Setting $g_{ij}(P,Q) := \frac{1}{2}(f_i(P)f_j(Q) + f_j(P)f_i(Q))$, we obtain a basis $(g_{ij} \colon 0 \le i \le j \le r-1)$ of the space of $\mathbb{Q}_p$-valued bilinear forms on $J(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p$, since the latter has dimension $r(r+1)/2$ and the g_{ij} are independent. Because h^{χ} is a $\mathbb{Q}_p$-valued bilinear form on $J(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p$, we can find constants $\alpha_{ij}^{\chi} \in \mathbb{Q}_p$ such that

$$h^{\chi} = \sum_{0 \le i \le j \le r-1} \alpha_{ij}^{\chi} g_{ij} \,. \tag{4.3}$$

If $\mathfrak{q}$ is a prime of K and $z \in X(K_{\mathfrak{q}}) \setminus \{\infty\}$, we write

$$h_{\mathfrak{q}}^{\chi}(z) := h_{\mathfrak{q}}^{\chi}((z) - (\infty), (z) - (\infty)) \,,$$

where the right hand side is determined by our choice of tangent vectors. Then, we have

$$h_{\mathfrak{p}_j}^{\chi}(z) = t_j^{\chi}(\tau_j(z)) \tag{4.4}$$

for $z \in X(K_j) \setminus \{\infty\}$ by [2, Theorem 2.2].

Now let $\mathfrak{q}$ be a prime of K not dividing p. Let $\mathcal{X}$ be a desingularization in the strong sense of the Zariski closure of X in weighted projective space $\mathbb{P}_{\mathcal{O}_{K_{\mathfrak{q}}}}(1, g+1, 1)$. Let $z \in X(K_{\mathfrak{q}})$ and extend the divisor $(z)-(\infty)$ to a $\mathbb{Q}$-divisor $\mathcal{D}_z$ on $\mathcal{X}$ such that $\mathcal{D}_z$ has intersection multiplicity 0 with all vertical divisors on $\mathcal{X}$. Then we have $h_{\mathfrak{q}}^{\chi}(z) = \chi_{\mathfrak{q}}(\pi_{\mathfrak{q}})\mathcal{D}_z^2$. The proof of [2, Proposition 3.3] (which treats the special case $K = \mathbb{Q}$ and $h = h^{\mathrm{cyc}}$) shows that if $z \in \mathcal{U}(\mathcal{O}_{K_{\mathfrak{q}}})$, then the value of $h_{\mathfrak{q}}^{\chi}(z)$ depends only on the irreducible component Γ_z of the special fiber of $\mathcal{X}$ that z reduces to and is explicitly computable from Γ_z. Furthermore, this value is 0 if z reduces to a smooth point modulo $\mathfrak{q}$ and if $\mathrm{ord}_{\mathfrak{q}}(f_{2g+1}) = 0$, where f_{2g+1} is the leading coefficient of f.

For $Q \in \mathcal{U}(\mathcal{O}_K)$ we conclude that

$$\begin{aligned}\rho^\chi(\sigma(Q)) &= \sum_{j=1}^{m} t_j^\chi(\tau_j(\sigma_j(Q))) - \sum_{0\le i\le j\le r-1} \alpha_{ij}^\chi f_i(Q) f_j(Q) \\ &= \sum_{j=1}^{m} h_{\mathfrak{p}_j}^\chi(Q) - h^\chi((Q)-(\infty),(Q)-(\infty)) \\ &= -\sum_{\mathfrak{q}\nmid p} h_{\mathfrak{q}}^\chi(Q)\end{aligned}$$

indeed takes values in an explicitly computable finite set. ∎

Remark 4.3: Theorem 1.2 follows at once from Theorem 4.2.

Remark 4.4: Let us make the following remark concerning the dependence on the branch of the logarithm. The function τ_j is a double Coleman integral. On residue discs where the integrands have no singularities, it is rigid analytic. However, there will be a finite number of residue discs where τ_j will be more complicated. Near a point where one of the integrands has a singularity, there will be a disc D where the function is given by a polynomial of degree at most 2 in $\log(z)$ with coefficients which are rigid analytic functions on D, with z a uniformizing parameter on D sending the singular point to 0 (these discs could in general be smaller than residue discs if the integrands have several singular points in the same residue disc). We note that in fact, due to their source in Green functions, the τ_j are simpler: On such a disc D they will be of the form $\varphi(z) + c\log(z)$, where φ is rigid analytic and c is a constant. Solving even a simple polynomial equation involving both z and $\log(z)$ is far more complicated, if possible at all, than an analytic equation. This is one reason why certain quadratic Chabauty techniques do not find all rational points but only those that avoid certain residue disks. On the other hand, whenever one stays away from these problematic disks the equation does not depend on the chosen branch of the logarithm. The dependence on the branch only appears when trying to compute the global height pairing.

Remark 4.5: Our assumption that f does not reduce to a square modulo any prime is only required to apply [2, Proposition 3.3]. Of course, we can always scale the variables to make f monic, and then it is automatically satisfied.

We can expect at most $\min(\dim_{\mathbb{Q}_p} V_K, \frac{r(r+1)}{2})$ independent height pairings h^χ. Recall that $\dim_{\mathbb{Q}_p} V_K \geq r_2+1$ (with equality if Leopoldt's conjecture holds for K). The set of all $\underline{z} \in \mathcal{U}(\mathcal{O}_K \otimes \mathbb{Q}_p)$ such that $\rho^\chi(\underline{z}) \in T^\chi$ holds for the corresponding functions can only be finite when $r_2 + 1 = d$, i.e. when $K = \mathbb{Q}$ or K is an imaginary quadratic field.

In general, we need at least $d - (r_2 + 1) = r_K$ additional functions $\mathcal{U}(\mathcal{O}_K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$ to cut out a finite subset of $\mathcal{U}(\mathcal{O}_K \otimes \mathbb{Q}_p)$ containing $\sigma(\mathcal{U}(\mathcal{O}_K))$. It is natural to take these from the relations among the functions f_i, as in §3. Therefore we need the maximal number n of independent relations to be at least r_K. Because of (4.2), this means that we want $r_K + r \leq dg$, which is precisely (4.1), to hold.

Let $\rho_1, \ldots, \rho_{r_2+1} \colon \mathcal{U}(\mathcal{O}_K \otimes \mathbb{Z}_p) \to \mathbb{Q}_p$ be functions coming from p-adic heights associated to nontrivial continuous idele class characters $\chi \in V_K$ as above, with corresponding finite sets $T^{(k)} \subset \mathbb{Q}_p$. Assuming that (4.1) holds, we obtain functions $\rho_{r_2+2}, \ldots, \rho_d \colon X(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$ which vanish in $\sigma(X(K))$ from independent relations among the f_i as in Section 3. Set $T^{(l)} = \{0\} \subset \mathbb{Q}_p$ for $r_2 + 2 \leq l \leq d$. Then

$$B := \{\underline{z} \in \mathcal{U}(\mathcal{O}_K \otimes \mathbb{Z}_p) : \ \rho_l(\underline{z}) \in T^{(l)} \ \text{ for all } \ 1 \leq l \leq d\}$$

contains $\sigma(\mathcal{U}(\mathcal{O}_K))$ and is explicitly computable. Thus, we get a method to p-adically approximate $\mathcal{U}(\mathcal{O}_K)$ in practice whenever B is finite.

In analogy with the results of Dogra [20], we raise the following

Question 4.6: Suppose that Condition 4.1 is satisfied and that we have

$$\operatorname{rk}(\operatorname{Jac}(Y)/F) + r_F \leq [F : \mathbb{Q}] \cdot g \tag{4.5}$$

for every subfield $F \subset K$ and for every smooth projective curve Y/F such that $Y \times_F K \cong_K X$. Is it true that B can only be infinite for geometric reasons?

Remark 4.7: Siksek's method always succeeds in constructing a set B containing $X(K)$, provided that $r \leq d(g-1)$. As was explained at the end of Section 3, this assumption on the rank is however not sufficient to guarantee finiteness of B. On the contrary, even definability of a set B is not ensured by (4.5). If $K = \mathbb{Q}$ and (4.5) holds, then either Condition 4.1 is satisfied or classical Chabauty is applicable (or both). For general K, it is instead possible to construct examples where (4.5) holds, but we are neither in the situation of Condition 4.1 nor in Siksek's. Indeed, let X be a genus 2 hyperelliptic curve over an imaginary

quadratic field K. Suppose that X does not not descend to $\mathbb{Q}$ and that its Jacobian splits as the product of two elliptic curves E_1 and E_2. If $\mathrm{rk}(E_1/K) = 3$ and $\mathrm{rk}(E_2/K) = 1$ and E_1 cannot be defined over $\mathbb{Q}$, then we expect that $\dim_{\mathbb{Q}_p}(U) = 3$. For example, consider the hyperelliptic curve over $\mathbb{Q}(i)$

$$X\colon y^2 = (14i-6)x^5 + (-3i+5)x^4 + 20ix^3 - 15x^2 - 6ix + 1.$$

Its Jacobian splits as the product of

$$E_1\colon y^2 = x^3 + (-3i-10)x^2 + (54i+72)$$
$$E_2\colon y^2 = x^3 + (-3i-10)x + (-3i-9)$$

of respective ranks 3 and 1. Let $P = (2, -3i-7)$, $Q = (7i+1, -6i+22) \in E_1(\mathbb{Q}(i))$ and let ω_0 be an invariant differential on E_1. Then, choosing $p = 13$, we get $(\int_\infty^{\sigma_1(P)} \omega_0)(\int_\infty^{\sigma_2(Q)} \omega_0) \neq (\int_\infty^{\sigma_2(P)} \omega_0)(\int_\infty^{\sigma_1(Q)} \omega_0)$, so (1.3) is surjective for E_1. Thus the dimension of U for J is 3.

When $K = \mathbb{Q}$ it is conjectured by Waldschmidt that it is sufficient that J is simple of Mordell-Weil rank at most g for Condition 4.1 to hold (see [37]). The situation is expected to be more complicated for higher degree number fields, see [32, Remark 6.4].

Remark 4.8: The equations attached by Theorem 4.2 to dependent height pairings can sometimes be independent. To see this, consider an elliptic curve E over $\mathbb{Q}$ of rank 0. Then all global height pairings are identically zero on $E(\mathbb{Q})$; nevertheless, the cyclotomic height (with respect to a choice of splitting) gives an equation whose zero set is, in general, not identical to $E(\mathbb{Q}_p)_{\mathrm{tors}}$, i.e. to the zero set of the p-adic logarithm on $E(\mathbb{Q}_p)$. See [4, 11] for computational evidence and relations with a conjecture of Kim on effectiveness.

This phenomenon in rank 0 also provides us with an example of how different choices of splittings of the de Rham cohomology can lead to linearly independent equations. Indeed, recall from Section 2.2 that the cyclotomic p-adic height pairing on $E/\mathbb{Q}$ depends on a choice of subspace $W \subset H^1_{\mathrm{dR}}(E/\mathbb{Q}_p)$, complementary to the space of holomorphic form and isotropic with respect to the cup product pairing. The latter condition is automatically satisfied in the elliptic curve case and we see that the local height at p is then given by

$$h_p^{(W)}(z) = 2D_2(z) + c_W \left(\int_\infty^z \omega_0 \right)^2,$$

where $D_2(z)$ is the dilogarithm (a double Coleman integral), $c_W \in \mathbb{Q}_p$ depends on W, and $\int_\infty^z \omega_0$ is the p-adic logarithm. Choosing two different subspaces W_1, W_2 we then get $h_p^{(W_1)}(z) = 0 = h_p^{(W_2)}(z)$ if and only if $h_p^{(W)}(z) = 0 = \int_\infty^z \omega_0$ for any W. Thus, for all $z \in \mathcal{U}(\mathbb{Z}_p)$ such that $h_p^{(W_1)}(z) = 0$ but $\int_\infty^z \omega_0 \neq 0$, we have $h_p^{(W_2)}(z) \neq 0$; examples of such z can be found in the computations for [4, 11].

In contrast, when $r = g$, different splittings will not result in independent equations, see [7, Remark 3.12].

5. Quadratic Chabauty for rational points on bielliptic curves over number fields

Let X/K be the genus 2 bielliptic curve

$$y^2 = a_6x^6 + a_4x^4 + a_2x^2 + a_0 \qquad (a_i \in \mathcal{O}_K)$$

which has degree 2 maps φ_1, φ_2 to two elliptic curves:

$$\begin{aligned} E_1 &: y^2 = x^3 + a_4x^2 + a_2a_6x + a_0a_6^2, & \varphi_1(x,y) &= (a_6x^2, a_6y) \\ E_2 &: y^2 = x^3 + a_2x^2 + a_4a_0x + a_6a_0^2, & \varphi_2(x,y) &= (a_0x^{-2}, a_0yx^{-3}). \end{aligned} \tag{5.1}$$

When K is either $\mathbb{Q}$ or an imaginary quadratic field and both E_1 and E_2 have Mordell-Weil rank 1 over K, it was shown in [6] that a suitable choice of continuous idele class character of K gives rise to a locally analytic function on $X(K_j)$ which vanishes on $X(K)$, provided that $K_j \simeq \mathbb{Q}_p$ and X has good reduction at each $\mathfrak{p}_j$.

In this section, we combine the ideas of [6] with those of Section 4 to approximate $X(K)$ inside $X(K \otimes \mathbb{Q}_p)$ when K is an arbitrary number field and p is a prime, unramified in K, above which the given model for X has everywhere good reduction. As in Sections 3 and 4, we do not investigate here whether the systems of d equations in d variables that we define have finitely many zeros.

For ease of exposition, and since we assumed in Section 3 that X possesses a K-rational point, we now restrict to curves X for which the defining polynomial is monic, i.e. for the rest of this section we take

$$a_6 = 1.$$

Then X can be embedded into its Jacobian J via the Abel-Jacobi map with respect to one of $\infty^{\pm} = (1 : \pm 1 : 0) \in X(K)$. The proof of the main theorem (Theorem 5.2 below) can easily be adapted to allow for any $a_6 \in \mathcal{O}_K$.

For the construction, it is sufficient to work under Assumption 5.1 below and

$$\mathrm{rk}(J/K) + r_K \leq dg = 2d. \tag{5.2}$$

For each $A \in \{J, E_1, E_2\}$, let

$$f_0^A, \ldots, f_{dg(A)-1}^A \colon A(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p \to \mathbb{Q}_p$$

be the $\mathbb{Q}_p$-valued linear functionals of Section 3 on A (here by $g(J)$ we mean the genus of X) and define, for $0 \leq i \leq j \leq dg(A) - 1$, the bilinear form g_{ij}^A by

$$g_{ij}^A(P, Q) = \frac{1}{2}(f_i^A(P) f_j^A(Q) + f_j^A(Q) f_i^A(P)), \quad \text{for } P, Q \in A(K) \otimes \mathbb{Q}_p.$$

Let χ be a nontrivial continuous idele class character of K and for each $k \in \{1, 2\}$ let h^{χ, E_k} be the global p-adic height pairing of Section 2 on E_k with respect to χ. Similarly, for a prime $\mathfrak{q}$ of K, denote by $h_{\mathfrak{q}}^{\chi, E_k}$ the local height at $\mathfrak{q}$. We work under the following assumption:

Assumption 5.1: Condition 4.1 holds for each of E_1 and E_2. For this, it is necessary that

$$\mathrm{rk}(\tilde{E}_k/F) \leq [F : \mathbb{Q}] \quad \text{for } k \in \{1, 2\}$$

for all subfields F of K and for all $\tilde{E}_k/F$ isomorphic to E_k over K.

Possibly after reordering the $g_{ij}^{E_k}$, we can then find

$$\alpha_{ij}^{\chi, E_k}, \quad 0 \leq i \leq j \leq \mathrm{rk}(E_k/K) - 1,$$

such that

$$h^{\chi, E_k} = \sum_{i,j} \alpha_{ij}^{\chi, E_k} g_{ij}^{E_k}. \tag{5.3}$$

By abuse of notation, we also write $h^{\chi, E_k}(P)$ for $h^{\chi, E_k}(P, P)$ and similarly for $g_{ij}^{E_k}$. Embed $E_k(K)$ in $E_k(K \otimes \mathbb{Q}_p)$ via σ. Note that, while h^{χ, E_k} only makes sense as a function of $E_k(K)$, each $g_{ij}^{E_k}$ is the restriction of a function on $E_k(K \otimes \mathbb{Q}_p)$, which we also denote by $g_{ij}^{E_k}$. Furthermore, if $\underline{z} \in E_k(K \otimes \mathbb{Q}_p)$, we write $h_{\mathfrak{p}_j}^{\chi, E_k}(\underline{z})$ for $h_{\mathfrak{p}_j}^{\chi, E_k}(z_j)$, which is locally analytic away from the disk of the point at infinity ∞_{E_k}.

Let $Q_1 = (0, \sqrt{a_0}) \in E_1(K(\sqrt{a_0}))$, $Q_2 = (0, a_0) \in E_2(K)$ and, for a point $P \in X(K_j)$, denote by $]P[$ the residue disk centered at P in $X(K_j)$. For $k = 1, 2$, define

$$X^{(k)}(K \otimes \mathbb{Q}_p) = \prod_{j=1}^{m} \left(X(K_j) \setminus \left( ]\sigma_j(\varphi_k^{-1}(Q_k))[\cup]\sigma_j(\varphi_k^{-1}(-Q_k))[\right) \right)$$
$$X^{(k)}(K) = \sigma(X(K)) \cap X^{(k)}(K \otimes \mathbb{Q}_p),$$

where, if Q_1 is not defined over K, we let $\sigma_j(\varphi_1^{-1}(\pm Q_1)) = (0, \pm\sqrt{\sigma_j(a_0)})$ if $a_0 \in \mathcal{O}_j^2$ and $]\sigma_j(\varphi_1^{-1}(\pm Q_1))[= \emptyset$ otherwise.

If a_0 is not a square in K, we need to extend the local and global heights on E_1/K to E_1/L where $L = K(\sqrt{a_0})$. Let χ' be the continuous idele class character of L defined by composing the trace maps of χ with the field traces $L_{\mathfrak{p}'}/K_{\mathfrak{p}_j}$ at each $\mathfrak{p}' \mid \mathfrak{p}_j$ and normalised so that it restricts to 2χ on $\mathbb{A}_K^*/K^*$. Write

$$h^{\chi, E_1}(Q_1) = \frac{1}{2} h^{\chi', E_1}(Q_1)$$

and, for a prime $\mathfrak{q}$ of K,

$$h_{\mathfrak{q}}^{\chi, E_1}(Q_1) = \frac{1}{[L_{\mathfrak{q}'} : K_{\mathfrak{q}}]} h_{\mathfrak{q}'}^{\chi', E_1}(Q_1),$$

where $\mathfrak{q}'$ is any prime of L above $\mathfrak{q}$. Since $\mathrm{Gal}(L/K)$ acts on Q_1 by multiplication by ± 1 and by definition of χ', the quantity $h_{\mathfrak{q}}^{\chi, E_1}(Q_1)$ is well-defined and all properties of $h_{\mathfrak{q}}^{\chi, E_1}$ for points over K hold for Q_1.

The following result is a version of Theorem 1.5 which is computationally more useful, since the function of Theorem 1.5 is defined only on a proper subset of $X^{(k)}(K \otimes \mathbb{Q}_p)$ for each k.

THEOREM 5.2: *For each $k \in \{1, 2\}$, there exists an explicitly computable finite set $T^{\chi,k} \subset \mathbb{Q}_p$ such that the locally analytic function $\rho^{\chi,k} \colon X^{(k)}(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$, defined by*

$$\rho^{\chi,k}(\underline{z}) := \sum_{j=1}^{m} 2h_{\mathfrak{p}_j}^{\chi, E_{3-k}}(\varphi_{3-k}(z_j)) - h_{\mathfrak{p}_j}^{\chi, E_k}(\varphi_k(z_j) + Q_k) - h_{\mathfrak{p}_j}^{\chi, E_k}(\varphi_k(z_j) - Q_k)$$
$$-2\sum_{i,j} \alpha_{ij}^{\chi, E_{3-k}} g_{ij}^{E_{3-k}}(\varphi_{3-k}(\underline{z})) + 2\sum_{i,j} \alpha_{ij}^{\chi, E_k} g_{ij}^{E_k}(\varphi_k(\underline{z})) + 2h^{\chi, E_k}(Q_k),$$

takes values in $T^{\chi,k}$ when restricted to $X^{(k)}(K)$.

Proof. Let $\mathfrak{q}$ be any prime of K and $\ell \in \{1,2\}$. By [6, Lemma 7.4], the local height $h_{\mathfrak{q}}^{\chi,E_\ell}$ satisfies the quasi-parallelogram law, i.e. for all points $P, R \in E_\ell(K_{\mathfrak{q}})$ such that $P, R, P \pm R \neq \infty_{E_\ell}$, we have

$$h_{\mathfrak{q}}^{\chi,E_\ell}(P+R)+h_{\mathfrak{q}}^{\chi,E_\ell}(P-R) = 2h_{\mathfrak{q}}^{\chi,E_\ell}(P)+2h_{\mathfrak{q}}^{\chi,E_\ell}(R)-2\chi_{\mathfrak{q}}(x(R)-x(P)). \tag{5.4}$$

This, together with (5.3), implies that $\rho^{\chi,k}(X^{(k)}(K))$ is contained in

$$T^{\chi,k} := \Bigg\{ \sum_{\mathfrak{q}\nmid p} h_{\mathfrak{q}}^{\chi,E_k}(\varphi_k(z_{\mathfrak{q}}) + Q_k) + h_{\mathfrak{q}}^{\chi,E_k}(\varphi_k(z_{\mathfrak{q}}) - Q_k) - 2h_{\mathfrak{q}}^{\chi,E_{3-k}}(\varphi_{3-k}(z_{\mathfrak{q}})) : (z_{\mathfrak{q}}) \in \prod_{\mathfrak{q}\nmid p} X(K_{\mathfrak{q}}) \setminus \{\varphi_k^{-1}(\pm Q_k)\} \Bigg\}.$$

The elementary proof of finiteness of $T^{\chi,k}$ given in [11, Proposition 6.5] when $K = \mathbb{Q}$ and χ is the cyclotomic character uses properties of the local heights away from p that hold also in this more general setting. Any detail that is omitted here can thus be deduced from [11]. Let $\mathfrak{q} \nmid p$ and define

$$W_{\mathfrak{q}}^{\chi,E_\ell} = \{h_{\mathfrak{q}}^{\chi,E_\ell}(P) \,:\, P \in E_\ell(K_{\mathfrak{q}}), x(P) \in \mathcal{O}_{\mathfrak{q}}\}.$$

As in the proof of Theorem 4.2, $W_{\mathfrak{q}}^{\chi,E_\ell}$ is finite and identically zero for almost all $\mathfrak{q}$. On the other hand, if $P \in E_\ell(K_{\mathfrak{q}})$ with $x(P) \notin \mathcal{O}_{\mathfrak{q}}$, then

$$h_{\mathfrak{q}}^{\chi,E_\ell}(P) = \chi_{\mathfrak{q}}(x(P)). \tag{5.5}$$

Let $z \in X(K_{\mathfrak{q}}) \setminus \{\varphi_k^{-1}(\pm Q_k)\}$ and define

$$w_{\mathfrak{q}}^{\chi,E_k}(z) = h_{\mathfrak{q}}^{\chi,E_k}(\varphi_k(z) + Q_k) + h_{\mathfrak{q}}^{\chi,E_k}(\varphi_k(z) - Q_k) - 2h_{\mathfrak{q}}^{\chi,E_{3-k}}(\varphi_{3-k}(z)).$$

If $\varphi_k(z) = \infty_{E_k}$, then $w_{\mathfrak{q}}^{\chi,E_k}(z) = 2h_{\mathfrak{q}}^{\chi,E_k}(Q_k) - 2h_{\mathfrak{q}}^{\chi,E_{3-k}}(Q_{3-k})$; otherwise, by (5.4), we have

$$\begin{aligned} 2^{-1}w_{\mathfrak{q}}^{\chi,E_k}(z) &= h_{\mathfrak{q}}^{\chi,E_k}(\varphi_k(z)) + h_{\mathfrak{q}}^{\chi,E_k}(Q_k) - \chi_{\mathfrak{q}}(x(\varphi_k(z))) - h_{\mathfrak{q}}^{\chi,E_{3-k}}(\varphi_{3-k}(z)) \\ &= h_{\mathfrak{q}}^{\chi,E_k}(\varphi_k(z)) + h_{\mathfrak{q}}^{\chi,E_k}(Q_k) + \chi_{\mathfrak{q}}(x(\varphi_{3-k}(z))) - \chi_{\mathfrak{q}}(a_0) - h_{\mathfrak{q}}^{\chi,E_{3-k}}(\varphi_{3-k}(z)). \end{aligned}$$

If $0 \leq \mathrm{ord}_{\mathfrak{q}}(x(z)) \leq \mathrm{ord}_{\mathfrak{q}}(a_0)/2$, then both $x(\varphi_1(z))$ and $x(\varphi_2(z))$ are integral and

$$\chi_{\mathfrak{q}}(x(\varphi_1(z))) \in \{n\chi_{\mathfrak{q}}(\pi_{\mathfrak{q}}) : 0 \leq n \leq \mathrm{ord}_{\mathfrak{q}}(a_0)\}.$$

In the remaining cases, exactly one of $x(\varphi_1(z))$ and $x(\varphi_2(z))$ is non-integral. Thus, by (5.5) and finiteness of $W_{\mathfrak{q}}^{\chi,E_\ell}$, we deduce that $w_{\mathfrak{q}}^{\chi,E_k}(z)$ takes values in a finite set $T_{\mathfrak{q}}^{\chi,k}$. Furthermore, since Q_ℓ is an integral point and a_0 divides

the discriminant of E_2, $T_{\mathfrak{q}}^{\chi,k} \subseteq \{0\}$ for all primes $\mathfrak{q}$ that divide neither the discriminant of E_1 nor the one of E_2. ∎

Assuming Leopoldt's conjecture, we have r_2+1 choices of independent characters χ and then Theorem 5.2 gives at most r_2+1 independent locally analytic functions on each $X^{(k)}(K \otimes \mathbb{Q}_p)$ vanishing on the global points $X^{(k)}(K)$. As in Section 4, we construct r_K other functions using the relations among the functionals f_i^J imposed by our assumption (5.2). In practice, each such relation can be reduced to a relation among the $f_i^{E_k}$ for some k.

Remark 5.3: As soon as $m > 1$ and $a_0 \in \mathcal{O}_j^2$ for some j, we have

$$X^{(1)}(K \otimes \mathbb{Q}_p) \cup X^{(2)}(K \otimes \mathbb{Q}_p) \subsetneq X(K \otimes \mathbb{Q}_p).$$

Thus, in order to turn the method outlined in this section into a strategy to compute $X(K)$, one also needs to deal with the residue disks that are not covered by Theorem 5.2. If, for instance, there are no K-rational points in these disks, then we can use the Mordell-Weil sieve to prove this. See also Remark 5.4 for a class of examples where we can immediately prove that there exist no K-rational points in such disks.

Remark 5.4: A quadratic Chabauty computation over number fields can sometimes be replaced with several quadratic Chabauty computations over $\mathbb{Q}$. For example, suppose that X is defined over $\mathbb{Q}$ and that we want to determine $X(K)$, where $K = \mathbb{Q}(\sqrt{d})$ for some square-free $d \in \mathbb{Q}$. Assume that $\mathrm{rk}(E_1/\mathbb{Q}) = \mathrm{rk}(E_2/\mathbb{Q}) = 1$, $\mathrm{rk}(E_1/K) = 2$ and $E_2(K) = E_2(\mathbb{Q})$. If $P \in X(K)$, then $\varphi_2(P) \in E_2(K) = E_2(\mathbb{Q})$ and so $x(P)^2 \in \mathbb{Q}$, $y(P)/x(P) \in \mathbb{Q}$. It follows that computing $X(K)$ is equivalent to computing $X(\mathbb{Q})$ and $X'(\mathbb{Q})$ where

$$X' \colon y^2 = x^6 + \frac{a_4}{d}x^4 + \frac{a_2}{d^2}x^2 + \frac{a_0}{d^3}.$$

The curve X' is a genus 2 bielliptic curve whose corresponding elliptic curves are the quadratic twists $E_1^{d^{-1}}$ and $E_2^{d^{-2}} \cong_{\mathbb{Q}} E_2$. In particular, $\mathrm{rk}(E_1^{d^{-1}}/\mathbb{Q}) = 1$ and $\mathrm{rk}(E_2^{d^{-2}}/\mathbb{Q}) = 1$. Quadratic Chabauty can thus be used to determine both $X(\mathbb{Q})$ and $X'(\mathbb{Q})$.

We also note that, even when p is split in K, in this example we have

$$\sigma(X(K)) = X^{(1)}(K) \cup X^{(2)}(K).$$

Indeed, $X(K \otimes \mathbb{Q}_p) \setminus (X^{(1)}(K \otimes \mathbb{Q}_p) \cup X^{(2)}(K \otimes \mathbb{Q}_p))$ consists of those points $(z_1, z_2) \in X(\mathbb{Q}_p) \times X(\mathbb{Q}_p)$ such that $\overline{z_i} \in \{\overline{(0, \pm\sqrt{a_0})}\}$, $z_j \in \{\overline{\infty^{\pm}}\}$ if $\{i,j\} =$

$\{1,2\}$, where $\sqrt{a_0}$ is a fixed square root of a_0 in $\mathbb{Q}_p$. Suppose that $(z_1,z_2)=\sigma(z)$ for some $z\in X(K)$. Then $x(z_1)^2=x(z_2)^2$ since $\varphi_2(z)\in E_2(\mathbb{Q})$. In particular, $\mathrm{ord}_p(x(z_1))=\mathrm{ord}_p(x(z_2))$: a contradiction.

6. Algorithms and examples for integral points over quadratic fields

To illustrate our method, we give detailed algorithms for carrying out the process described in Section 4 for elliptic curves over real and imaginary quadratic fields and curves of genus 2 over imaginary quadratic fields. We then apply these algorithms in several examples. Because of current limitations of our implementation, we restrict to the case where p is split in K, so that the Coleman integration takes place over $\mathbb{Q}_p$. The extension to more general good primes p is straightforward.

We keep the notation of Section 4. Let K be a quadratic number field and let p be a prime number such that $p\mathcal{O}_K=\mathfrak{p}_1\mathfrak{p}_2$ is split. Let $\chi_1,\dots,\chi_{r_2+1}\in V_K$ be independent continuous idele class characters. By Example 2.8, they correspond to pairs $c^{(k)}=(c_1^{(k)},c_2^{(k)})\in\mathbb{Q}_p^2$ such that $h_{\mathfrak{p}_j}^{\chi_k}(z)=c_j^{(k)}\cdot\tau_j(z)$ for all $j\in\{1,2\}$ and $z\in X(K_j)\setminus\{\infty\}$. Writing

$$h^{(k)}:=h^{\chi_k}=\sum_{0\le i\le j\le r-1}\alpha_{ij}^{(k)}g_{ij}\,,$$

we get

$$\rho_k(\underline{z}):=\rho^{\chi_k}(\underline{z})=\sum_{j=1}^{d}c_j^{(k)}\tau_j(z_j)-\sum_{i,j}\alpha_{ij}^{(k)}f_i(\underline{z})f_j(\underline{z}) \tag{6.1}$$

for $\underline{z}\in\mathcal{U}(\mathcal{O}_K\otimes\mathbb{Z}_p)$.

Algorithms for the case $K=\mathbb{Q}$ are discussed in great detail in [3]; they readily generalize to more general number fields K provided p is totally split. For instance, it is easy to see that the sets $T^{(k)}$ can be computed in practice using the method of [3, §3.4]. The p-adic heights can be computed using a straightforward adaptation of [8, Algorithm 3.8], and we deduce the constants $\alpha_{ij}^{(k)}$ as in [3, §3.2]. For the p-adic analytic computations we use `Sage` [35], the remaining computations are done in `Magma` [12].

Remark 6.1: Since [3, §3] contains a detailed precision analysis for each of these algorithms, we deduce that the p-adic objects in our results above are indeed explicitly computable in the sense described in the introduction; they are provably computable to any desired finite precision.

We want to construct two functions ρ_1, ρ_2 that map

$$\sigma(\mathcal{U}(\mathcal{O}_K)) \subset \mathcal{U}(\mathcal{O}_K \otimes \mathbb{Z}_p)$$

into an explicitly computable finite set $T^{(1)}$ ($T^{(2)}$, respectively) and have a finite common solution set. Once we have done this, we have to check if each solution $\underline{z} = (z_1, z_2)$ actually comes from a K-rational point, that is, whether $z_1 = \sigma_1(Q)$ and $z_2 = \sigma_2(Q)$ for some $Q \in \mathcal{U}(\mathcal{O}_K)$. We can use, for instance, that if this is the case, then we must have $x(z_1)x(z_2) \in \mathbb{Q}$ and $x(z_1) + x(z_2) \in \mathbb{Q}$.

The functions $f_i^{(j)} \colon \mathcal{U}(\mathcal{O}_K \otimes \mathbb{Z}_p) \to \mathbb{Q}_p$ are given by

$$f_i^{(j)}(\underline{z}) = \int_\infty^{z_j} \omega_i \,;$$

the corresponding linear functionals in $(J(K) \otimes \mathbb{Q}_p)^\vee$ will also be denoted by $f_i^{(j)}$.

6.1. Elliptic curves over real quadratic fields. Let E/K denote an elliptic curve over a real quadratic field[2] K given by a Weierstrass equation[3] with good reduction at both $\mathfrak{p}_1$ and $\mathfrak{p}_2$. We set $f_0 := f_0^{(1)}$ and $f_1 := f_0^{(2)}$. Equation (4.1) is satisfied if and only if $r = \mathrm{rk}(E/K) = 0$ or 1; we assume that $r = 1$. It follows that there is a linear dependence $f_0 = bf_1$ between the functionals f_0 and f_1 on $E(K) \otimes \mathbb{Q}_p$ The first function ρ_1 is constructed using the cyclotomic p-adic height pairing h^{cyc}. By (6.1), we have

$$\rho_1(\underline{z}) := \rho^{\mathrm{cyc}}(\underline{z}) = \tau_1(z_1) + \tau_2(z_2) - \alpha f_0(\underline{z})^2,$$

where

$$h^{\mathrm{cyc}} = \alpha g_{00} = \alpha f_0^2 \,,$$

[2] The algorithm described in this subsection works also when K is imaginary; however, while in the real case the rank assumption here is optimal, in the imaginary case we can work with curves of larger rank, as is explained in §6.2.

[3] The setup in the previous section required an equation of the form $y^2 = f(x)$, but for elliptic curves we can extend it easily to cover general Weierstrass equations.

that is, $\alpha = \alpha_{00}^{(1)}$. We can compute α by comparing $h^{\mathrm{cyc}}(Q)$ and $f_0^2(Q)$ for some nontorsion point $Q \in E(K)$. Letting $T := T^{(1)}$ denote the finite set of values that $-\sum_{\mathfrak{q}\nmid p} h_{\mathfrak{q}}^{\mathrm{cyc}}(z_{\mathfrak{q}} - \infty)$ can take for $(z_{\mathfrak{q}}) \in \prod_{\mathfrak{q}\nmid p} \mathcal{U}(\mathcal{O}_{K_{\mathfrak{q}}})$, we then must have

$$\rho_1(\sigma_1(Q), \sigma_2(Q)) \in T$$

for all $\mathcal{O}_K$-integral points $Q \in E(K)$.

The second function comes from the dependence between f_0 and f_1 and is given by

$$\rho_2(\underline{z}) = \int_\infty^{z_1} \omega_0 - b \int_\infty^{z_2} \omega_0\,;$$

we have $\rho_2(\sigma_1(Q), \sigma_2(Q)) = 0$ for all $Q \in E(K)$. We can use any nontorsion $Q \in E(K)$ and compare $f_0(Q)$ to $f_1(Q)$ to find b.

Note that, if E is defined over $\mathbb{Q}$ and $w \in T$, we can always reduce the system

$$\begin{cases} \rho_1(z_1, z_2) = w \\ \rho_2(z_1, z_2) = 0 \end{cases}$$

to one equation in one variable. Indeed, first observe that

- if $\mathrm{rk}(E/\mathbb{Q}) = \mathrm{rk}(E/K) = 1$, then for every $Q \in E(K)$ there exists n such that $nQ \in E(\mathbb{Q})$. Thus, by linearity, $f_0(Q) = f_1(Q)$;
- if $\mathrm{rk}(E/\mathbb{Q}) = 0$, then for every $Q \in E(K)$ we have $Q + Q^c \in E(\mathbb{Q}) = E(\mathbb{Q})_{\mathrm{tors}}$, where Q^c is the Galois conjugate of Q. We deduce that $f_0(Q) + f_1(Q) = f_0(Q + Q^c) = 0$.

Furthermore,

$$\int_\infty^z \omega_0 = \int_\infty^{z'} \omega_0 \iff z - z' \in E(\mathbb{Q}_p)_{\mathrm{tors}}.$$

Suppose that $\mathrm{rk}(E/\mathbb{Q}) = 1$ and that we want to find all $Q \in \mathcal{U}(\mathcal{O}_K)$ such that $(\overline{\sigma_1(Q)}, \overline{\sigma_2(Q)}) = (\overline{P_1}, \overline{P_2}) \in \overline{E}(\mathbb{F}_p) \times \overline{E}(\mathbb{F}_p)$. If there are no torsion points in $E(\mathbb{Q}_p)$ reducing to $\overline{P_1} - \overline{P_2}$, then the above shows that no such Q exists. Otherwise, we solve

$$\rho_1((x(s), y(s)), (x(s), y(s)) + R) = w$$

where $(x(s), y(s))$ is a parametrization for the points in $E(\mathbb{Q}_p)$ reducing to $\overline{P_1}$ and R is the unique torsion point[4] in $E(\mathbb{Q}_p)$ such that $\overline{P_2} - \overline{P_1} = \overline{R}$ (cf. Example 6.3). The case $\mathrm{rk}(E/\mathbb{Q}) = 0$ is very similar.

[4] Since p is odd, the group $E_1(\mathbb{Q}_p)$ of $\mathbb{Q}_p$-points on the formal group at p is torsion-free. Therefore, $E(\mathbb{Q}_p)_{\mathrm{tors}}$ can be realized as a subgroup of $\overline{E}(\mathbb{F}_p)$.

Example 6.2: Consider the elliptic curve 199.1-c1 [27] over $K = \mathbb{Q}(a)$, where a is a root of $x^2 - x - 1$. It admits the global minimal model

$$E\colon y^2 + y = x^3 + (a+1)x^2 + ax.$$

The prime $p = 11$ is the smallest prime splitting in K. The curve has everywhere good reduction, except at $(-3a + 16)$, where it has Kodaira symbol I_1: thus, $T = \{0\}$. The common zero set of ρ_1 and ρ_2 contains the integral points

$$\pm(-1,0), \pm(0,0), \pm(a,2a), \pm(-2a+3, 4a-7), \pm(a+1, 3a+1), \pm(-a,0),$$
$$\pm(42a+27, -420a-259), \pm(-6a+8, -18a+29), \pm(-a+1, a-2)$$

and 138 other pairs of points in $\sigma_1(E)(\mathbb{Q}_p) \times \sigma_2(E)(\mathbb{Q}_p)$, where $\sigma_i(E)/\mathbb{Q}_p$ is the curve obtained from the Weierstrass equation for E via the embedding $\sigma_i\colon K \hookrightarrow \mathbb{Q}_p$.

Example 6.3: Consider the elliptic curve with LMFDB label 192.a3 [27]

$$E\colon y^2 = x^3 - x^2 - 4x - 2$$

and let $K = \mathbb{Q}(\sqrt{3})$. We have that $\mathrm{rk}(E/K) = \mathrm{rk}(E/\mathbb{Q}) = 1$ and that $p = 13$ is of good ordinary reduction for E and is split in K. As explained above, in this setting we can reduce our computations to finding solutions to power series equations in one variable. Note in particular that $\#\overline{E}(\mathbb{F}_p) = 12 \not\equiv 0 \bmod p$, so each residue disk contains precisely one torsion point of $E(\mathbb{Q}_p)$.

The only inputs in this computation which come from our specific choice of quadratic field K are the reduction type of E at the bad primes (and consequently the set T) and the choice of prime p, since we require that p is split.

For this reason, it is not surprising that, besides recovering the integral points

$$\pm(3,2), (-1,0), (1 \pm \sqrt{3}, 0), \pm(25 \pm 15\sqrt{3}, 180 \pm 104\sqrt{3}),$$

we also recognize in our zero set the points

$$\pm\left(\frac{-1 \pm \sqrt{-3}}{2}, \frac{-3 \pm \sqrt{-3}}{2}\right), \pm(-1 \pm i, 2),$$

all of which belong to the 2-saturation of $E(\mathbb{Q})$.

6.2. Elliptic curves over imaginary quadratic fields. The following brief discussion on elliptic curves over imaginary quadratic fields will be useful for the computation of rational points on bielliptic curves over imaginary quadratic fields of §7.1. Let K be an imaginary quadratic number field and

let E be an elliptic curve defined over K with $r = \mathrm{rank}(E/K) = 2$, such that E has good reduction at both $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Suppose that f_0 and f_1 are linearly independent. Note that:

LEMMA 6.4: *Suppose that E as above can be defined over $\mathbb{Q}$. Then f_0 and f_1 are linearly independent if and only* $\mathrm{rk}(E/\mathbb{Q}) = 1$.

Proof. If $\mathrm{rk}(E/\mathbb{Q}) = r$ (resp. $\mathrm{rk}(E/\mathbb{Q}) = 0$), then $f_0 = f_1$ (resp. $f_0 = -f_1$) on $E(K)$ (cf. also the discussion before Example 6.2). Conversely, suppose that $\mathrm{rk}(E/\mathbb{Q}) = 1$ and that f_0 and f_1 are linearly dependent on $E(K) \otimes \mathbb{Q}_p$. Since neither of f_0 and f_1 is identically zero on $E(K)$ (as $E(K)$ contains points of infinite order), then there exists $\alpha \in \mathbb{Q}_p$ such that $f_0 = \alpha f_1$. Let $P \in E(\mathbb{Q})$ of infinite order. Then $f_0(P) = f_1(P)$ and hence $\alpha = 1$. Thus, for all $Q \in E(K)$, we have $\int_\infty^{\sigma_1(Q)} \omega_0 = \int_\infty^{\sigma_2(Q)} \omega_0$, so that $\sigma_1(Q - Q^c) \in E(\mathbb{Q}_p)_{\mathrm{tors}}$, where Q^c is the Galois conjugate of Q. Let $R \in E(K)_{\mathrm{tors}}$ such that $Q = Q^c + R$ and let n be the additive order of R. Then $nQ = nQ^c$, i.e. $nQ \in E(\mathbb{Q})$, contradicting $\mathrm{rk}(E/K) > \mathrm{rk}(E/\mathbb{Q})$. ∎

Under our assumption, the bilinear forms g_{ij} $(0 \le i \le j \le 1)$ generate $\mathcal{B}$, the space of $\mathbb{Q}_p$-valued bilinear forms on $E(K) \otimes \mathbb{Q}_p$. Hence the p-adic heights h^{cyc} and h^{anti} can be expressed as linear combinations

$$h^{\mathrm{cyc}} = \sum \alpha_{ij}^{\mathrm{cyc}} g_{ij} \quad \text{and} \quad h^{\mathrm{anti}} = \sum \alpha_{ij}^{\mathrm{anti}} g_{ij}.$$

Using independent nontorsion points $P, Q \in E(K)$, we can find all $\alpha_{ij}^{\mathrm{cyc}}$ (resp. $\alpha_{ij}^{\mathrm{anti}}$) by computing $f_0(P), f_1(P), f_0(Q), f_1(Q)$ and $h^{\mathrm{cyc}}(P), h^{\mathrm{cyc}}(Q), h^{\mathrm{cyc}}(P + Q)$ (resp. $h^{\mathrm{anti}}(P), h^{\mathrm{anti}}(Q), h^{\mathrm{anti}}(P + Q)$).

When E is defined over $\mathbb{Q}$, we have $\alpha_{00}^{\mathrm{cyc}} = \alpha_{11}^{\mathrm{cyc}}$ and $\alpha_{01}^{\mathrm{anti}} = 0$, $\alpha_{00}^{\mathrm{anti}} = -\alpha_{11}^{\mathrm{anti}}$. Indeed, for all $R_1, R_2 \in E(K)$, we have $h^{\mathrm{cyc}}(R_1, R_2) = h^{\mathrm{cyc}}(R_1^c, R_2^c)$ and hence

$$(\alpha_{00}^{\mathrm{cyc}} - \alpha_{11}^{\mathrm{cyc}})(g_{00}(R_1, R_2) - g_{11}(R_1, R_2)) = 0;$$

the first claim then follows since the g_{ij} are a basis for $\mathcal{B}$. Similarly, the anti-cyclotomic height pairing changes of sign if we first act by Galois, proving the second claim.

6.3. GENUS 2 CURVES, IMAGINARY QUADRATIC FIELDS. Suppose that $X\colon y^2 = f(x)$ has genus 2 and rank 4 over an imaginary quadratic field K. Let p be a split prime of good, ordinary reduction and let $\sigma_1, \sigma_2\colon K \hookrightarrow \mathbb{Q}_p$ denote the two

embeddings corresponding to the primes $\mathfrak{p}_1, \mathfrak{p}_2$ of K above p. Then we have 4 functionals $f_i^{(j)}\colon J(K)\otimes_{\mathbb{Z}}\mathbb{Q}_p \to \mathbb{Q}_p$, extended linearly from the functions

$$f_i^{(j)}(Q) = \int_{\infty}^{\sigma_j(Q)} \omega_i,$$

on $X(K)$, which we assume to be independent. For simplicity, we renumber them

$$f_0 = f_0^{(1)},\ f_1 = f_0^{(2)},\ f_2 = f_1^{(1)},\ f_3 = f_1^{(2)}\,.$$

As in the proof of Theorem 4.2, the functions $g_{ij}(P,Q) = \frac{1}{2}(f_i(P)f_j(Q) + f_i(Q)f_j(P))$, for $0 \le i \le j \le 3$ form a basis of the bilinear forms on $J(K)\otimes_{\mathbb{Z}}\mathbb{Q}_p$. We can express the p-adic height pairings h^{cyc} and h^{anti} in terms of the g_{ij}:

$$h^{\mathrm{cyc}} = \sum_{i,j} \alpha_{ij}^{\mathrm{cyc}} g_{ij} \quad \text{and} \quad h^{\mathrm{anti}} = \sum_{i,j} \alpha_{ij}^{\mathrm{anti}} g_{ij}.$$

In order to compute the constants $\alpha_{ij}^{\mathrm{cyc}}$ and $\alpha_{ij}^{\mathrm{anti}}$, we find divisors $D_1, \dots, D_4 \in \mathrm{Div}^0(X)$ such that the corresponding points generate a finite index subgroup of $J(K)$ modulo torsion. Then we have, for each pair (k,l), the relationships

$$h^{\mathrm{cyc}}(D_k, D_l) = \sum_{0\le i\le j\le 3} \alpha_{ij}^{\mathrm{cyc}} \cdot \left(\frac{1}{2}\left(f_i(D_k)f_j(D_l) + f_j(D_k)f_i(D_l)\right)\right)$$

and

$$h^{\mathrm{anti}}(D_k, D_l) = \sum_{0\le i\le j\le 3} \alpha_{ij}^{\mathrm{anti}} \cdot \left(\frac{1}{2}\left(f_i(D_k)f_j(D_l) + f_j(D_k)f_i(D_l)\right)\right).$$

That is, we can solve the linear system relating the height pairings h^{cyc} and h^{anti} to the natural basis $(g_{ij}\colon 0 \le i \le j \le 3)$ to recover the $\alpha_{ij}^{\mathrm{cyc}}$ and the $\alpha_{ij}^{\mathrm{anti}}$.

Every $\mathcal{O}_K$-integral point Q on X must satisfy

$$\rho^{\mathrm{cyc}}(\sigma_1(Q), \sigma_2(Q)) \in T^{\mathrm{cyc}}; \quad \rho^{\mathrm{anti}}(\sigma_1(Q), \sigma_2(Q) \in T^{\mathrm{anti}}\,,$$

where

$$\rho^{\mathrm{cyc}}(\underline{z}) = \tau_1(z_1) + \tau_2(z_2) - \sum_{ij} \alpha_{ij}^{\mathrm{cyc}} f_i(\underline{z}) f_j(\underline{z})$$

$$\rho^{\mathrm{anti}}(\underline{z}) = \tau_1(z_1) - \tau_2(z_2) - \sum_{ij} \alpha_{ij}^{\mathrm{anti}} f_i(\underline{z}) f_j(\underline{z})$$

and where T^{cyc} and T^{anti} are the respective possible values for the sum of the local heights away from p of an $\mathcal{O}_K$-integral point on X.

Example 6.5: We consider the curve

$$X\colon y^2 = x^5 - x^4 + x^3 + x^2 - 2x + 1$$

over $K = \mathbb{Q}(\sqrt{-3})$ and note that $\mathrm{rk}(J/\mathbb{Q}) = 2$ and $\mathrm{rk}(J/K) = 4$. Let

$$P_1 = (0,1), \qquad P_2 = (1,1), \qquad P_3 = \left(\sqrt{-3}, 2\sqrt{-3}+1\right),$$
$$P_4 = \left(\frac{1}{2}(\sqrt{-3}+1), \frac{1}{2}(-\sqrt{-3}+1)\right), \quad Q_1 = \left(\frac{1}{2}(-\sqrt{-3}+1), \frac{1}{2}(\sqrt{-3}+1)\right),$$
$$Q_2 = (-1,1), \qquad Q_3 = (2,5), \qquad Q_4 = (4,29),$$

and let $D_i = (P_i) - (Q_i)$ for $i = 1, \ldots, 4$. The points $[D_1], [D_2], [D_3], [D_4]$ generate a finite index subgroup G of $J(K)$. The smallest good ordinary split prime for this curve is $p = 7$.

We recover the following $\mathcal{O}_K$-integral points on X:

$$(-1, \pm 1), (\sqrt{-3}, \pm(2\sqrt{-3}+1)), (0, \pm 1), (2, \pm 5), (4, \pm 29),$$
$$(\sqrt{-3}+1, \pm(-\sqrt{-3}+4)), (-\sqrt{-3}, \pm(-2\sqrt{-3}+1)), (1, \pm 1),$$
$$(-\sqrt{-3}+1, \pm(\sqrt{-3}+4)), \left(-\frac{1}{2}\sqrt{-3}+\frac{1}{2}, \pm\left(\frac{1}{2}\sqrt{-3}+\frac{1}{2}\right)\right),$$
$$\left(\frac{1}{2}\sqrt{-3}+\frac{1}{2}, \pm\left(-\frac{1}{2}\sqrt{-3}+\frac{1}{2}\right)\right).$$

We apply the Mordell-Weil sieve to show that these are indeed the only integral points. To this end, we apply quadratic Chabauty for the primes 7 and 19. The subgroup G is not saturated at 3, so we use the modified Mordell-Weil sieve as described in [6, Appendix B]. In the notation given there, we used the auxiliary integer $N = 10$ and 20 primes of K to rule out all but one pair of residue classes modulo 7^4 and 19^3, respectively; the largest norm of a prime used in this computation was 4591. In order to show that the remaining pair does not correspond to an integral point either, we used the auxiliary integer $N = 8$.

Remark 6.6: It appears to be difficult to find examples over number fields K of degree > 2 for which the computation of integral points using our method is applicable in practice. Some restrictions are due to external components of our algorithms. For instance, we need to compute the Mordell-Weil rank r, find r independent points in $J(K)$, compute regular models and intersections over K (the `Magma`-command `RegularModel` uses arithmetic in K, not in a completion)

and apply the Mordell-Weil sieve over K. These computations often fail or are prohibitively expensive for number fields of degree > 2.

Therefore our current implementation is also limited to quadratic fields. To go beyond this, we would have to algorithmically compute a basis of the space of continuous idele class characters, extend our implementation of the root finding methods discussed in Appendix A. Moreover, the Coleman integration and p-adic heights routines, currently restricted to $\mathbb{Q}_p$, would have to be extended to finite extensions to be able to deal with generators of (a finite index subgroup of) $J(K)/\mathrm{tors}$ that do not split into sums of points over $\mathbb{Q}_p$.

7. Examples for rational points

In this section we present examples for Section 5, of which we retain the notation, when K is a quadratic field [5]. To simplify the exposition, we further assume that X is defined over $\mathbb{Q}$. We let p be an odd prime which splits in K and such that X has good reduction at each prime above p. For simplicity we assume that a_0 is a square in K.

7.1. Rank 4 over imaginary quadratic fields. Let $X/\mathbb{Q}$ be as above and let K be an imaginary quadratic field. If $\mathrm{rk}(E_k/\mathbb{Q}) = 1$ and $\mathrm{rk}(E_k/K) = 2$ for each k, then (5.2) and Assumption 5.1 are both satisfied in view of Lemma 6.4. Theorem 5.2 with $\chi = \chi^{\mathrm{cyc}}$ and $\chi = \chi^{\mathrm{anti}}$ provides us, for each $k \in \{1, 2\}$, with two locally analytic functions $\rho^{\mathrm{cyc},k}$ and $\rho^{\mathrm{anti},k}$ on $X^{(k)}(K \otimes \mathbb{Q}_p)$ and finite sets $T^{\mathrm{cyc},k}$ and $T^{\mathrm{anti},k}$. Varying k and looking at the intersection B^k of the loci $\rho^{\mathrm{cyc},k}(\underline{z}) \in T^{\mathrm{cyc},k}$ and $\rho^{\mathrm{anti},k}(\underline{z}) \in T^{\mathrm{anti},k}$, we obtain a set of points containing all the points in $\sigma(X(K))$ that do not map to $(\overline{\infty^{\pm}}, \overline{(0, \pm\sqrt{a_0})})$ or to $(\overline{(0, \pm\sqrt{a_0})}, \overline{\infty^{\pm}})$ under reduction to $\overline{X}(\mathbb{F}_p) \times \overline{X}(\mathbb{F}_p)$.

As already mentioned, the discussion of §6.2 is used in the computation of the constants of Theorem 5.2. To p-adically approximate the set B^k, we need to compute roots of systems of two equations in two variables. We do so using Algorithm 1, Lemma A.3 and the discussion in Appendix A. Note that $\rho^{\mathrm{cyc},k}$ and $\rho^{\mathrm{anti},k}$ are both invariant under the automorphisms $\theta\colon (x, y) \mapsto (\pm x, \pm y)$ of X. Thus, from the points in B^k reducing to $(\overline{P}, \overline{Q}) \in \overline{X}(\mathbb{F}_p) \times \overline{X}(\mathbb{F}_p)$ we can

[5] We focus on examples over quadratic fields for the same reasons as discussed in Remark 6.6.

deduce the points in B^k reducing to $(\theta(\overline{P}), \theta(\overline{Q}))$. This cuts down the number of pairs of residue disks that we need to consider.

Example 7.1: Consider

$$X = X_0(91)^+ : y^2 = x^6 - 3x^4 + 19x^2 - 1.$$

The associated elliptic curves E_1 (91.a1 [27]) and E_2 (91.b2 [27]) each have rank 1 over $\mathbb{Q}$ and applying quadratic Chabauty with $p = 5$ recovers the rational points

$$\{\infty^{\pm}, (1, \pm 4), (-1, \pm 4), (1/3, \pm 28/27), (-1/3, \pm 28/27)\} \tag{7.1}$$

together with 2 other 5-adic points up to automorphisms. We now carry out quadratic Chabauty for $p = 5$ and $K = \mathbb{Q}(i)$, over which the elliptic curves E_1 and E_2 attain rank 2. Denote by $T^{\mathrm{cyc},k}$ and $T^{\mathrm{anti},k}$ the explicitly computable finite sets of Theorem 5.2 for $\chi = \chi^{\mathrm{cyc}}$ and $\chi = \chi^{\mathrm{anti}}$, respectively.

Claim 1: $T^{\mathrm{cyc},1} = T^{\mathrm{cyc},2} = T^{\mathrm{anti},1} = T^{\mathrm{anti},2} = \{0\}$.

Proof. $X_0(91)^+$ has bad reduction at 7 and 13. Furthermore, E_1 and E_2 are minimal at the primes of $\mathbb{Q}(i)$ above 7 and 13 and the reduction type at all these primes is I_1. ∎

Besides the $\mathbb{Q}$-rational points listed in (7.1), in $B^1 \cup B^2$ we also recover the following points defined over $\mathbb{Q}(i)$:

$$(0, \pm i), (\pm(-2i + 1), \pm(-8i + 12)), (\pm(2i + 1), \pm(8i + 12)), \tag{7.2}$$

as well as 20 other 5-adic points up to automorphisms $(x, y) \mapsto (\pm x, \pm y)$. We apply the Mordell-Weil sieve to show that these p-adic points do not correspond to $\mathbb{Q}(i)$-rational points and that there are no $\mathbb{Q}(i)$-rational points mapping to the pairs of points

$$(\overline{\infty^{\pm}}, \overline{(0, \pm\sqrt{-1})}), (\overline{(0, \pm\sqrt{-1})}, \overline{\infty^{\pm}}).$$

This proves that all $\mathbb{Q}(i)$-rational points on $X_0(91)^+$ are either listed in (7.1) or in (7.2).

A technical remark (with reference to Appendix A): there are four pairs of residue disks in $\overline{X}(\mathbb{F}_p) \times \overline{X}(\mathbb{F}_p)$, up to automorphism, such that a root in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ of the corresponding system of equations is also a root modulo p of the determinant of the Jacobian matrix. Of these, two correspond to the global points $(0, i)$ and ∞ (and thus the determinant of the Jacobian matrix

has a zero at those points by Remark A.2), another one lifts to no root in $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$ for sufficiently large n and for the remaining one we can apply the multivariate Hensel's lemma after lifting the root modulo some small power of p (cf. Algorithm 1). Furthermore, the strategy outlined after Remark A.2 also shows that there are no other points in the residue disks of $(0, i)$ and ∞. Therefore, we conclude that the approximations that we have computed are in one-to-one correspondence with the elements in $B^1 \cup B^2$ (up to automorphism). Amongst the 20 extra points, we recognize the pair of rational points $\underline{z} = ((1, 4), (-1, 4))$. Indeed, z_1 and z_2 both map to $(1, 4)$ in $E_1(\mathbb{Q})$ and map to the torsion points $(-1, -4)$ and $(-1, 4)$ in $E_2(\mathbb{Q})$. Thus $g_{ij}^{E_2}(\varphi_2(\underline{z})) = 0$. The claim then follows since the local heights are invariant under pre-multiplication by -1.

Finally, note that, since $T^{\mathrm{anti},k} = \{0\}$, in this case $B^1 \cup B^2$ is closed under $(z_1, z_2) \mapsto (z_2, z_1)$. Quotienting by this symmetry, the 20 extra pairs of points become 14.

7.2. Rank 3 over real quadratic fields. Keep the notation of the beginning of Section 7 and let K now be a real quadratic field[6]. Then (5.2) forces $\mathrm{rk}(J/K) \leq 3$. Since we need Assumption 5.1 to also hold, we suppose here that $\mathrm{rk}(E_1/K) = 2$, $\mathrm{rk}(E_1/\mathbb{Q}) = 1$ and $\mathrm{rk}(E_2/K) = 1$. This is sufficient by Lemma 6.4 and by the non-degeneracy of the p-adic logarithm on an elliptic curve.

For a fixed $k \in \{1, 2\}$, Theorem 5.2 determines only one function ρ_1^k and one finite set T^k in this case; the second function ρ_2 that we need comes from the dependence of $f_0^{E_2}$ and $f_1^{E_2}$ (see also §6.1). Let

$$B^k = \{\underline{z} \in X^{(k)}(K \otimes \mathbb{Q}_p) : \rho_1^k(\underline{z}) \in T^k, \rho_2(\underline{z}) = 0\}.$$

Note that it suffices to run through $\overline{X}(\mathbb{F}_p) \times \overline{X}(\mathbb{F}_p)/\sim$ where $(P, Q) \sim (R, T)$ if and only if $P = T$ and $Q = R$, as our equations are symmetric with respect to the two embeddings of K into $\mathbb{Q}_p$ (cf. the discussion of §6.2). As before, we can also use the invariance of our zero sets under the hyperelliptic and bielliptic automorphisms of X to reduce even further the number of pairs of disks that we need to consider.

In view of Remark 5.4, the resulting algorithm is often an alternative to a series of quadratic Chabauty computations over the rationals. This is in particular the case in the following example.

[6] The strategy also works if K is imaginary. See also footnote 2 in §6.1.

Example 7.2: Consider

$$X\colon y^2 = x^6 + x^2 + 1.$$

In [11, Example 6.3] quadratic Chabauty over $\mathbb{Q}$ was used to provide an alternative proof of Wetherell's result [38] that

$$X(\mathbb{Q}) = \{\infty^{\pm}, (0, \pm 1), (\pm 1/2, \pm 9/8)\}.$$

Let $K = \mathbb{Q}(\sqrt{34})$. We have $\mathrm{rk}(E_1/\mathbb{Q}) = 1$, $\mathrm{rk}(E_1/K) = 2$ and $\mathrm{rk}(E_2/\mathbb{Q}) = \mathrm{rk}(E_2/K) = 1$. We now determine $X(K)$ exactly, by applying quadratic Chabauty over K with the split prime $p = 3$. We may choose

$$\rho_2(\underline{z}) = \int_{\infty}^{\varphi_2(z_1)} \omega_0^{E_2} - \int_{\infty}^{\varphi_2(z_2)} \omega_0^{E_2},$$

where $\infty := \infty_{E_2}$. Denote by T^k the explicitly computable finite set of Theorem 5.2 for $\chi = \chi^{\mathrm{cyc}}$.

Claim 2: $T^1 = \{0, 2\log 2, \frac{5}{2}\log 2\}$, $T^2 = \{-2\log 2, -4\log 2, -\frac{9}{2}\log 2\}$.

Proof. The elliptic curves E_1 and E_2 have everywhere good reduction except at the primes above 2 and 31. Furthermore, the models

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

are globally minimal also over K. The prime 31 is inert in K and E_1 and E_2 have reduction type I_1 with Tamagawa number 1 at $31\mathcal{O}_K$. Thus, the only nontrivial contributions to T^k can come from the unique prime $\mathfrak{q}$ of K above 2. The curve E_1 has Tamagawa number 1 (and Kodaira symbol I_0^*) at $\mathfrak{q}$, so $h_{\mathfrak{q}}^{E_1}$ is identically zero on integral points. The curve E_2 has reduction type I_1^* with Tamagawa number 4 at $\mathfrak{q}$ and we have

$$h_{\mathfrak{q}}^{E_2}(x, y) = \begin{cases} 0 & \text{if } |x|_{\mathfrak{q}} = 1, \\ -\log 2 \text{ or } -\frac{5}{4}\log 2 & \text{if } |x|_{\mathfrak{q}} < 1 \end{cases}$$

(see e.g. [11, Proposition 2.4]); in particular, $h_{\mathfrak{q}}^{E_2}(Q_2) = -\log 2$.

For $z \in X(K_{\mathfrak{q}})$, $\varphi_1(z) \neq \pm Q_1$ resp. $\varphi_2(z) \neq \pm Q_2$, let

$$w_{\mathfrak{q}}^{E_1}(z) = h_{\mathfrak{q}}^{E_1}(\varphi_1(z) + Q_1) + h_{\mathfrak{q}}^{E_1}(\varphi_1(z) - Q_1) - 2h_{\mathfrak{q}}^{E_2}(\varphi_2(z))$$
$$w_{\mathfrak{q}}^{E_2}(z) = h_{\mathfrak{q}}^{E_2}(\varphi_2(z) + Q_2) + h_{\mathfrak{q}}^{E_2}(\varphi_2(z) - Q_2) - 2h_{\mathfrak{q}}^{E_1}(\varphi_1(z)).$$

Using the quasi-parallelogram law (5.4), we find

- If $|x(z)|_{\mathfrak{q}} \leq 1$, then $w_{\mathfrak{q}}^{E_1}(z) = 0$ and $w_{\mathfrak{q}}^{E_2}(z) = -2\log 2$.

- If $|x(z)|_{\mathfrak{q}} > 1$, then

$$w_{\mathfrak{q}}^{E_1}(z) \in \left\{2\log 2, \frac{5}{2}\log 2\right\} \quad \text{and} \quad w_{\mathfrak{q}}^{E_2}(z) \in \left\{-4\log 2, -\frac{9}{2}\log 2\right\}.$$

∎

Since $E_2(K) = E_2(\mathbb{Q})$ (as $\operatorname{rank}(E_2/K) = \operatorname{rank}(E_2/\mathbb{Q})$ and $E_2(K)_{\mathrm{tors}} = \{\infty\}$), Remark 5.4 tells us that $X(K) \subset X^{(1)}(K \otimes \mathbb{Q}_p) \cup X^{(2)}(K \otimes \mathbb{Q}_p)$ and, in particular, $X(K) \subseteq B^1 \cup B^2$. We have

$$\overline{X}(\mathbb{F}_3) = \{\overline{\infty^{\pm}}, \overline{(0,\pm 1)}, \overline{(\pm 1, 0)}\}.$$

It follows from the observations at the beginning of §7.2 that it suffices to consider the points in $X^{(k)}(K \otimes \mathbb{Q}_p)$ reducing to one of the following pairs of residue disks in $\overline{X}(\mathbb{F}_3) \times \overline{X}(\mathbb{F}_3)$:

$$(\overline{\infty^+}, \overline{\infty^+}), (\overline{\infty^+}, \overline{\infty^-}), (\overline{\infty^+}, \overline{(1,0)}) \text{ with } k = 1;$$
$$(\overline{(0,1)}, \overline{(0,1)}), (\overline{(0,2)}, \overline{(0,1)}), (\overline{(0,2)}, \overline{(1,0)}), (\overline{(1,0)}, \overline{(1,0)}), (\overline{(1,0)}, \overline{(2,0)}) \text{ with } k = 2.$$

By Claim 2, the intersection of B^k with a residue pair (for k dependent on the pair and chosen as above) is given by the union of the zeros of three systems of two equations in two variables (by a similar argument to the one at the end of Remark 5.4, some pairs could be excluded a priori from containing points in $X(K)$ by valuation considerations, but we leave them all in the computation here). Using the algorithms of Appendix A, we recover in $B^1 \cup B^2$ exactly the points in Table 1 (the residue pairs contained in $X^{(k)}(K \otimes \mathbb{Q}_p)$ that intersect B^k trivially are not listed).

Besides recovering representatives of the points in

$$X(\mathbb{Q}) \cup \left\{\left(\frac{11}{204}\sqrt{34}, \pm\frac{44909}{249696}\sqrt{34}\right), \left(-\frac{11}{204}\sqrt{34}, \pm\frac{44909}{249696}\sqrt{34}\right)\right\}$$

up to automorphisms, our zero sets contain some points $\underline{z} = (z_1, z_2) \in X(\mathbb{Q}_p) \times X(\mathbb{Q}_p)$ which we do not recognize as points coming from $X(K)$. Using one of the following arguments, we can prove that each of these points is indeed not K-rational. Suppose that $\underline{z} \in \sigma(X(K))$. Then, since $E_2(K) = E_2(\mathbb{Q})$, the computed approximations of $\varphi_2(z_1)$ and $\varphi_2(z_2)$ must agree. If this holds, let $\varphi_2(z)$ be either of $\varphi_2(z_1)$ and $\varphi_2(z_2)$.

(O1) If $\varphi_2(z)$ is in the formal group at p, it was shown in [11, Example 6.3] that we must have $\mathrm{ord}_p(x(\varphi_2(z))) \leq -4$.

(O2) Else, since $E_2(\mathbb{Q})$ is generated by $Q_2 = (0,1)$, if $\varphi_2(z) = nQ_2$ for some $n \in \mathbb{Z}$, then

$$n \equiv n_1 := \frac{\int_\infty^{\varphi_2(z)} \omega_0^{E_2}}{\int_\infty^{Q_2} \omega_0^{E_2}} \bmod 3;$$

on the other hand, $\overline{Q_2} \in \overline{E_2}(\mathbb{F}_3)$ has order 6. Thus, if $\overline{\varphi_2(z)} = n_2\overline{Q_2}$, we also have

$$n \equiv n_2 \bmod 6.$$

If $n_1 \not\equiv n_2 \bmod 3$, then $\underline{z} \notin \sigma(X(K))$.

The extra points in the residue pair $(\overline{(0,1)}, \overline{(0,1)})$ are precisely the extra points of the computation over $\mathbb{Q}$ ([11, Example 6.3]). Also note that the criterion (O1) could be deduced from (O2).

residue pair	k	recovered in B^k	if not in $X(K)$, why?
$(\overline{\infty^+}, \overline{\infty^+})$	1	∞^+ $\left(\frac{11}{204}\sqrt{34}, \frac{44909}{249696}\sqrt{34}\right)$ $\left(-\frac{11}{204}\sqrt{34}, -\frac{44909}{249696}\sqrt{34}\right)$	
$(\overline{(0,1)}, \overline{(0,1)})$	2	$(0,1)$ $x(z_1) = x(z_2) = \pm(2 \cdot 3 + 2 \cdot 3^3 + O(3^5))$	$\mathrm{ord}_p(x(\varphi_2(z))) = -2$
$(\overline{(0,2)}, \overline{(0,1)})$	2	$x(z_1) = \pm(2 \cdot 3 + 3^2 + 2 \cdot 3^3 + O(3^5)) = -x(z_2)$	$\mathrm{ord}_p(x(\varphi_2(z))) = -2$
$(\overline{(1,0)}, \overline{(1,0)})$	2	$\left(-\frac{1}{2}, \pm\frac{9}{8}\right)$	
$(\overline{(1,0)}, \overline{(2,0)})$	2	$x(z_1) = 1 + 3 + 3^3 + O(3^5) = -x(z_2)$, $y(z_1) = -y(z_2)$	(O2) with $n_1 = \pm 1$, $n_2 = 3$

Table 1. Computation of $B^1 \cup B^2$ for Example 7.2.

Appendix A. Roots of multivariate systems of p-adic equations

Some of the algorithms of Sections 6 and 7 require us to solve systems of two p-adic equations in two variables. In particular, in each pair of residue disks we reduce the problem to that of finding all $(t_1, t_2) \in \mathbb{Z}_p \times \mathbb{Z}_p$ such that

$$\begin{cases} \rho_1(pt_1, pt_2) = 0 \\ \rho_2(pt_1, pt_2) = 0 \end{cases} \tag{A.1}$$

for some $\rho_1(t_1, t_2), \rho_2(t_1, t_2) \in \mathbb{Q}_p[[t_1, t_2]]$.

The power series ρ_1 and ρ_2 are convergent on $p\mathbb{Z}_p \times p\mathbb{Z}_p$ and, possibly after multiplying by a power of p, we may assume that $\rho_1(pt_1, pt_2), \rho_2(pt_1, pt_2) \in \mathbb{Z}_p[[t_1, t_2]] \setminus p\mathbb{Z}_p[[t_1, t_2]]$.

A careful study of the valuation of the coefficients of ρ_1 and ρ_2 allows us to conclude that if $(\alpha, \beta) \in \mathbb{Z}_p \times \mathbb{Z}_p$ is a solution to (A.1), then ($\alpha \bmod p^n, \beta \bmod p^n$) is a solution modulo (p^n) to the system

$$\begin{cases} \rho_1(pt_1, pt_2) + O(t_1, t_2)^{\tilde{n}} = 0 \\ \rho_2(pt_1, pt_2) + O(t_1, t_2)^{\tilde{n}} = 0 \end{cases} \tag{A.2}$$

for some integer $\tilde{n}$. How reversible is this process? In other words, if we find all the solutions of (A.2) mod p^n, how do we know if each such solution *lifts* to a *unique* solution to (A.1)?

In some cases, we can apply a multivariate version of Hensel's lemma (see Theorem A.1 below). Let us first introduce some notation. Let $m \in \mathbb{N}$ and, for an element $\underline{a} = (a_1, \ldots, a_m) \in \mathbb{Q}_p^m$, define $\mathrm{ord}_p(\underline{a}) = \min_{1 \le i \le m}\{\mathrm{ord}_p(a_i)\}$. Then ord_p satisfies the following properties:

(a) For any $k \in \mathbb{Q}_p$, $\mathrm{ord}_p(k\underline{a}) = \mathrm{ord}_p(k) + \mathrm{ord}_p(\underline{a})$.

(b) $\mathrm{ord}_p(\underline{a} + \underline{b}) \ge \min\{\mathrm{ord}_p(\underline{a}), \mathrm{ord}_p(\underline{b})\}$ with equality if $\mathrm{ord}_p(\underline{a}) \ne \mathrm{ord}_p(\underline{b})$.

For $\underline{f} = (f_1, \ldots, f_m) \in \mathbb{Z}_p[[x_1, \ldots, x_m]]^m$ and $\underline{x} = (x_1, \ldots, x_m)$, define the Jacobian matrix

$$J_{\underline{f}}(\underline{x}) := \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_m} \\ \vdots & \ddots & \vdots & \\ \frac{\partial f_m}{\partial x_1} & \frac{\partial f_m}{\partial x_2} & \cdots & \frac{\partial f_m}{\partial x_m} \end{bmatrix} (\underline{x}).$$

Denote by $\mathbb{Z}_p\langle x_1, \ldots, x_m\rangle$ the subring of $\mathbb{Z}_p[[x_1, \ldots, x_m]]$ consisting of those power series whose coefficients tend to 0 as the degree of the corresponding monomials tends to infinity.

THEOREM A.1 (Multivariate Hensel's lemma [19, Theorem 4.1]): *Let* $\underline{f} = (f_1, \dots, f_m) \in \mathbb{Z}_p\langle x_1, \dots, x_m\rangle^m$. *Assume that* $\underline{a} \in \mathbb{Z}_p^m$ *satisfies*

$$\operatorname{ord}_p(\underline{f}(\underline{a})) > 2\operatorname{ord}_p(\det(J_{\underline{f}}(\underline{a}))).$$

Then there is a unique $\underline{\alpha} \in \mathbb{Z}_p^m$ *such that* $\underline{f}(\underline{\alpha}) = \underline{0}$ *and* $\operatorname{ord}_p(\underline{\alpha} - \underline{a}) > \operatorname{ord}_p(\det(J_{\underline{f}}(\underline{a})))$. *Furthermore,* $\operatorname{ord}_p(\underline{\alpha} - \underline{a}) \geq \operatorname{ord}_p(\underline{f}(\underline{a})) - \operatorname{ord}_p(\det(J_{\underline{f}}(\underline{a})))$.

Even though [19] is not the only reference for Theorem A.1 (see for example also [25, Theorem 23]), the proof given by Conrad in [19] has the advantage of being constructive: it uses Newton's method to explicitly find approximations of $\underline{\alpha}$ and it shows how fast these converge to $\underline{\alpha}$. In particular, with the notation of the theorem, let $\underline{a}_1 = \underline{a}$ and define, for $N \geq 1$,

$$\underline{a_{N+1}} = \underline{a_N} - \underline{f}(\underline{a_N}) \cdot (J_{\underline{f}}(\underline{a_N})^T)^{-1}.$$

By [19, (3.9)], we have the inequality

$$\operatorname{ord}_p(\underline{a_{N+1}} - \underline{a_N}) \geq \operatorname{ord}_p(\det(J_{\underline{f}}(\underline{a}))) + 2^{N-1}(\operatorname{ord}_p(\underline{f}(\underline{a})) - 2\operatorname{ord}_p(\det(J_{\underline{f}}(\underline{a})))),$$

combining this with Property (b) and with the assumption that

$$\operatorname{ord}_p(\underline{f}(\underline{a})) - 2\operatorname{ord}_p(\det(J_{\underline{f}}(\underline{a}))) > 0,$$

we obtain

$$\operatorname{ord}_p(\underline{a_M} - \underline{a_N}) \geq \operatorname{ord}_p(\det(J_{\underline{f}}(\underline{a}))) + 2^{N-1}(\operatorname{ord}_p(\underline{f}(\underline{a})) - 2\operatorname{ord}_p(\det(J_{\underline{f}}(\underline{a}))))$$

for all $M > N$. Thus, taking limits as $M \to \infty$,

$$\operatorname{ord}_p(\underline{\alpha} - \underline{a_N}) \geq \operatorname{ord}_p(\det(J_{\underline{f}}(\underline{a}))) + 2^{N-1}(\operatorname{ord}_p(\underline{f}(\underline{a})) - 2\operatorname{ord}_p(\det(J_{\underline{f}}(\underline{a})))).$$

We sketch a possible strategy to compute roots of systems of equations of the form (A.1), omitting technicalities on precision. This immediately generalizes to the case where (A.1) is replaced by a system of m equations in m variables for arbitrary $m \geq 2$.

Algorithm 1: Computing roots of (A.1)

Input: A system $\underline{\rho} = (\rho_1, \rho_2)$ of the form (A.1).
Output: L – list of roots modulo p^n of $\underline{\rho}$.

(1) Reduce to (A.2).
(2) Compute $R_p = \{(t_1, t_2) \in \{0, \dots, p-1\}^2 : \underline{\rho}(pt_1, pt_2) \equiv 0 \bmod p\}$.

(3) Let $\underline{a} \in R_p$. If $\mathrm{ord}_p(\det(J_{\underline{\rho}}(\underline{a}))) = 0$, by Theorem A.1 there exists a unique root $\underline{\alpha} \in \mathbb{Z}_p^2$ of (A.1) such that $\mathrm{ord}_p(\underline{\alpha} - \underline{a}) > 0$. Compute $\underline{\alpha}$ to the desired precision using the discussion following Theorem A.1 and append it to L.

(4) Let $\underline{a} \in R_p$ such that $\mathrm{ord}_p(\det(J_{\underline{\rho}}(\underline{a}))) \neq 0$. Fix an $r \geq 3$, $r \leq n$ and naively find $R_{p^r}(\underline{a}) = \{(t_1, t_2) \in \{0, \dots, p^r - 1\}^2 : \underline{\rho}(pt_1, pt_2) \equiv 0 \bmod p^r \text{ and } (t_1, t_2) \equiv \underline{a} \bmod p\}$. For each $\underline{b} \in R_{p^r}(\underline{a})$ do the following:
   (i) if $2\,\mathrm{ord}_p(\det(J_{\underline{\rho}}(\underline{b}))) < r$, compute using Theorem A.1 an approximation of the unique root $\underline{\beta} \in \mathbb{Z}_p^2$ such that $\mathrm{ord}_p(\underline{\beta} - \underline{b}) > \mathrm{ord}_p(\det(J_{\underline{\rho}}(\underline{b})))$ and append it to L. Remove from $R_{p^r}(\underline{a})$ all $\underline{b}'$ such that $\mathrm{ord}_p(\underline{b}' - \underline{b}) > \mathrm{ord}_p(\det(J_{\underline{\rho}}(\underline{b})))$.
   (ii) if $2\,\mathrm{ord}_p(\det(J_{\underline{\rho}}(\underline{b}))) \geq r$, then if $r = n$ append $\underline{b}$ to L; if $r < n$, choose some $s > r$, $s \leq n$, naively find $R_{p^s}(\underline{b}) = \{(t_1, t_2) \in \{0, \dots, p^s - 1\}^2 : \underline{\rho}(pt_1, pt_2) \equiv 0 \bmod p^s \text{ and } (t_1, t_2) \equiv \underline{b} \bmod p^r\}$ and for each $\underline{c} \in R_{p^s}(\underline{b})$ repeat (i), (ii) with the appropriate modification in notation.

Remark A.2: If the algorithm never appends to L in 4 (ii), each element in L is the approximation of a unique root of (A.1) and, conversely, each root of (A.1) reduces to an element of L. Otherwise, we can try to increase n. However, there are some residue disks where the systems that we consider provably have roots at which the determinant of the Jacobian matrix also vanishes, so Theorem A.1 is not applicable. Indeed, let X be as in Section 5. Then X admits the automorphisms $\theta\colon (x, y) \mapsto (\pm x, \pm y)$. Composing φ_k with θ we obtain either the identity or multiplication by -1 on E_k. Since local heights are even, it follows that if a function ρ comes from a height function as in Theorem 5.2, then all its partial derivatives vanish[7] at a K-rational point fixed by a nontrivial automorphism θ. A function coming from relations of the linear functionals f_i on E_k is odd and will thus have non-simple zeros in the above sense at those points (x, y) which are fixed by a nontrivial automorphism θ that projects to the identity on E_k.

We now explain how to deal with the disks of Remark A.2 where Hensel is not applicable, for the explicit algorithms that we described in Section 7. Suppose

[7] E.g. for the pair of disks containing a point fixed by $(x, y) \mapsto (-x, y)$, we can set $t_1 = x_1$, $t_2 = x_2$ as uniformizers. Then $\rho(t_1, t_2) = \rho(-t_1, -t_2)$ giving vanishing of the partial derivatives at $t_1 = t_2 = 0$.

first that we are in the situation of §7.1, of which we retain the notation. Let H be the subgroup of the automorphism group of X generated by the hyperelliptic involution and the bielliptic automorphism $(x, y) \mapsto (-x, y)$.

LEMMA A.3: *Let K and $X/\mathbb{Q}$ be as in §7.1. Let $P \in X(K)$ such that $\theta(P) = P$ for a nontrivial automorphism $\theta \in H$; if $y(P) = 0$, further assume that $x(P)^2 \in \mathbb{Q}$. Let $k \in \{1, 2\}$ such that $P \in X^{(k)}(K)$ and let $w \in T^{\mathrm{anti},k}$ such that $\rho^{\mathrm{anti},k}(\sigma(P)) = w$. Then we can choose local coordinates t_1 and t_2 for $\sigma_1(P)$ and $\sigma_2(P)$, such that, in the residue pair $\overline{\sigma_1(P)} \times \overline{\sigma_2(P)} \in \overline{X}(\mathbb{F}_p) \times \overline{X}(\mathbb{F}_p)$, we have*

$$\rho^{\mathrm{anti},k}(t_1, t_2) - w = \sum_{i=1}^{\infty} c_i(t_1^{2i} - t_2^{2i}) = (t_1^2 - t_2^2) \sum_{i=1}^{\infty} c_i \left(\sum_{j=0}^{i-1} t_1^{2j} t_2^{2i-2-2j} \right)$$

for some $c_i \in \mathbb{Q}_p$.

Proof. Write a point in $X(\mathbb{Q}_p) \times X(\mathbb{Q}_p)$ as $((x_1, y_1), (x_2, y_2))$. We fix the following choices for t_1 and t_2. If $\theta(x, y) = (-x, y)$, let $t_i = x_i$; if $\theta(x, y) = (x, -y)$, let $t_i = y_i$; finally, if $P = \infty^{\pm}$, let $t_i = 1/x_i$. As observed in Remark A.2, we have

$$\rho^{\mathrm{anti},k}((x_1, y_1), (x_2, y_2)) = \rho^{\mathrm{anti},k}(\theta(x_1, y_1), \theta(x_2, y_2));$$

our choice of local coordinates then yields

$$\rho^{\mathrm{anti},k}(t_1, t_2) = \rho^{\mathrm{anti},k}(-t_1, -t_2).$$

Since by §6.2 we have $\alpha_{01}^{\mathrm{anti},E_j} = 0$ for each $j \in \{1, 2\}$, this implies that there exist some power series f_1 and f_2 such that

$$\rho^{\mathrm{anti},k}(t_1, t_2) = f_1(t_1^2) - f_2(t_2^2) + 2h_p^{\mathrm{anti},E_k}(Q_k).$$

In view of our assumptions, we also have that $x_1(t_1)^2 = x_2(t_2)^2|_{t_2=t_1}$ and thus that $\varphi_j(x_1(t_1), y_1(t_1)) = \pm\varphi_j(x_2(t_2), y_2(t_2))|_{t_2=t_1}$. Since $\alpha_{00}^{\mathrm{anti},E_j} = -\alpha_{11}^{\mathrm{anti},E_j}$ by §6.2, we conclude that $f_1 = f_2$. Finally, the lemma follows by definition of w. ∎

Remark A.4: Since $h_p^{\mathrm{anti},E_k}(Q_k) = 0$, we must have $w = 0$.

In the notation of Lemma A.3, the points $(z_1, z_2) \in X^{(k)}(K \otimes \mathbb{Q}_p)$ reducing to $\overline{\sigma_1(P)} \times \overline{\sigma_2(P)}$ and such that $\rho^{\mathrm{anti},k}(z_1, z_2) = w$ satisfy one of the following:

(i) $t_1(z_1) = t_2(z_2)$ and $\rho^{\mathrm{cyc},k}(t_1(z_1), t_1(z_1)) \in T^{k,\mathrm{cyc}}$;
(ii) $t_1(z_1) = -t_2(z_2)$ and $\rho^{\mathrm{cyc},k}(t_1(z_1), -t_1(z_1)) \in T^{k,\mathrm{cyc}}$;

$$\text{(iii)} \quad \begin{cases} \sum_{i=1}^{\infty} c_i \left(\sum_{j=0}^{i-1} t_1(z_1)^{2j} t_2(z_2)^{2i-2-2j} \right) = 0 \\ \rho^{\mathrm{cyc},k}(t_1(z_1), t_2(z_2)) \in T^{k,\mathrm{cyc}}. \end{cases}$$

If $c_1 \neq 0$, then $(0,0)$ is not a root of (iii), so in Algorithm 1 we can hope for no root to be appended in 4 (ii). We also note that the one-variable power series of (i) and (ii) are power series in t_1^2.

In the setting of §7.2, we follow a similar strategy (and adopt some of the notation of the imaginary case). Recall that the second function ρ_2 is given by

$$\rho_2(z_1, z_2) = \int_{\infty}^{\varphi_2(z_1)} \omega_0^{E_2} - b \int_{\infty}^{\varphi_2(z_2)} \omega_0^{E_2},$$

where $b = 1$ or $b = -1$, depending on the rank of E_2 over $\mathbb{Q}$. We assume here that $b = 1$ as in Example 7.2. Let $P \in X^{(k)}(K)$ be fixed by $\theta \in H \setminus \{\mathrm{id}\}$ and let t_1 and t_2 be local coordinates chosen in the same way as in the proof of Lemma A.3. Then, in the residue disk of $\sigma(P)$, we have

$$\rho_2(-t_1, -t_2) = \begin{cases} \rho_2(t_1, t_2) & \text{if } \varphi_2 \circ \theta = \mathrm{id}, \\ -\rho_2(t_1, t_2) & \text{if } \varphi_2 \circ \theta = -\mathrm{id}. \end{cases}$$

Assume for simplicity that $P \in X(\mathbb{Q})$, so the local expansion of $\int_{\infty}^{\varphi_2(z_1)} \omega_0^{E_2}$ evaluated at t_2 gives the local expansion of $\int_{\infty}^{\varphi_2(z_2)} \omega_0^{E_2}$. We conclude that

$$\rho_2(t_1, t_2) = \begin{cases} (t_1^2 - t_2^2)\tilde{\rho_2}(t_1, t_2) & \text{if } \varphi_2 \circ \theta = \mathrm{id}, \\ (t_1 - t_2)\tilde{\rho_2}(t_1, t_2) & \text{if } \varphi_2 \circ \theta = -\mathrm{id}, \end{cases}$$

for some $\tilde{\rho_2}(t_1, t_2) \in \mathbb{Q}_p[[t_1, t_2]]$.

References

[1] J. S. Balakrishnan and A. Besser, *Coleman-Gross height pairings and the p-adic sigma function*, Journal für die Reine und Angewandte Mathematik. [Crelle's Journal] **698** (2015), 89–104. MR 3294652

[2] J. S. Balakrishnan, A. Besser and J. S. Müller, *Quadratic Chabauty: p-adic heights and integral points on hyperelliptic curves*, Journal für die Reine und Angewandte Mathematik. [Crelle's Journal] **720** (2016), 51–79.

[3] J. S. Balakrishnan, A. Besser and J. S. Müller, *Computing integral points on hyperelliptic curves using quadratic Chabauty*, Mathematics of Computation **86** (2017), 1403–1434.

[4] J. S. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers, *A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves*, Mathematische Annalen **372** (2018), no. 1-2, 369–428. MR 3856816

[5] J. S. Balakrishnan and N. Dogra, *Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties*, International Mathematics Research Notices, to appear.

[6] J. S. Balakrishnan and N. Dogra, *Quadratic Chabauty and rational points, I: p-adic heights*, Duke Mathematical Journal **167** (2018), no. 11, 1981–2038, With an appendix by J. Steffen Müller. MR 3843370

[7] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Annals of Mathematics. Second Series **189** (2019), no. 3, 885–944. MR 3961086

[8] J. S. Balakrishnan, J. S. Müller and W. A. Stein, *A p-adic analogue of the conjecture of Birch and Swinnerton-Dyer for modular abelian varieties*, Mathematics of Computation **85** (2016), no. 298, 983–1016.

[9] J. S. Balakrishnan, M. Çiperiani, J. Lang, B. Mirza, and R. Newton, *Shadow lines in the arithmetic of elliptic curves*, Directions in number theory, Assoc. Women Math. Ser., vol. 3, Springer, [Cham], 2016, pp. 33–55.

[10] A. Besser, *p-adic Arakelov theory*, Journal of Number Theory **111** (2005), no. 2, 318–371. MR 2130113

[11] F. Bianchi, *Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture*, Preprint, arXiv:1904.04622, 2019.

[12] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24** (1997), no. 3–4, 235–265, Computational algebra and number theory (London, 1993). MR 1 484 478

[13] N. Bruin, *Chabauty methods using elliptic curves*, Journal für die Reine und Angewandte Mathematik. [Crelle's Journal] **562** (2003), 27–49. MR 2011330 (2004j:11051)

[14] N. Bruin and M. Stoll, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS Journal of Computation and Mathematics **13** (2010), 272–306. MR 2685127 (2011j:11118)

[15] A. Brumer, *On the units of algebraic number fields*, Mathematika. A Journal of Pure and Applied Mathematics **14** (1967), 121–124. MR 0220694 (36 #3746)

[16] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, Comptes Rendus de l'Académie des Sciences. Série I. Mathématique **212** (1941), 882–885. MR 0004484 (3,14d)

[17] R. Coleman, *Torsion points on curves and p-adic abelian integrals*, Annals of Mathematics. Second Series **121** (1985), 111–168.

[18] R. Coleman and B. Gross, *p-adic heights on curves*, Algebraic number theory (J. Coates, R. Greenberg, B. Mazur, and I. Satake, eds.), Advanced Studies in Pure Mathematics, vol. 17, Academic Press, Boston, MA, 1989, pp. 73–81. MR 92d:11057

[19] K. Conrad, *A multivariable Hensels lemma*, `https://kconrad.math.uconn.edu/blurbs/gradnumthy/multivarhensel.pdf`, accessed online: 24/06/2019.

[20] N. Dogra, *Unlikely intersections and the Chabauty-Kim method over number fields*, Preprint arXiv:1903.05032 (2019).

[21] B. H. Gross, *Local heights on curves*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 327–339. MR MR861983

[22] D. R. Hast, *Functional transcendence for the unipotent Albanese map*, Preprint, arXiv:1911.00587 (2019).

[23] M. Kim, *The motivic fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$ and the theorem of Siegel*, Inventiones Mathematicae **161** (2005), no. 3, 629–656. MR 2181717 (2006k:11119)

[24] M. Kim, *The unipotent Albanese map and Selmer varieties for curves*, Kyoto University. Research Institute for Mathematical Sciences. Publications **45** (2009), no. 1, 89–133. MR 2512779 (2010k:14029)

[25] F.-V. Kuhlmann, *Maps on ultrametric spaces, Hensel's lemma, and differential equations over valued fields*, Communications in Algebra **39** (2011), no. 5, 1730–1776. MR 2821504

[26] H.-W. Leopoldt, *Zur Arithmetik in abelschen Zahlkörpern*, Journal für die Reine und Angewandte Mathematik **209** (1962), 54–71. MR 0139602 (25 #3034)

[27] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, `http://www.lmfdb.org`, 2019, [Online; accessed 21 May 2019].

[28] B. Mazur, *Modular curves and arithmetic*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983), PWN, Warsaw, 1984, pp. 185–211. MR 804682 (87a:11054)

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

[30] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*, Explicit methods in number theory, Panor. Synthèses, vol. 36, Soc. Math. France, Paris, 2012, pp. 99–117. MR 3098132

[31] J. Nekovář, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Birkhäuser Boston, Boston, MA, 1993, pp. 127–202. MR 95j:11050

[32] B. Poonen, *The p-adic closure of a subgroup of rational points on a commutative algebraic group*, Unpublished Manuscript, `http://www-math.mit.edu/~poonen/papers/leopoldt.pdf`, 2007.

[33] P. Schneider, *p-adic height pairings. I*, Inventiones Mathematicae **69** (1982), no. 3, 401–409. MR MR679765 (84e:14034)

[34] S. Siksek, *Explicit Chabauty over number fields*, Algebra & Number Theory **7** (2013), no. 4, 765–793. MR 3095226

[35] W. A. Stein et al., *Sage Mathematics Software (Version 5.6)*, The Sage Development Team, 2013, `http://www.sagemath.org`.

[36] N. Triantafillou, *Restriction of scalars, the Chabauty-Coleman method, and $\mathbb{P}^1\backslash\{0, 1, \infty\}$*, Ph.D. thesis, MIT, 2019.

[37] M. Waldschmidt, *On the p-adic closure of a subgroup of rational points on an Abelian variety*, Afrika Matematika **22** (2011), no. 1, 79–89. MR 2793038

[38] J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, ProQuest LLC, Ann Arbor, MI, 1997, Thesis (Ph.D.)–University of California, Berkeley. MR 2696280